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

CJIS

ANNUAL REPORT 2010

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

THE POWER TO CONNECT, THE POWER TO IDENTIFY, THE POWER TO KNOW

CJIS

ANNUAL REPORT 2010

State of CJIS

We exceed customer expectations by delivering the right information at the right time and place.

The FBI's work through the CJIS Division reaches around the world, helping to fight and prevent crime and terrorism. In FY 2010, we continued to accommodate ever-increasing requests for identification and information sharing services. These services support those on the front lines fighting and deterring crime and terrorism, such as police officers, criminal investigators, U.S. marshals, and federal agents.

Expansion in the use of our services also reflects increased civil use of CJIS systems. Pursuant to various statutes, the CJIS Division's staff conducts fingerprint-based background checks for those applying for sensitive positions such as teachers, bankers, and hazardous materials handlers.

Highlights from fiscal year 2010 include the following:

- The Integrated Automated Fingerprint Identification System (IAFIS) marked 167,792 average daily responses for fingerprint identification.
- The National Crime Information Center set a new single day record on August 4, 2010, processing more than 9.1 million transactions.
- The National Instant Criminal Background Check System, used during gun purchases, conducted 14.1 million background checks.
- The Law Enforcement National Data Exchange database surpassed 100 million records of nationwide incident and case reports that can be searched for investigative purposes.
- The Law Enforcement Online program's Virtual Command Center capability was used in circumstances from criminal investigations to major sporting events, counterterrorism exercises, disaster response, and major international meetings.
- The staff of the Uniform Crime Reporting Program helped more tribal agencies begin to contribute their crime statistics to the program, boosting the total number of tribal agencies actively submitting data to 4 times the prior number.
- The CJIS Division Intelligence Group processed more than 3,800 Security Risk Assessments regarding individuals who work with, possess, or transport toxins and other select agents.
- The Next Generation Identification program made progress on several initiatives, including the piloting of the Repository

"This *2010 CJIS Annual Report* reflects the dedication of our 2,500+ employees and our collaboration with our partners in the law enforcement, national security, and intelligence communities we serve." — Daniel D. Roberts, *Assistant Director, CJIS Division*

for Individuals of Special Concern capability with six law enforcement agencies.

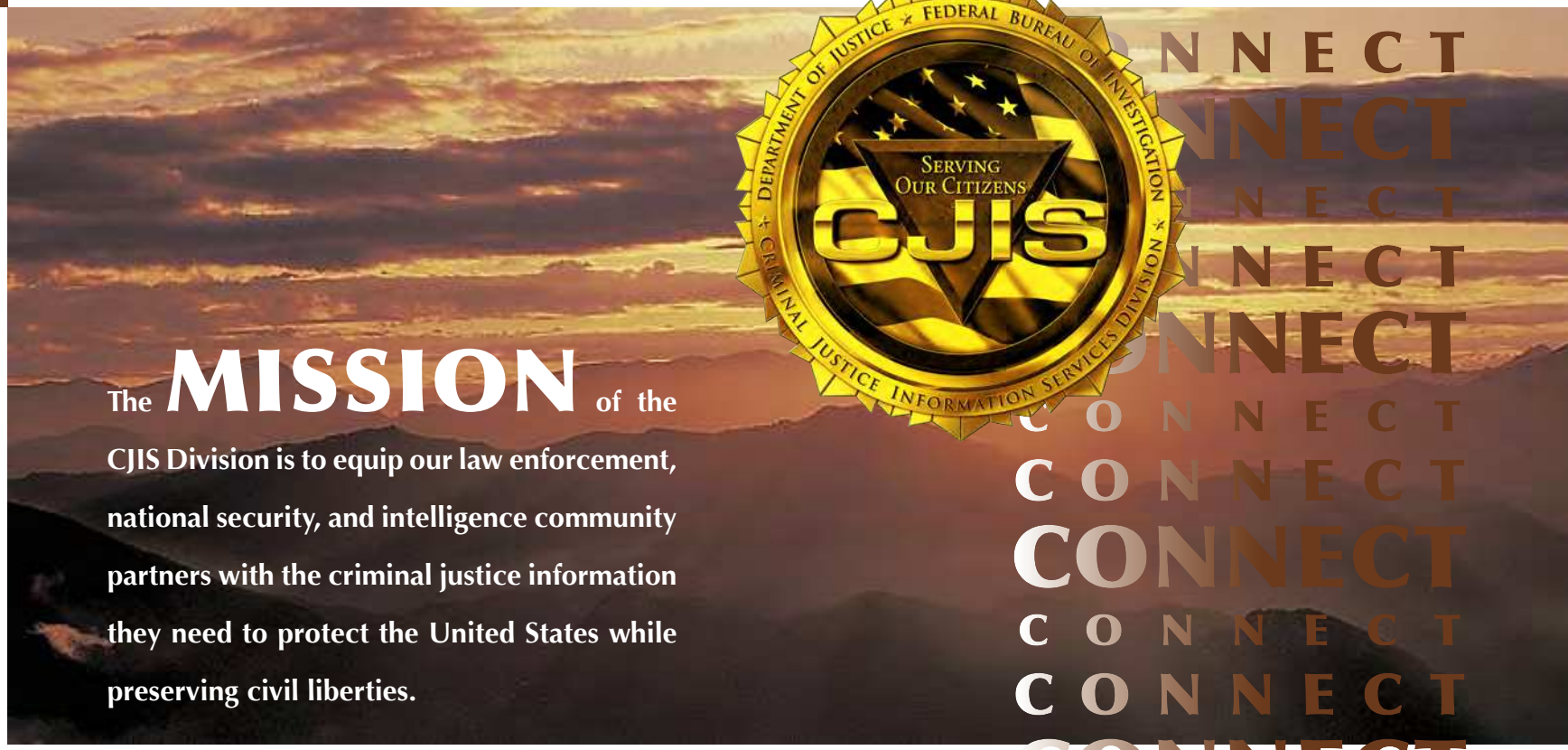
- The Biometric Center of Excellence (BCOE) gained information on how best to support the operational activities of the FBI through an extensive outreach campaign. BCOE staff visited 11 Field Offices during 2010 for in-depth, facilitated discussions.

In support of identifying possible terrorists, CJIS participated in one of the most significant fingerprint collection operations in the Division's history. Nineteen agents and three support personnel participated in the Afghanistan Prison Biometric Project; a 6-week effort to fingerprint prisoners in Afghan prisons and teach guards how to take fingerprints. Through this mission, valuable information was collected that enabled the FBI to identify and link several prisoners to FBI and Department of Defense (DoD) cases based on biometric matches to unsolved latent prints.

And, our Biometric Interoperability program also continued to benefit our national security. Since its inception, the collaboration between the CJIS Biometric Interoperability staff and the Department of Homeland Security has resulted in the removal of 35,000 violent criminals from the United States.

In addition to expanding our services, our Division is also expanding its campus. In spring 2010, construction began on the first phase of the Biometrics Technology Center (BTC). Once complete, the BTC will enable the co-location of the FBI's biometric operations (and the BCOE) with the biometric identification operations of the DoD. This will create a unique collaboration opportunity for the two agencies in partnership with academia.

This *2010 CJIS Annual Report* reflects the dedication of our 2,500+ employees and our collaboration with our partners in the law enforcement, national security, and intelligence communities. Our growth and exploration of "new frontiers" in biometric identification and information sharing is made possible through this collective effort. By leveraging the crime-fighting resources we have today, and the technological advances we make in the future, we will be able to better protect our citizens.



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

INTELLIGENT RISK TAKING

VALUE Our Employees

REWARD INNOVATION

PUBLIC SAFETY

EXEMPLIFY *Integrity* AND PROFESSIONALISM

CONNECT

Culture of Quality

OPEN COMMUNICATIONS

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

CONTINUOUSLY EXPLORE

KNOW

VISION

IDENTIFY

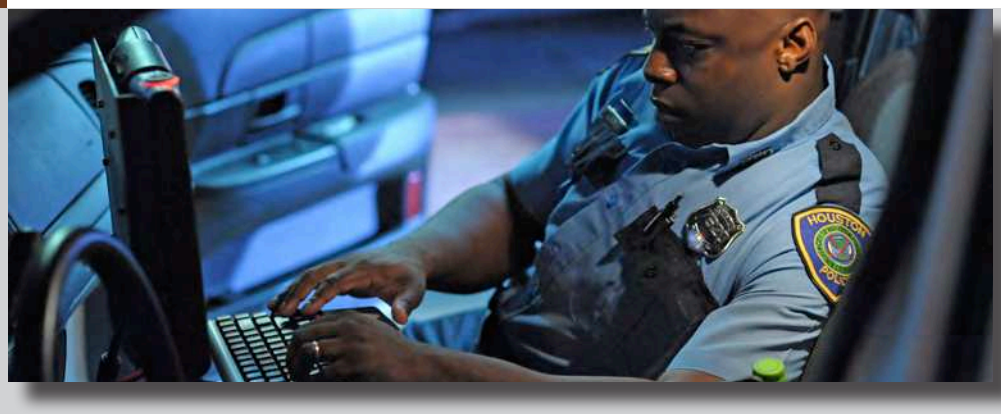
GOALS

MANAGE more information and PROCESS it faster

PROVIDE accurate and complete INFORMATION

Preserve civil LIBERTIES

Provide additional VALUE-ADDED services



National Crime Information Center (NCIC)

National Instant Criminal Background Check System (NICS)

Law Enforcement National Data Exchange (N-DEx)

CJIS Division Intelligence Group (CDIG)

Law Enforcement Online (LEO)

Uniform Crime Reporting (UCR) Program

Connect

Information on-the-spot

We provide cops on the street with facts they need when they need them.

Connect

When the **National Crime Information Center (NCIC)** began operation in January 1967, it had five files that contained about 95,000 records of stolen property and wanted criminals. Currently, the NCIC contains more than 11.7 million active records in 20 files concerning wanted and missing/unidentified persons and stolen property, with 92,000+ users.

The NCIC has been a source of information on which its partners have relied throughout the ensuing years. Part of its success has been its ability to meet the changing needs of its users, and in keeping with that legacy, the NCIC is pursuing the following goals in FY 2011:

Work with the National Institute of Justice to house the National Missing and Unidentified Persons System (NamUs) within the CJIS Division's technical infrastructure.

Create the ability to:

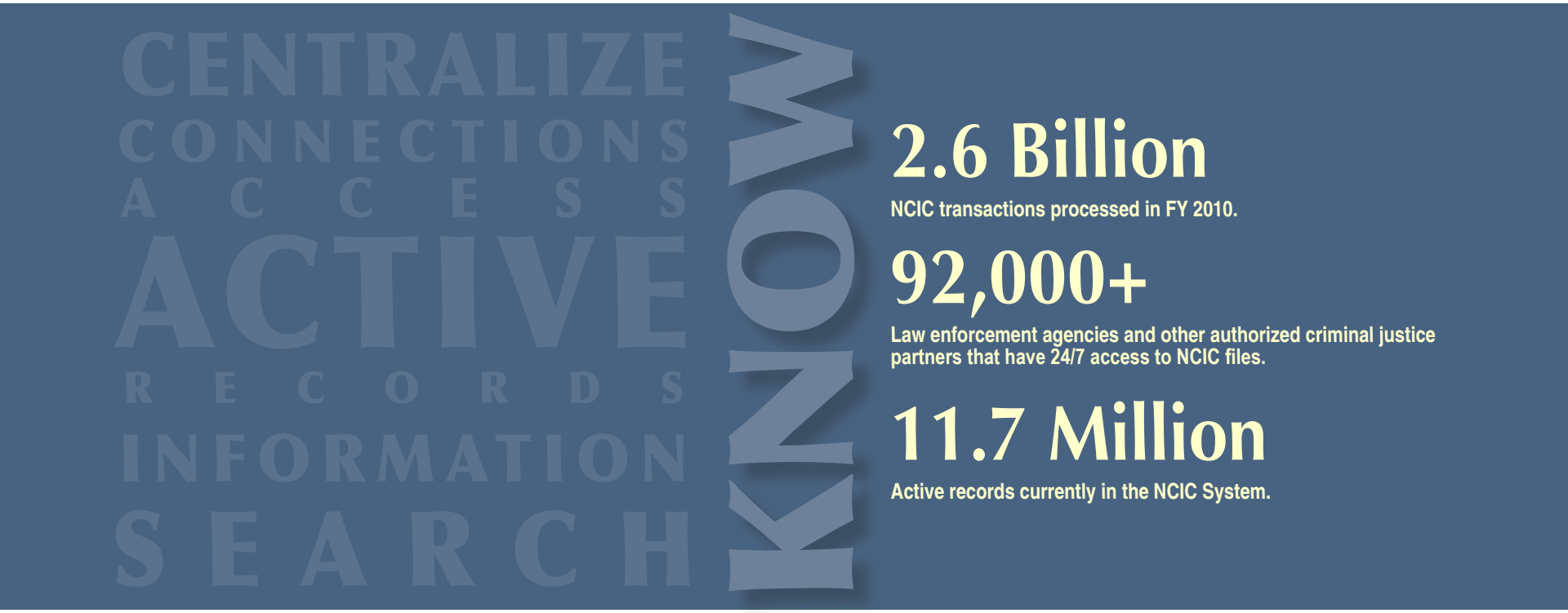
- link records entered by the same agency that are entered more than 30 days apart.
- link image records to multiple records and transfer ownership of the images.
- flag multiple warrants and generate caveats in response.
- expand images to the Gun File.

Allow:

- the entry of lost critical infrastructure equipment and items associated with public safety and homeland security into the Article File.
- the entry of nicknames/"street" names.

Continue to:

- upgrade its name search capabilities.
- expand the U.S. Secret Service Protective File to include individuals who pose a risk to law enforcement protectees.



IN ACTION

On July 19, 2010, a sergeant in Troy, Missouri, pulled over a woman whose car was missing one of two required license plates. The driver identified herself and stated that the passenger was her 16-year-old niece. However, as the sergeant questioned the woman, he noticed that her story was inconsistent and that she seemed nervous and avoided eye contact with him. In addition, the teenager was hesitant to talk. When the sergeant submitted the information to the NCIC, he found that the name that the woman had given him matched an alias in a Wanted Person File record. He discovered that she was from Wasilla, Alaska, where she was wanted for custodial interference. The woman had picked up her daughter from her ex-husband on June 28, 2008, for visitation, but she had never returned, and the authorities had been looking for her during the ensuing 2 years. The sergeant took the woman into custody, and the teenager was reunited with her father.

ACCOMPLISHMENTS

- **Another single day record was set on August 4 when more than 9.1 million NCIC transactions were processed.**
- **The NCIC Mobile Program continued to expand, enabling all FBI agents and U.S. marshals to conduct NCIC and DMV inquiries using wireless devices through the Law Enforcement Online (LEO) system. At the end of FY 2010, 1,399 members were using this capability.**
- **The National Sex Offender Register (NSOR) was modified to add 34 base fields and support additional supplemental fields. The retention of records in this file was changed from 10 years to indefinitely. In addition, an audit was implemented to ensure accuracy of these records.**
- **The Gang File (formerly part of the Violent Gang and Terrorist Organization File [VGTOF]) was modified to allow unlimited retention of gang member records.**

Instant checks

We determine eligibility to purchase guns and explosives.

Connect

The FBI developed the **National Instant Criminal Background Check System (NICS)**, which ensures the timely transfer of firearms to eligible gun buyers and prevents the transfer of firearms to those prohibited, through a cooperative effort with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Department of Justice, and state and local law enforcement agencies.

The NICS was developed 12 years ago as a result of the Brady Handgun Violence Prevention Act of 1993 (Brady Act). The Brady Act requires Federal Firearms Licensees (FFLs) to request background checks on individuals attempting to receive a firearm. The NICS enables FFLs to request an immediate determination as to whether the receipt of a firearm by a prospective gun buyer would violate federal or state law.

The NICS automatically searches more than 67 million records contained in three databases (the National Crime Information Center [NCIC], the Interstate Identification Index, and the NICS Index) when authorized gun dealers or FFLs request a NICS check. These records include wanted persons, subjects of protective/restraining orders, and other persons prohibited from receiving or possessing firearms. If an applicant's name and descriptive information matches any records in the databases, the NICS staff and/or state agencies perform further research to determine the eligibility of the applicant.

The NICS E-Check, which allows FFLs to contact the NICS via the Internet to initiate required background checks, experienced major growth in 2010. The NICS E-Check gives FFLs the ability to retrieve background check results 24/7, to print daily logs in case of ATF inspections, and to print completed background check search results.

Training provided by the NICS State Support Team was a great part of the NICS success in fiscal year 2010. The president of the Law Enforcement Information and Records Association (LEIRA) sent a letter of appreciation to the NICS staff for their engaging and interactive NICS 101 training provided during a LEIRA Conference. The main objective of the training was to provide information to the law enforcement participants about federal prohibitors for firearm purchases.

14,088,406

NICS background checks for gun transfers completed.

70,972

NICS gun transfers denied federally (in requests processed by Examiners), keeping firearms out of the hands of felons, fugitives, and other prohibited persons.

67 Million+

Records searched during each NICS background check.

The NICS Section has received approval to establish a database to place the names of individuals who are denied the right to purchase or receive a firearm based on a firearm background check into the National Crime Information Center (NCIC). Sharing these entries, along with intelligence from other CJIS databases, with Field Offices enhances public safety.

IN ACTION

On January 16, 2010, two individuals approached an FFL together in an attempt for one of them to purchase a firearm. The NICS staff processed the transaction; one subject was matched with hits in the NCIC. While validating the warrant as active with the originating agency, the NICS Legal Instruments Examiner (Examiner) learned the subject was also on a state Top Ten Fugitive list. The Examiner provided the details of the attempted purchaser and the address of the FFL to the originating agency. Within 20 minutes, the Examiner received a return call from the originating agency and was advised the individual had been apprehended along with the other individual who also had an active warrant.

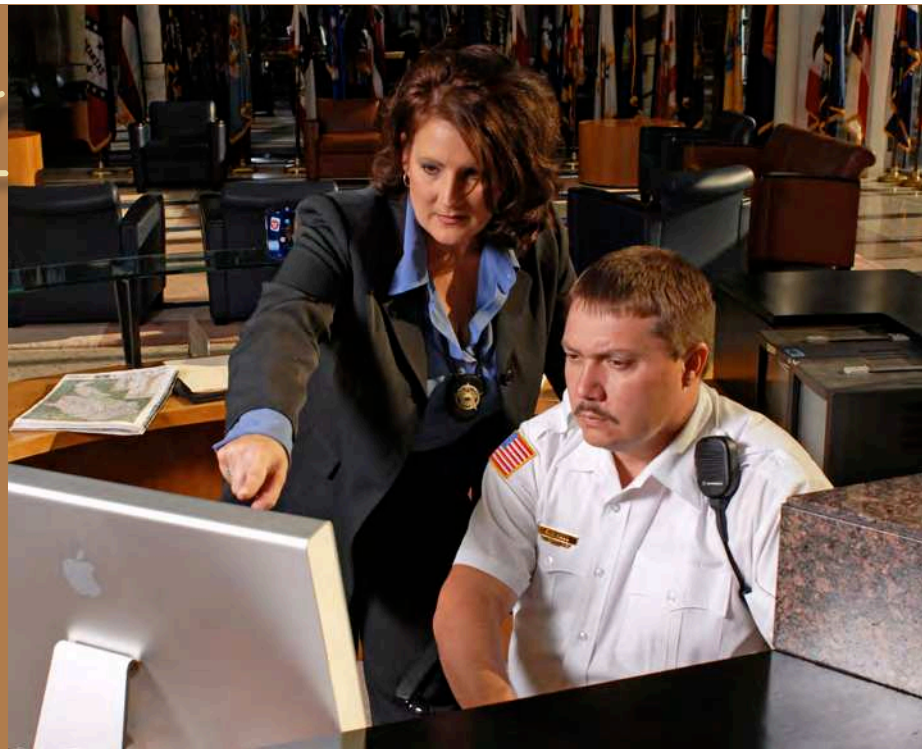
ACCOMPLISHMENTS

- More than 14 million NICS background checks were conducted.
- The NICS Section exceeded its mandate of 90 percent immediate determination rate (eligibility determinations made while the FFL is on the telephone) with a rate of 91.36 percent.
- 100 percent of all the NICS transactions delayed based on the name check search were reviewed within three business days.
- NICS processed 70,972 federal denials (federal denials exclude those background checks processed by the states) in 2010, creating a total of 798,272 federal denials since the inception of NICS.

Linking common threads

We connect investigative information for law enforcement across the Nation.

Connect



The **Law Enforcement National Data Exchange (N-DEx)** reached a major milestone in fiscal year 2010 when it surpassed 100,000,000 searchable records within this powerful investigative tool. The N-DEx helps criminal justice agencies combat crime and terrorism through the secure collection and processing of criminal justice data from participating agencies' records management systems.

N-DEx also enables queries of the National Crime Information Center, the Interstate Identification Index, and OneDOJ. The OneDOJ System, which enables internal sharing among agencies within the Department of Justice, is slated to be fully integrated with N-DEx before the end of 2010.

A result of collaboration among local, county, state, tribal, and federal criminal justice entities to establish a secure national criminal justice information sharing capability at the Sensitive but Unclassified Level, the N-DEx has been developed and deployed in increments. Increment 1 gave users the ability to search nationwide incident and case reports based on people, vehicles/property, location, and/or crime characteristics, which supports multi-jurisdictional task forces. Increment 2 provided N-DEx users with the ability to subscribe to a certain kind of search (e.g., a particular alias of a suspect) for any information that becomes available, to be notified if other officers or agencies have requested the same information, and to participate in online collaboration. In addition, an automated process links information across and within jurisdictions and provides a recurring electronic report to designated N-DEx users.

Increment 3, set to be available by the end of 2010, will provide a "Google-like" search capability with the same refined results. Also with this increment, probation and parole data will be added as well as expanded Web services.

Meeting the real-world needs of the criminal justice community has been a key factor to N-DEx's success from the very beginning, a goal that continues to guide the program.

N-DEx capabilities provide the missing links and create partnerships that lead to more effective investigations that help apprehend criminals and disrupt threats to national security.

IN ACTION

A recent traffic stop for a DUI followed by an N-DEx search revealed information from multiple origins that provided a comprehensive look at the criminal record of the subject. The criminal history covered 20 years and included multiple arrests and incarcerations from Florida, New York, Pennsylvania, and West Virginia. A complete time line of the subject's interactions with the criminal justice community was available with one click on the N-DEx system.

ACCOMPLISHMENTS

- **N-DEx completed key enhancements to Increment 2. These enhancements include the addition of the Joint Automated Booking System data and images, connectivity to the Unclassified Network for FBI users, enhancements to the LEXS-SR Server Interface, and the deployment of Geospatial capability in OneDOJ.**
- **Services of N-DEx were established on an interfacing Web domain (www.ndex.fbi.gov).**
- **N-DEx introduced software that agencies can use to generate secure identity assertions from their existing user accounts, allowing agencies to use their own credentials for N-DEx access.**
- **The N-DEx Program Office was recognized by the Christopher Columbus Fellowship Foundation with the 2010 Homeland Security Award for Cyber Security and Information Sharing.**

Seeing the big picture
We analyze information and piece it together.

Connect

The **CJIS Division Intelligence Group (CDIG)** provides tactical intelligence to FBI Field Intelligence Groups; other intelligence community agencies; and local, state, and federal law enforcement organizations to promote public safety and prevent terrorism. This mission positions CDIG to meet current and emerging national security and criminal threats, while serving all law enforcement agencies. CDIG provides its expertise in understanding CJIS systems information in order to ensure that data is used and analyzed to its full potential.

IN ACTION

On June 8, the Grove (Oklahoma) Police Department arrested six individuals for possession of fraudulent credit cards, identification cards, and driver's licenses. During the booking process, the individuals gave police officers names that returned no criminal history data. Special Agents from the Tulsa Resident Agency were suspicious of the individuals' identities and contacted CDIG to assist in examining the fingerprint images collected during the booking. CDIG staff performed additional analysis, which resulted in discovering the true identities of four of the individuals and their criminal histories. After further questioning by agents and law enforcement authorities, one of the individuals agreed to an interview, and he provided information on one of the other subjects who was leading an active credit card fraud business. He also gave officers information on 50 other persons who were participating in the criminal activity.

In April, CDIG's Bioterrorism Risk Assessment Group (BRAG), which conducts risk assessments of persons who possess, use or transport select biological agents and/or toxins (BSAT), followed up on a subject who had been arrested in September 2009 on a Homicide-Negligent

3,879

Security Risk Assessments completed on individuals who work with, possess, or transport select agents and toxins as it relates to their professional responsibilities.

287

Guardian Reports and e-mail notifications to FBI Field Offices on Suspicious Activity of Known or Suspected Terrorists encountered by local, state, or federal law enforcement.

37

Intelligence Information Reports containing unevaluated raw data disseminated to U.S. agencies.

Manslaughter Vehicle Warrant. The arresting officer advised that the subject was in custody, and the warrant was being removed. After many phone conversations with the local District Attorney's office, the BRAG learned that the subject pled guilty and was sentenced on March 31 on numerous Driving-Under-the-Influence charges, including Homicide by Vehicle. Based on the individual's criminal history, the BRAG recommended the applicant be restricted him from access to the BSAT.

ACCOMPLISHMENTS

- **The CDIG developed highly sensitive intelligence products and services for the intelligence community.**
- **Working with other agencies, staff is working to develop new system capabilities for license plate readers and an International Vehicle File for the National Crime Information Center.**
- **CDIG eliminated hard copy records and created a paperless environment through BRAG's scanning/ purge project. These centralized records provide better continuity of records and easier data retrieval.**

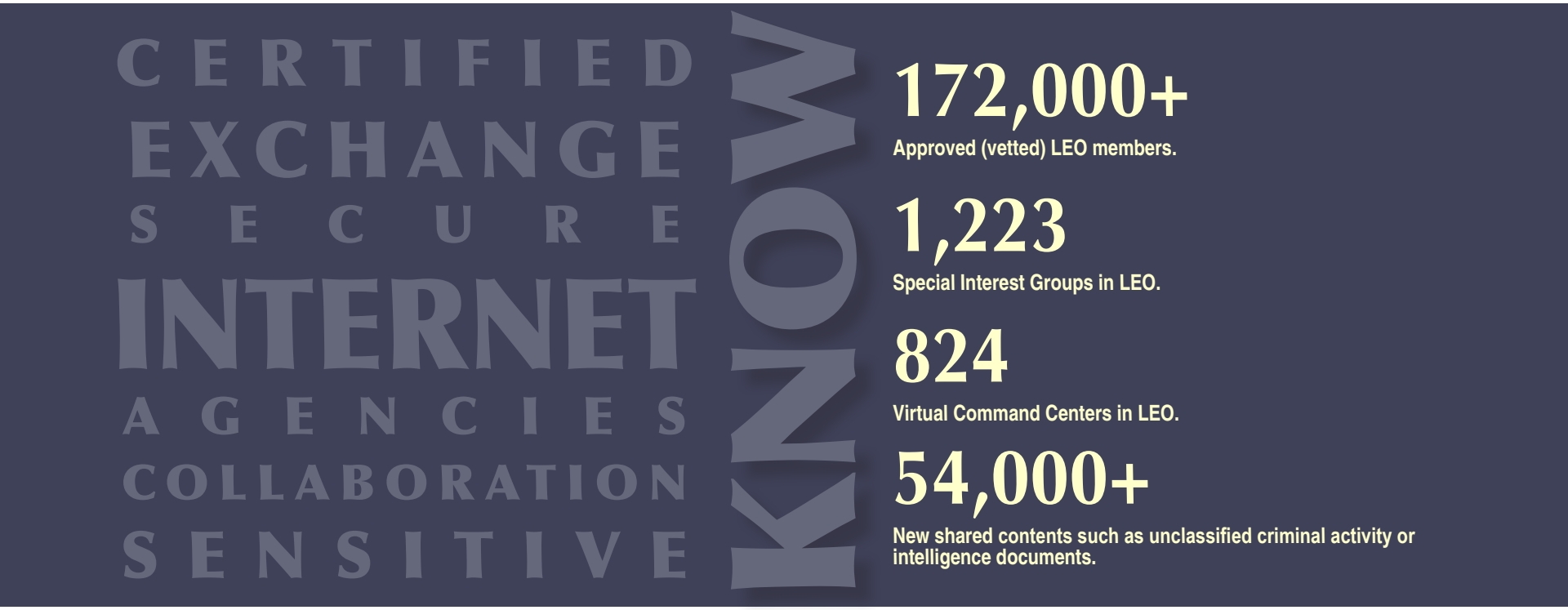
Online community
We enable law enforcement collaboration.

Connect

At the core of the FBI's Information Sharing Initiative is the **Law Enforcement Online (LEO)** system. LEO provides an Internet site for secure, protected communication and the exchange of unclassified but sometimes sensitive information. This virtual "swap shop" has helped create collaboration and cooperation among local, state, tribal, and federal law enforcement personnel for nearly 15 years. LEO offers a variety of services to the criminal justice community, including:

- Access to LEO Special Interest Groups (LEOSIGs), authorized groups of users with specific organizational purposes.
- Use of secure E-mail.
- Connection to the "Roll Call" to get concise information on various topics.
- Entry to Chat, providing real-time, secure discussions on law enforcement topics.
- Use of an Electronic Calendar, which has national and state postings of dates of interest.
- Access to the LEO Library, a comprehensive multimedia repository.
- Exposure to eLearning, online topical learning modules.
- A voice in the Forums, places to ask a general question or post an answer.
- Connection to a Global Address Book of other LEO members.
- Use of Virtual Command Centers (VCCs), critical Internet-based real-time monitoring of the detached parts of an operation, from a local agency's function to national security needs.
- Access to the National Alert System, a high-priority means to disperse vital information to homeland security and law enforcement partners across the country.

With more than 170,000 vetted members, LEO continues to succeed because it evolves as law enforcement's needs evolve—from offering training support to expanding and improving the individual sites that make up the system. Upcoming improvements include enhanced e-mail capabilities as well as upgrades that will expand the search and chat features and provide language translation abilities. In addition, planned improvements to content management



will more quickly bring updated pages to the user.

LEO's VCC continues to gain approval across the law enforcement community. FY 2010 witnessed use of the VCC in a wide variety of circumstances from criminal investigations to major sporting events and from counterterrorism exercises and investigations to major international meetings.

IN ACTION

At the conclusion of a 2-year investigation, the San Francisco and Oakland Immigration and Customs Enforcement offices used the VCC to coordinate serving 10 search warrants throughout the San Francisco Bay area. The warrants netted the largest seizure in San Francisco history, with over $25 million of stolen goods recovered.

The FBI's Washington Field Office used the VCC to provide situational awareness for all security forces working the 2010 Nuclear Security Summit in Washington, D.C. Delegations from 46 countries attended the summit, which was the largest gathering of heads of state called by a U.S. president since the 1945 United Nations Conference on International Organization.

ACCOMPLISHMENTS

- **Personnel traveled abroad and provided hands-on training to LEO's international partners in Chile, Peru, Brazil, and the Dominican Republic in support of the international information sharing mission.**
- **LEO rolled out the "My SIGs" page to provide easy access to all of the SIGs in which the user is a member.**
- **Staff established newly connected databases through LEO for the Polygraph Information Network, Jewelry Security Alliance, and the Heartland of America Regional Forensic Laboratory.**
- **At the 2010 LEO Moderator's Conference held in Baltimore, Maryland, LEO staff trained over 125 moderators from as far away as Alaska and Hawaii on LEO capabilities and tools.**

Crunching the numbers
We provide a national perspective of crime.

Connect

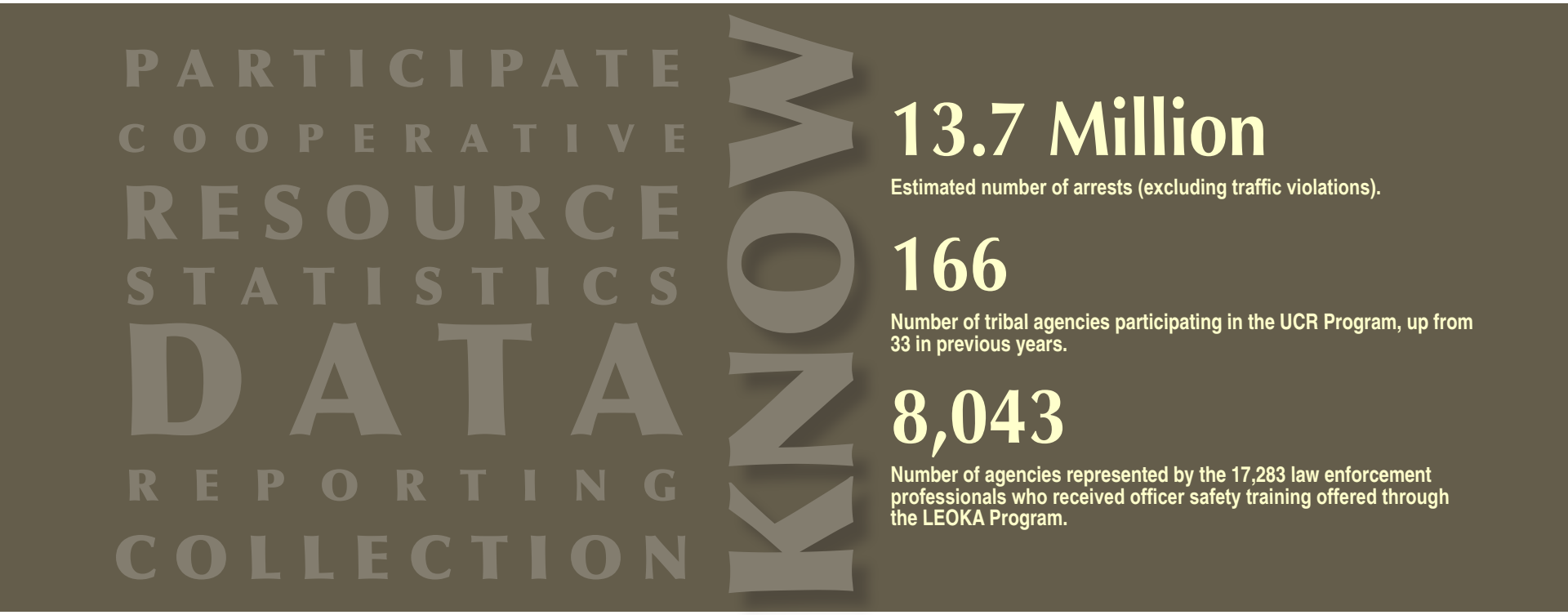
The **Uniform Crime Reporting (UCR) Program**, marking its 80th year, gathers and disseminates crime statistics. Using these statistics, UCR staff publishes three reports each year to the Internet. These high-profile releases include: *Crime in the United States*, a comprehensive collection of data including crime offenses, clearances, arrests, and police employment information; *Law Enforcement Officers Killed and Assaulted (LEOKA)*, a statistical perspective covering the felonious deaths and assaults of officers, as well as information regarding officers who died from accidents while on duty; and *Hate Crime Statistics*, a report focused on bias-motivated crimes.

During the fiscal year, UCR managers continued to pursue an upgrade of the program's aging technology. The UCR Redevelopment Project has secured all of the necessary approvals from FBI Headquarters, and work will begin in 2011 to design and develop the new internal data-processing system. When complete, this new system will ensure a more effective and efficient program.

UCR data serves as a valuable resource for many real-world applications, including law enforcement administration, operation, and management; officer safety training; and research. Also, the Bureau of Justice Assistance uses these statistics to allocate funds from the Edward Byrne Memorial Justice Assistance Grant (JAG) Program. JAG funds may be used for law enforcement state and local initiatives, technical assistance, training, personnel, and information systems.

IN ACTION

In FY 2010, UCR Program staff helped more tribal law enforcement agencies become UCR data contributors. There are 166 active tribal agency contributors, up from just 33 in prior years. Of these agencies, 83 submitted a full



year of data and are included in the agency listings of the 2009 edition of *Crime in the United States* (just 11 agencies were published in the 2008 edition).

UCR staff continued to work with members of the Law Enforcement National Data Exchange (N-DEx) in anticipation of receiving and processing data extracts for use with the UCR's National Incident-Based Reporting System (NIBRS). Ensuring that data extracts from the N-DEx can be accepted into the NIBRS eliminates the need for double reporting by agencies that participate in both the UCR and N-DEx Programs.

ACCOMPLISHMENTS

- **The UCR Program began collecting cargo theft statistics. These statistics will help define the scope of the national cargo theft crime problem and its negative effect on the economy of the United States.**
- **The UCR Redevelopment Project has secured necessary approvals to begin to design and develop the new internal data-processing system.**
- **With input from the CJIS Advisory Process, UCR staff developed policy for future collection of human trafficking offenses.**
- **The LEOKA Program staff provided officer safety training classes both nationally and internationally as part of the LEOKA Program in FY 2010. This included a total of 17,283 students representing 8,043 law enforcement agencies who received the LEOKA training.**

Integrated Automated Fingerprint Identification System (IAFIS)

Next Generation Identification (NGI)

Biometric Interoperability

Biometric Center of Excellence (BCOE)

Collections Program

Identify

Automated identification

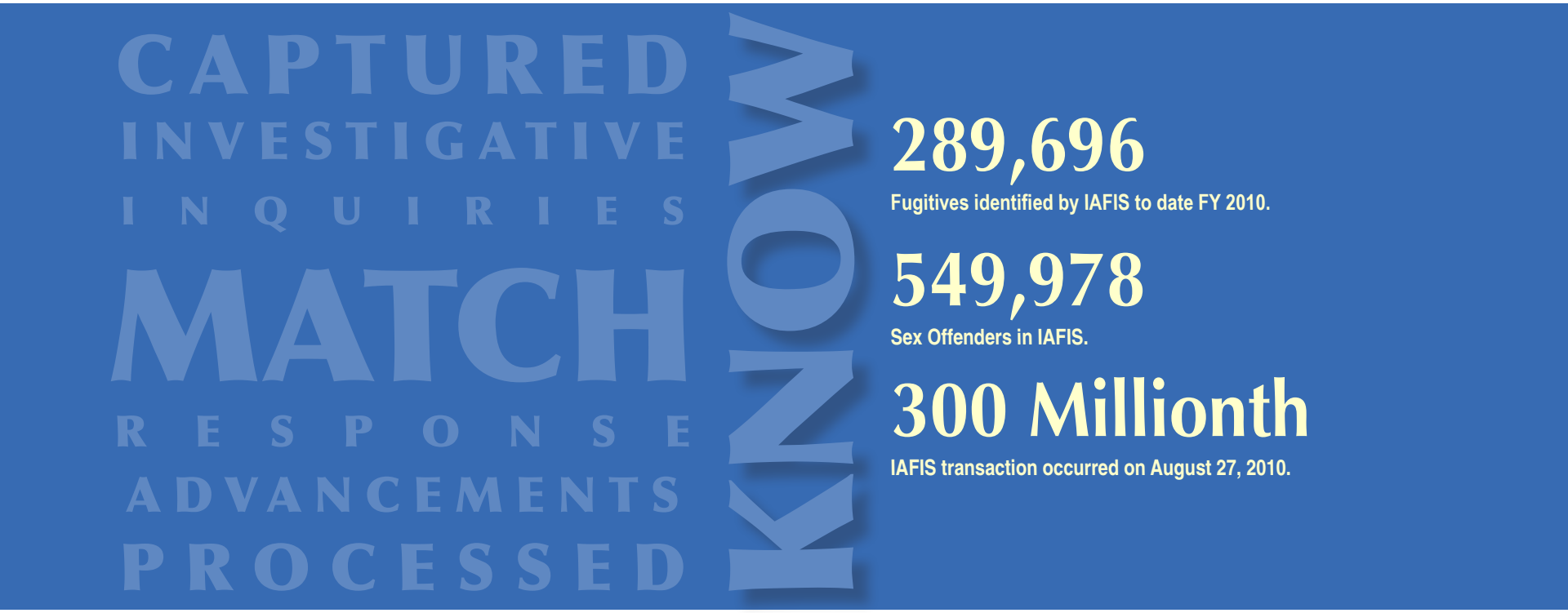
We manage the world's largest criminal database of fingerprints and criminal history.

Identify

For the first time in its 11-year history, Division staff used the **Integrated Automated Fingerprint Identification System (IAFIS)** to conduct fingerprint checks on 335,968 potential Census workers. In four days, April 28 through May 1, Division staff processed the huge amount of Census fingerprint submissions in addition to their customary workload. The IAFIS is the world's largest repository of biometric-supported criminal history information and provides law enforcement with access to specialized files for identification of known criminals through fingerprint identification and for investigative purposes through name-based inquiries. It also accesses criminal history record information for noncriminal justice, or civil submissions, such as those individuals being screened for employment or licensing; which protects our children, our communities, and our Nation from criminal and terroristic threats.

The IAFIS relies on biographic, fingerprints, and/or criminal history data on file to identify an individual. When a rolled or flat ten-print submission is received, the IAFIS accesses more than 67.7 million criminal fingerprints, 26.3 million civil fingerprints, and 387,189 unsolved latent fingerprints (those left behind at crime/terrorism scenes) to look for a match. If a match is found, the submission then goes through the IAFIS Interstate Identification Index (i.e., III) segment to access biographic and criminal history information. Finally, the IAFIS delivers a response to the requesting agency on whether a match was found. On average, the III receives 19.6 million name-based inquiries each month for criminal justice and authorized noncriminal justice purposes.

More than 86,000 local, state, tribal, federal, and international partners electronically submit requests to IAFIS, which operates 24 hours a day, 365 days a year. The IAFIS is supported by more than 900 service providers focusing on fingerprint comparison, criminal history maintenance, and various other functions.



IN ACTION

In July 2010, the IAFIS helped to identify the "Barefoot Bandit," the U.S. teenager who stole cars, boats, and airplanes while dodging U.S. law enforcement for 2 years. He was captured on July 11 in the Bahamas after crashing a stolen airplane. On July 8, 2010, the CJIS Division received a request from the Legat Barbados to provide copies of fingerprints from the IAFIS database based on the suspect's name, date of birth, and FBI number supplied by the Legat. These fingerprints were then compared with latent fingerprints obtained from a previously stolen plane. On July 14, 2010, the CJIS Division provided copies of all fingerprints for the "Barefoot Bandit," Colton Harris-Moore, in the IAFIS database to the Miami Field Office. (Harris-Moore was due in court on July 16, and the Field Office needed his fingerprints for comparison purposes.)

ACCOMPLISHMENTS

- **Average daily fingerprint submissions rose from 42,203 in 1999 to 167,822 in FY 2010. Average daily responses increased from 34,728 in 1999 to 167,792. For FY 2010, IAFIS receipts at 61,255,074 doubled FY 2007 receipts of 26,061,552.**
- **IAFIS criminal submissions were processed in an average of 8 minutes, 42 seconds, and IAFIS noncriminal/civil submissions in an average of 55 minutes, 24 seconds.**
- **More than 67.7 million subject criminal history records were maintained, which grew by an average of 8,000-10,000 new identities per day.**
- **The III received more than 235 million name-based transactions in FY 2010.**

Fingerprints and beyond

We are developing the future of identification services.

Identify

The **Next Generation Identification system (NGI)** will replace the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and will support state-of-the-art biometric identification and investigation services. This technology upgrade will also accommodate the increased information sharing and processing needs of local, state, tribal, federal, and international agencies.

The NGI has been developed in collaboration with local, state, and federal partners through the CJIS Division's shared management approach. The CJIS Advisory Process and The National Crime Prevention and Privacy Compact Council have been instrumental in establishing business processes, policy, privacy considerations, and best practices for NGI services. With Full Operational Capability (FOC) scheduled for 2014, significant achievements have occurred in the NGI development this year.

The NGI continued its progress with the Advanced Fingerprint Identification Technology (AFIT) and is on track for its scheduled implementation in early 2011. AFIT will replace the FBI's existing Automated Fingerprint Identification System (AFIS), improving search accuracy to over 99 percent while adding enhanced processing speed, automation, and flat-print searching.

The CJIS Division is currently piloting the Repository for Individuals of Special Concern (RISC) capability with six law enforcement agencies. This feature provides a rapid automated search of Wanted Persons, Sex Offenders, Known or Appropriately Suspected Terrorists, and persons of special interest. Mobile Identification devices used to submit RISC searches allow law enforcement officers to quickly assess the threat level of encountered individuals. This capability is on schedule for full deployment mid-year 2011.

The RISC Pilot is one example of an NGI Quick Way to Implement New Solutions (QUICKWINS). The NGI QUICKWINS are specific capabilities developed for limited implementation before the final release of the NGI. Two

20,250

Red responses provided for Wanted Person or Sexual Offender Registry Subjects as a result of a RISC Pilot transaction.

1,665,273

Palmprints stored electronically as a part of the Additional Biometric Receipt and Store NGI QUICKWINS.

22

States with the improved capability to submit dispositions as a result of the NGI QUICKWINS.

additional QUICKWINS that have also been successfully implemented are the Additional Biometric Receipt and Store, which captures biometrics of palm and iris images, and Disposition Reporting Improvements, which provides the first mechanism to electronically submit dispositions to the FBI.

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

IN ACTION

On June 16, 2010, Houston Police Department (HPD) officers encountered a subject that attempted to conceal his identity during a traffic stop. The officers captured his fingerprints using a Mobile Identification (ID) device. The search resulted in a Red response from CJIS, revealing the subject was wanted for Aggravated Sexual Assault of a Juvenile.

ACCOMPLISHMENTS

- **Deployed more than 800 NGI Advanced Technology Workstations (ATWs) to the FBI's CJIS and Laboratory Divisions. Each ATW includes a 30-inch high-resolution monitor to increase operational efficiency and productivity for the IAFIS service providers.**
- **The first NGI User's Conference was held in August 2010, including panel discussions and feedback from attendees representing more than 84 local, state, and federal law enforcement agencies.**
- **Added three additional law enforcement agencies to participate in the RISC pilot.**

Partnering to identify

We collaborate with other federal agencies and international partners to identify criminals and terrorists.

Identify

Photo courtesy of U.S. Customs and Border Protection

Biometric Interoperability facilitates the exchange of biometrics, e.g., 10-print rolled and flat fingerprints, between the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the biometric systems of other federal and international agencies. The improved information sharing between the FBI and its federal and international partners enhances the ability to identify criminals and terrorists, securing our Nation's streets and borders.

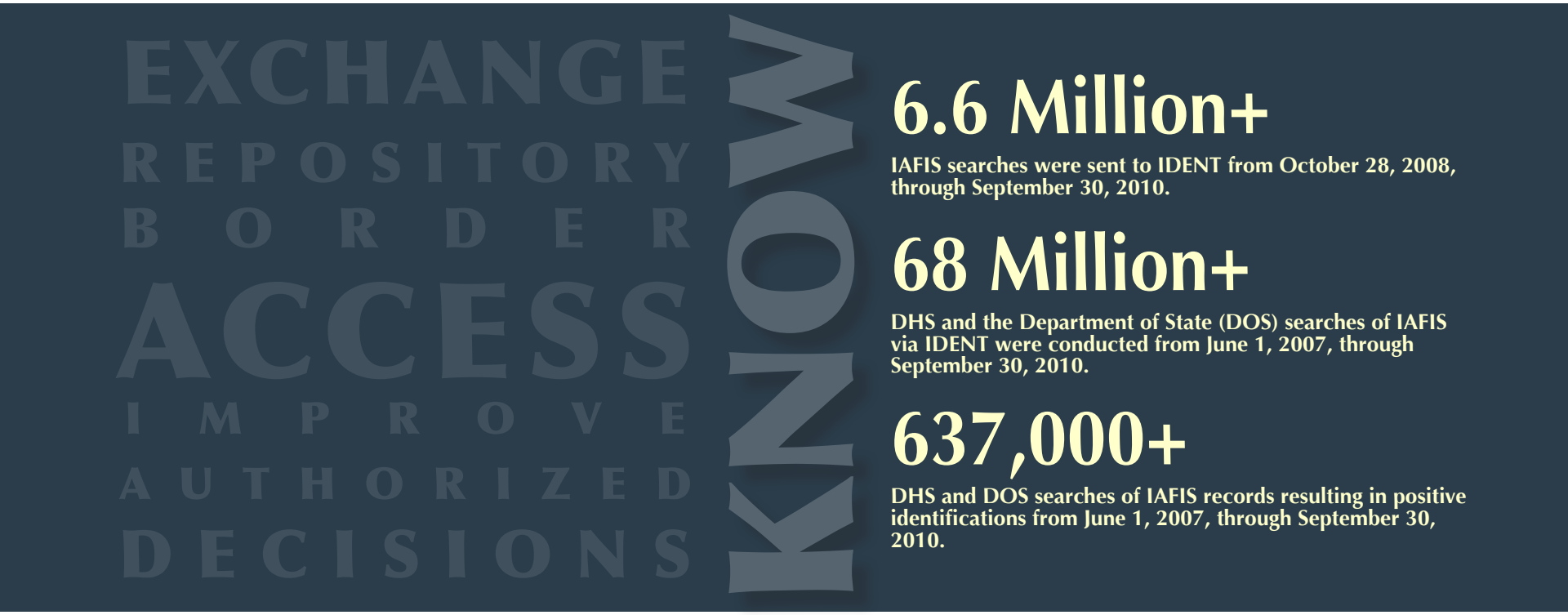
The results of Biometric Interoperability's collaborative efforts with the Secure Communities Program include the removal of 35,000 violent criminals from the United States since the program began in 2008. Secure Communities, a program of the Department of Homeland Security's (DHS's) Immigration and Customs Enforcement (ICE), uses the interoperability of the IAFIS and IDENT databases to accurately and efficiently identify criminal aliens who pose a significant threat to public safety.

For their efforts in building partnerships and providing resources to state and local law enforcement agencies through outreach, training and other collaborative support to enhance the identification of dangerous offenders, the Biometric Interoperability team received three awards in 2010:

- The CJIS Assistant Director's Award for **Excellence in Outstanding Contributions to Community Partnerships for Public Safety.**
- The DHS ICE Assistant Secretary's **Protecting the Homeland Award.**
- The Federal Executive Board's **Excellence in Government—Gold Team Award.**

IN ACTION

On June 6, the Newark Police Department (NPD) arrested a subject for possession of marijuana and drug paraphernalia. His fingerprints returned an IDENT/IAFIS response indicating



he provided an assumed name at booking and had previously been deported because of a lengthy criminal history in three states. He had prior convictions for burglary, carrying a concealed weapon, multiple drug-related crimes, and charges for criminal gang affiliation. In 1999, the suspect had attempted to enter the United States without inspection three times. He used aliases, claimed Mexican citizenship, and was allowed to voluntarily return to Mexico each time. In 2001, he was granted Temporary Protected Status (TPS) while using a different alias and claiming to be a citizen of El Salvador. In 2008, his re-application for TPS was denied because of criminal charges in Ohio. In January 2009, ICE deported the man to El Salvador. On June 7, the day after officers identified the subject as a convicted criminal alien, ICE reinstated his previous order of removal. The man is now being detained, awaiting deportation to El Salvador.

ACCOMPLISHMENTS

- **In September 2009, DHS deployed 10-print scanners to the Customs and Border Protection's primary processing lanes. Because of this update, IAFIS information is now available to DHS stakeholders via IDENT.**
- **FBI Special Agents using mobile fingerprint capture devices in selected domestic and remote locations now have access to the full IDENT and the Department of Defense's Automated Biometric Identification System (ABIS) database via the IAFIS.**
- **In 2010, jurisdictions submitting searches to IDENT via IAFIS grew from 88 to 658 in 32 participating states.**

Exploring new frontiers

We ensure the ongoing advancement of FBI identification services.

Identify

By combining the biometric expertise of the CJIS Division (fingerprint identification), the Laboratory (LAB) Division (DNA and latent fingerprints), the Operational Technology Division (facial image and voice identification), and the Special Technologies and Applications Office ([STAO] specialized technology), the FBI's Science and Technology Branch (STB) established the **Biometric Center of Excellence (BCOE).** The BCOE is the FBI's program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for integration into operations.

The STB formed the BCOE to focus on the FBI's overall biometrics agenda and develop partnerships within the biometric community. The BCOE fosters collaboration, improves information sharing, and advances the adoption of optimal biometric and identity management solutions within the FBI and across the law enforcement and national security communities. Since its inception in October 2007, the BCOE has used its partnerships with law enforcement, academia, and private industry to research and develop, test and evaluate, and promote standards for traditional biometric modalities as well as emerging capabilities (e.g., palmprints; iris; handwriting; and scars, marks, and tattoos recognition). The BCOE has also taken great measures to ensure valid legal approaches are used within these emerging technologies to protect the privacy rights of individuals. In addition, it has worked diligently to secure funding for these chosen initiatives.

The Biometric Steering Committee, a group of senior FBI leaders with expertise in biometrics, was created by the STB to guide the FBI's biometrics efforts; review policy, technical, and operational issues; and make recommendations. At this year's meetings (October 2009 and April 2010), the topics discussed included privacy issues, operational prototypes, technology, interoperability of systems, real-time biometric capture and identifications, finding fugitives and missing persons with facial recognition, and rapidly processing DNA in a booking environment.

BIOMETRIC
MANAGEMENT
PARTNERSHIPS
CENTER
MODALITIES
COMMUNITY
EXPERTISE
KNOW

31

BCOE sponsored biometric projects, 22 with federal agencies such as National Institute of Standards and Technology, Department of Defense, and Department of Homeland Security; and 9 with academia.

14

BCOE sponsored collaborative events with U.S. government agencies, industry, state and local agencies, and international law enforcement.

In February 2010, the BCOE launched an outreach campaign to determine how it can best support the operational activities of FBI Field Offices and Divisions at Headquarters. Following an initial written inquiry to the field concerning current biometric projects, capabilities, and needs, the BCOE staff visited 11 offices during the summer of 2010 for in-depth, facilitated discussions. In addition to educating the field on the FBI's current biometric systems and tools, as well as the capabilities being pursued today, BCOE staff tried to determine the biometric needs of the field as they relate to operational use. Another goal of the visits was to understand current biometric use in the field that may have broader application across the FBI. Information from the outreach campaign will help the BCOE ensure that staff in the field have knowledge of and access to the relevant biometric tools and technologies that can provide investigative leads and verify prosecutorial evidence.

The BCOE sponsored the establishment of the DNA Task Force to examine the feasibility of collecting and processing DNA within the criminal justice arena, specifically during the booking process. The DNA Task Force's first meeting was held in April 2010 with attendees from law enforcement as well as representatives from academia and industry. A second meeting followed in September 2010.

ACCOMPLISHMENTS

- **The STB formed the Biometric Steering Committee to direct the FBI's biometrics efforts.**
- **The BCOE surveyed and met with several FBI Field Offices to determine the current use and future needs of biometrics across the FBI, including Divisions at Headquarters.**
- **The BCOE sponsored the establishment of the DNA Task Force to advance the collection and processing of DNA for criminal justice use.**

On location

We identify criminals and terrorists across the globe.

Identify

During 2010, the global **Collections Program** undertook one of the most significant fingerprint collection operations in the Division's history. Nineteen agents and 3 support personnel took part in the Afghanistan Prison Biometric Project—fingerprinting prisoners and teaching guards how to take fingerprints in several Afghan prisons from February 19 to April 2.

The global Collections Program, which provides biometric-related support to national and international law enforcement, includes the Foreign Fingerprint Exchange (FFE), the Quick Capture Platform (QCP), the Flyaway Program, and other initiatives.

Through the **FFE**, the Division staff acquires, reviews, analyzes, and compares biometric samples and related information from foreign governments with data in the Integrated Automated Fingerprint Identification System (IAFIS). The Division also asks agencies in foreign countries for their biometric data and channels the information through the FBI's International Operations Division or Legal Attachés or the INTERPOL.

Front line investigators can glean tactical intelligence in real time through the **QCP**, which simultaneously queries the IAFIS, the Department of Homeland Security's IDENT System, and the Department of Defense Biometric Identity Management Agency's Automated Biometric Identification System. The QCP provides direct access to more than 181 million records and is invaluable in the investigation of known or suspected terrorists, transnational criminals, and illegal aliens. Because of its compact size—it weighs about 22 pounds and can fit into a backpack—it is often deployed to hostile environments and other remote areas.

The **Flyaway Program**, which provides critical on-site fingerprint identification to domestic and international law enforcement agencies, is comprised of 46 Division employees. Within 4 hours of a need arising, a team of seven members from the program can be deployed. Information gained from such on-site identifications is extremely important to national security and border protection.

356,608

Fingerprints collected via the FFE.

26

FFE missions conducted to collect fingerprints from foreign governments.

IN ACTION

From February 19 to April 2, the Afghanistan Prison Biometric Project collected 8,395 person-centric biometrics, including fingerprints from 7,220 prisoners in the Pul-e Charkhi, Saraposa, and Herat prisons in Afghanistan; fingerprints from 572 prison guards and staff; and conducted 603 background checks. The team also trained 50 prison guards on how to take clear and legible ink fingerprints. The team's efforts resulted in one match to a criminal history record in the United States, 12 latent matches, and 5,940 new records in the IAFIS.

In August 2010, the QCP was used in the arrest of two fugitives wanted for murder in Philadelphia, Pennsylvania. A tip brought agents to a house and upon entering the home, they encountered two individuals who did not have identification and provided false names. The first individual was fingerprinted, and the submission indicated that the individual was wanted. After further questions, the second individual gave agents his correct name; it was determined that the second individual was also wanted. Both were apprehended, and one of the suspects confessed to involvement in the murder.

ACCOMPLISHMENTS

- **16 FFE assessments of foreign national biometric capabilities and information sharing potential were conducted.**
- **Staff held 13 training sessions on collecting fingerprints in foreign countries.**
- **The global Collections Program staff hosted visits by delegations from Afghanistan, India, Indonesia, and Kazakhstan.**
- **Seven Flyaway on-site fingerprint identification missions were conducted in Afghanistan, American Samoa, New York, and as part of the FBI's hiring blitz.**

Pulling it together

We connect and identify . . . giving our partners the power to know.

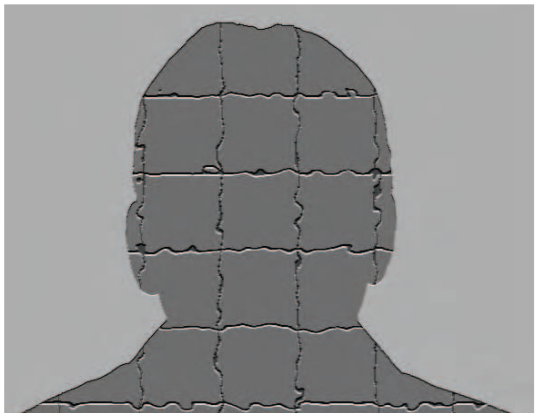
LAW ENFORCEMENT

CONNECT

INTELLIGENCE

IDENTIFY

NATIONAL SECURITY



KNOW

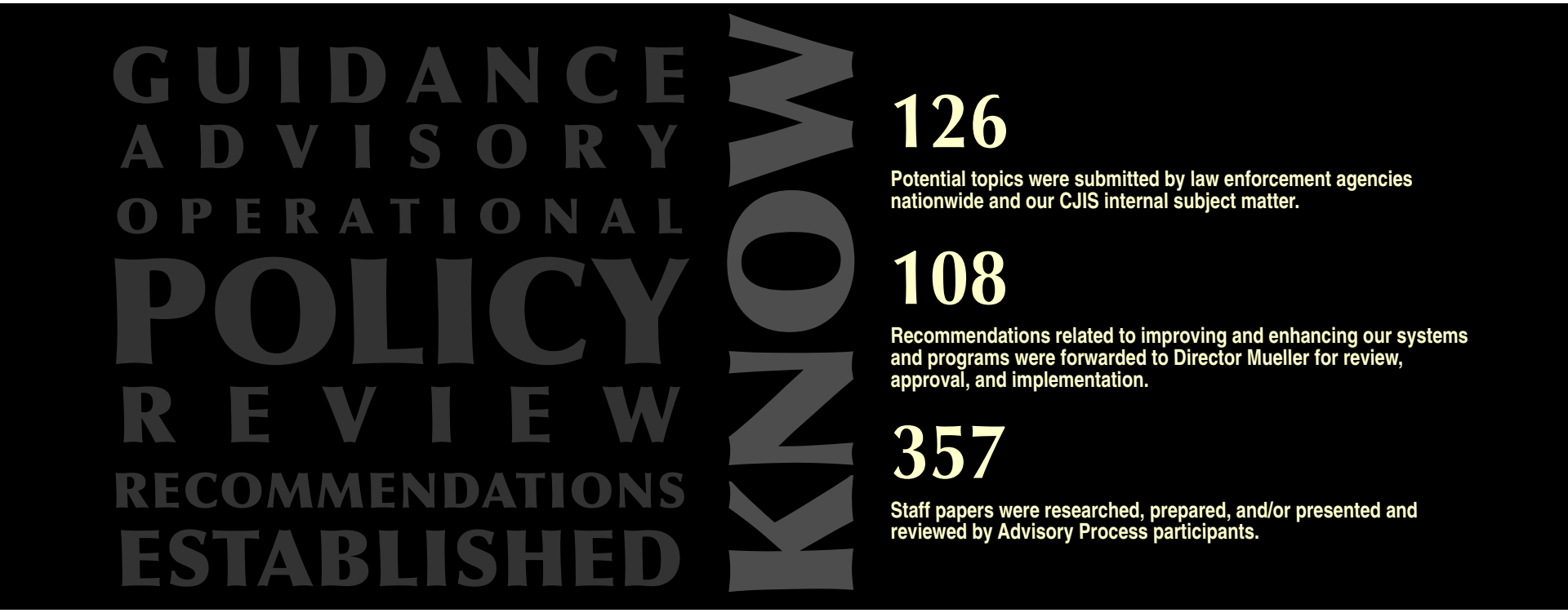
The advisory process

We partner with law enforcement to fight crime and prevent terrorism.

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

The process begins with the review of operational, policy, and technical issues by Working Group members representing all 50 states, U.S. territories, federal agencies, tribal agencies, and the Royal Canadian Mounted Police. This includes five Working Groups: North Central, Northeastern, Southern, Western, and Federal. Recommendations made by the Working Groups are forwarded to specialized Ad Hoc Subcommittees that are established to thoroughly review controversial policies, issues, and program changes and formulate alternatives and recommendations for the consideration of the entire APB. Currently, there are nine ad hoc subcommittees:

- Bylaws—responsible for evaluating proposed changes to the Bylaws for the CJIS APB and Working Groups and for recommending appropriate language with proper notice to the APB for approval.
- Identification Services—responsible for all projects related to the FBI's fingerprint identification programs/initiatives and the criminal justice use of criminal history information.
- Information Sharing—reviews and evaluates the development of the Law Enforcement National Data Exchange (N-DEx) Program.
- National Crime Information Center (NCIC)—addresses issues related to the NCIC Program.
- Public Safety Strategy—reviews issues being considered by the various APB Working Groups and subcommittees, topics, programs, and issues being addressed by other law enforcement professional associations/organizations, and current events in the criminal justice and information processing arena.



- Sanctions—responsible for evaluating the results of audits conducted of participants in CJIS programs.
- Security and Access—responsible for reviewing the hardware and software security policy for current CJIS Division computer systems as well as those systems under development and reviews issues regarding requests from agencies and organizations wanting access to information in CJIS programs.
- Uniform Crime Reporting—responsible for reviewing issues concerning the UCR Program, including Summary UCR, the National Incident-Based Reporting System, Law Enforcement Officers Killed and Assaulted (LEOKA), and Hate Crimes.
- Crisis Management—provides input to the FBI's Crisis Management procedures and the Operational Response and Investigative Online Network (ORION), which is sponsored by the FBI's Critical Incident Response Group (CIRG).

The final analysis and recommendations made by the Subcommittees, including commentary made at the Working Group meetings, are presented to the APB for final approval. APB members review and discuss all the material and provide final written recommendations, which can include alternatives not previously discussed to the FBI Director for final consideration.

ACCOMPLISHMENTS

Supported the APB with the:

- **Rewrite of the CJIS Security Policy.**
- **Addition of a seat on the APB for a Tribal Representative.**
- **Approved plan to make information from the National Instant Criminal Background Check System, regarding persons who have been denied the purchase of a firearm, available to law enforcement agencies through NCIC.**
- **Establishment of a policy whereby criminal history information corrected by the Office of Personnel Management (OPM) during background investigations can be used to post dispositions in CJIS and state repositories.**

The Compact

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

The **National Crime Prevention and Privacy Compact Act of 1998 (Compact**) provided for the establishment of the Compact Council, which administers access to criminal history record information for the purpose of screening an individual's suitability for employment, licensing, or placement in positions of trust. This type of access to criminal history record information is referred to as a "noncriminal justice purpose" and endeavors to enhance public safety, welfare, and security of the United States while recognizing the importance of individual privacy rights.

The national repository for sharing national criminal history information is the FBI's Interstate Identification Index (III), a major segment of the Integrated Automated Fingerprint Identification System (IAFIS). It was determined in the late 1970s that state criminal history records were more complete than records maintained by the FBI, in that the states may have additional arrest and disposition information within the state files, such as District Attorney records and court records. Because states had varying statutes or policies that restricted the dissemination of records for noncriminal justice purposes, it was determined a federal law, or Compact, was necessary to facilitate interstate criminal record dissemination authority. For this reason, on October 9, 1998, President Clinton signed into law the Compact.

Article VI of the Compact, required the formation of a 15-member Compact Council whose responsibility is to create policy and publish rules and regulations related to the noncriminal justice use of criminal history record information available through the III. The CJIS Division provides mission critical support to the Compact Council and serves as the location for the FBI's Compact Officer. The FBI's Compact Officer is responsible for ensuring that all agencies abide by the rules and regulations created by the Compact Council.

Once a state ratifies the Compact, it has the authority to share their state's criminal history record information (on an interstate basis) for all authorized purposes, including for noncriminal justice fingerprint-based background checks.

23,686,228

Background checks for screening an individual's suitability for employment, licensing, or placement in positions of trust.

29

States have ratified the Compact with the addition of Vermont in FY 2010.

14

Compact States are National Fingerprint File participants.

To date, 29 states have ratified the Compact with the addition of Vermont in FY 2010. As Compact states are able to implement the necessary technical and operational changes, they are required to participate in the FBI's National Fingerprint File (NFF) Program which ensures that the most comprehensive criminal history record information is provided for all noncriminal justice purposes. NFF states use their records to respond to the majority of criminal history requests (as opposed to the FBI maintaining and responding on behalf of the state). By 2011, 20 states are projected to be NFF.

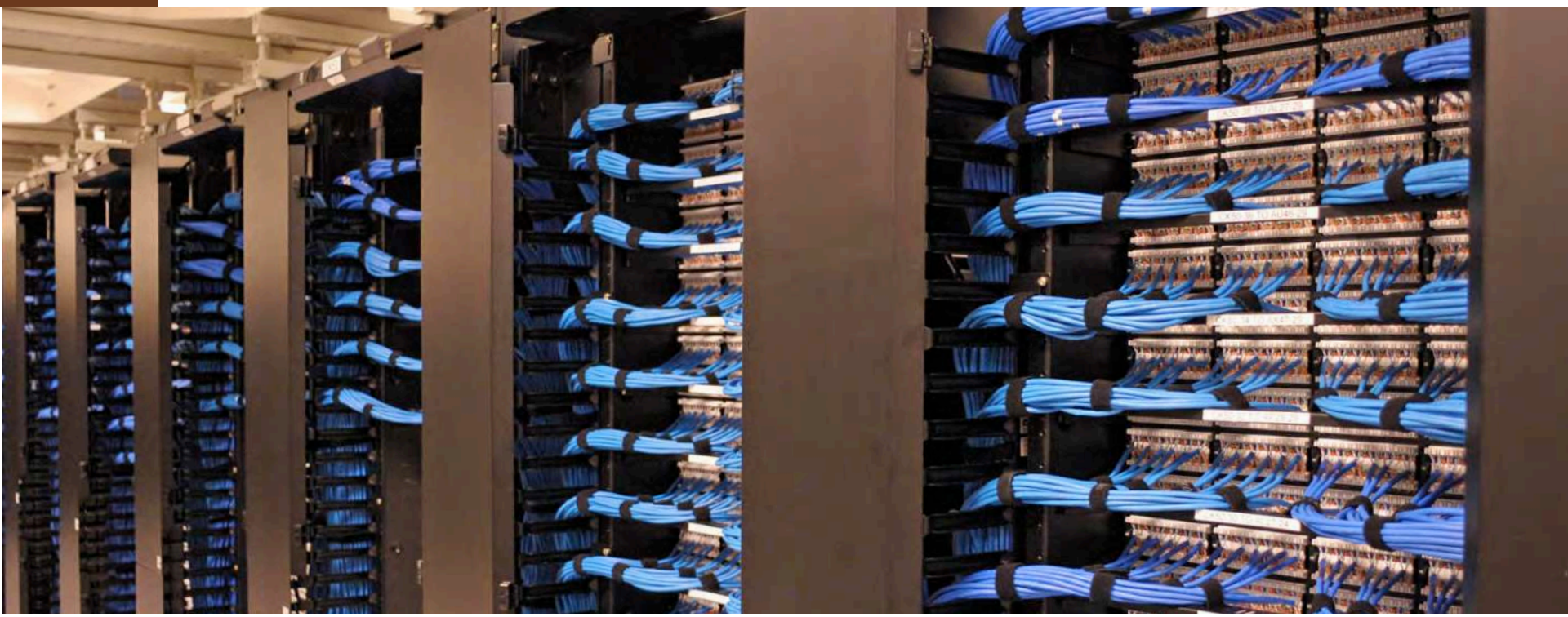
ACCOMPLISHMENTS

Supported Compact Council to:

- **Rename and repurpose the Standards Committee to the Standards and Policy Committee, which is responsible for assessing technical and performance standards and formulating policies, procedures, and rules.**
- **Rename and repurpose the Policy and Planning Committee to the Planning and Outreach Committee, which will update and monitor the Compact Council's Strategic Plan and bylaws and execute outreach initiatives to increase Compact ratification, NFF participation, and to expand the Compact Council's partnerships throughout the noncriminal justice community.**
- **Finalize a process for initializing federal noncriminal justice criminal history record checks of individuals who (when evacuated to a shelter during an existing or impending emergency or disaster) will have access to children, the elderly, or disabled persons (vulnerable populations).**

Enabling our services

We provide the technology to connect CJIS services across the globe.



Technology provides the backbone that enables CJIS to deliver its services to its customers in a timely and effective manner. With an ever-expanding need for rapid response times and an increase in processing capacity, CJIS operates the critical systems that support our Nation's efforts to fight crime and provide for the public's safety on a daily basis—365 days a year.

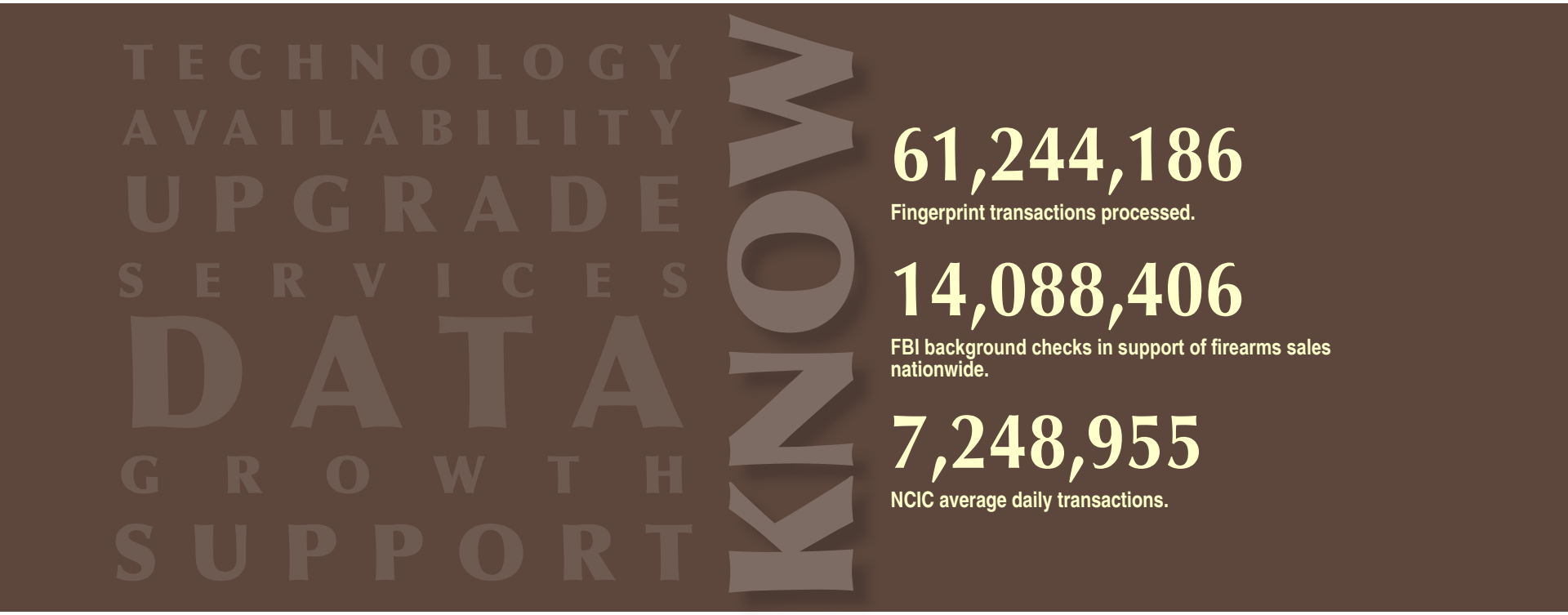
The **Integrated Automated Fingerprint Identification System (IAFIS)** continues to see a dramatic rise in fingerprint submissions as approximately 70,000–75,000 prints originate daily from Customs and Border Protection and 30,000 prints daily from the Department of State. The IAFIS, which averaged 80,189 receipts per day only three years ago, averaged 167,822 receipts per day in Fiscal Year 2010 and topped a record for outgoing responses of 297,816 on April 30, 2010. From April 28 through April 30, 2010, the U.S. Census Bureau submitted 324,710 fingerprint cards to ensure the suitability of candidates to serve as a Census Bureau employee during the recent U.S. Census. The IAFIS handled these Census Bureau submissions with no impact to other CJIS customers.

The CJIS IT infrastructure also provides the technology to support the growth in these other vital systems:

The **National Instant Criminal Background Check system (NICS)** completed 14,088,406 background checks in support of firearms sales nationwide.

The **National Crime Information Center (NCIC)** averaged 7.2 million transactions per day in Fiscal Year 2010 and set a new daily record of 9,121,887 transactions–8.09 percent higher than a year ago. Response times for the year averaged 0.0565 seconds, including 21 days in August with over 8 million transactions per day.

Given this high-tech infrastructure and the 1 million unique users of CJIS systems, CJIS, in cooperation with the Security Division, was asked to establish and operate the one of the



Department of Justice Trusted Internet Connections (TIC) after the Office of Management and Budget's launched a government-wide TIC Initiative in November 2007. The TIC's objective is to optimize and standardize Internet connections for the Federal government. Operating from the CJIS Data Center, the TIC serves as a centralized information security service for the national law enforcement community, providing improved secure information sharing capabilities, and ensuring the secure transmission of business data while monitoring and managing security from an enterprise level.

RESPONSE TIMES

IAFIS Criminal Fingerprint processing:
Goal 2.0 Hours; *Actual* 8 minutes, 42 seconds

IAFIS Noncriminal (Civil) Fingerprint processing:
Goal 24 Hours; *Actual* 55 minutes, 24 seconds

NCIC transaction processing:
Goal 2.0 Seconds; *Actual* 0.0565 seconds

NICS Immediate Determination Rate (IDR):
Goal Greater than 90 percent; *Actual* 91.36 percent

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

SYSTEM AVAILABILITY

IAFIS	**Goal 97.5 percent;**	**Actual 99.44 percent**
NCIC	**Goal 99.5 percent;**	**Actual 99.79 percent**
NICS	**Goal 99.5 percent;**	**Actual 99.79 percent**

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

Situated in Clarksburg, WV on nearly 1,000 rolling acres, the CJIS Division campus includes a Main Building, Service Center, The Lasting Impressions Child Development Center, Central Plant, and Visitor's Center. Looking forward, there is a new addition coming to the CJIS campus as the CJIS Division is partnering with the Department of Defense (DoD) to develop a new Biometrics Technology Center (BTC). This coexistence of the two federal agencies will provide a very unique collaboration between the FBI and the DoD to protect the United States while preserving civil liberties.

The BTC's artist rendering shown here is scheduled for completion in late spring 2014. The BTC 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; to house the FBI's Biometric Center of Excellence that will provide training, conference space, office and developmental facilities; and to accommodate joint biometric research and development effort between the FBI and the DoD. The BTC will be comprised of a main building consisting of 400,000 square feet of the CJIS Division space (roughly 3/4 the size of the current facility) and 60,000 square feet of DoD space.

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