



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

A large, multi-paned window in a modern office building, with a person working at a desk visible in the lower left corner.

# CJIS Annual Report 2012

"Collaboration is the hallmark of our best work as a Division."



As the Assistant Director of the FBI's Criminal Justice Information Services (CJIS) Division, I have the honor of presenting the 2012 edition of the **CJIS Annual Report**. This publication showcases the work of the Division's more than 2,500 employees who provide vital criminal justice information services to our partners in the law enforcement, criminal justice, national security, and intelligence communities we serve.

During the fiscal year, the CJIS Division met ever-increasing requests for biometric identification services, background checks for gun purchases, and checks of our National Crime Information Center. We were able to do this while expanding our ability to share information and create connections through the Law Enforcement National Data Exchange and Law Enforcement Online programs and developing our CJIS Intelligence Program. We also took on an additional

responsibility to serve FBI field offices with a centralized Public Access Line that accepts tips and complaint calls from throughout the United States and routes the information for appropriate handling.

Collaboration is the hallmark of our best work as a Division. With our partners, we are able to maximize our crime-fighting resources and technological advances. As we go forward, we will continue to provide outstanding services to our customers and all those protecting and serving our communities and our country.

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

**NATIONAL CRIME INFORMATION CENTER**

Providing cops on the street with facts they need when they need them. 4

**NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM**

Determining eligibility to purchase firearms and explosives. 6

**LAW ENFORCEMENT NATIONAL DATA EXCHANGE**

Linking common threads and putting the right information in the right hands, right now. 8

**CJIS INTELLIGENCE PROGRAM**

Working all the angles by analyzing information and piecing it together. 10

**LAW ENFORCEMENT ONLINE**

Enabling law enforcement collaboration. 12

**UNIFORM CRIME REPORTING PROGRAM**

Crunching the numbers and providing a national perspective of crime. 14

**BIOMETRIC IDENTIFICATION SERVICES**

Delivering vital identification facts in record time. 16

**BIOMETRIC INTEROPERABILITY**

Collaborating with domestic and international partners to identify. 18

**FBI BIOMETRIC CENTER OF EXCELLENCE**

Implementing the future of identification services. 20

**GLOBAL COLLECTIONS PROGRAM**

Identifying criminals and terrorists across the globe. 22

**CJIS ADVISORY POLICY BOARD AND COMPACT COUNCIL**

Seeking the input of our partners to shape CJIS services. 24

**CRIMINAL JUSTICE INFORMATION SERVICES DIVISION**

Where connections and identifications generate the power to know. 26

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

Since 1967, the **National Crime Information Center (NCIC)** has been providing valuable information for quick answers to crucial questions from law enforcement. That first year, there were about 95,000 active records of stolen property and wanted criminals. In 2012, the NCIC contained more than 18.1 million active records with information that law enforcement personnel needed, such as wanted and missing/unidentified persons, stolen property, gangs, terrorists, and registered sex offenders. The files of information maintained by the NCIC are accessed via 92,000 connections to law enforcement and other criminal justice partners. This information assists the Division's partners in meeting their missions to keep their communities and the nation safe.

The FBI manages the NCIC system and continues to work with law enforcement to keep abreast of the ever-growing demand for information. In addition to the expanded NCIC License Plate Reader service, in 2012, the NCIC added a flagging mechanism to indicate multiple warrants for the same individual by the same Originating Agency Identifier (ORI) in the NCIC Wanted Person File. The FBI also added the ability to capture ethnicity in the NCIC person records.

Upcoming projects include continued collaboration with the National Missing and Unidentified Persons System (NamUs), operated by the Department of Justice, to develop an automated information sharing partnership that will provide law enforcement, forensic personnel, and the general public with tools to help find missing persons and identify the unknown dead.

Whether its role is routine or unanticipated, the NCIC is always poised to meet the changing needs of the criminal justice community.

**ACCOMPLISHMENTS**

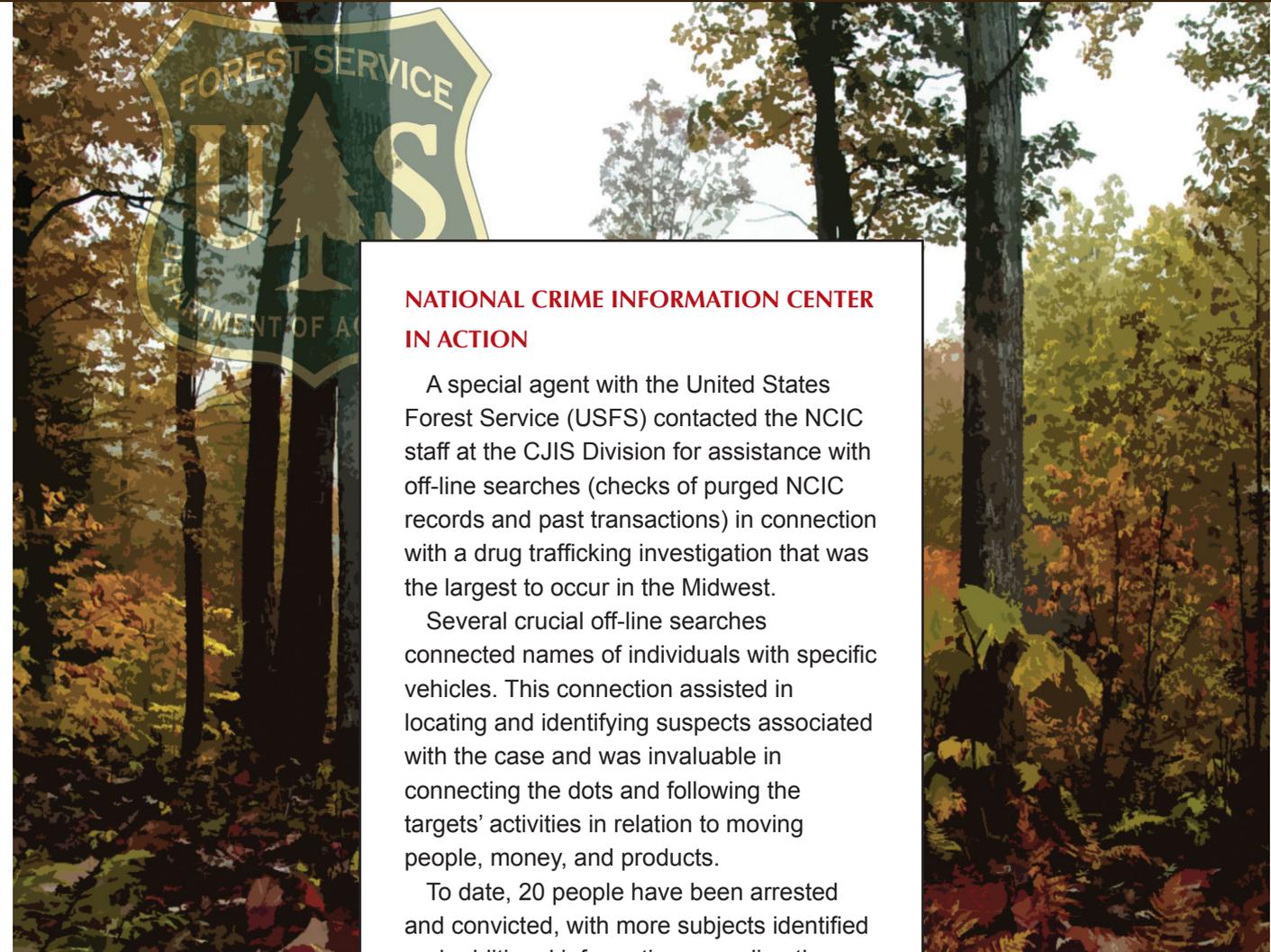
- In August 2012, the NCIC Violent Person File was created to increase officer safety by maintaining readily available information on individuals with a violent criminal history or who have made a credible threat against law enforcement officers.

*“ In 2012, the NCIC contained more than 18.1 million active records with information that law enforcement personnel needed . . . ”*

- On August 19, the first phase of the National Instant Criminal Background Check System (NICS) Denied Transaction File (NDTF) (approximately 65,000 denied transactions) became available within the NCIC. The NDTF, which contains records on persons denied access to a firearm as a result of a NICS background check, is currently searchable by using a unique message key. In the future, the NDTF will include all denials and may be searched through all routine person inquiries.
- NCIC added the capability for record owners to indicate their intent to share Vehicle and Article Files and the ability for information on foreign sex offenders to be entered into the National Sex Offender Registry.

**QUICK FACTS**

- In fiscal year 2012, the NCIC processed an average of 8,758,485 million transactions per day.
- The NCIC's average response time per transaction was 0.0220 seconds.
- The NCIC recorded a daily record high on July 2, 2012, with 12,201,739 transactions processed.



**NATIONAL CRIME INFORMATION CENTER IN ACTION**

A special agent with the United States Forest Service (USFS) contacted the NCIC staff at the CJIS Division for assistance with off-line searches (checks of purged NCIC records and past transactions) in connection with a drug trafficking investigation that was the largest to occur in the Midwest.

Several crucial off-line searches connected names of individuals with specific vehicles. This connection assisted in locating and identifying suspects associated with the case and was invaluable in connecting the dots and following the targets' activities in relation to moving people, money, and products.

To date, 20 people have been arrested and convicted, with more subjects identified and additional information regarding the drug trafficking organization uncovered. Approximately \$1 million worth of property, illegal drugs, and contraband was seized, including marijuana, cocaine, firearms, vehicles, and cash.

## Determining eligibility to purchase firearms and explosives.

In response to the Brady Handgun Violence Prevention Act of 1993, the **National Instant Criminal Background Check System (NICS)** provides immediate determinations to Federal Firearm Licensees (FFLs) as to whether a prospective gun buyer should receive a weapon according to federal or state laws. Fourteen years after its development, the NICS continues to be a cooperative effort of the FBI; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Justice; and local and state law enforcement agencies. When authorized gun dealers or FFLs request a NICS background check on an individual attempting to receive a firearm, the NICS automatically searches records in the National Crime Information Center (NCIC), the Interstate Identification Index (III), and the NICS Index. If an applicant's name and descriptive information matches any records in the databases—such as wanted persons, subjects of protective/restraining orders, or other persons prohibited from receiving or possessing firearms—the NICS staff and/or state agencies perform further research to determine the applicant's eligibility.

The NICS Index contains disqualifying information on individuals who are prohibited from possessing a firearm when it may not be available through the NCIC or the III. Until 2012, the NICS Index contained only information regarding individuals determined to have federal firearm prohibitions. In April, the NICS Index expanded to include entries on individuals possessing state firearm prohibitions and/or state permit prohibitions. Now, depending upon the state of purchase, the buyer's state of residence, and the type of check being performed, the NICS Index can automatically respond with the information contained in these entries.

Overall, the number of transactions the NICS has processed has increased rapidly each year. It took 6 years, 1998 to 2004, for the first 50 million transactions to be processed. Then, in less than 5 years, the 100 millionth transaction was processed in April 2009. Just a little more than 3 years after that, the NICS processed its 150 millionth transaction in July 2012.

Providing exemplary efficiency in its processing of transactions, the NICS became the model for the FBI's newly-created Public Access Line (PAL) Unit, which began its call center operations on September 24. Currently administered by the NICS management,

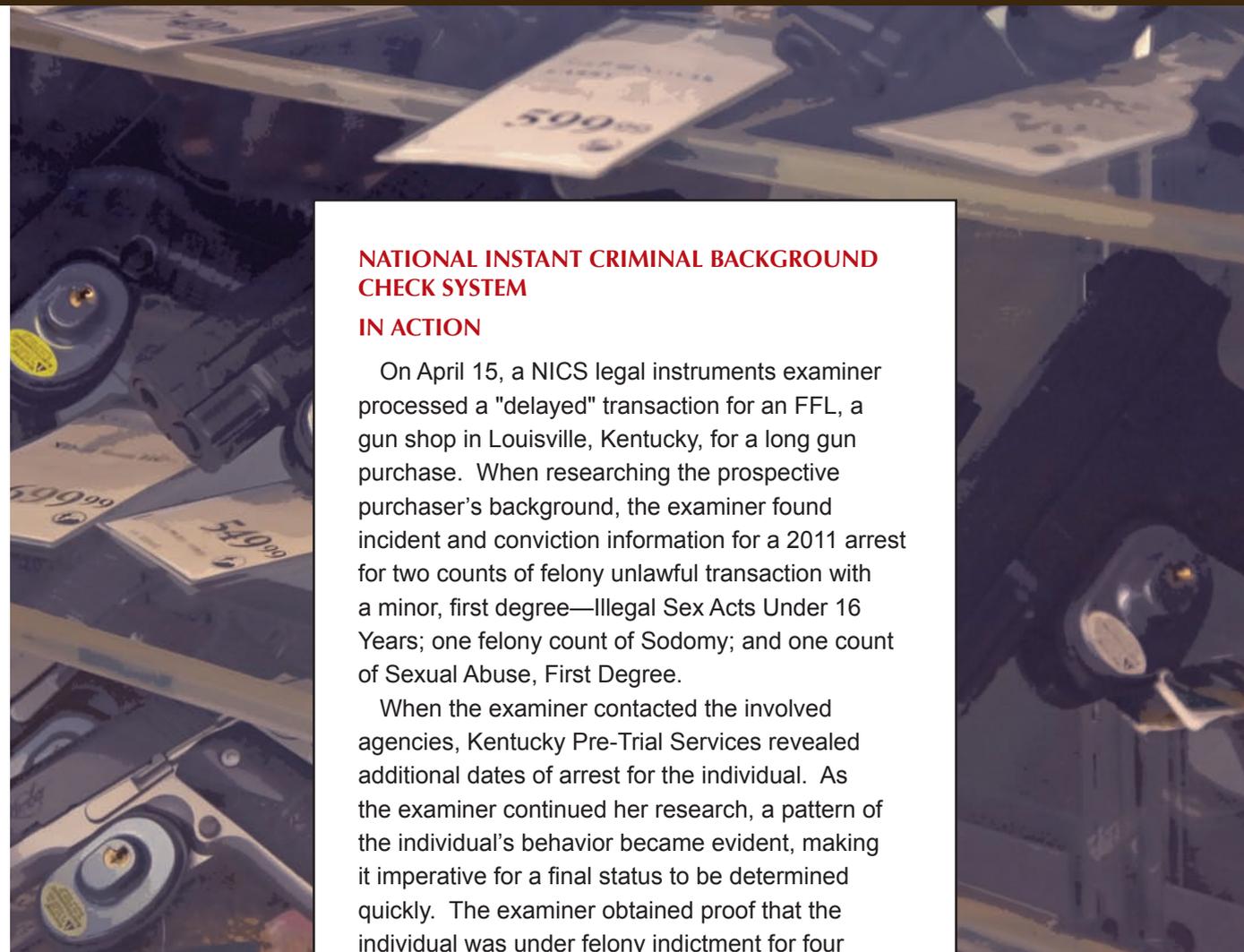
the PAL serves as the FBI's central intake point through which the public may provide tips or information about potential or on-going crimes or national security threats. Staffed with 64 professional customer service representatives and 5 Supervisory Special Agents, the PAL operates 24/7. After launching first with the FBI's Pittsburgh Division, the PAL is currently handling tips called into 12 FBI field offices. Not only will the PAL provide the public with a single point of contact to share information, but it will also enable Special Agents to be in the field focusing on investigations rather than fielding calls and collecting information.

### ACCOMPLISHMENTS

- The NICS staff exceeded its mandate of a 90-percent immediate determination rate (eligibility determinations made while the FFL is on the telephone) with a rate of 91.72 percent.
- Of all the NICS transactions delayed based on the name check search, 100 percent were reviewed within 3 business days.
- In fewer than 9 months, the PAL prepared work space, processed more than 1,000 applications, hired and trained 64 new employees, and began operations, enabling Special Agents and other field office staff to focus on investigative responsibilities.

### QUICK FACTS

- 17,924,601 million NICS background checks for gun transfers were completed in FY 2012.
- Nearly 77 million records were searched during each NICS background check.
- 83,144 NICS gun transfers were denied federally in FY 2012, creating a total of 958,278 federal denials since the NICS began.



### NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM

#### IN ACTION

On April 15, a NICS legal instruments examiner processed a "delayed" transaction for an FFL, a gun shop in Louisville, Kentucky, for a long gun purchase. When researching the prospective purchaser's background, the examiner found incident and conviction information for a 2011 arrest for two counts of felony unlawful transaction with a minor, first degree—Illegal Sex Acts Under 16 Years; one felony count of Sodomy; and one count of Sexual Abuse, First Degree.

When the examiner contacted the involved agencies, Kentucky Pre-Trial Services revealed additional dates of arrest for the individual. As the examiner continued her research, a pattern of the individual's behavior became evident, making it imperative for a final status to be determined quickly. The examiner obtained proof that the individual was under felony indictment for four different dates of arrest, all of which contained multiple offenses for similar sex-related crimes. She also learned that several firearms were found during a search of the person's home during a previous investigation and that he was scheduled to appear in court in a few days.

As a result, the examiner provided the FFL with a transaction status of "deny," obtained information from the FFL regarding the attempted purchase, and furnished the court agencies with all pertinent information so the local justice system could determine the appropriate actions for this individual.

*Linking common threads and putting the right information in the right hands, right now.*

The **Law Enforcement National Data Exchange**, or N-DEx, is the first and only national investigative information sharing system. N-DEx is a national tool that provides criminal justice agencies with a system for sharing, searching, linking, and analyzing criminal justice information across our country to a degree never before possible. By using N-DEx as a pointer and data discovery system, users can detect relationships between people, crime characteristics, property, and locations; eliminate information gaps by linking information across jurisdictions; “connect the dots” between non-obvious and seemingly unrelated data; and obtain point-of-contact information for investigators and agencies working investigations.

Diverse information is accessible from N-DEx, including incident and case reports, arrest reports, computer-aided dispatch calls, traffic citations, photos, and booking and incarceration data. Agencies can use this data to conduct nationwide searches across jurisdictions; search names, identifications, people, and telephone numbers; and collaborate with others working on similar investigations.

N-DEx also promotes collaboration among agencies. The system allows users to coordinate task forces and form additional investigative partnerships. N-DEx’s subscription/notification feature provides a real-time deconfliction tool for users to learn that other criminal justice agencies may have an interest in whom or what they are investigating. This kind of notification allows users to discover where other investigations may intersect with theirs.

### ACCOMPLISHMENTS

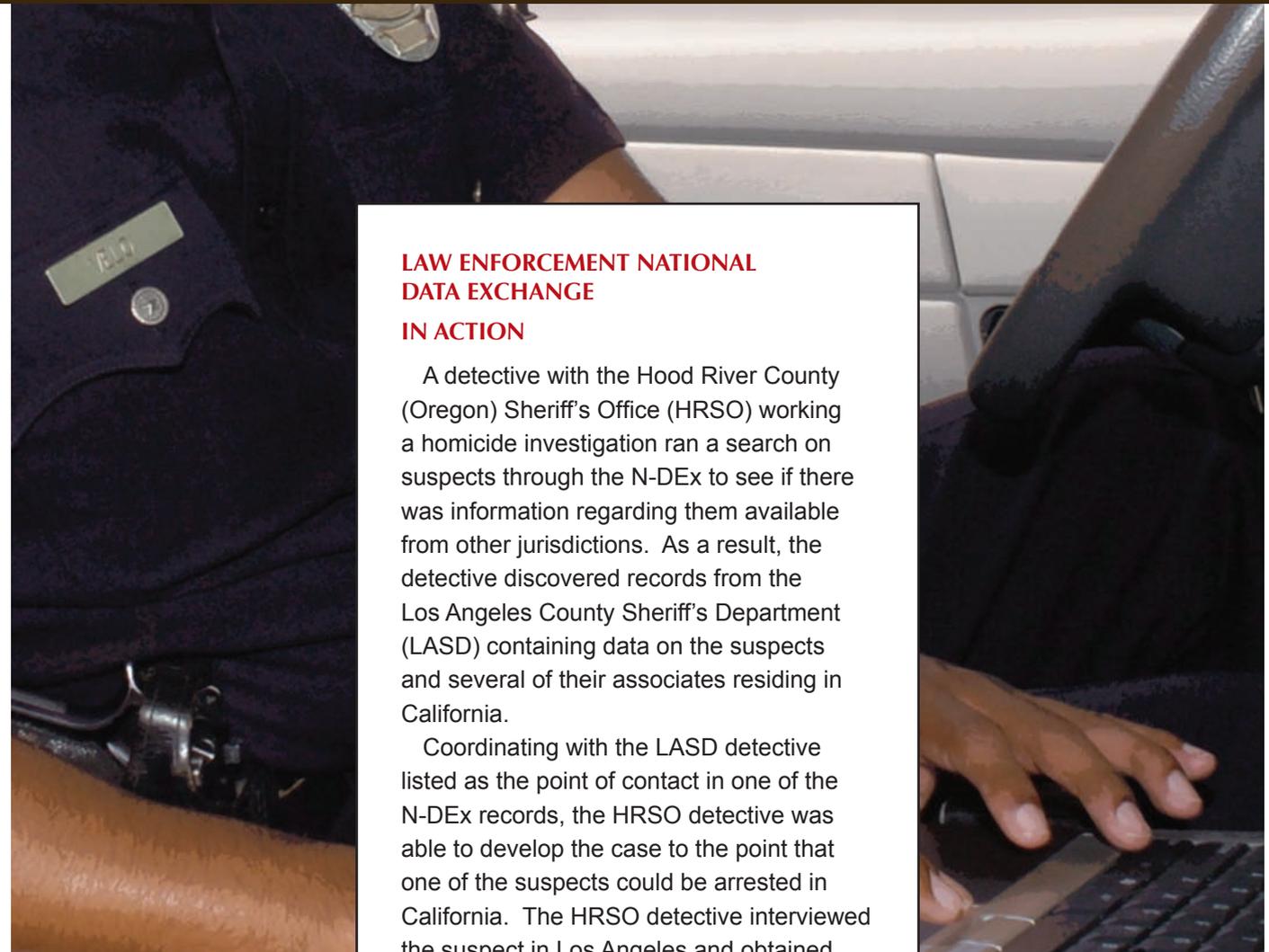
- During FY 2012, N-DEx worked with developers of the FBI’s records management system, Sentinel, to create an interface that allows FBI investigators to share case data as appropriate through N-DEx in a timely, relevant, and secure fashion. This effort helps the FBI fulfill its information-sharing mandate with the criminal justice community.
- In June 2012, N-DEx expanded access to include more of the criminal justice community, such as corrections, probation, parole, the courts, and prosecuting attorney’s offices.

*“ Diverse information is accessible from N-DEx including incident and case reports, arrest reports, computer-aided dispatch calls, traffic citations, photos, and booking and incarceration data . ”*

- The Indiana Department of Correction (DOC) began to submit its incarceration records in July 2012, making it the first DOC agency in the nation to share its information via N-DEx. Since then, DOCs in Kansas and Nebraska have begun to submit data. In the near future, DOCs from Oklahoma, Mississippi, West Virginia, and Virginia will submit their incarceration data using N-DEx.
- N-DEx users can access 38 million records from the Department of Homeland Security and soon will be able to access more than 44 million records from Interpol.

### QUICK FACTS

- There are nearly 1 billion entities (persons, places, things, and events) within nearly 150 million searchable records in the N-DEx.
- More than 66,000 users are registered on the N-DEx system.
- Approximately 4,000 agencies contribute data to the N-DEx.



### LAW ENFORCEMENT NATIONAL DATA EXCHANGE IN ACTION

A detective with the Hood River County (Oregon) Sheriff’s Office (HRSO) working a homicide investigation ran a search on suspects through the N-DEx to see if there was information regarding them available from other jurisdictions. As a result, the detective discovered records from the Los Angeles County Sheriff’s Department (LASD) containing data on the suspects and several of their associates residing in California.

Coordinating with the LASD detective listed as the point of contact in one of the N-DEx records, the HRSO detective was able to develop the case to the point that one of the suspects could be arrested in California. The HRSO detective interviewed the suspect in Los Angeles and obtained additional critical information which resulted in three convictions.

The gunman in the case was convicted of Aggravated Murder and received a sentence of 37 years to life. In addition, the two female accomplices were charged with Homicide. However, the two agreed to testify against the shooter and received sentences of 8½ years each for the charge of Robbery, First Degree.

*Working all the angles by analyzing information and piecing it together.*

The FBI strives to be the best in the world at identity intelligence, and the **CJIS Intelligence Program** is a prime example of our efforts.

In July 2012, the CJIS Division brought together representatives from each of the FBI's field offices around the country to train them to become Subject Matter Experts (SMEs) on the many programs provided by the CJIS Division. This training not only benefits FBI staff at field offices, but also helps our law enforcement partners throughout the country and, in some cases, around the world.

A large part of the SME training involved the CJIS Intelligence Program, which gathers, analyzes, and distributes information to other government agencies, as well as to local, state, tribal, and international law enforcement organizations.

At the training, attendees learned about the groups and units at the CJIS Division that collaborate with one another, with other programs in the Division, and with other government agencies, to provide law enforcement with crucial identity intelligence information. The Intelligence Program includes:

- The **CJIS Division Intelligence Group (CDIG)**, which promotes public safety and prevents terrorism by providing tactical intelligence to FBI Field Intelligence Groups and the law enforcement, intelligence, and homeland security communities by using information contained in the CJIS Division's databases.
- The **Interoperability Initiatives Unit (IIU)**, which facilitates collaborative efforts with local, state, tribal, federal, and international partners to implement and expand efforts to share information among biometric-based systems used by the FBI and its partners through coordination, outreach, reporting, and best practices development.
- The **Global Initiatives Unit (GIU)**, which improves law enforcement effectiveness, and promotes public safety through the global exchange of biometric and other identity data by providing rapid identification services.
- The **Special Identities Unit (SIU)**, which plays a critical role in supporting the FBI and other law enforcement and intelligence

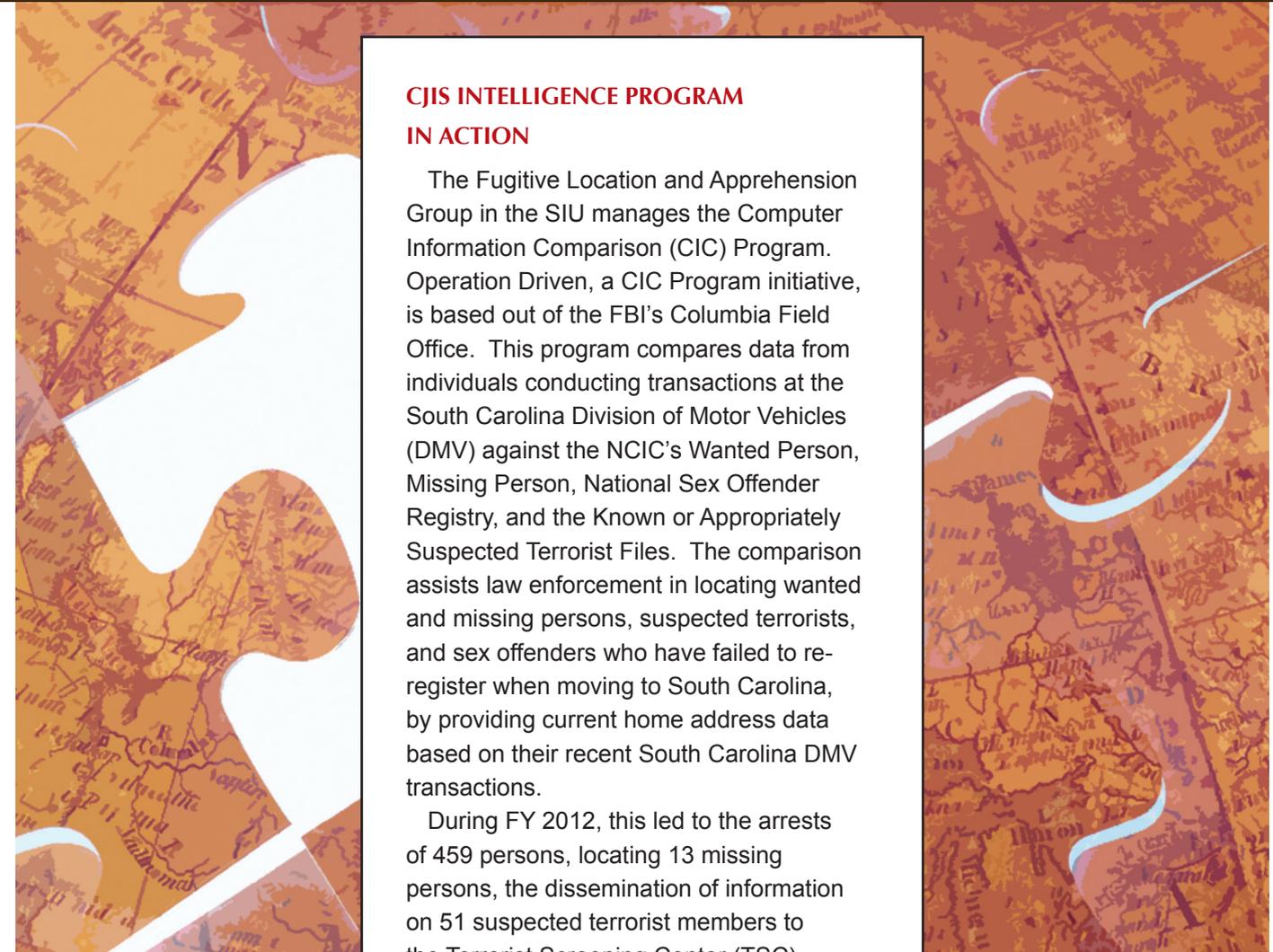
agencies by monitoring and reporting identity inquiries against the Integrated Automated Fingerprint Identification System (IAFIS) and the National Crime Information Center (NCIC).

- The **Crime Analysis, Research and Development (CARD) Unit**, which conducts strategic research and analysis of CJIS Division Programs (e.g., the NCIC and the Uniform Crime Reporting [UCR] Program), as well as external data sources (e.g., Census, Labor). The CARD Unit may identify, for example, areas of a state where there may be violent criminal enterprises operating.

Now armed with the information from the CJIS Intelligence Program and its capabilities, these CJIS SMEs can more effectively do their jobs at their respective field offices and better assist their law enforcement partners in the territories they cover.

### ACCOMPLISHMENTS

- New software, the Biometric Collection Integrated Platform (BCIP), was delivered to the GIU Biometric Identification Tools Program Office in September 2012. This software was designed to be easily configured across biometric capture devices, missions, and vendors. The transition of the software to current and new Quick Capture Platforms will take place in FY 2013.
- In FY 2012, an FBI Supervisory Special Agent (SSA) who was assigned to GIU was stationed in Kabul, Afghanistan. This SSA promoted the sharing of latent fingerprints collected by GIU during sensitive site exploitation missions throughout Afghanistan by the U.S. and coalition partners with the Afghan Ministry of Interior (MoI) Biometric Center (BC). A total of 27,582 latent prints were provided to the MoIBC and have resulted in 35 latent fingerprint identifications to 24 individuals.
- CDIG produced the CJIS Division's first Intelligence Bulletin titled "Émigré Community Conditions Favorable to a Rise in Criminal Activity." The Intelligence Bulletin was published to the FBI's intelligence portal on April 5.



### CJIS INTELLIGENCE PROGRAM IN ACTION

The Fugitive Location and Apprehension Group in the SIU manages the Computer Information Comparison (CIC) Program. Operation Driven, a CIC Program initiative, is based out of the FBI's Columbia Field Office. This program compares data from individuals conducting transactions at the South Carolina Division of Motor Vehicles (DMV) against the NCIC's Wanted Person, Missing Person, National Sex Offender Registry, and the Known or Appropriately Suspected Terrorist Files. The comparison assists law enforcement in locating wanted and missing persons, suspected terrorists, and sex offenders who have failed to re-register when moving to South Carolina, by providing current home address data based on their recent South Carolina DMV transactions.

During FY 2012, this led to the arrests of 459 persons, locating 13 missing persons, the dissemination of information on 51 suspected terrorist members to the Terrorist Screening Center (TSC), and the dissemination of 11,879 sex offender records to the South Carolina Law Enforcement Division (SLED). For all CIC Programs for FY 2012, 8,042 persons were arrested and 30 missing persons were found.

### QUICK FACTS

- CDIG produced 391 intelligence electronic communications, including intelligence notes, firearms denials, and refugee notifications that have been disseminated to local, state, and federal law enforcement agencies.
- CDIG produced 112 Intelligence Information Reports regarding biometric efforts within the greater Intelligence Community.
- CARD wrote 82 Intelligence Notes for FBI field offices.

The **Law Enforcement Online (LEO)** system has enabled more efficient law enforcement collaboration for the past 17 years as it has supplied the criminal justice community with free, safe communication. In 2012, LEO continued, through its secure Internet site and Virtual Command Centers (VCCs), to provide Internet-based monitoring and sharing of information for complex operations and investigations—remotely and in real time.

Delivery of the LEO Enterprise Portal (LEO-EP) homepage in FY 2012 is the latest step toward innovative, one-stop access to CJIS and other services and data that are crucial to modern law enforcement. Users of the LEO-EP can use single sign-on technology to gain authorized access to many different services, including the Law Enforcement National Data Exchange, the Joint Automated Booking System, the National Gang Intelligence Center, the Internet Crime Complaint Center, and many others.

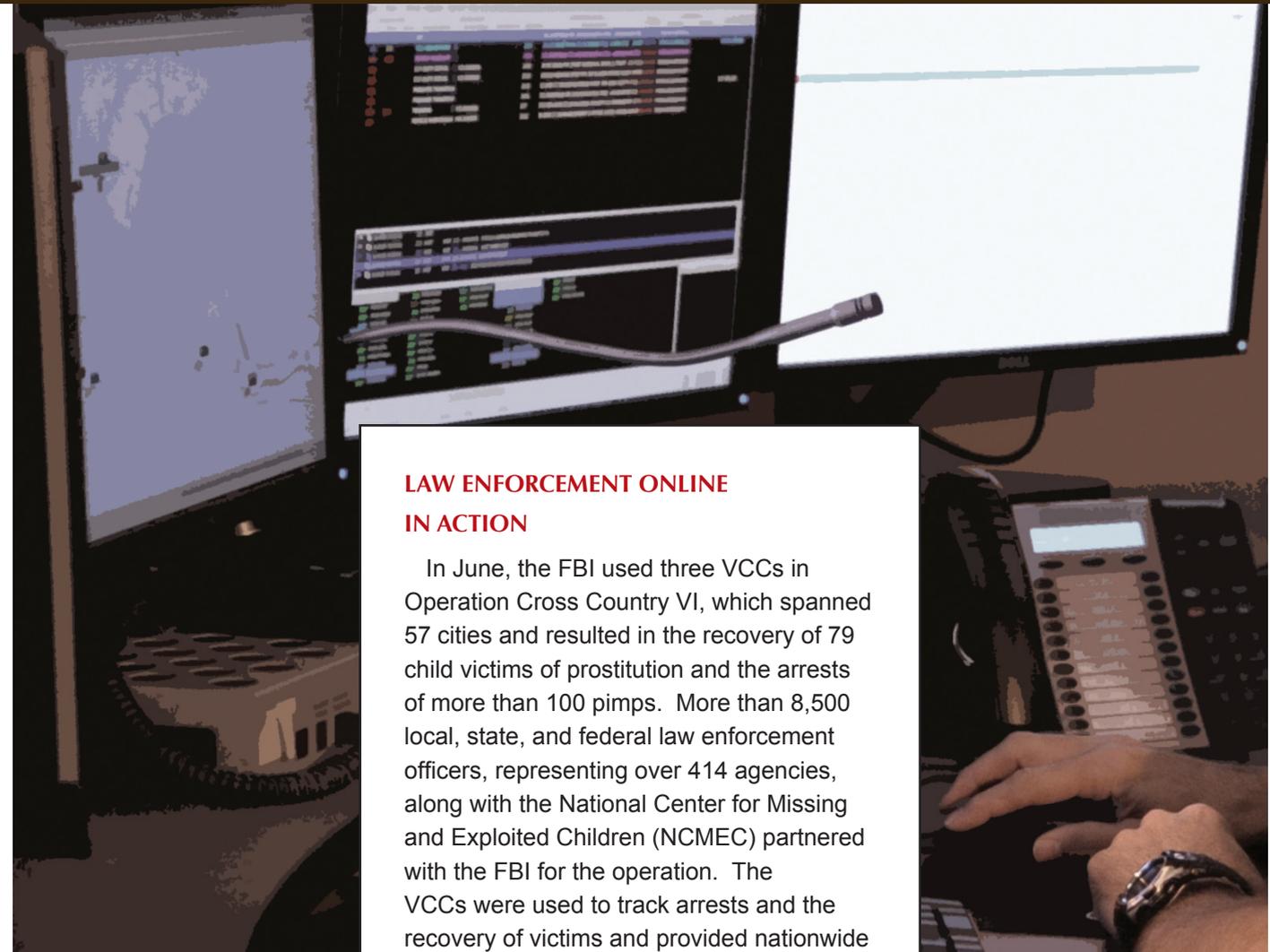
LEO has long offered a variety of features and services to the criminal justice community, including:

- Access to LEO Special Interest Groups (SIGs), which provide multi-level access for members to participate in communities of specialized interests.
- Access to the Virtual Office capability, a secure, private environment which allows a law enforcement agency to store and retrieve critical information, such as investigative forms, building blueprints, contact lists, or emergency action plans to better prepare law enforcement for “active shooter” or other major first responder events.
- Use of secure e-mail between LEO users and other partnering government and law enforcement systems.
- Access to the Intelink search portal and external connectivity with other secure networks to enhance information and intelligence sharing.
- Training through eLearning, which supplies topical learning modules and resources.
- Access to the National Alert System, which delivers timely and sensitive information securely to LEO members via e-mail and text messaging.

One of the most collaborative features of LEO is the VCC. This widely-used capability is accessed through the Internet, so it is extremely flexible. It can be used or viewed from multiple geographic locations, and incidents can be managed in real time, 24/7, with both operational and technical support. Since its rollout in 2002, it has been used to securely monitor the moving parts of more than 3,100 events, including political conventions and major sporting events. Often, agencies need to post, track, and spread information in a protected way for an investigation or occurrence. In these instances, VCCs are used to safely share information about street-level and tactical activities among law enforcement centers and command posts. This key resource fosters synergy and collaboration between local, state, tribal, and federal law enforcement agencies and organizations as they join forces to combat crime and terrorism.

**ACCOMPLISHMENTS**

- The LEO-EP homepage was delivered in early FY 2012. LEO personnel assisted in the delivery and negotiation of Memorandums of Understanding and supporting documents to bring on board four new Identity Providers (IdPs): the U.S. National Central Bureau of Interpol, the FBI CJIS’s Omninet Network, the FBI’s Unclassified Network, and the Texas Department of Public Safety. Also added were two new Service Providers (SPs): the U.S. Department of Justice’s myFX (a Web-based server) and the FBI’s National Crime Information Center Mobility. The LEO Program office is currently collaborating with several new potential IdPs and SPs.
- LEO is expanding partnerships in support of the CJIS Division’s Tribal Initiative. Through this initiative, LEO staff worked with Indian Country law enforcement regarding connectivity to CJIS Systems/Programs, assisting with connectivity issues, and helping ensure policy compliance. LEO staff also provided guidance on the establishment of Tribal SIGs as well as Virtual Offices and VCCs to ensure smooth communications among Indian Country law enforcement agencies.



**LAW ENFORCEMENT ONLINE  
IN ACTION**

In June, the FBI used three VCCs in Operation Cross Country VI, which spanned 57 cities and resulted in the recovery of 79 child victims of prostitution and the arrests of more than 100 pimps. More than 8,500 local, state, and federal law enforcement officers, representing over 414 agencies, along with the National Center for Missing and Exploited Children (NCMEC) partnered with the FBI for the operation. The VCCs were used to track arrests and the recovery of victims and provided nationwide situational awareness during the 3-day operation.

- During FY 2012, the Division worked to “rehost” the LEO network onto new computer servers. This technology upgrade provided significant improvements for users, including the change to a portal environment which makes it more “user friendly;” the development of a content management system which makes document location easier; and enhanced e-mail and calendar functionality.

**QUICK FACTS**

- Law enforcement opened more than 720 VCC event boards in FY 2012.
- There are over 58,800 active LEO members.
- More than 540 Special Interest Groups were created in FY 2012. There are now a total of over 1,830 LEO SIGs.

*Crunching the numbers and providing a national perspective of crime.*

The idea of collecting national crime statistics originated in the mid-1800s. The International Association of Chiefs of Police (IACP) took a leading role in promoting the concept in the latter part of that century. However, it wasn't until 1930 that 400 cities submitted their first data to the IACP. The compilation of this early data was the basis for what is now the nation's premier crime data collection system, the FBI's **Uniform Crime Reporting (UCR) Program**.

Although the UCR Program has experienced many changes throughout the decades since its debut, the primary objective remains the same: to provide dependable and valuable crime statistics for use by law enforcement, criminologists, sociologists, legislators, municipal planners, the media, and the public.

## ACCOMPLISHMENTS

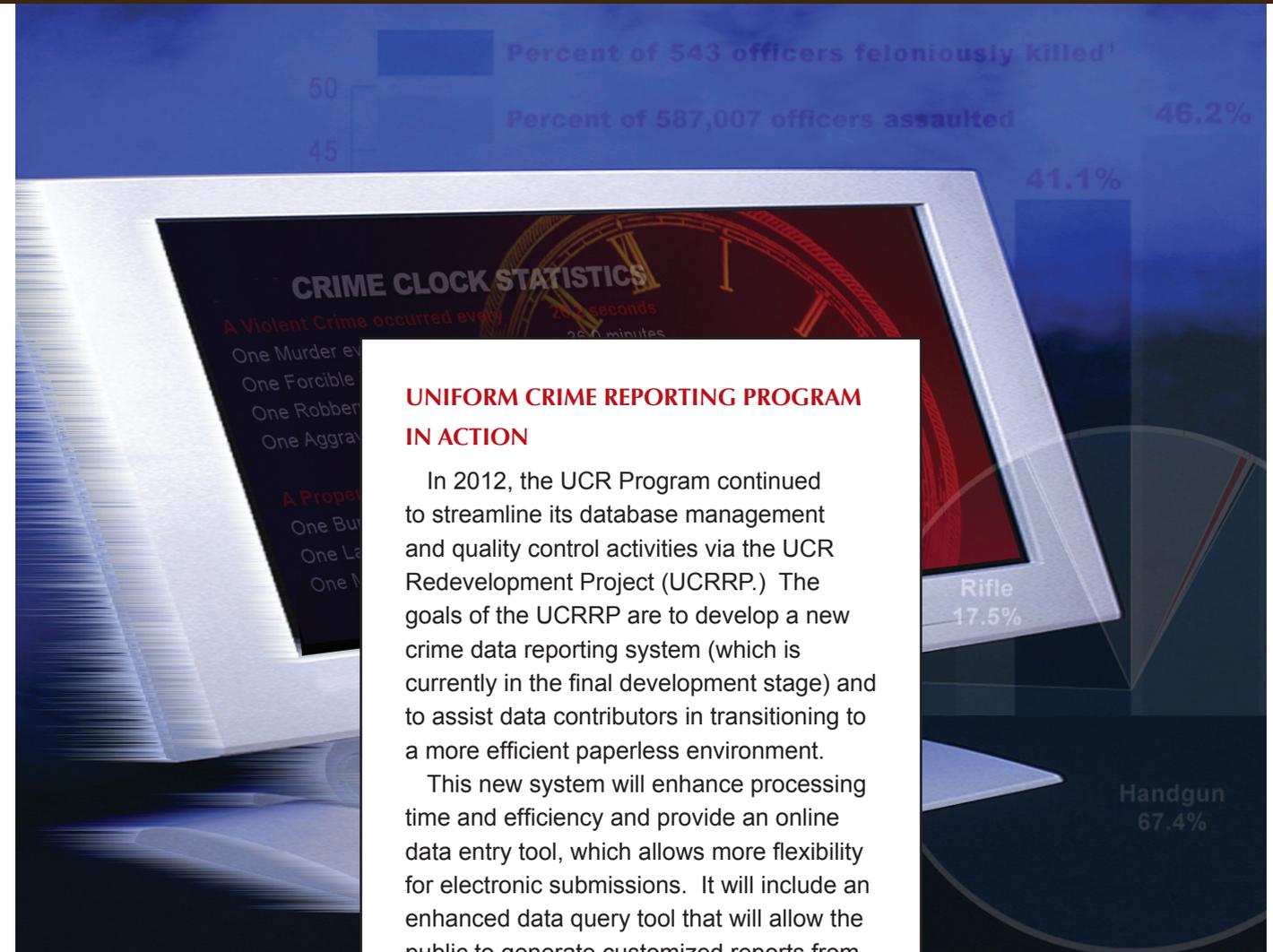
- In 2012, the FBI's UCR Program staff developed data collection methods to capture crime data on human trafficking—incidents which involve commercial sex acts or involuntary servitude—in response to the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, Title 28 United States Code (U.S.C.) Section 534. The capability to accept these data from contributors will be available in January 2013.
- The national UCR's Hate Crime Statistics Program will also begin accepting data from contributors in 2013 on crimes motivated by "gender and gender identity" bias, as well as bias-motivated "crimes committed by, and crimes directed against, juveniles." This change complies with the Matthew Shepard and James Byrd, Jr., Hate Crime Prevention Act of 2009, 28 U.S.C. § 249.

*“ Although the UCR Program has experienced many changes throughout the decades since its debut, the primary objective remains the same: to provide dependable and valuable crime statistics . . . ”*

- During FY 2012, the UCR Program staff provided 259 vital officer safety training classes as part of its Law Enforcement Officers Killed and Assaulted Program. A total of 19,702 national and international law enforcement officers representing 5,137 agencies attended this critical training.

## QUICK FACTS

- The average number of visits to the UCR Program's Internet homepage was more than 367,000 each month in FY 2012.
- Upon request, the UCR Program staff disseminates copies of the program's master files dating back to 1960.
- The current editions of *Crime in the United States*, *Law Enforcement Officers Killed and Assaulted*, and *Hate Crime Statistics* are available at [www.fbi.gov/about-us/cjis/ucr](http://www.fbi.gov/about-us/cjis/ucr).



## UNIFORM CRIME REPORTING PROGRAM IN ACTION

In 2012, the UCR Program continued to streamline its database management and quality control activities via the UCR Redevelopment Project (UCRRP.) The goals of the UCRRP are to develop a new crime data reporting system (which is currently in the final development stage) and to assist data contributors in transitioning to a more efficient paperless environment.

This new system will enhance processing time and efficiency and provide an online data entry tool, which allows more flexibility for electronic submissions. It will include an enhanced data query tool that will allow the public to generate customized reports from UCR data published to the Internet. This new system will also provide a more timely and comprehensive distribution of UCR data to law enforcement and the public.

In 2012, the CJIS Division's **Biometric Identification Services** operated with more speed and accuracy than ever before. Using the power of Next Generation Identification (NGI) technology, the FBI's Integrated Automated Fingerprint Identification System (IAFIS) sifts through the world's largest electronic repository of biometric identification and criminal history information. In record time, it delivers vital facts to help law enforcement solve and prevent crimes and terrorist activities and assists employers in hiring qualified workers.

This is the first complete year that the system has operated with the improved technology implemented by the NGI program. The NGI expansion and enhancements started in 2010 and will continue through 2014. Recent enhancements made it possible for facial images to be searched along with the standard rolled and flat fingerprints. The NGI technology also increased interoperability, which allowed the FBI's biometric identification system to have more flexibility to interact with other biometric matching services, such as those maintained by the U.S. Departments of Defense and Homeland Security. The advancements have already increased accuracy and response times and are paving the way for new services to be offered to the FBI's 18,000 local, state, tribal, federal, and international partners.

This year, the CJIS Division began a Facial Recognition Pilot using the new NGI capabilities. The Facial Recognition Pilot permits authorized criminal justice agencies to submit queries for a facial recognition search of a national repository of mug shots, within the Interstate Identification Index (III), for criminal justice purposes. The pilot provides responses in the form of a ranked investigative candidate list associated with criminal identities and supported by fingerprints.

A limited Rap Back Pilot service was also deployed in 2012 and will be followed by a nationwide deployment of the full Rap Back functionality in 2014. The Rap Back Service will provide an on-going status notification of any change in criminal history (e.g., an arrest or a conviction) reported to the FBI after an individual's initial criminal history check. This service can be used both for noncriminal justice applicants, employees, volunteers, licensees, etc., and for individuals under criminal investigation or under the supervision of criminal justice agencies.

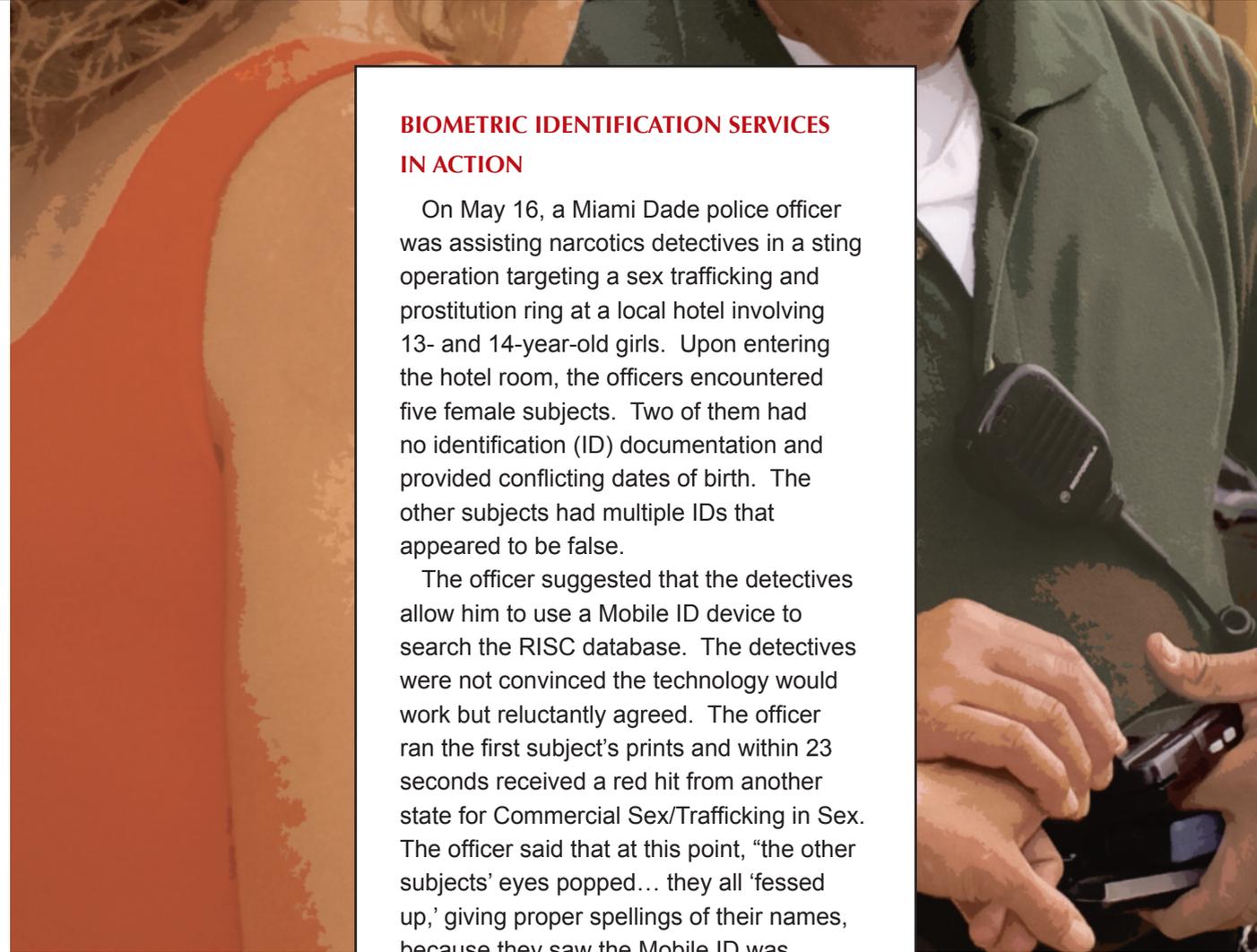
Also in FY 2012, the CJIS Division ended the contract that supported scanning hard copy fingerprint identification cards into an electronic format that could be entered into the IAFIS. Staff began scanning an enormous backlog of fingerprints and identification data in 1998. As law enforcement agencies updated their technology, paper submissions declined significantly, and agencies are now required to submit all biometric information via electronic means. While the scanning contract was in place, more than 83 million prints and pieces of information were scanned.

## ACCOMPLISHMENTS

- Since becoming nationally available in 2011, the NGI Repository of Individuals of Special Concern (RISC) is being used by 10 states, representing over 500 law enforcement agencies with more states and agencies in the process of establishing connectivity. RISC provides a mobile fingerprint identification service that can be used in the field to quickly identify wanted persons, known or appropriately suspected terrorists, sex offenders, and persons of special interest.
- In 2012, CJIS continued to expand its collection of palm prints and has nearly 5 million submissions. This process is part of establishing the National Palm Print Service. When the service is implemented next year, law enforcement agencies will be able to submit a latent palm print gathered at a crime scene and search against a database of palm prints.

## QUICK FACTS

- Biometric Identification Services identified 323,450 fugitives in FY 2012.
- Enhancements to the system have increased accuracy to 99.6 percent while decreasing response times for criminal submissions to an average of 8 minutes, 52 seconds. Noncriminal/civil response times average 1 hour, 8 minutes, 38 seconds.
- The 400 millionth fingerprint transaction was processed on July 13.



## BIOMETRIC IDENTIFICATION SERVICES IN ACTION

On May 16, a Miami Dade police officer was assisting narcotics detectives in a sting operation targeting a sex trafficking and prostitution ring at a local hotel involving 13- and 14-year-old girls. Upon entering the hotel room, the officers encountered five female subjects. Two of them had no identification (ID) documentation and provided conflicting dates of birth. The other subjects had multiple IDs that appeared to be false.

The officer suggested that the detectives allow him to use a Mobile ID device to search the RISC database. The detectives were not convinced the technology would work but reluctantly agreed. The officer ran the first subject's prints and within 23 seconds received a red hit from another state for Commercial Sex/Trafficking in Sex. The officer said that at this point, "the other subjects' eyes popped... they all 'fessed up,' giving proper spellings of their names, because they saw the Mobile ID was unbeatable."

The detectives were impressed when the handheld mobile unit delivered two RISC hits. The officer was able to identify all the subjects either using the unit, or by the names they provided after witnessing the rapid ID unit's capabilities. The officer reported, "It was priceless, and so were the subjects' faces when I started telling the detectives who they were, their pasts, and their warrants."

Initiated in 2005, **Biometric Interoperability** is increasing the ability for the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and Next Generation Identification to connect with other biometric systems around the world. What began as an effort to ensure the FBI's IAFIS could exchange information with the Department of Homeland Security's (DHS's) Automated Biometric Identification System (IDENT) has grown substantially. Today, it provides for the seamless sharing of biometric information among these systems, as well as the Department of Defense's (DoD's) Automated Biometric Identification System (ABIS) and others. As a result, many criminals and terrorists who may have otherwise gone unnoticed have been identified.

Although previously available to select local and state agencies, the push to provide interoperability between the IAFIS and the IDENT for agencies nationwide began November 8, 2011. Currently, the systems are compatible in local and state law enforcement agencies in all 50 states (2 states have limited availability), the District of Columbia, 4 U.S. territories, and federal agencies submitting Criminal Answer Required transactions. With this connectivity, local and state agencies use a single query that searches both systems. In addition, the FBI has authorized and provided the ability for select stakeholders to search the FBI's IAFIS, the DHS' IDENT, and the DoD's ABIS in a single query, thus providing a response from all three systems. The sharing of biometric identification data between these agencies greatly enhances the ability of law enforcement and intelligence agencies to identify and track high-risk individuals, i.e., special interest aliens, gang members, and other persons of interest.

On May 14, the CJIS Division, the DoD, and the Texas Department of Public Safety (TXDPS) implemented the Latent Interoperability Pilot. Prior to the pilot, local and state law enforcement agencies could search the latent fingerprints of criminal cases against the FBI's IAFIS; however, searches of the ABIS and IDENT were limited, accepted only on a case-by-case basis, and processed manually. Now, the Latent Interoperability Pilot allows the TXDPS, in coordination with Texas state law enforcement offices, to extend latent feature and image searches beyond the IAFIS to include a search of ABIS in a single query. Consequently, the TXDPS receives candidate lists from both systems for review and identification.

## ACCOMPLISHMENTS

- On March 30, the United States Special Operations Command (USSOCOM) and the Biometric Identity Management Agency of the DoD, the Immigration and Customs Enforcement (ICE) of the DHS, and the FBI signed an agreement that allows limited searches of the IDENT. (The USSOCOM leads the military's Special Forces in planning and carrying out global operations against terrorist networks.) Prior to the agreement, the FBI was interoperable with the ABIS and the IDENT; however, the ABIS and IDENT were not connected with each other. As a result of the agreement, on April 18, the USSOCOM began submitting IAFIS transactions for persons encountered through Operation Enduring Freedom and Operation Iraqi Freedom for searches of a subset of the IDENT repository. This is a significant milestone because the USSOCOM is the first entity from the DoD to access IDENT information using the FBI's IAFIS. More importantly, this interoperability initiative increases the likelihood that our special forces will identify potential adversaries, which directly increases the effectiveness of combat operations. These transactions between IAFIS and IDENT will continue until a direct connection is established between the ABIS and the IDENT.
- Just under 7 months after it was begun, deployment of IAFIS and IDENT interoperability to state and local law enforcement agencies nationwide was completed on June 5.

## QUICK FACTS

- On July 13, the IAFIS processed its 400 millionth transaction. This transaction was a result of interoperability with the IDENT and was submitted for a search of IAFIS/IDENT by the Department of State.
- From the inception of interoperability to September 30, there have been 25,728,999 IAFIS searches sent to IDENT, resulting in 1,737,311 matches to IDENT data.
- As of September 30, there have been 125,298,357 IDENT searches sent to IAFIS, resulting in 1,143,150 identifications with IAFIS data.

## BIOMETRIC INTEROPERABILITY IN ACTION

On March 17, a 27-year-old, alleged drunk driver hit a porch where two young boys were playing. A 7-year-old boy was taken to the local hospital where he was pronounced dead, and a 4-year-old suffered burns on more than 40 percent of his body from a hot grill that the car had also struck.

Initially charged with DUI, the driver was also charged with intoxicated manslaughter and intoxicated assault. Because of the interoperability between local, state, and federal systems—and particularly a search of the IDENT—authorities also determined that the suspect was in the country illegally. Consequently, authorities filed additional immigration charges against the suspect and placed a detainer on him. He is being held without bail, and he could face a maximum sentence of life in prison.

The **FBI Biometric Center of Excellence (BCOE)** was created in 2007 to support the FBI's overall biometrics mission, major programs, and strategic initiatives that comprise the FBI's biometric services. The BCOE explores and advances new and enhanced biometric technologies and capabilities for use in operations. The BCOE leverages the skill and expertise of FBI staff from across the Science and Technology Branch including the CJIS Division, the Laboratory Division, and the Operational Technology Division.

In FY 2012, the BCOE demonstrated governmentwide leadership in advancing facial recognition technology through its sponsorship of several interagency collaborations. The BCOE sponsored the United States Government Facial Recognition Legal Series (Legal Series), comprised of interagency legal and policy forums specific to facial recognition. The Legal Series brought together lawyers, policy experts, technical personnel, and biometric program managers from nearly 40 federal law enforcement and homeland security agencies, the military, and the intelligence community to discuss the legal and policy challenges of facial recognition.

The Legal Series began in August 2011 with a forum sponsored by the BCOE and the Office of the Director of National Intelligence in Chantilly, Virginia, and continued with three more forums in FY 2012. The second meeting in the Legal Series, sponsored by the BCOE and the U.S. Immigration and Customs Enforcement of the Department of Homeland Security (DHS), was held in Fairfax, Virginia. Topics included interagency information sharing challenges and best practices. On March 14, 2012, the BCOE and the Department of Defense (DoD) co-sponsored a forum at the FBI Academy, in Quantico, Virginia, on privacy and civil liberty considerations with regard to facial recognition deployment. The final forum in the Legal Series was held on June 11, 2012, focusing on public perception as a critical factor in effective policy development. As a result of the BCOE's recommendations following the Legal Series, the National Science and Technology Council is developing guidelines to be used by federal agencies to construct facial recognition technology policy.

**ACCOMPLISHMENTS**

- The BCOE, through a partnership with Michigan State University, continued to develop the TattooID tool. The tool will allow searches of tattoo images, key

*“ The BCOE leverages the skill and expertise of FBI staff from across the Science and Technology Branch . . . ”*

words, or characters to find similar images with the goal of determining gang associations or activities and potentially linking gang crimes across the country.

- In collaboration with the DoD and DHS, the BCOE continued to sponsor the development of portable Rapid DNA machines that will quickly process DNA for law enforcement in booking stations.
- The BCOE released a new law enforcement video, *Biometrics: Supporting the Mission*, educating viewers on how investigations may be strengthened through the use of biometrics.
- During FY 2012, the FBI's BCOE continued to leverage the expertise of academia. Through an agreement signed in 2008 by the FBI and West Virginia University (WVU) to establish WVU as the BCOE's liaison to the academic research community, the FBI has access to leading academic biometric experts and opportunities to initiate biometric research activities at WVU and other academic institutions. Some of these institutions include Clemson University, Florida International University, Michigan State University, University of Miami, University of North Carolina Wilmington, and the University of Notre Dame.

**QUICK FACTS**

- In FY 2012, the BCOE sponsored 30 ongoing applied biometric research projects to further the field of biometrics.
- In FY 2012, the BCOE sponsored 10 collaborative events that advanced biometric discussion and development.

**FBI BIOMETRIC CENTER OF EXCELLENCE IN ACTION**

The FBI has been expanding its capabilities to bring advanced DNA analysis to law enforcement since 2008. The aim is to analyze DNA in near real-time (less than 2 hours) and submit a search to the National DNA Index System using enhanced Combined DNA Index System software that can be operated outside of a laboratory environment with minimal user training.

In September 2012, the BCOE reached a milestone in this endeavor by introducing two new devices, representing the latest in Rapid DNA (R-DNA) technology, at the Biometric Consortium Conference in Tampa, Florida, in September. The first, the Automated Nuclear DNA Equipment (ANDE), was built in partnership with the DoD and the DHS and is processing in under 2 hours. The second device, the IntegenX Apollo RapidHit 200, can process in 90 minutes. Both devices are processing samples in significantly less time than it requires a traditional laboratory technician to process now--which can currently require 2 or more days with multiple instruments, separate rooms, and numerous complex steps.

The R-DNA devices were transferred to the FBI's Laboratory Division for additional testing and evaluation. Initial reports show high success rates for both instruments. This unparalleled technology will enable law enforcement to quickly determine if a subject in custody is linked to another crime.

The **Global Collections Program** provides biometric-related support to national and international law enforcement through initiatives such as the Foreign Biometric Exchange (FBE), the Quick Capture Platform (QCP), the Flyaway Program, and others.

Through the FBE, the CJIS Division acquires biometric records and related information from foreign government sources for analysis, comparison, and storage within the FBI's Integrated Automated Fingerprint Identification System. The CJIS Division also receives and processes case-related biometric inquiries from international sources (typically law enforcement agencies), while facilitating similar requests from U.S. agencies and FBI field offices for queries of foreign partners' databases.

The CJIS Division also administers a biometric acquisition program, known as the Biometric Identification Tools Program (B-ID), to continue making biometric collections easier and faster. A major component of the B-ID Program is the QCP, a biometric system that enables frontline investigators to collect, store, and match fingerprint data during domestic and international operations. Initially developed for combat theater operations, the QCP can be deployed for operations in areas where access to CJIS Division services would otherwise be impossible, such as the war zone in Afghanistan. The QCP is the only tactical collection platform that provides such a fast response, searching against nearly 200 million records, at any time from any place in the world.

The Biometric Collections Integrated Platform (BCIP) is a new technology enhancement being developed to work with the Quick Capture and Flyaway platforms. This software will create a consistent user experience across multiple platforms and will provide the flexibility needed to be modified and updated for various missions. During FY 2012, the BCIP code was delivered to CJIS and successfully completed a Government Acceptance Review. After the software is piloted on existing missions, a deployment schedule will be developed.

The 9/11 Act amended the VISA Waiver Program (VWP) to require the Program to include several enhanced security measures.

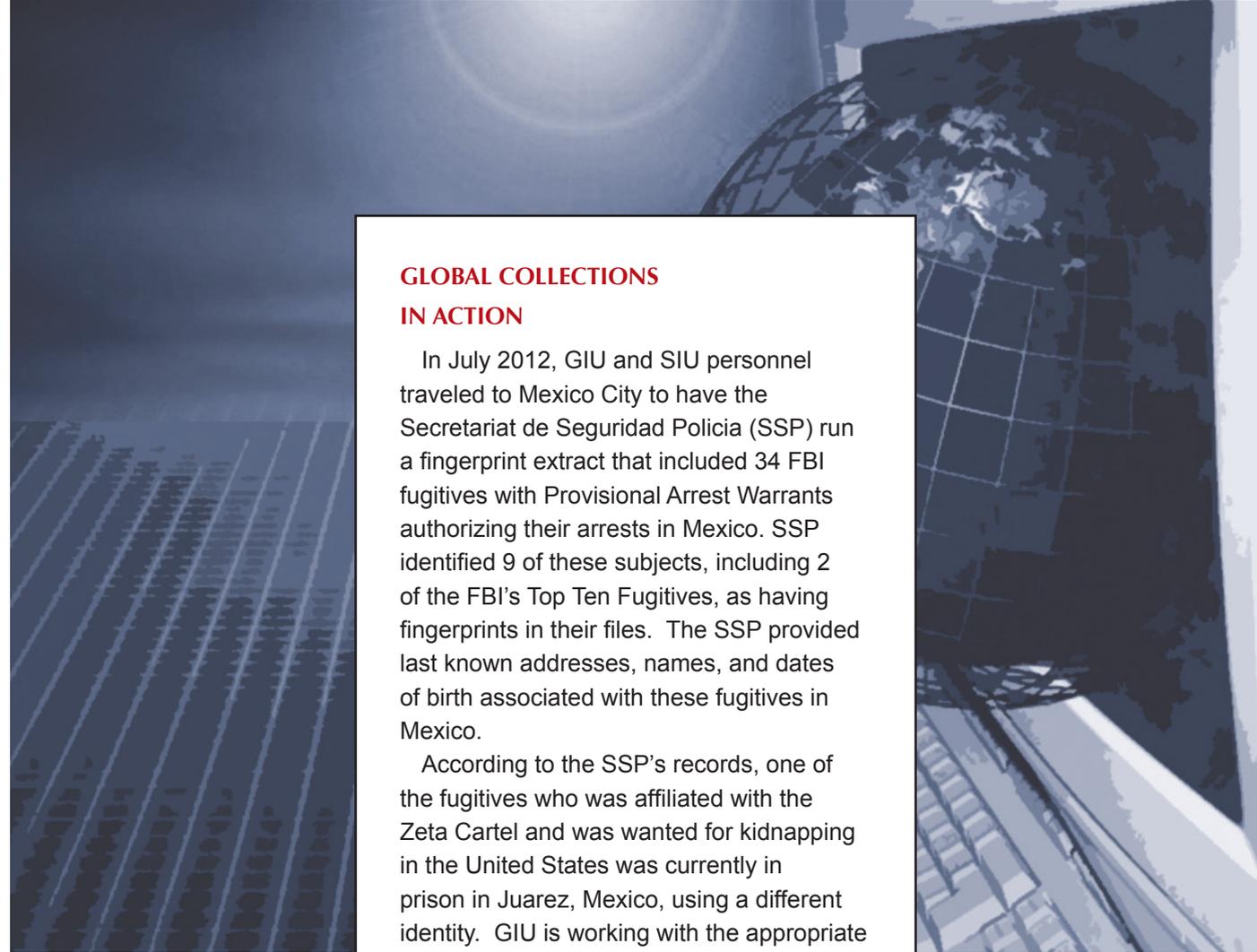
(The VWP enables nationals of participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa.) The FBI's Global Initiatives Unit (GIU) is currently working with the Department of Homeland Security (DHS) to manage the implementation of the Preventing and Combating Serious Crime (PCSC) Agreements, which require all VWP countries to provide each other with electronic access to their fingerprint databases on a query (hit/no hit) basis.

## ACCOMPLISHMENTS

- The CJIS Division acquired over 90,000 criminal fingerprint records from the Dominican Republic in FY 2012, through a cooperative effort involving the GIU, the Department of Defense (DoD), and the FBI's Office of the Legal Attaché in Santo Domingo. Also, the CJIS Division assisted in the development of a State Department plan to transition the Dominican Republic's fingerprint program from a DoD-managed system to one managed by the Dominican National Police.
- The Central America Fingerprint Exchange (CAFÉ) initiative has resulted in the collection of more than 350,000 records. This includes more than 40,000 criminal fingerprint records that were received from Guatemala in August 2012.

## QUICK FACTS

- The GIU collected 922,973 fingerprint records from foreign countries in FY 2012.
- In FY 2012, 19 Flyaway missions (missions where staff assisted law enforcement with critical on-site fingerprint identification) were completed.
- The VWP maintains agreements with 36 countries.



## GLOBAL COLLECTIONS IN ACTION

In July 2012, GIU and SIU personnel traveled to Mexico City to have the Secretariat de Seguridad Policia (SSP) run a fingerprint extract that included 34 FBI fugitives with Provisional Arrest Warrants authorizing their arrests in Mexico. SSP identified 9 of these subjects, including 2 of the FBI's Top Ten Fugitives, as having fingerprints in their files. The SSP provided last known addresses, names, and dates of birth associated with these fugitives in Mexico.

According to the SSP's records, one of the fugitives who was affiliated with the Zeta Cartel and was wanted for kidnapping in the United States was currently in prison in Juarez, Mexico, using a different identity. GIU is working with the appropriate FBI case agents, Lé gat Mexico, and the Criminal Investigative Division to use this information to locate and detain these fugitives in Mexico. As a result of this trip, myFX, a DOJ Web-based server, is being used to allow the SSP and the FBI to exchange criminal fingerprint files electronically. Since the SIU personnel returned from Mexico, both the FBI and the SSP have submitted criminal fingerprints electronically to search against the other's biometric databases.

## THE ADVISORY POLICY BOARD AND COMPACT COUNCIL

The CJIS Division continues to seek the input of law enforcement and to cooperate with that larger community to accomplish shared goals. Two ways CJIS collaborates are through the **CJIS Advisory Policy Board (APB)** and the **National Crime Prevention and Privacy Compact Council (Council)**.

The APB is chartered under the provisions of the Federal Advisory Committee Act of 1972 and is made up of criminal justice professionals who provide guidance and voice the viewpoint of CJIS systems' users, reflecting the efforts of one federal and four regional working groups and numerous ad hoc subcommittees. Although the National Crime Information Center (NCIC) APB dates back to 1969, former FBI Director Louis J. Freeh established the Advisory Process to cover all CJIS services in the fall of 1994.

The National Crime Prevention and Privacy Compact Act of 1998 led to the establishment of the 15-member Council. The Council establishes rules and procedures to facilitate the use of criminal history record information (CHRI) for noncriminal justice purposes (e.g., screening for employment, licensing, or placement in a position of trust).

## ADVISORY POLICY BOARD

In FY 2012, the APB, consisting of 34 representatives from criminal justice and national security agencies, tackled numerous topics in the pursuit of improving and advancing CJIS systems. In its year-end meeting in December 2011, the APB recommended that the Law Enforcement National Data Exchange (N-DEx) support criminal justice employment background investigations. To that end, it was further suggested that the N-DEx Program Office incorporate into the *N-DEx Policy and Operating Manual* the policies and language regarding notice and consent, redress, and audits in order for the N-DEx system to be accessed for criminal justice employment background checks.

At that same meeting, the APB also advocated a change to the definition of rape within the Uniform Crime Reporting (UCR) Summary Reporting System. The new definition replaces the words "forcibly and against her will" with the statement "without

the consent of the victim." Further, the new definition does not stipulate that the victim must be female. Consistent with the new definition, the APB also voted to remove the term "forcible" from specific sex offenses collected by the FBI's UCR Program.

At the June 2012 meeting of the APB, the Board recommended the creation of a Violent Person File (VPF) in the NCIC. Statistical evidence indicates that, of offenders who feloniously kill a police officer, 44 percent have a history of violent crimes and 23 percent have a previous record for assaulting a police officer. The NCIC VPF flags individuals who meet specific criteria for inclusion based on prior convictions for assault or murder of a law enforcement officer, previous convictions for violent offenses against other persons, or past convictions for a violent offense where a firearm or weapon was used. The ability to access this information quickly through the NCIC will greatly enhance officer safety in the field.

## COMPACT COUNCIL

In FY 2012, the Council worked to balance the need for access to CHRI for noncriminal justice purposes and the need for protecting an individual's privacy. The Council continued to focus its efforts on compliance with privacy and security standards. To further privacy protections, the Council, collaborating with the FBI's Office of the General Counsel, developed two Guiding Principles documents. These documents incorporate the legal requirements that define an applicant's rights and an agency's responsibilities during the background check process. The Guiding Principles documents are available at <http://www.fbi.gov/about-us/cjis/cc> under the "Other References" section.

To provide access to information and in the interest of better communication, the Council launched its Special Interest Group (SIG) on Law Enforcement Online (LEO) in February 2012. The Council's SIG contains links to the Council's membership contact list, a copy of the Bylaws, future meeting information, meeting topic papers and meeting minutes, a copy of the Compact, guides to the outsourcing of noncriminal justice administrative functions, and state statutes for civil retention. The Council's SIG, and several topically-focused sub-SIGs, may be accessed on LEO at [www.leo.gov/http://leowcs.leopriv.gov/lesig/ncppcc/](http://www.leo.gov/http://leowcs.leopriv.gov/lesig/ncppcc/).



The Rap Back Task Force was created by the Council in 2009 to assist in the identification of noncriminal justice user requirements for the Rap Back service. The Rap Back service, with scheduled delivery in 2014, will allow authorized agencies to receive notification of criminal activity by individuals already employed, licensed, or holding positions of trust. With the completion of the Rap Back

service design, the Task Force was reconstituted into a 13-member focus group which concentrated on the operational and policy impacts related to Rap Back implementation. The focus group continues to provide recommendations to the Council, through the Standards and Policy Committee, on topics such as privacy strategies.



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.

A new addition is being built on the CJIS campus. 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 unique collaboration between the FBI and the DoD to protect the United States while preserving civil liberties.



2012



2011

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 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 include 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.

*The **CJIS MISSION** 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.*



### ***Sign up for alerts to new editions of the CJIS Link newsletter***

*Here is another way to stay informed about what is new at the CJIS Division and what it can do to support your agency: sign up at <http://www.fbi.gov/about-us/cjis> to receive an e-mail alert when the FBI publishes a new edition of the quarterly newsletter, the **CJIS Link (Link)**, to its Website at <http://www.fbi.gov/about-us/cjis/cjis-link>.*

*The **Link** is a key way the CJIS Division keeps agencies informed about CJIS services and benefits, showcases the successes of those CJIS programs and systems in supporting law enforcement, provides contact information, and alerts readers to new initiatives at CJIS.*