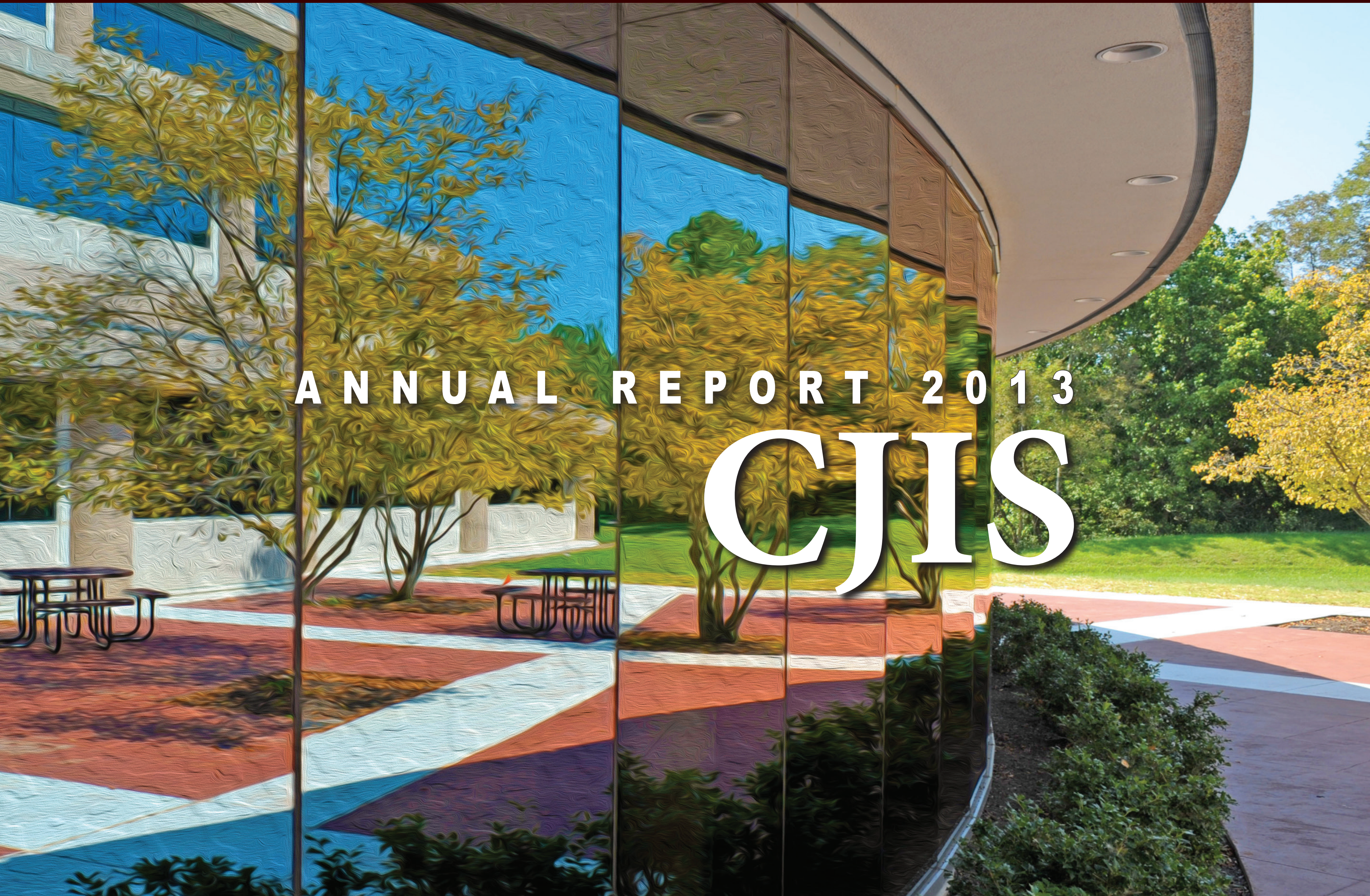
U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

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



ANNUAL REPORT 2013

CJIS

U.S. Department of Justice

Federal Bureau of Investigation

Criminal Justice Information Services Division

DESPITE CHALLENGES, THE CJIS DIVISION CONTINUES TO SERVE WITH EXCELLENCE

During the 2013 fiscal year, the FBI's Criminal Justice Information Services (CJIS) Division faced many challenges with the implementation of across-the-board federal spending reductions from the Budget Control Act of 2011 (BCA). These cuts, known as sequestration, resulted in severe staffing and budget decreases.

Despite these obstacles, however, we have been able to maintain our high level of service to our partners in the law enforcement, national security, and intelligence communities. Our response times for our systems continued to meet and exceed expectations; we continued to handle unprecedented volumes of background checks for gun purchases; and we were able to successfully roll out the third major increment of our Next Generation Identification system that provides exciting new capabilities in the area of biometric identification. In addition, we continued the development of our Biometric Technology Center building on our campus.

As the Assistant Director of the CJIS Division, I am pleased to present the 2013 edition of the *CJIS Annual Report*. This publication reflects the efforts of the Division's 2,500 employees during the past fiscal year. The outstanding work they do, in cooperation with our partners, helps promote the safety of law enforcement members on the front lines and support the investigation and prevention of crime and terrorism in communities across the United States and throughout the world. As we head into fiscal year 2014, we know we will continue to face challenges. However, we remain committed to providing excellent service to those who rely on our vital criminal justice information tools in order to perform their duties for our Nation and its people.

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

CONTENTS

Scan this QR Code with your smartphone to learn more about the FBI's Criminal Justice Information Services (CJIS) Division. If your QR Reader takes you to the mobile FBI site, you may wish to access the full "desktop" site from the button at the bottom of the page in order to open all the links on the CJIS site, or you can visit www.fbi.gov/about-us/cjis.

NATIONAL CRIME INFORMATION CENTER

Serving investigators and aiding officer safety since 1967, NCIC continues to evolve and improve

A law enforcement staple since 1967, the **National Crime Information Center (NCIC)** continues to expand and improve in a never-ending mission to provide law enforcement with crucial information.

THE YEAR IN REVIEW A number of changes to the NCIC took effect in August 2013. One system improvement involved the addition of the linking case number (LKI) and linking agency identifier (LKA) fields to the Gang, the Known or Appropriately Suspected Terrorist, the Protection Order, and the Supervised Release Files. Users can now make a single inquiry and receive all related records from these files.

Another enhancement modified the entry requirement in the NCIC Wanted Person File for the extradition limitation field. This modification aids law enforcement in proper warrant management and increases the likelihood of subjects being returned to the entering agency if they are captured outside that agency's jurisdiction.

Two fields were added to the Protection Order File. The service information field and the date served field advise law enforcement that an order was served and when it occurred. Both provide information that can assist in making an arrest.

In response to liability concerns expressed by law enforcement regarding the code for "other weapon," the wording in the Protection Order File was modified. Without this modification, an individual could have been erroneously arrested for possession of a hunting knife, bow, or any other item that could be described as "other weapon," but may not be part of the prohibition in a protection order.

Finally, responses for record inquiries were modified to include the name of the validator field. As a result, CJIS System Agencies (CSAs) can now view the validator field for a record inquiry within their jurisdictions to assist local agencies with validations, quality control, and audits.

The CJIS Division has obtained approval from the CJIS Advisory Policy Board to start the development of the CJIS Information Broker (CIB) capability in Fiscal Year 2014. This enhancement to NCIC will provide the ability to search for and extract more specific information from the NCIC database. When available, this capability will provide quicker turnaround times for data extractions, prevent system overloads, and lessen resource demands on FBI personnel, as agencies will be able to perform more specific searches independently.

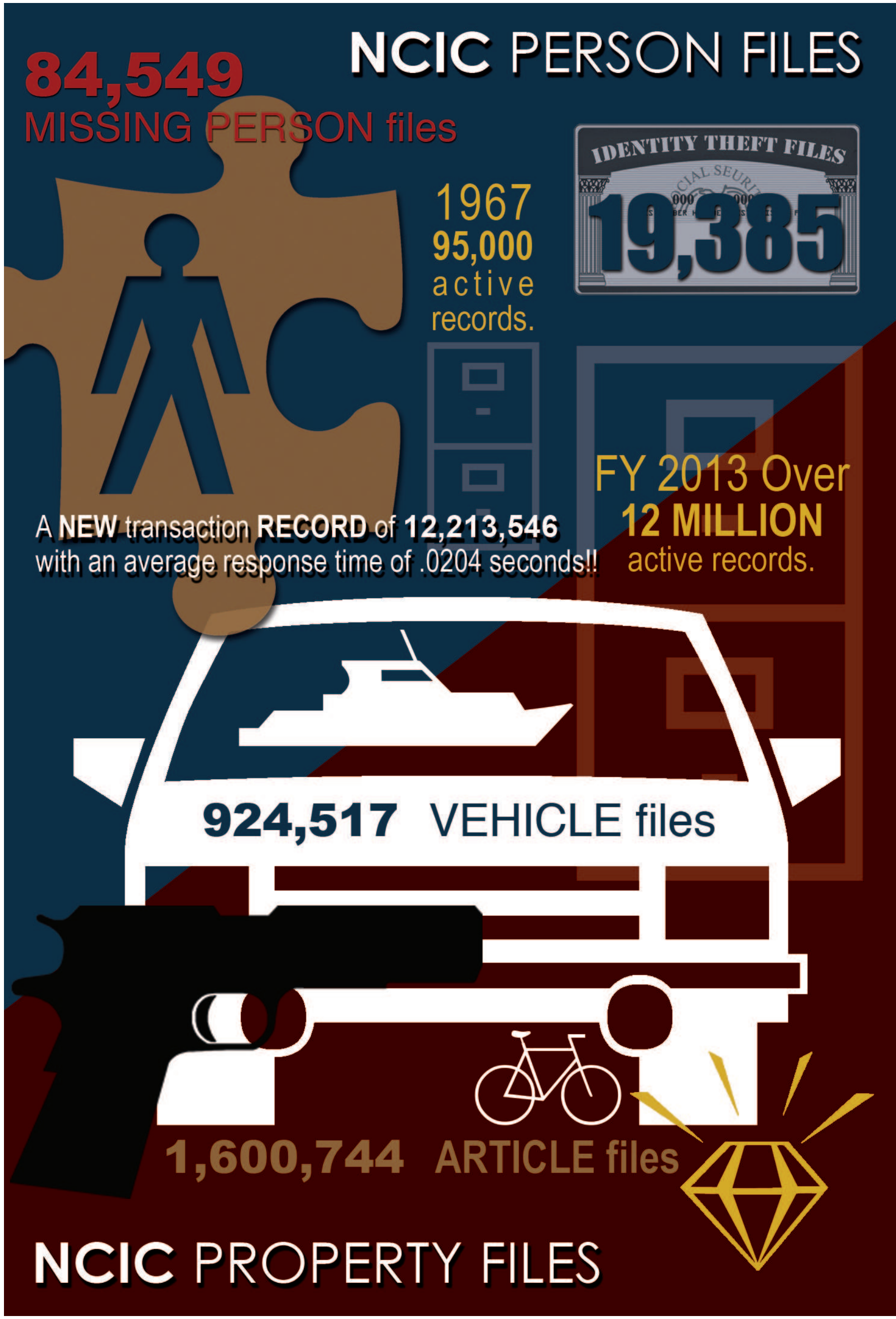
NCIC IN ACTION On January 11, the Investigative and Operational Assistance Group (IOAG) was contacted by a detective from the Parsippany-Troy Hills (New Jersey) Police Department for assistance in identifying two suspects who carjacked, kidnapped, and robbed a 71-year-old woman. The woman was taken from her car at gunpoint and transported to a bank where her personal identification number was used to withdraw money from an ATM. After stealing her credit cards, the suspects tied her hands, blindfolded her, and

ABOUT The **National Crime Information Center (NCIC)** is a computerized database of documented criminal justice information available to law enforcement agencies 24 hours a day, 365 days a year. The FBI manages the NCIC System and continues to work with law enforcement to satisfy the ever-growing demand for information on subjects such as wanted and missing/unidentified persons, stolen property, gangs, terrorists, and registered sex offenders. The 21 files of information maintained in the NCIC are accessed by law enforcement agencies and other criminal justice partners nationwide who are working to keep communities and the nation safe.

locked her in the trunk of her car in the commercial parking lot in frigid weather. Fortunately, the victim was able to free herself and get help.

During investigation, the detective learned what type of vehicle the suspects were driving and obtained surveillance video of the suspects, but he could not identify them. The IOAG conducted an off-line search for queries on the license plate numbers in the vicinity around the time of the incident. When he received the results, the detective manually checked the license plate number against records in the New Jersey Department of Motor Vehicles (DMV). He discovered that a Woodland Park police officer had checked the license plate number of a similar vehicle just minutes after the suspects used the stolen credit cards at a store in Woodland Park.

Further investigation revealed the vehicle had been rented in Newark. The detective matched the renter's DMV information and Facebook pictures to the surveillance footage from stores where the suspects had used the victim's credit card and was able to identify both suspects, who were subsequently arrested.



NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM

Closing a record-breaking year of background checks guarding public safety

When an authorized gun dealer or Federal Firearms Licensee (FFL) requests a **National Instant Criminal Background Check System (NICS)** background check on an individual who is attempting to purchase 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 match any records (i.e., wanted persons, subjects of protective or restraining orders, or other persons prohibited from receiving or possessing firearms) in the databases, the NICS staff and/or state agencies conduct further research to determine the applicant's eligibility.

THE YEAR IN REVIEW The NICS has been protecting public safety with firearm and explosive checks since 1998, but even in 2013, the program is still growing, adapting, and experiencing "firsts." The NICS processed the first Nuclear Regulatory Commission (NRC) Preemption Authority Background Check on July 25, and the first denied NRC transaction occurred on July 29, based on a disqualifying misdemeanor from the state of New York. (The Energy Policy Act of 2005 gave the NRC the authority to permit security forces at eight NRC-licensed facilities to possess and use firearms in the performance of their official duties.) The NICS staff conducted more than 1,500 background checks for NRC security personnel using the NICS E-Check.

In addition to the NRC checks, the NICS conducted a record number of firearm background checks in fiscal year 2013. In the week that followed the shooting at Sandy Hook Elementary School in Newtown, Connecticut, the NICS performed a record 1 million background checks. By June 12, 2013, the NICS had already processed 38 percent more transactions than the total number processed in fiscal year 2012.

To handle the unusual amount of checks, some NICS staff cancelled vacations, worked extra shifts, and some former NICS legal instruments examiners (NICS examiners) (who now work in other parts of the CJIS Division) returned on a temporary basis to make sure transactions were addressed within 3 business days.

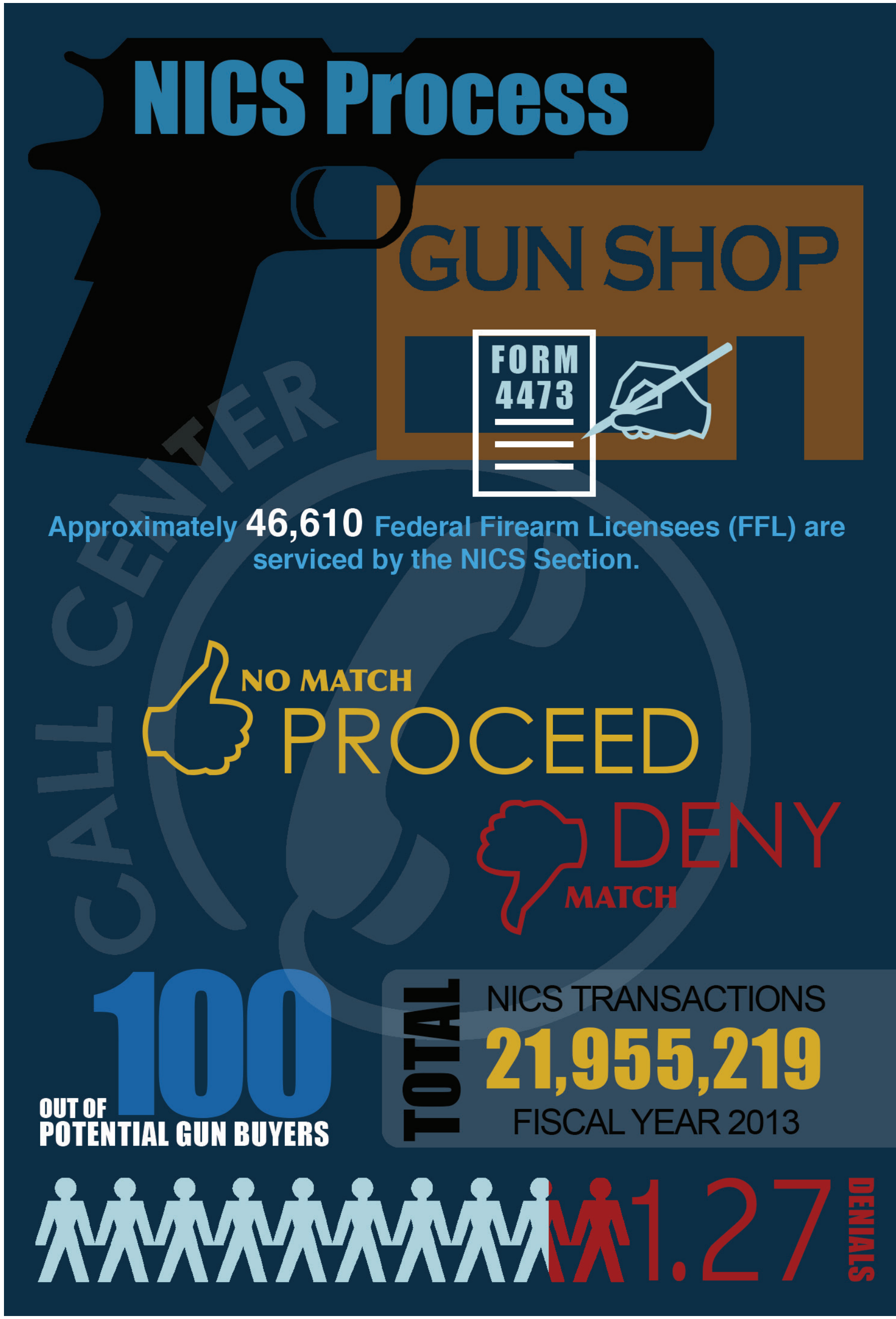
ABOUT The **National Instant Criminal Background Check System** Section conducts name-based background checks and performs research, analysis, and evaluation of information to determine an individual's eligibility for firearms and explosives possession as directed by applicable state and federal laws. The creation of the NICS was mandated by the Brady Handgun Violence Prevention Act of 1993.

The use of the NICS E-Check also expanded in 2013, with 28 percent of all transactions conducted electronically.

Currently, the NICS is being refreshed to automate more functions, upgrade hardware, operate more efficiently, and streamline processes. The enhancements, which are part of the New NICS Project and will be implemented in July 2014, will provide a quicker turnaround time for background checks, ultimately improving public safety and customer service.

NICS IN ACTION On May 31, a NICS examiner processed a transaction for an FFL, a pawn shop in Bryant, Arkansas, for a long gun purchase. Based on descriptors, the NICS examiner identified a warrant listed in the NCIC matching the attempted purchaser. The NICS examiner contacted the Saline County Sheriff's Office (SCSO) in Benton, Arkansas, to validate the status of the warrant. The warrant was confirmed as an active felony warrant for obtaining a controlled substance by fraud. The NICS examiner contacted the FFL, provided the deny status, obtained the address and all applicable information on the subject attempting the purchase, and provided the information to the SCSO. A deputy went to the pawn shop to apprehend the suspect. The deputy followed the individual to his residence. The individual was then taken into custody with “some difficulty” according to the SCSO. The NICS staff later learned the subject was a nurse whose license was revoked for stealing medication from a patient. The SCSO had been attempting to locate and apprehend the individual for some time.

On June 18, a NICS examiner processed a transaction for an FFL, a gun shop in Globe, Arizona, for a handgun purchase. The NICS examiner immediately identified a match in the NCIC that contained an active protection order issued by the Durham County (North Carolina) Sheriff’s Office (DCSO). The NICS examiner contacted the sheriff’s office to confirm the protection order details. The NICS examiner verified that all federal criteria were met, that the order contained a firearm restriction imposed by the judge as well as an order to surrender all firearms and ammunition, and that the subject’s concealed weapons permit was suspended during the duration of the order. Based on the information received, the NICS examiner provided the FFL with a deny status. Because the attempted purchase violated the protection order, the NICS examiner obtained all applicable information about the attempted purchase and purchaser and gave the information to the DCSO.



NATIONAL DATA EXCHANGE

More than 200 million criminal justice records to help investigators make connections

The **National Data Exchange (N-DEx)** continued to expand and enhance its services in 2013, allowing domestic criminal justice agencies to share information and collaborate to investigate and solve crimes.

With free and immediate access to over 200 million records from more than 4,200 agencies, N-DEx users can search on information spanning the entire criminal justice life cycle, such as incident and case reports; pre-trial, probation, and parole reports; booking and incarceration reports; traffic citations; and photos, such as mug shots and images of scars/marks/tattoos.

In addition to records from local, state, and tribal agencies, N-DEx provides access to records from the FBI and other federal agencies, including the Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Marshals Service, U.S. Air Force Office of Special Investigations, and the Department of Homeland Security.

Ownership of data submitted to N-DEx always remains with the submitting agency. Flexible sharing controls allow agencies to determine what they will share, with whom, and at what level of openness. These rules may be applied as broadly as all information from one agency or as specifically as an individual record. A requirement to contact the data-owning agency prior to using any information found within N-DEx not only ensures the completeness, timeliness, and accuracy of data, but also fosters dialogue between criminal justice professionals.

THE YEAR IN REVIEW During 2013, N-DEx continued to grow in both the number of records shared and the number of records searched. Compared to the last fiscal year, N-DEx has experienced:

- More than a 40 percent increase in searchable records available.
- A nearly 10 percent increase in contributing agencies.
- A nearly 200 percent increase in total authorized system users.
- More than a 50 percent increase in total system searches.

Since August 2013, N-DEx system users can access N-DEx records as part of the background check on prospective or current employees. This new use of N-DEx will allow employers who hire personnel for positions of trust to review a wider array of criminal justice information to determine a potential candidate's suitability for the job. For instance, along with the standard criminal history queries, searches can be supplemented with important information such as field interviews, incident reports, traffic citations, and data from local jails.

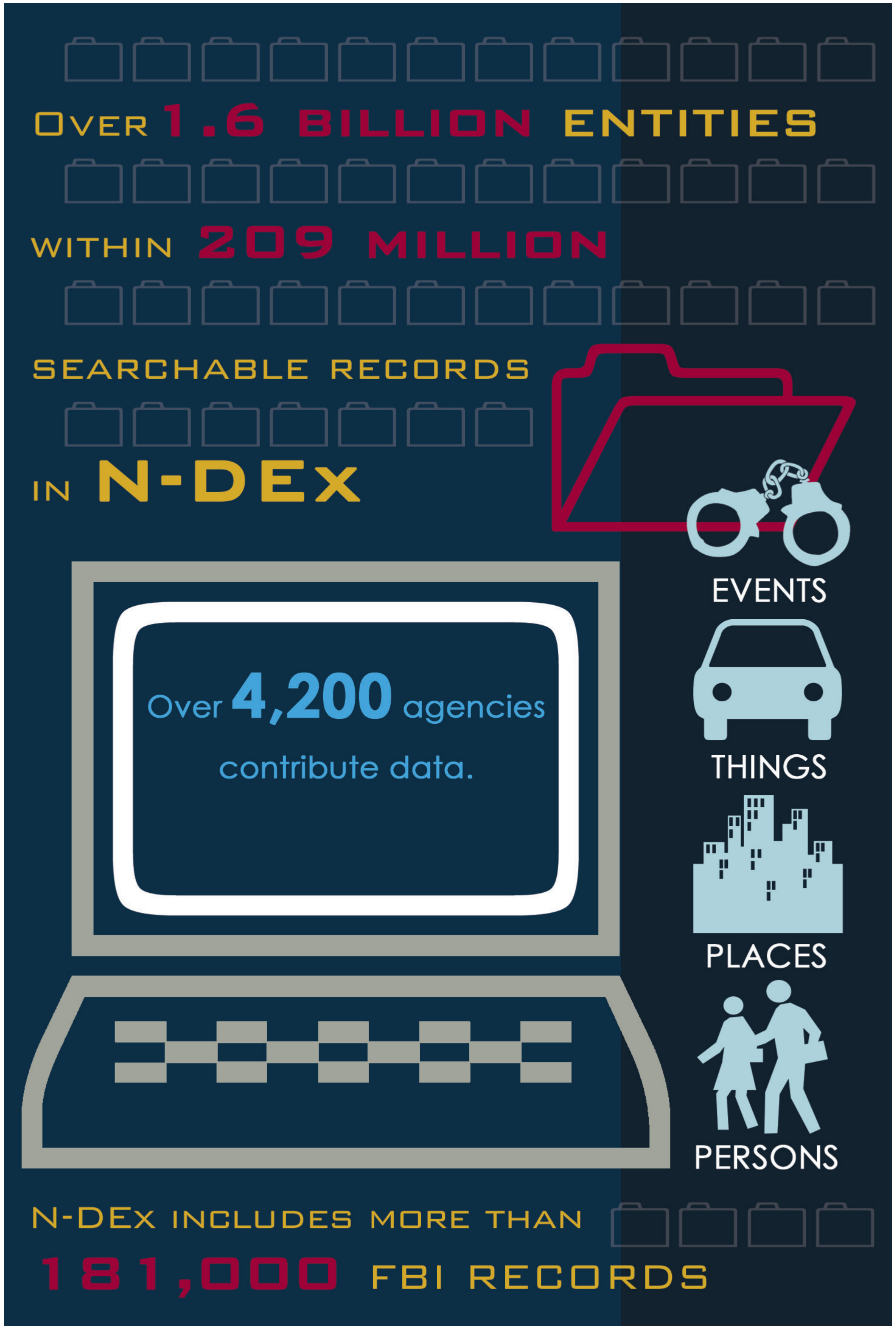
A number of significant enhancements were made to N-DEx this year, including more robust search filters; a batch query function to upload files containing thousands of people, vehicles, telephone numbers, or key words to be searched at one time; Geo Visualization improvements; the ability to view maps within detailed records; and the inclusion of both a data contributors list and an N-DEx news ticker.

ABOUT The **National Data Exchange** is the first and only national investigative information sharing system. Local, state, tribal, and federal criminal justice personnel can share, search, link, analyze, and collaborate on criminal justice information to a degree never before possible. By using N-DEx to gather additional information about a suspect or situation, users can detect relationships between people, crime characteristics, property, and locations; link information across jurisdictions; and identify victims and aggregate losses by "connecting the dots" between seemingly unrelated data.

N-DEx continues its commitment to increase participation by the corrections, probation, and parole communities. Data are currently being submitted by Department of Correction (DOC) agencies in Indiana, Kansas, Mississippi, and Nebraska. In the near future, DOC agencies from Iowa, Minnesota, Ohio, Oklahoma, Pennsylvania, Virginia, West Virginia, and Wisconsin will submit their data using N-DEx. In addition, N-DEx will include submissions from the Interstate Compact Offender Tracking System, or ICOTS, which is a Web-based system that facilitates the transfer of supervision of probationers and parolees from one state to another.

N-DEX IN ACTION A Milwaukee Police Department crime analyst entered a list, into the N-DEx, of vehicle identification numbers (VIN) belonging to vehicles that had been reported stolen. The N-DEx returned a record for a traffic violation from the Yankton Police Department in South Dakota containing information about one of the stolen vehicles. The victim/owner of the vehicle did not seek prosecution in the case and the stolen vehicle information had not been placed into the National Crime Information Center (NCIC) database. Because the Yankton Police Department's officer listed the vehicle's identification number in his report and the information was submitted to N-DEx, the analyst was able to locate the vehicle. The victim was notified and the Milwaukee Police Department's motor vehicle theft case was cleared.

An analyst with the New York Police Department's Real Time Crime Center searched N-DEx in an attempt to learn more information about a subject. N-DEx returned police reports from Virginia noting the subject had been combative with officers who encountered him at a hospital. The Virginia report provided helpful situational awareness for New York Police Department personnel before they met with the subject.



Over 1.6 billion entities within 209 million searchable records in N-DEx

Over 4,200 agencies contribute data.

N-DEx includes more than 181,000 FBI records

CJIS INTELLIGENCE PROGRAM

Gathering, analyzing, and developing raw data to produce identity intelligence

In 2013, the **CJIS Intelligence Program** continued to develop its products and services, generating identity intelligence to support FBI investigations and other criminal justice partners. While the FBI has long been involved in identity intelligence, technological advances continue to bring change to this emerging field.

For the CJIS Intelligence Program, identity intelligence is developed by gathering data about a person from separate resources and bringing the records together to create a complete information snapshot of an individual. The resulting report can further an investigation, rule out suspects, connect individuals as possible associates, prevent a crime, or enhance investigations in many other ways. This year, the Intelligence Program shared 799 products, such as intelligence notes, firearm denials, and refugee notifications. Vital information was provided in support of various local, state, and federal law enforcement cases, including the Boston Marathon Bombing.

To accomplish this work, the CJIS Intelligence Program leverages the resources of FBI and partner systems, including the biometric, biographical, and criminal history information included in these databases:

- Next Generation Identification/Integrated Automated Fingerprint Identification System (NGI/IAFIS)
- National Instant Criminal Background Check System (NICS)
- Interstate Identification Index (III)
- National Crime Information Center (NCIC)
- The Department of Defense's Automated Biometric Identification System (DoD's ABIS)
- The Department of Homeland Security's (DHS's) Automated Biometric Identification System.

Several groups make up the Intelligence Program, with staff working both within the Division and with local, state, tribal, federal, and international partners to gather and share information. The Intelligence Program includes:

- The **CJIS Division Intelligence Group (CDIG)**, which provides tactical intelligence to FBI Field Intelligence Groups and the law enforcement, intelligence and homeland security communities, by analyzing and sharing information contained in the CJIS Division's databases.
- The **Interoperability Initiatives Unit (IIU)**, which promotes collaborative efforts with domestic and international partners to implement and expand efforts to share information among biometric-based systems by helping those systems work together.
- The **Global Initiatives Unit (GIU)**, which provides rapid identification services around the world and facilitates the global exchange of biometric and criminal history data.
- The **Special Identities Unit (SIU)**, which tracks, monitors, and validates identities; performs specialized search and notifications concerning identities; and compiles reports from raw data in support of the FBI and other law enforcement and intelligence agencies.
- The **Crime Analysis, Research and Development Unit (CARD)**, which conducts strategic research and analysis of data contained in FBI systems (e.g., NCIC

ABOUT The **CJIS Intelligence Program** works to increase the sharing of information among domestic and international partners and then combines these resources with information in the FBI's own systems to promote public safety and prevent terrorism. By gathering and analyzing biometric, biographic, and criminal history records from various sources, staff of the CJIS Intelligence Program can piece together records to reveal a comprehensive report related to a specific case or person of interest.

and the Uniform Crime Reporting Program), as well as from external sources (e.g., the U.S. Census Bureau).

CJIS INTELLIGENCE PROGRAM IN ACTION One goal of the CJIS Intelligence Program is facilitating interoperability among U.S. government and partner systems. So, in 2012, when the DoD entered the name of a foreign national for hire into its ABIS for base access in Afghanistan, that information became available through interoperability to the FBI and its partners as well. The subject was later arrested by the FBI's Counterterrorism Division (CTD) Fly Team in Uganda in 2013 when he attempted to pick up a drug shipment.

The CTD Fly Team used the GIU's Quick Capture Platform (QCP) to record the subject's fingerprints in the field. Through an interoperability search of the FBI, DoD, and DHS biometric databases, a match from the subject's DoD ABIS file was returned to the QCP. The subject is currently detained.

Another goal of the program is to share relevant information from the FBI's databases. CDIG regularly analyzes records from CJIS systems looking for "red flags," or identity intelligence that could possibly impact public safety. During 2013, an FBI field office notified CDIG that information gleaned from a NICS report led to the arrest of a man who posed a threat to his wife. CDIG staff reported that the subject, who had an active restraining order, had attempted to purchase a firearm six times in a documented time period. The restraining order explicitly stated he was not to attempt to purchase a firearm. The man, whose wife had the restraining order against him, was going through a divorce and was reportedly experiencing a mental and/or physical issue that compounded the situation. CDIG passed the information about the attempts to purchase a firearm to the area's FBI field office, and the field office shared the report with the local police. Officers located the man at his friend's home and were able to apprehend and arrest him, possibly preventing the domestic incident his wife feared when she initiated the restraining order.

LAW ENFORCEMENT ENTERPRISE PORTAL

Opening the door to resources that help investigators make connections

Conveying, sharing, and accessing information and the meaningful exchange of facts, leads, news, and intelligence among criminal justice agencies is one of the top priorities of modern law enforcement. No tool is as effective as knowledge. Often, no asset is as valuable as time. The **Law Enforcement Enterprise Portal (LEEP)** was created to support those two facts and strengthen collaboration among the law enforcement, criminal justice, and public safety communities.

Customers no longer go to a bakery, a butcher, a dairy, and a farmers' market to shop each day because a one-stop supermarket is much more efficient; and the one-stop access of LEEP operates under the same principle. The LEEP is a secure electronic gateway that brings together information from and gives access to diverse resources in a reliable and effective way. The LEEP's concept is to present the user with a single sign-on to a portal that affords admission to a host of information systems. The LEEP offers criminal justice agencies the opportunity to provide access to their entire network of users and currently many participating agencies access an array of information directly through LEEP. When an entity (like the Chicago Police Department, Los Angeles County agencies, or the federal Drug Enforcement Administration) becomes a partner, their personnel can log on to the LEEP from an icon on their desktops and access a wealth of services with a single sign-on. Once through the portal, investigators can connect with many different resources that are part of the ever-growing suite of services. (Users can access authorized services under the "My Services" tab. Frequently used services can be added to the "My Favorites" tab for quick access.)

Resources on the LEEP are as wide ranging and diverse as cyber crime complaint data from the Internet Crime Complaint Center (IC3); the Regional Information Sharing Systems Network (RISSNET); the federal Joint Automated Booking System; the National Data Exchange (N-DEx), the only national investigative information-sharing system; and the Law Enforcement Online (LEO) secure communications intranet. In early 2014, the crime data collecting and publishing Uniform Crime Reporting Program service is scheduled to be available to authorized LEEP users. (Read more about UCR and N-DEx in this *CJIS Annual Report*.)

ABOUT The **Law Enforcement Enterprise Portal (LEEP)** allows criminal justice professionals access to a variety of vital resources from a single sign-on with a trusted agency's network—right from an icon on their computer desktop. Providing an effective single source for a host of trusted information-sharing and interactive sites, the LEEP can help streamline and facilitate a once time-consuming process of information gathering.

THE YEAR IN REVIEW The past year has brought a number of changes to the LEEP—its name change (from Law Enforcement Online Enterprise Portal) and its new look are just the beginning. In 2013, LEEP added the Federated Address Book (FAB), a searchable address book that provides name, phone number, email address, and organization of a user. LEEP users can also "opt out" of displaying their personal information in the FAB.

Another capability that rolled out was the automatic electronic "Rules of Behavior" form. This allows LEEP members to electronically accept the terms of use outlined on the form after entering their User ID during the authentication process. LEEP members will be required to agree to this form once a year via electronic signature.

A third enhancement enabled LEEP to "go mobile." Users are now able to view log-ins, enrollment pages, and external authentication; access portal services and navigation menus; and view help desk contact information—all from their mobile devices.

LEO members have had access to the LEEP and its connections since the portal was opened, but by the end of 2013, users from other LEEP partnered agencies will also be able to access LEO through their desktop sign-ons. This will provide LEEP users with all the functionality that LEO has provided for nearly 2 decades as the premier secure criminal justice communication network. With LEO access, users will be able to plug into:

- Special Interest Groups (SIGs), over 2,000 "communities" which afford participation in specific interests. For example, some agencies have used their SIGs to share data on schools (floor plans, photos, etc.) in their jurisdictions for reference in the event of a crisis.
- Virtual Offices, which allow agencies to securely store and retrieve documents, forms, manuals, etc. from remote locations. This is of special convenience to personnel (such as special and task force agents) that need to share information on location, privately and securely.
- eLearning and training opportunities.
- Virtual Command Centers (VCCs), which allow secure monitoring and participation in the moving parts of an event (political—such as the President's Inauguration; sporting—such as the National Basketball Association finals; and tactical—such as the Boston Marathon bombing) from different locations. The LEO VCC is currently being explored for use as a crisis management/situational awareness tool to coordinate law enforcement responses to "active shooter" emergencies at schools, churches, or other public areas. Over 3,800 VCCs have been opened in LEO to date.

LEEP IN ACTION With 180,000 potential users, the LEEP has made the "leap" from a great idea to the method of choice for accessing the widest array of data and technology available in policing and investigation. Beginning in 2014, criminal justice professionals can apply for authorization to LEEP services electronically. Officers and agents can then sign on at their desktops and call up a range of resources and opportunities—they can search N-DEx for case or arrest reports, photos, or booking data from all over the nation; report their own crime data; or access SIGs or set up a VCC on LEO. Investigators' time is one of their most important assets—LEEP maximizes that asset.

UNIFORM CRIME REPORTING PROGRAM

Using modern technology to provide a national perspective of crime

Since its beginning in 1930, the core objective of the **Uniform Crime Reporting (UCR) Program**—to provide dependable and valuable crime statistics for use by law enforcement, researchers, criminologists, sociologists, media, municipal planners, and the general public—has not changed. However, in 2013, the Program underwent a metamorphosis with an on-going technical revitalization, a change to the definition of rape, the addition of several offenses, an expansion of the racial data collected, and the release of a new publication.

THE YEAR IN REVIEW In fiscal year (FY) 2013, the FBI continued to revitalize the UCR's crime data collection and reporting systems through the UCR Redevelopment Project (UCRRP). The new UCR crime data reporting system is expected to be in place on January 5, 2014, and will completely automate reporting crime data. The new UCR system will include an online Web tool for entering data. The UCRRP's goal is to improve UCR efficiency, usability, and maintainability while increasing the value to users of UCR products. One new value to users, which will be available in 2014, is an enhanced external data query tool, the Crime Data Explorer (CDE), which will give the public the ability to view and download published UCR data from the Internet. The CDE will also allow data users to generate customized reports from a menu of variables.

While revitalization will not be fully implemented until 2014, the UCR Program is currently encouraging the electronic submission of data and moving away from hard copy paper submissions. During FY 2013, the Program reduced hard copy submissions by nearly 62 percent. As the new UCR moves forward, it will become, in effect, paperless.

In addition to its work with the technical collection of UCR data, the national UCR Program was busy behind the scenes to help make the data more reflective of today's crime issues. A number of those changes went into effect beginning January 1, 2013.

The definition of rape and other sex offenses captured in the UCR Program changed in 2013. Effective January 1, the Program removed the words "forcible" and "against the person's will" from the definition of rape and other sex offenses, and added the phrase "without the consent of the victim." This change impacted the data collected via the traditional Summary Reporting System (SRS), where previously an offense could only be counted as rape if the victim was female. The new definition recognizes both genders as victims. The shift also affects the definitions of rape and sexual offenses in the National Incident-Based Reporting System (NIBRS).

The UCR Program also began collecting information for the crimes of Human Trafficking to comply with the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008. Both the SRS and the NIBRS began capturing offense and arrest data for human trafficking involving both Commercial Sex Acts and Involuntary Servitude.

Another change that took place in 2013 was the expansion of race categories in the national UCR Program as well as some clarifying shifts in language. The categories changed from four:

- White,
- Black,
- American Indian or Alaskan Native, and
- Asian or Pacific Islander,

to now include five categories:

- White,
- Black or African American,

ABOUT The **Uniform Crime Reporting Program** gathers crime statistics from nearly 18,000 law enforcement agencies each year. Data are published in a series of high-profile, annual reports (*Crime in the United States*, a comprehensive collection of offense, arrest, and police employment data; *Law Enforcement Officers Killed and Assaulted*, a statistical perspective of the felonious deaths and assaults of officers; and *Hate Crime Statistics*, a report of bias-motivated crimes) as well as periodic, topical releases.

- American Indian or Alaska Native,
- Asian, and
- Native Hawaiian or Pacific Islander.

In addition, two ethnicity categories were redefined: Hispanic or Latino and Not Hispanic or Latino.

The UCR Program's hate crime statistics data collection also underwent changes in 2013. Two new bias motivations—gender and gender identity—were added, and the UCR Program received approval to expand religious biases to include all self-identified religious affiliations listed by the Pew Research Center (2008) and the U.S. Census Bureau (2012). In addition, the hate crime data collection will add an Anti-Arab bias. Data collection for these added biases will begin in 2015.

Another facet of the UCR Program is the Law Enforcement Officers Killed and Assaulted (LEOKA) Program. In FY 2013, program staff provided 102 officer-safety training classes. A total of 8,810 national and international law enforcement officers attended the training. With growing budgetary restrictions, the program continued its education of officers with the release of three topic papers on Law Enforcement Online (LEO) through the Law Enforcement Enterprise Portal (LEEP). (Read more about LEO and LEEP in this annual report.)

UCR IN ACTION In August 2013, the UCR Program released its first compilation featuring NIBRS data. *NIBRS 2011*, represents crime data reported by 5,880 law enforcement agencies around the nation, or approximately 32 percent of all UCR agencies. The data include information on incidents, offenses, victims, and known offenders for 46 specific crimes in 22 major offense categories. The publication, available on the FBI's website, provides a window into the richness of NIBRS data. The NIBRS data presented shows a more detailed picture of crime than has been previously available and helps make connections among many facets of crime within a particular incident, providing details on victims, offenders, location, weapons and a host of other variables.

Calendar Year 1939
1,214 Cities---Total Population 39,147,097
ROBBERY
FEDERAL BUREAU OF INVESTIGATION
UCR
UNIFORM CRIME REPORTING
VINTAGE to VIRTUAL
....MURDER.....RAPE.....BURGLARY.....LARCENY.....
14,827
84,376
2,103,787
6,150,598

BIOMETRIC IDENTIFICATION SERVICES

Meeting the ever-increasing demand for identification information

Biometric identity information—fingerprints, palmprints, face images and more—is critical to investigators as they identify suspects and solve crimes. The CJIS Division provides this key support through **Biometric Identification Services**. These include:

- 24/7 fingerprint identification and criminal history record information services to criminal justice agencies and other authorized entities.
- Research, analytical, and project management support related to the automated fingerprint identification system and future services in development by Next Generation Identification (NGI).
- Support for comparisons of latent prints (prints left behind at a crime scene).
- Support to FBI field offices by comparing face images of subjects who are the focus of active field investigations against those housed in selected databases both internal and external to the FBI.
- Training for current and future biometric initiatives and testimonies to law enforcement and criminal justice communities.

THE YEAR IN REVIEW In fiscal year 2013, the Biometric Support Unit's Rap Back Team collaborated with NGI staff to provide oversight with the current Rap Back pilot as well as in the future with the full operating capability of the Rap Back service. The service will benefit non-criminal justice applicants, such as employees, volunteers, licensees, and criminal justice agencies with individuals under criminal investigation or under supervision. The current system for criminal history background checks provides for a one-time view of an individual's criminal history status. The Rap Back will provide an on-going status notification from the FBI of any criminal activity that occurs by those individuals after that initial criminal history check. In June 2013, the Department of Homeland Security's (DHS's) Immigration and Customs Enforcement (ICE) became the first Rap Back pilot agency. Collaboration between the Rap Back Team and NGI Development Team will continue to ensure the successful implementation of the National Rap Back service.

The Latent and Forensic Support Unit (LFSU) specialists continued to support the FBI Laboratory Division (LD) through the Major Case Conversion Project (MCCP). MCCP is a high-priority, high-profile project also referred to as the Digital Image Conversion to the Electronic Biometric Transmission Specification (EBTS). LFSU specialists convert hard copy Major Case Prints (MCPs) into EBTS format in preparation for intake into the NGI's National Palm Print System (NPPS). The MCPs were collected from known and suspected terrorists at detainee camps in Guantanamo Bay, Afghanistan, and Iraq. Guantanamo Bay and Iraq MCPs and more than 10,000 MCPs collected from Afghanistan have been prepared for inclusion in the NPPS.

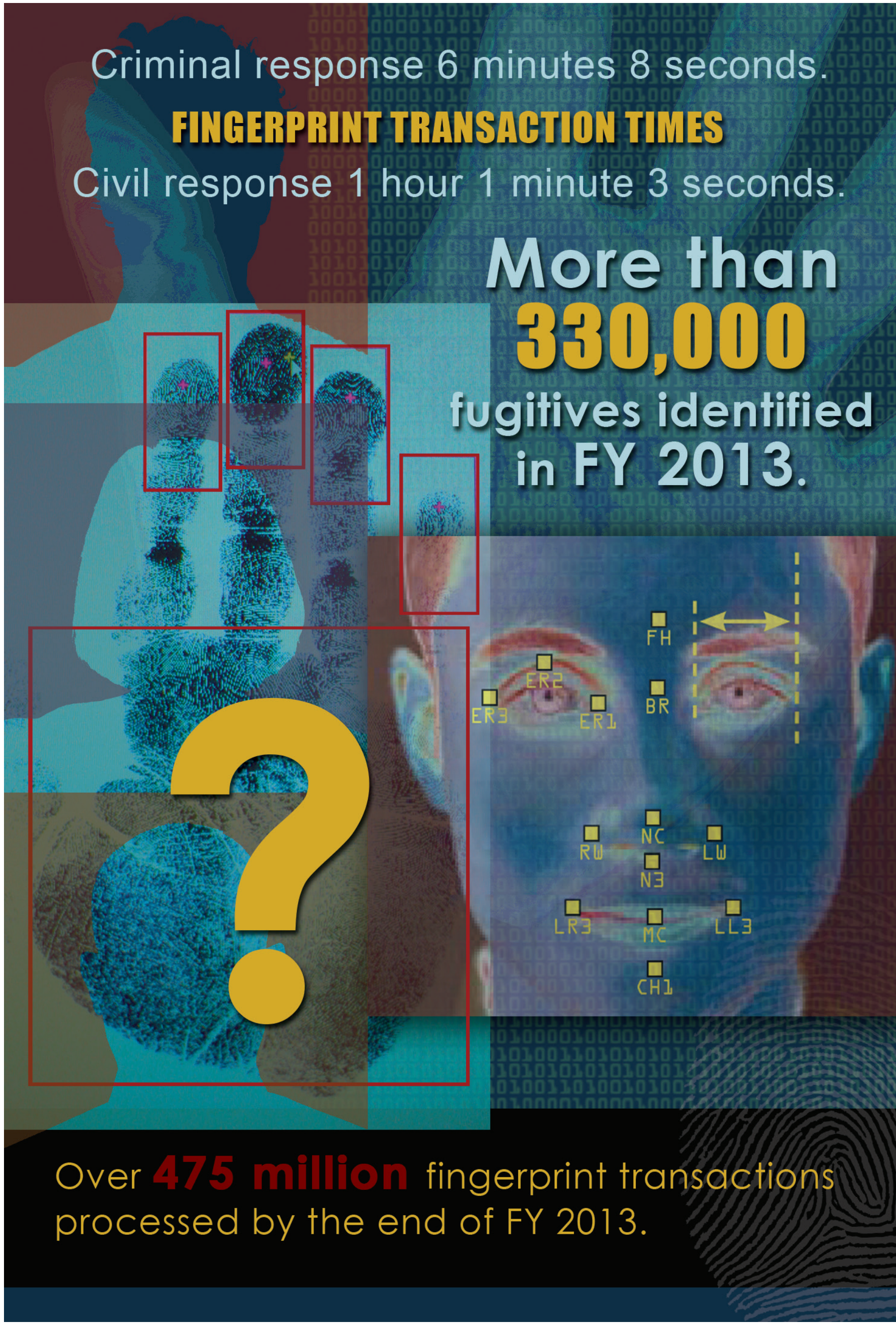
During the year, the LFSU provided Unsolved Latent File case information to national security partners such as the Department of Defense, the DHS, the LD, and the Terrorist Explosive Device Analytical Center to assist in approximately 16 time-sensitive and/or high-profile terrorist investigations. These investigations included shootings at the Empire State Building, a Sikh Temple in Wisconsin, and the Family Research Council in Washington, D.C., as well as the bombing of a Social Security Administration building in Arizona.

The Facial Analysis, Comparison, and Evaluation (FACE) Services Unit currently has face recognition search capabilities to approximately 288 million images.

ABOUT The CJIS Division provides 24/7 **biometric identification services** that support the law enforcement, criminal justice, civil, investigative, intelligence, and national security communities.

BIOMETRIC IDENTIFICATION SERVICES IN ACTION From June 4 through June 6, 2013, the FACE Services Unit received multiple Image Search Requests, via e-mail, from a special agent with the Memphis Field Office and a task force officer from the Tennessee Bureau of Investigation regarding a case of computer intrusion crime. The investigation was a collaborative effort between Austria's Federal Criminal Police Office, United States Secret Service, and Computer Crime and Intellectual Property Section. The investigation involved cyber-based, high-technology crimes in which the subjects were believed to be money "mules" who traveled to the United States as a part of a Romanian organized crime crew involved in Internet and credit card fraud. The request included 16 unknown probe images and one known probe image. Searches conducted in the Consular Consolidated Database returned seven likely candidates. Likely candidate responses containing the probe image, the likely candidate images, and the biographical data of each were returned to the special agent.

On September 5, 2013, the special agent informed a management and program analyst with the FACE Services Unit that a positive identification provided by the FACE Services staff led to the arrest of one of the subjects. According to Customs and Border Patrol records, the subject arrived in the United States on May 26, 2013. The special agent and task force officer were aware the subject was planning to leave the country from the airport in Miami. In early July, the special agent obtained an authorized arrest warrant for conspiracy to commit wire fraud. On July 15, 2013, the special agent and task force officer located and arrested the man at the Miami International Airport as he was getting ready to board a plane to depart the country. Officials took him to the FBI Miami Field Office for fingerprinting and DNA collection before he was transported to a Federal Detention Center in Miami.



Criminal response 6 minutes 8 seconds.

FINGERPRINT TRANSACTION TIMES

Civil response 1 hour 1 minute 3 seconds.

More than **330,000** fugitives identified in FY 2013.

Over **475 million** fingerprint transactions processed by the end of FY 2013.

NEXT GENERATION IDENTIFICATION

Modernizing biometric identification services

Today, the term biometrics is not limited to fingerprints. It also includes palmprints, irises, and face recognition. In an effort to harness new technologies, as well as to improve the application of tenprint and latent print searches, the CJIS Division is incrementally developing a new system to offer modernized biometric identification services.

Since the first incremental build was deployed in 2011, the **Next Generation Identification (NGI)** system has introduced the rapid mobile fingerprint identification search of the Repository for Individuals of Special Concern (RISC), the Interstate Photo System Face Recognition Pilot (IPSFRP), and the Rap Back Pilot. NGI also added enhanced processing speed, automation, and additional tenprint and latent searching capabilities.

THE YEAR IN REVIEW In fiscal year (FY) 2013, the RISC added six states and one federal agency and, on August 14, processed its one-millionth transaction. NGI anticipates adding seven more states and another federal agency in early 2014, pushing the total to 24 agencies participating in RISC.

Currently, four states are actively using the IPSFRP system, which contains more than 16 million searchable mug shot photos. The face recognition pilot allows authorized law enforcement agencies to submit investigative probe images for an automated face recognition search with no human intervention. Once the probe image is processed, the IPSFRP returns a candidate list of photos to be evaluated for investigative purposes only.

The Rap Back service, planned for implementation in the summer of 2014, will eliminate the need for repeated background checks on a person from the same applicant agency. The new service allows authorized agencies to subscribe to notifications from NGI when select activities are reported. These results may affect whether that person should remain in a position of trust. Rap Back will also provide the ability for agencies to receive immediate notifications involving reported activities of individuals under criminal justice supervision or investigation.

ABOUT In February 2011, **Next Generation Identification (NGI)** initiated the first phase of replacing the Integrated Automated Fingerprint Identification System (IAFIS), which will be complete in 2014.

Also in FY 2013, the Department of Homeland Security's Immigration and Customs Enforcement took advantage of a short-term Rap Back Pilot. Though limited in its capabilities, the pilot is providing insight into areas such as identification rates and resource requirements that will prove useful when the pilot concludes and full implementation begins.

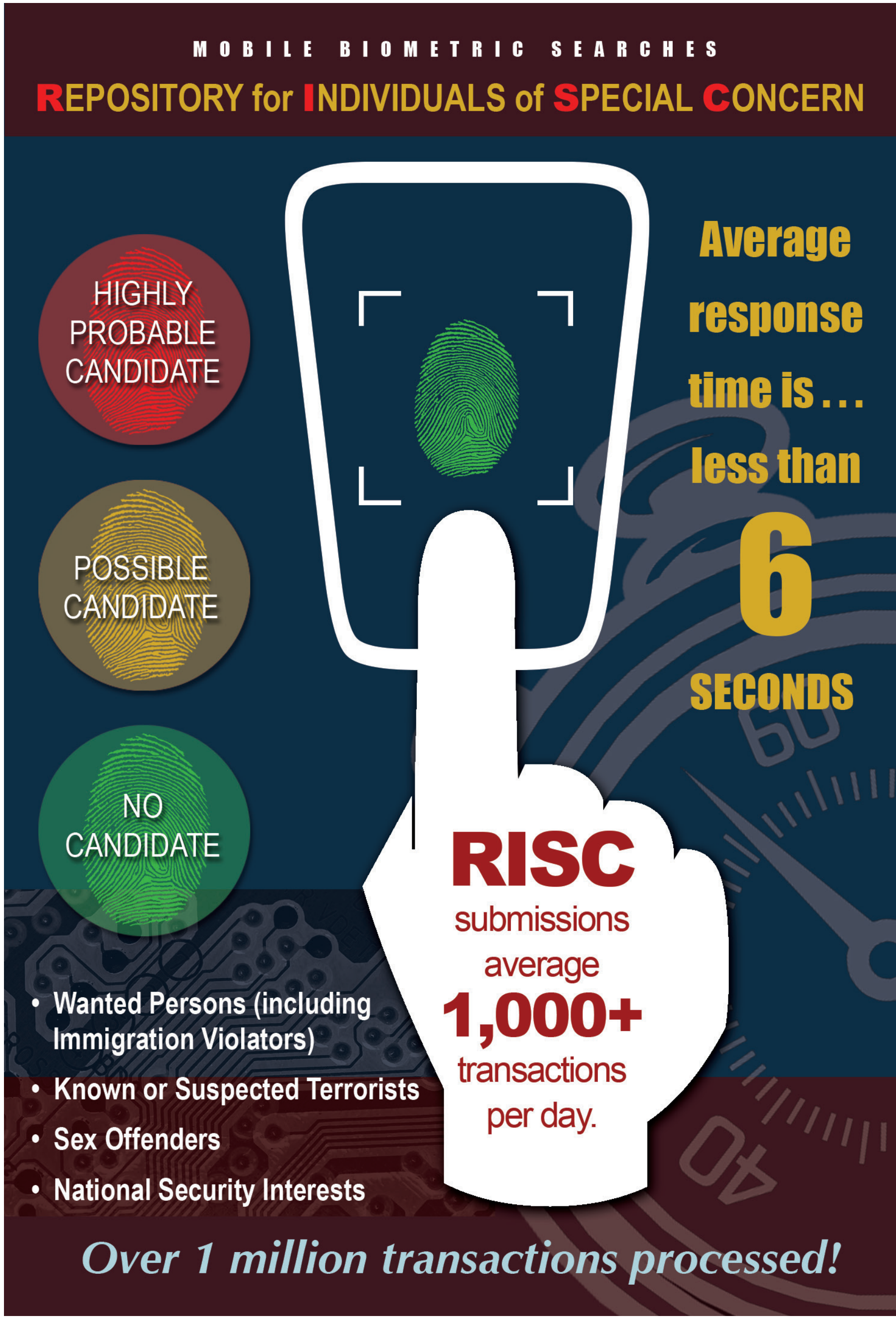
On May 5, the NGI system deployed the largest augmentation to the system. This third increment includes establishment of the new National Palm Print System (NPPS), which contains palmprints that are now searchable on a nationwide basis. The NPPS and improvements in latent fingerprint search performance are providing powerful new and enhanced crime-solving capabilities for more than 18,000 local, state, tribal, and federal law enforcement agencies across the country.

In addition, this build provided immediate benefit to latent functionality through increased accuracy, providing users with the ability to search all event prints and expanding the criminal and civil searches against the Unsolved Latent File (ULF). These enhanced capabilities are already generating new investigative leads in unsolved and/or cold cases.

The transition from IAFIS to NGI will continue into 2014, when NGI will complete its fourth incremental enhancement, which will be the largest of the six scheduled increments. In this phase, the Rap Back and Face Recognition capabilities will convert from pilot services to full operational capacity and all remaining IAFIS functions will migrate to the NGI architecture. In addition, NGI is in the process of implementing an Iris Pilot System.

NGI IN ACTION In June 1985, the Dallas Police Department began investigating a brutal homicide that, according to authorities, elicited deep emotion from investigators. After years of searching for new investigative leads and suspects, the case went cold. Soon after the third increment of NGI was fully implemented, the Florida Department of Law Enforcement (FDLE) transmitted a civil applicant fingerprint submission to the FBI for a background check. Although there was no criminal record on file, the biometrics were searched against the ULF because FDLE elected to participate in expanded cascade services. As a result, a person of interest was identified in this unsolved homicide investigation. Based upon this investigative lead, Texas and Florida law enforcement personnel are collaborating to further investigate the person of interest and determine if they now have a viable suspect in this previously cold case.

On June 12, 2013, a Florida Highway Patrol Officer encountered a subject that did not yield to a Brevard County deputy who had his sirens on. After the vehicle was stopped, the officer questioned the driver, but he suspected the subject provided him with a false name. The officer captured the subject's fingerprints using a Mobile ID device. The FBI RISC returned a hit, but the local and state AFIS did not. The warrant was for Failure to Appear/ Obscene Material from the U.S. Marshals Service (West Virginia). Because of the RISC response, the subject was arrested. The subject was discovered to have been a high school counselor that pleaded guilty to possessing child pornography, but he did not show up in court for sentencing. His story had aired on *America's Most Wanted* in September of 2012.



MOBILE BIOMETRIC SEARCHES

REPOSITORY for INDIVIDUALS of SPECIAL CONCERN

HIGHLY PROBABLE CANDIDATE

POSSIBLE CANDIDATE

NO CANDIDATE

Average response time is . . . less than 6 SECONDS

RISC submissions average 1,000+ transactions per day.

- Wanted Persons (including Immigration Violators)
- Known or Suspected Terrorists
- Sex Offenders
- National Security Interests

Over 1 million transactions processed!

FBI BIOMETRIC CENTER OF EXCELLENCE

Moving R-DNA closer to the field and advancing other biometrics

THE YEAR IN REVIEW Throughout fiscal year (FY) 2013, the **Biometric Center of Excellence (BCOE)** advanced a number of biometric technologies toward operational use and improved the existing capabilities of others. Among the BCOE's accomplishments were the transition of the Rapid Deoxyribonucleic Acid (R-DNA) project to the FBI's Laboratory Division (LD), the delivery of the tattoo test dataset, and the publication of documents about friction ridge impressions and latent fingerprint determinations. Collaborative efforts included the BCOE's liaison with the Field Office CJIS Subject Matter Experts (FO CJIS SMEs) in the FBI's continued movement with the defensive biometrics initiative, and the creation of the Scientific Working Group (SWG) for voice standards, known as SWG–Speaker.

In January 2013, following the development of three R-DNA machines last fall, the BCOE transitioned the management of the R-DNA initiative to the LD for further testing and evaluation. Ultimately, the R-DNA machines will be made available to law enforcement and national security personnel as well as private and government laboratories. Once operational, the time it takes to process DNA samples will be reduced from several days in a lab to less than 2 hours on-site with the potential of searching the National DNA Index System.

The BCOE also moved closer to image-based matching solutions for tattoos and symbols, which are regularly used to support identifications and investigations. Working with the MITRE Corporation, the BCOE developed a tattoo dataset consisting of approximately 150,000 unlabeled tattoo images and 8,000 labeled tattoo images. The images were labeled according to the American National Standards Institute (ANSI)/National Institute of Standards and Technology (NIST) classification system and provide a set of "knowns" in the gallery. The BCOE will use the dataset to test and evaluate image-based matching technology.

To keep its partners informed of developments with applied research projects, the BCOE, in coordination with the LD, released two significant documents: "Assessing the Clarity of Friction Ridge Impressions" and "Understanding the Sufficiency of Information for Latent Fingerprint Value Determinations." The articles, funded by the BCOE as part of the Quality/Quantity Project, were published in *Forensic Science International*. In addition, the "White Box Study," which focuses on how latent print examiners make decisions, was completed, and the results will be released in five publications.

As follow-up to the outreach effort of the FBI FO CJIS SME Training in 2012, the BCOE designated specific contacts for the SMEs to help ensure that they are aware of the CJIS biometric services available to them. During FY 2013, the BCOE facilitated five Webinars with five FOs to identify biometric gaps, collect new ideas, and provide education regarding future biometric initiatives.

Throughout FY 2013, the BCOE, internal governmental entities, and external partners continued exploring defensive biometrics, which involve the methods and techniques used by criminals to avoid or confound biometric collection or identification. This information will help field personnel understand procedures used to avoid biometric detection. It will also be used to enhance current biometric systems.

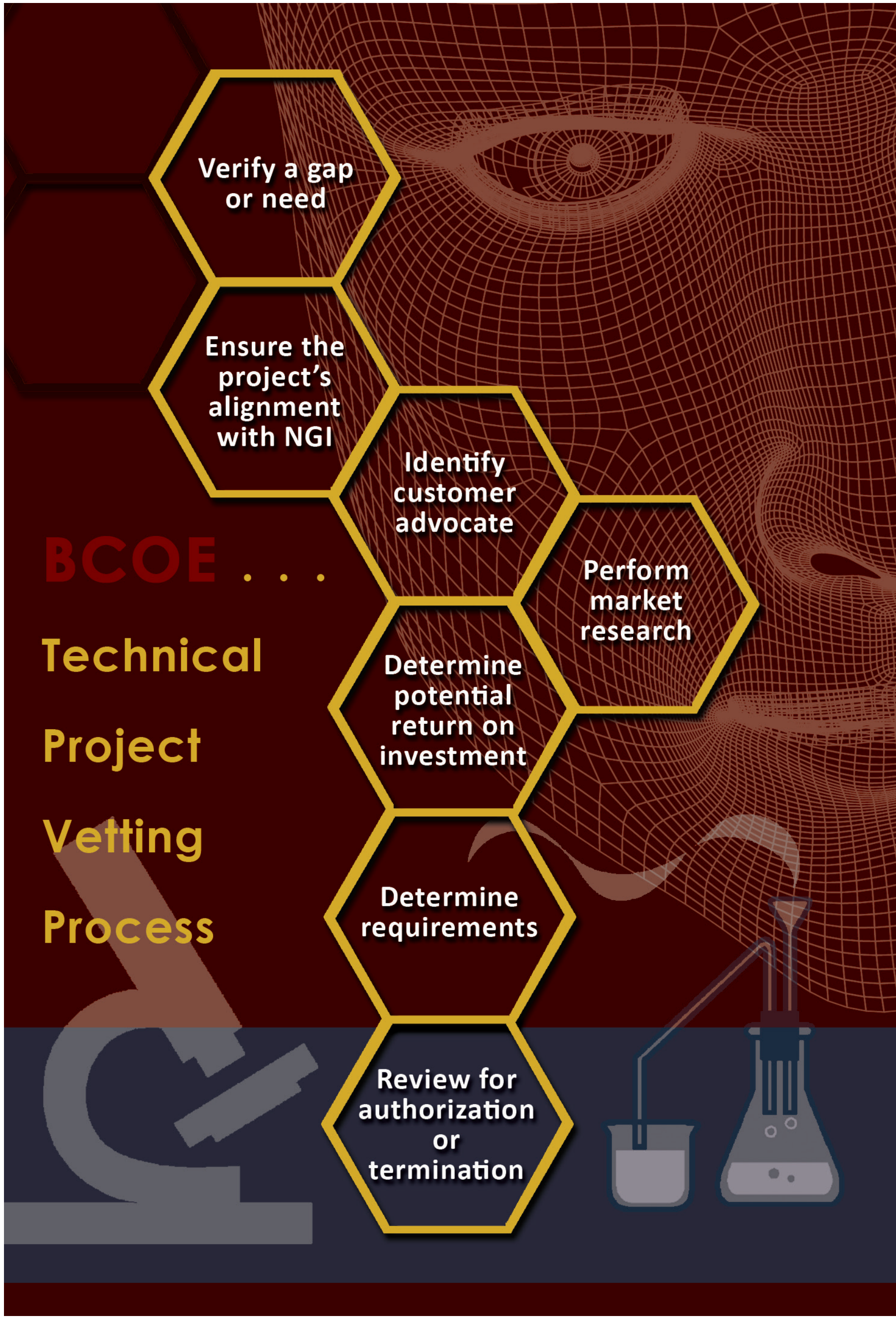
ABOUT Created in 2007, the **Biometric Center of Excellence (BCOE)** enriches the FBI's biometric technologies and capabilities through research and development. While combining the expertise of FBI staff from across the Science and Technology Branch (including the CJIS Division, the Laboratory Division, and the Operational Technology Division), the BCOE also partners with law enforcement and intelligence agencies, academia, and private industry to expand the use of biometrics in identification services and investigative operations. The BCOE ensures valid legal approaches to protect the privacy rights of individuals regarding emerging technologies.

In March 2013, representatives from the BCOE, the NIST, the Massachusetts Institute of Technology—Lincoln Laboratory, the Central Intelligence Agency, the United States Secret Service, and other academic partners founded the SWG–Speaker. In addition to examining various aspects of the voice as a biometric modality, the SWG–Speaker is working with the NIST to establish standards for voice recordings.

Over the course of the year, the BCOE also refined its Technical Project Vetting Process, the rigorous review that each proposed project undergoes to ensure it has true operational value in accordance with the FBI's biometric priorities. This process has become even more important during budget reductions and with competing national security priorities.

Each of these projects, as well as those selected through the Technical Project Vetting Process in the future, will ultimately improve identification services. This will strengthen the FBI's ability to combat crime and terrorism as biometric technologies move more quickly from the lab into the field.

BCOE IN ACTION In 2013, BCOE and LD staff received the FBI Director's Outstanding Scientific Advancement Award for their contributions to law enforcement through the Black Box Study. Conducted in 2011 and 2012, the study was the first large-scale analysis of the accuracy and reliability of latent print examiners' decisions. Its results were published in the *Proceedings of the National Academy of Sciences* and introduced in court the next day (Minnesota vs. Terrell Dixon). The results have been cited frequently thereafter, proving their importance to both the operation of forensic laboratories and fingerprint examiner testimony in the legal system. The Black Box Study results changed how examiners in the FBI and other agencies (nationally and internationally) testify in court. The study results have in some cases negated the need for Daubert hearings, which are evaluations by trial judges on the admissibility of defined "expert" or technical testimony or evidence. The reduction of such hearings has resulted in the criminal justice community saving both time and money. The Black Box Study is also expected to affect laboratory standard operating procedures for fingerprint evidence examiner training, certification and competency testing, and quality assurance.



BCOE . . .

Technical Project Vetting Process

Verify a gap or need

Ensure the project's alignment with NGI

Identify customer advocate

Perform market research

Determine potential return on investment

Determine requirements

Review for authorization or termination

ADVISORY POLICY BOARD/COMPACT COUNCIL/FO CJIS SUBJECT MATTER EXPERTS

Shared goals accomplished by working together

Cooperation with, input from, and information sharing with both law enforcement and authorized non-criminal justice agencies at all levels is vital to accomplishing shared goals. To this end, the CJIS Division maintains strong working relationships with the **CJIS Advisory Policy Board (APB)**, the **National Crime Prevention and Privacy Compact Council (Council)**, and the **FBI Field Office CJIS Subject Matter Experts (FO CJIS SMEs)**.

The APB was 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. The Advisory Process has covered all CJIS services since the fall of 1994.

The National Crime Prevention and Privacy Compact Act of 1998 established a 15-member Council of state and federal agencies' representatives that are appointed by the U.S. Attorney General. The Council establishes rules, policies, and procedures to facilitate the use of criminal history record information for non-criminal justice purposes.

The FO CJIS SME program was established in 2012 to promote CJIS services in FBI field offices. Each field office has at least one FO CJIS SME who serves as a point of contact regarding CJIS Division services.

APB YEAR IN REVIEW To ensure collaboration between the FBI and law enforcement and criminal justice agencies, the APB seeks these agencies' input on how CJIS services represent their data and how they may best access the data CJIS provides. In addition to reviewing policy, strategic, technical, and operational issues related to all CJIS systems, the APB makes recommendations to the FBI Director, who has approved hundreds of recommendations in the last decade.

At their June 2013 meeting, the APB made recommendations involving several programs. Items forwarded for approval include:

- The Next Generation Identification *(NGI) RAP Back Service Criminal Justice Policy and Implementation Guide, Version 1.2*, which introduces the key implementation considerations for the criminal justice use of Rap Back and informs potential participants of the requirements and responsibilities necessary to participate.
- The modification of the Uniform Crime Reporting (UCR) Program's Hate Crime Statistics Program data collection elements to include all self-identified religions in the United States as listed in the Pew Research Center's Pew Forum on Religion and Public Life (2008) and the Statistical Abstract (2012) published by the United States Census Bureau. Also, the APB moved to include an anti-Arab bias motivation.
- A request for the FBI to pursue a regulation change to expand access of the National Instant Criminal Background Check System for use when hiring a law enforcement officer who will use a firearm.
- Providing the Department of Defense (DoD) with an update from the National Crime Information Center's National Sex Offender Registry records every 24 hours for status verification of trusted individuals, assuring proper registration of sex offenders, and ensuring only authorized individuals gain access to DoD installations.
- A change to the CJIS Security Policy declaring a police vehicle as a secure location and removing the requirement for Advanced Authentication under certain conditions.
- A request for CJIS to conduct a pilot program (under certain constraints) where National Data Exchange data submission extracts may be provided to the UCR Program for National Incident-Based Reporting System reporting.

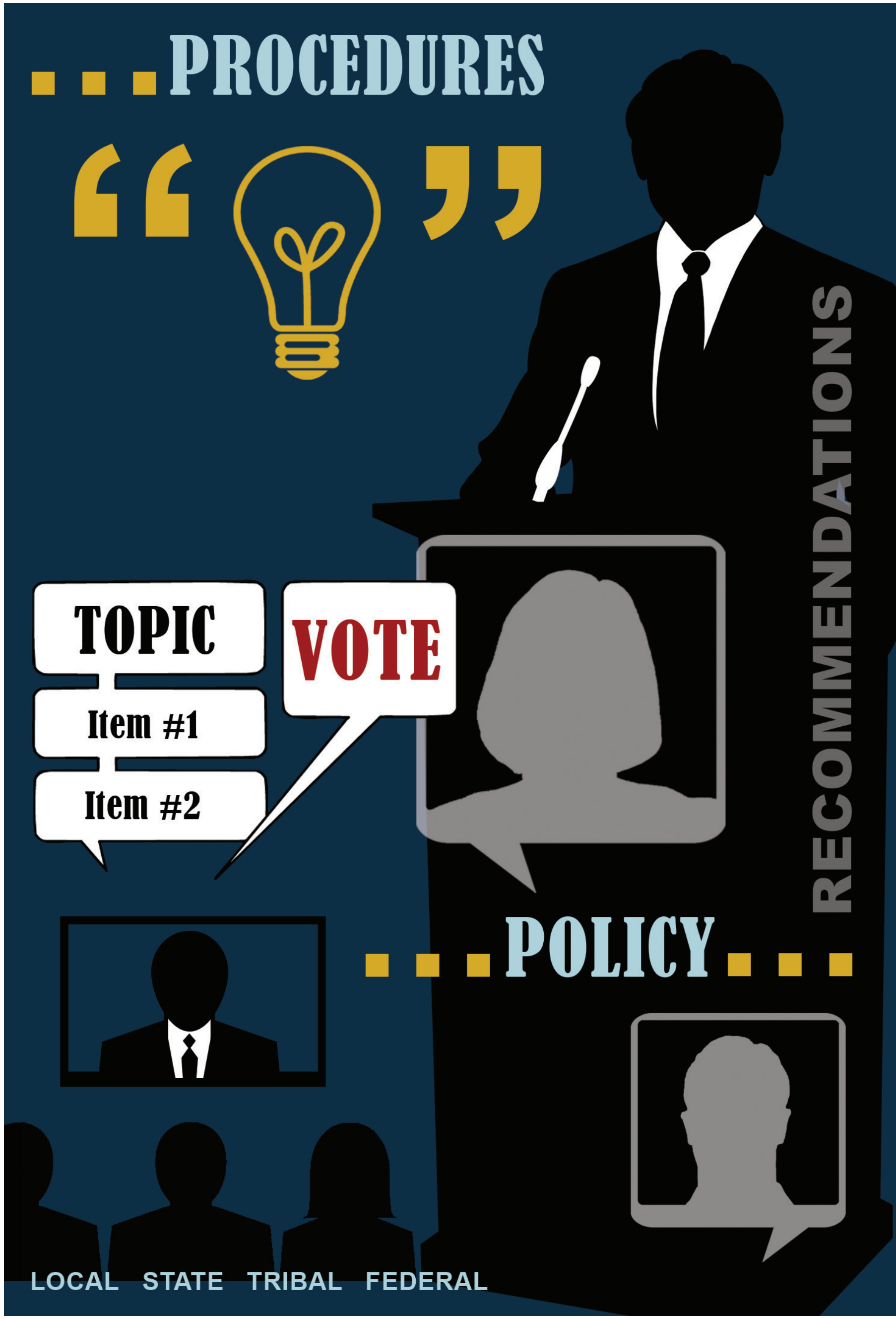
COUNCIL YEAR IN REVIEW In fiscal year (FY) 2013, the Council continued enhancing public safety while respecting individuals' privacy through the sharing of criminal history record information with authorized non-criminal justice users. Compact ratification benefits the noncriminal justice community by ensuring that the most complete and accurate criminal history record is available in a timely way for licensing and employment purposes on an interstate basis. In March, New York became the 30th state to ratify the Compact.

Compact ratification is also the first step towards participation in the National Fingerprint File (NFF) program. In FY 2013, Missouri and Iowa became the 17th and 18th states, respectively, to participate in the NFF program. (NFF participation eliminates record duplication, enhances individual privacy protections, and helps better protect our nation's most vulnerable populations by improving the quality of the criminal history record information provided.)

With Rap Back service scheduled to be available in 2014, the Council's 13-member Rap Back Focus Group continued to concentrate on operational and policy impacts related to implementation. The Focus Group collaborated extensively with the CJIS Division to develop the *NGI Non-criminal Justice Rap Back Policy and Implementation Guide*, a document intended for use by Rap Back participants as they prepare to implement the service. The Focus Group continues to provide recommendations to the Council.

In March, the Council hosted the Civil Fingerprint Image Quality Discussion in conjunction with its Standards and Policy Committee meeting. This event brought 22 fingerprinting vendors together with the Standards and Policy Committee and CJIS subject matter experts. The discussion allowed the Council to leverage its relationship with the vendor community to begin developing innovative solutions for improving civil fingerprint image quality.

FO CJIS SMEs YEAR IN REVIEW FO CJIS SMEs have a valuable role in connecting FBI field office staff with CJIS services. In July 2012 the CJIS Division held a conference for FBI personnel from all 56 field offices. The information presented described how CJIS services assist with both investigative and intelligence missions. During 2013, a virtual conference educated additional FO CJIS SMEs and provided updated information to current FO CJIS SMEs. As a result of the FO CJIS SME Program, FBI field offices have the information they need to leverage CJIS services for routine case development and crises events.



CJIS INFORMATION TECHNOLOGY

Leveraging new technology to support 24/7/365 services

ABOUT The **CJIS Division's data center** serves as the backbone for the vital law enforcement and criminal justice services that the Division provides to its partners. Every day, the CJIS Division processes millions of transactions across its information technology (IT) systems, ensuring system availability and quick response times that range from minutes to fractions of seconds.

The staff of the Information Technology Management Section (ITMS) completed dozens of system builds in fiscal year (FY) 2013 that represented thousands of system enhancements and fixes. These were accomplished in a way that minimized disruption to the Division's 24/7/365 services. The ITMS also supported major IT development across the Division's programs in FY 2013, including the Law Enforcement Enterprise Portal, the Uniform Crime Reporting Redevelopment Project, and the signing and implementation of international governmental agreements that provide IT connectivity for criminal justice information sharing. Two major projects that the staff of ITMS focused on during the year included the development of a Common Compute Platform and a major Telecommunications Infrastructure Upgrade.

The **Common Compute Platform** brings an industry-standard "cloud computing" IT platform to the data center that is both powerful and flexible. As the centerpiece of where the Division's IT infrastructure is heading, the Common Compute Platform supports server virtualization, access to data networks, and access to data storage. This capability enables the Division to provide a common platform as a service to other FBI and Department of Justice entities. It also increases efficiencies, lowers maintenance and overhead costs, and simplifies upgrades to new operating systems.

The **Telecommunications Infrastructure Upgrade** transitions the entire CJIS Division complex from an aging telecommunications system to an integrated, hybrid Voice Over Internet Protocol (VoIP) solution with enhancements for the Division's call centers. The VoIP solution will help CJIS call centers be more efficient and increase the services the Division can provide to external customers.

EXCELLENCE IN SERVICE

Public Access Line provides a single point of contact for tips from the public

ABOUT The FBI established the **Public Access Line (PAL)** to serve as the central intake point for the public to provide information to the FBI about criminal activities and threats to national security.

With a staff dedicated to providing customer service and the development of a uniform process for handling calls, the PAL enables special agents to focus on investigative duties, rather than screening calls. The PAL has significantly improved how the FBI communicates with the public.

The PAL provides service 24/7/365 to 28 FBI field offices across the nation.

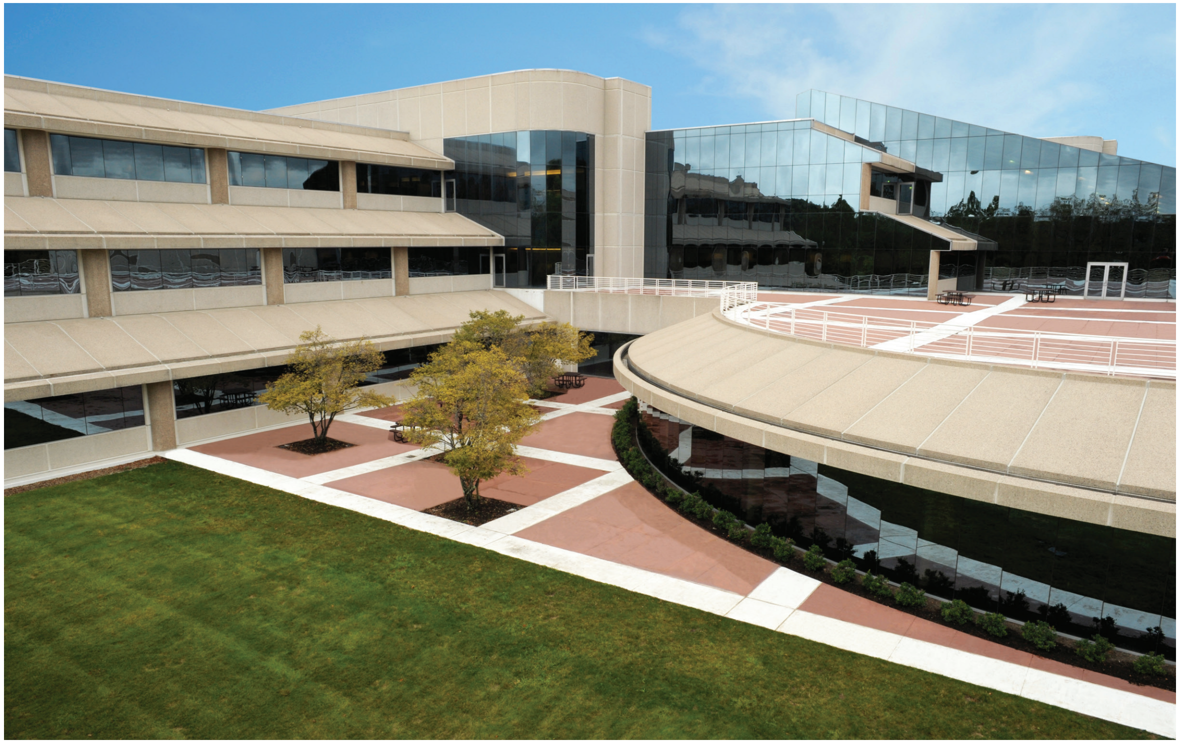
PAL IN ACTION At 2:49 p.m. on April 15, two pressure cooker bombs detonated near the finish line of the Boston Marathon, killing three spectators and injuring 264 people. The bombing triggered a manhunt that resulted in the death of a police officer on April 18, and a shoot-out with suspects that injured 16 other officers.

PAL staff assisted with the investigation by handling approximately 34,000 telephone calls in the week following the bombing. (During a normal week, the PAL receives between 5,000 and 6,000 telephone tips.) The PAL staff assessed the calls, screened them for relevancy, and determined whether to enter the information into the FBI's crisis information system. PAL staff forwarded more than 1,500 leads to investigators.

"The PAL was critical," said a supervisory intelligence analyst in Boston. "Without the PAL, we would have been completely overwhelmed with the level of calls."

OUR CAMPUS

Where connections and identifications generate the power to know



On a West Virginia hilltop amid 1,000 rolling acres, the **CJIS Division campus** strikes a contrast to the surrounding forest and farmland. The Clarksburg facility includes a main building of 526,000 square feet housing offices and a state-of-the-art data center that serves as home to the many programs serving law enforcement and criminal justice entities across the nation. A service center, central plant, visitor's center, and a child care center make up the original campus that was completed in July 1995.

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 CJIS Link (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.

Scan this QR Code with your smartphone to learn more about the *Link* or sign up for e-mail updates. If your QR Reader takes you to the mobile FBI site, you may wish to access the full "desktop" site from the link at the bottom of the page in order to open the links to recent editions of *The CJIS Link.*

The newest addition to the campus is the **FBI's Biometrics Technology Center,** which will house the CJIS Division's Biometric Services Section and the Department of Defense's (DoD) Defense Forensics and Biometrics Agency. The projected date for completion is fall of 2014. The 360,000 square feet of modern office space will house the Biometric Center of Excellence, placing needed biometric services in one location to provide training, conference, office space, and development facilities for the FBI's and DoD's joint biometric research.

2013

Original architect rendering.

http://www.fbi.gov/about-us/cjis

Criminal Justice Information Services Division