



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



# CJIS ANNUAL REPORT 2014



# The CJIS Division Annual Report 2014

*“What we have accomplished together will ensure that those who stand to protect our nation are equipped with the best possible tools.”*



A handwritten signature in black ink, appearing to read 'S. Morris'.

**Stephen L. Morris**

*Assistant Director of the FBI's CJIS Division*

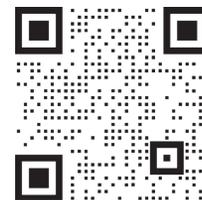
For me, returning in May 2014 to lead the Criminal Justice Information Services (CJIS) Division as Assistant Director has been “coming home.” Having served in two previous positions here, this proud South Carolina native has found a natural sense of belonging in the rolling hills and scenic beauty of north central West Virginia. Most of all, however, I am drawn to the strong sense of community shared by the people who live here, including the nearly 2,500-member staff of the CJIS Division. It is their pride in their work, and their dedication to the FBI’s mission, that makes our division successful in providing the vital criminal justice information that helps our partners solve and prevent crime and terrorism.

During fiscal year 2014, CJIS Division staff improved and expanded services across the board, most notably launching the full capabilities of the Next Generation Identification system. With this, the FBI completed a giant leap forward in its ability to aid law enforcement in identifying criminals and investigating and solving crime, furthering the FBI’s extraordinary leadership in the area of biometric identification. The entire division, our stakeholders, and the customers we serve, share in this accomplishment, as we are all interconnected. We also owe a debt of thanks to the visionaries, developers, and leaders who came before us and helped set us on this successful path.

Just as I am appreciative of the community surrounding me here in West Virginia, I am also appreciative of those who are part of our extended CJIS Division community—our users, our counterparts in states and other federal agencies, and our advisory groups, including the members of the council administering the National Crime Prevention and Privacy Compact, and the CJIS Advisory Policy Board, which celebrated its 20th anniversary this year. This edition of the *CJIS Annual Report* showcases the results of our collaboration. What we have accomplished together will ensure that those who stand to protect our nation are equipped with the best possible tools.

# Contents

National Crime Information Center <i>NCIC continues to change how criminal justice information is shared</i>	4
National Instant Criminal Background Check System <i>E-Checks continue to grow as process improves</i>	6
National Data Exchange <i>Increase in agencies participating helps investigators make connections</i>	8
Law Enforcement Enterprise Portal <i>Providing a gateway to a myriad of services</i>	10
Uniform Crime Reporting Program <i>With expanding data collection, UCR continues to provide a national perspective of crime</i>	12
Next Generation Identification <i>Managing the world's largest repository of biometric and criminal history information</i>	14
Biometric Identification Services <i>Continuing to expand the biometric frontier</i>	16
FBI Biometric Center of Excellence <i>Exploring new and enhanced biometrics</i>	18
CJIS Intelligence Program <i>Gathering, analyzing, and developing raw data to produce identity intelligence</i>	20
Global Operations <i>Identifying criminals and terrorists across the globe</i>	21
Public Access Line <i>A single point of contact for crime tips</i>	22
CJIS Information Technology <i>The backbone of the criminal justice services the CJIS Division provides</i>	23
CJIS Advisory Policy Board <i>Marking 20 years of collaboration</i>	24
Compact Council and CJIS Field Coordinators <i>Working together toward common goals</i>	26
Our Campus <i>Where connections and identifications generate the power to know</i>	28



Scan this QR Code with your smartphone to learn more about the FBI's 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](http://www.fbi.gov/about-us/cjis).

# National Crime Information Center

*NCIC continues to change how criminal justice information is shared*

In January 1967, the **National Crime Information Center (NCIC)** went online for the first time and forever changed the way that law enforcement shared information. With five files and 95,000 records, it was the start of agencies in all 50 states communicating what they know in a centralized, computerized location. Today, the NCIC has 21 files of information—covering a wide array of categories including wanted persons, persons who pose a threat to safety, stolen vehicles and property, and identity theft. These files contain more than 12.2 million records. In the last decade alone, the NCIC has provided investigative services that have resulted in nearly 114,000 arrests and more than \$3 billion in property recoveries. In July, the NCIC set a new record by processing 14,618,589 records in a single day—that’s a transaction every 0.0182 seconds.

## THE YEAR IN REVIEW

Since that beginning nearly 48 years ago, the NCIC has become a fundamental tool in police work in the twenty-first century. The NCIC is used by not only law enforcement officers, but judges, prosecutors, correction officers, court administrators, and a variety of criminal justice officials in performing their daily duties. Since the NCIC is a vital cog in the investigative and criminal justice machine, the stewards of the system are keenly aware of the need to constantly refine and improve it to meet the needs of modern policing and criminal justice agencies. Monthly maintenance and a system enhancement in 2014 provided ongoing tweaks to the system to ensure

constant availability and to improve response time. Mobile access to NCIC Wanted, Vehicle, Gun and Article files for federal agencies—currently the FBI and U.S. Marshals Service have access—pare poised to expand to a wider federal clientele. NCIC staff is planning to provide mobile access to the Bureau of Alcohol, Tobacco, Firearms and Explosives and AMTRAK in 2015.

Still, even with continual building and upgrading, it has been 15 years since the last major overhaul of NCIC. With an eye to the future, the management team of NCIC has started preparing for the next major revamp that will produce NCIC 3<sup>rd</sup> Generation, or N3G.

In deciding how to upgrade a criminal justice staple like the NCIC, the FBI realized it couldn’t make decisions in a vacuum and build what developers “think” the user might need. No one knows better what works in the NCIC and what could be improved—as well as what needs to be added—than the day-to-day user of the system. In fiscal year 2014, the staff of NCIC completed the N3G Requirements Canvass with

its federal partners and in 2015 they will complete dialogues with state and local criminal justice partners about what they would like to see in improved with the current NCIC system.

Also in 2015, NCIC efficiency will benefit from the CJIS Information Broker (CIB), a new, developing tool that will provide innovative methods for exchanging timely, accurate,

“With an eye to the future, the management team of NCIC has started preparing for the next major revamp that will produce NCIC 3<sup>rd</sup> Generation, or N3G.”

and relevant criminal justice information among local, state, tribal, and federal law enforcement agencies, as well as other criminal justice agencies. The CIB will improve the CJIS Division's process performance, enhance technical capabilities for information sharing, and reduce turnaround time for CJIS products and special requests for information. CIB Increment 1 (anticipated to be fully operational in spring 2015) will move NCIC extract management from the NCIC operational environment to the CIB.

### **NCIC IN ACTION**

Beginning in January 2014, the FBI has been contacted periodically by the Lancaster (Nebraska) Police Department (LPD) to run NCIC off-line searches on multiple suspects in an ongoing drug investigation. (An off-line search scours current and older NCIC records and matches persons and license plates to traffic stops and other interactions with law enforcement.) Off-line search results revealed travel patterns and pinpointed suspect locations at specific times, all of which were crucial to the LPD's investigation. The investigation that the off-line searches supported has so far resulted in confiscation of approximately \$2 million in currency, 68 pounds of marijuana (with an estimated street value of \$200,000), and 16 pounds of methamphetamine (with an estimated street value of \$260,000). In addition, 23 suspects have been arrested in connection with this major drug operation.



**Lynda G. Lovette** is the NCIC Terminal Agency Coordinator for one of the nation's largest municipal police agencies, the Baltimore City Police Department. She said that the NCIC system proves its value to Baltimore's officers every day. "When I talk to patrol officers, they express that NCIC is a timely and effective tool for them on the street," she said. "They appreciate the mobility and accessibility of the database as they are able to access real-time information with images when needed." Lovette said the system never fails to provide reliable, fast responses. "We depend on it every day, and it works," she said, "I can't put it any simpler than that. It works."

# National Instant Criminal Background Check System

## *E-Checks continue to grow as process improves*

Sixteen years after its development pursuant to the Brady Handgun Violence Prevention Act of 1993, the **National Instant Criminal Background Check System (NICS)** continues to provide immediate determinations of whether the receipt of firearms by prospective gun buyers will violate state or federal law. The NICS is a cooperative effort of the FBI; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Justice; and local and state law enforcement agencies. It provides a variety of important services, such as efficient, final determinations for firearm background checks; appeals service; automated background checks through the NICS E-check; and promotion, training and support to point-of-contact (POC) states, NICS Index contributors, Federal Firearm Licensees (FFLs), and state, tribal, and federal law enforcement.

### **THE YEAR IN REVIEW**

In fiscal year (FY) 2014, the NICS Section exceeded its mandated 90-percent immediate determination rate (eligibility determinations made while the FFL is on the telephone) with a rate of 91.32 percent. Also, the NICS Section continued to refine the NICS E-check, which enables FFLs to conduct unassisted NICS background checks via the Internet. The FFL electronically enters the prospective firearm buyer's descriptive data directly into the NICS and initiates the search process. As a direct result of input from users, several enhancements were added in 2014 to improve the FFL experience. For example, a link was provided that allows easy transitions to secondary accounts, which means an FFL doesn't need to exit E-check to log into another account. (This is a great time-saver for corporate-level employees who are monitoring activity in various stores.) Other enhancements included adding the FFL ID,

address, and user ID to the user interface; providing a countdown of the number of days until password expiration; and more flexible report capabilities. The ability of the FFL to view expiration dates (a firearm background check is only valid for 30 days) was also added. This gave FFLs the capacity to notify their customers prior to the expiration of the NICS transaction.

Because of funding limits during the government's sequestration at the beginning of FY 2014, the NICS Section explored alternate training methods that would not require employees to travel as extensively as they had in the past. Staff identified Lync Online as a viable distance learning option, and created a limited number of Lync training sessions in 2014. The NICS Section also established a "train-the-trainer" initiative in which it offers POC states the opportunity for the FBI to train a designated trainer who will ultimately handle training within their state. This not only cuts down on travel costs for the FBI but enables the states to be in control of scheduling their own NICS training. To date, four states have committed to the "NICS Train-the-Trainer" concept.

Looking ahead to 2015, NICS will continue to improve with the scheduled launch of the "New NICS" in April. The first phase of New NICS will bring several enhancements that will:

- enable the FBI to adapt and make future NICS changes more nimbly.
- allow more efficient and effective use of NICS workforce expertise.

- provide the technical capability to remain operational and process NICS transactions 24/7 (currently there is nightly required downtime for “batch” maintenance routines).
- provide an enhanced name search/match algorithm.

### **NICS IN ACTION**

On February 24, a NICS examiner processed a transaction for an FFL (a pawn shop in Jonesboro, Georgia) for a handgun purchase. The NICS examiner identified a warrant in the National Crime Information Center (NCIC) and a Georgia state record with descriptive data matching the buyer. A review of the state record showed arrests for drug violations and disorderly conduct and a December 2013 conviction for misdemeanor marijuana that disqualified the individual from purchasing a weapon. The NCIC record contained a warrant (issued the day before the attempted purchase) from the DeKalb County (Georgia) Sheriff’s Office for murder/homicide. The NICS examiner called the sheriff’s office to verify the warrant was active and that the agency was interested in apprehending the individual. Based on the active warrant and the recent drug conviction, the examiner provided the FFL with a deny status and forwarded all information about the incident to the wanting agency. Subsequently, the NICS learned the subject’s warrant was a result of a fatal shooting at a local nightclub that occurred on February 23. The individual was arrested on February 25 as a result of the NICS check.



**Kathy Witt** serves as the Sheriff of Fayette County, Kentucky, and has devoted much of her 31-year law enforcement career to strengthening domestic violence laws in her state. She said the FBI’s NICS Program makes a great contribution to public safety and the law enforcement community by helping to keep firearms out of the hands of those who are prohibited from having them. “The NICS Index alone provides valuable information for making a determination for firearms that wouldn’t be available for review otherwise,” she said, citing the system maintained by NICS with disqualifying information on individuals that may not be available through the NCIC or other criminal justice information systems. “NICS has experienced tremendous success in making strides to increase data available to FFLs and law enforcement.”

Recently, Witt was able to tour the NICS Section at the CJIS Division and see staff of the call center interact with FFLs. “I am really proud of the work they do and how committed they are to excellence in meeting their mission,” she said.

# National Data Exchange

## *Increase in agencies participating helps investigators make connections*

The **National Data Exchange, or N-DEX**, is the only national investigative information-sharing system enabling local, state, tribal, and federal criminal justice agencies to search, link, and analyze information across jurisdictional boundaries. Records in N-DEX span the criminal justice lifecycle, including information related to cases, arrests, missing persons, service calls, bookings, holdings, incarcerations, pre-trial and pre-sentencing proceedings, warrants, supervised releases, citations/tickets, and field contacts/field interviews. All of this information promotes safety at an initial patrol stop, during the effective supervision of an offender, and in the efforts to promote victim safety.

The N-DEX connects many regional and local information-sharing systems and leverages their collective power to provide access to more than 228 million records from over 5,000 agencies. N-DEX connects users to a number of federal agencies in addition to the FBI, including the Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); U.S. Marshals Service; the Department of Defense; and the Department of Homeland Security.

By using N-DEX and the system's straightforward search technology, users can detect relationships between people, crime characteristics, property, and locations. N-DEX can eliminate information gaps and identify victims and aggregate losses by "connecting the dots" between seemingly unrelated information. It can also deconflict investigations and promote collaboration among participating agencies across the nation. During fiscal year (FY) 2014, N-DEX made a number of significant enhancements to the system, including updates to search

features. Users now have additional search customization options, and searches of names are made more expansive by automatically including similar names. Simple searches now include a response of "suggested searches," providing a rephrasing of queried terms using synonyms and similar phrases to offer a potentially more productive search.

As the technology of N-DEX continues to advance, so does the scope of information available to users. N-DEX staff and Regional Information Sharing Systems (RISS) officials crafted an implementation plan for N-DEX access via RISSNET, RISS's secure cloud service, which contains sensitive but unclassified law enforcement information. The service is supported nationwide by six regional centers and reaches more than 9,000 agencies and 120,000 users.

### **THE YEAR IN REVIEW**

During FY 2014, N-DEX experienced a 7 percent increase in the number of searchable records, a nearly 20 percent increase in the number of contributing agencies, and more than a 60 percent increase in the number of total system searches. N-DEX becomes an even more valuable tool as more agencies and organizations provide access to data. For instance, a case study demonstrating the usefulness of N-DEX was conducted in a region where a significant number of agencies make their records available to the system. One participating agency selected some active cases and used N-DEX to conduct searches on various entities within the cases. Previously-known information was searched, such as names, addresses, license plates, phone numbers, and makes and models of vehicles. The N-DEX searches were immediately successful in providing additional leads and corroborative investigative information.

Also in FY 2014, N-DEX implemented an award program for the “Success Story of the Year” in an effort to identify and highlight the efforts of criminal justice agencies to enhance public safety and reduce crime through effective information sharing. This program showcases situations in which N-DEX information made a significant contribution to investigations or for which prosecutorial or preventive actions have taken place in the last two years. The first winning submission will be recognized in FY 2015.

### **N-DEX IN ACTION**

- N-DEX was used to locate information and possible leads for a Department of State (DOS) most wanted fugitive investigation. Using simple name and alias searches, the investigator discovered substantial material relating to a mortgage fraud investigation involving the fugitive’s brother, sister, and other closely-related associates. The case reports made a significant number of connections relevant to the investigation, demonstrating the depth and breadth of the subject’s scheme. The investigator indicated that this “wholly reduced the amount of time and manpower energy which would have otherwise been required to ascertain the same information previously reported.”
- An analyst assigned to a Social Security Fraud and Disability Task Force was investigating an individual for possible Social Security disability fraud. The subject of the investigation was receiving Social Security benefits after claiming a disability. The analyst conducted a person search of N-DEX and was able to locate an ATF case report involving the subject’s arrest for transporting stolen firearms. The analyst contacted the ATF case agent and was told that the subject was operating a business in which he was paid in marijuana for stolen firearms. This information helped the task force in its fraud investigation.



**Scott D. Edson**, Commander of the Los Angeles County Sheriff’s Department, sees the development of the N-DEX system as a great example of collaboration between the FBI and the law enforcement and criminal justice investigators who use the system. “The N-DEX program has been requirements-driven since the beginning,” he said.

“The FBI sought input from local, state, and federal agencies, and this has resulted in an excellent system.” Edson said the N-DEX has broken down significant barriers to information sharing between agencies, something that has been a challenge. “We have learned that we must share the kind of information that N-DEX handles, the incident reports that list the people, places, and types of things that can be valuable to the cop on the street, crime analysts, and investigators.”

Edson said the ability of N-DEX to not only accept individual agency data, but also tap into state and regional information sharing systems makes it even more powerful. “There are thousands of agencies in the system, and while there are many more to go, N-DEX has the potential to link all incident-based information among all law enforcement,” he said. “More information leads to knowledge-based policing, which leads to safer communities across the nation.”

# Law Enforcement Enterprise Portal

*Providing a gateway to a myriad of services*

Just as a mall has a myriad of stores available to shoppers, the **Law Enforcement Enterprise Portal (LEEP)** encompasses a variety of services available to law enforcement agencies and our criminal justice partners. The LEEP is a secure gateway that provides law enforcement agencies, intelligence groups, and criminal justice entities with a way to meaningfully exchange facts, leads, news, and intelligence as well as a way to strengthen case development.

## THE YEAR IN REVIEW

In fiscal year (FY) 2014, seven agencies (and their subagencies), known as Identity Providers, partnered with the LEEP to give their employees access to LEEP resources: the Los Angeles Joint Regional Intelligence Center, the Maryland Department of Public Safety, the Minnesota Bureau of Criminal Apprehension, iGuardian, the South Carolina Law Enforcement Division, South Sound 911 from Washington State, and the Randall County Sheriff's Office in Texas.

Also, in FY 2014, the LEEP added seven new services: the Critical Incident Planning and Mapping System (CIPMS)-

Rapid Responder, eGuardian, iGuardian, the Active Shooter Special Interest Group, the Repository for Individuals of Special Concern (RISC), the Virtual Academy, and Malware Investigator.



- The CIPMS, a mapping system that provides information to first responders in Washington State, is a program of the Washington Association of Sheriffs and Police Chiefs. While the system is available only to personnel in Washington State, all providers have access to its informational page.

- eGuardian is a system that supplies law enforcement, law enforcement support, and force protection personnel with the ability to report,

track and share information about threats, events, and suspicious activities with an eye toward terrorism, cyber, or other criminal activity.

- iGuardian is a portal developed for partners working within critical telecommunications, defense, banking and finance, and energy infrastructures and is available over the sensitive but unclassified InfraGard network.

- The Active Shooter law enforcement source page contains training and informational videos, resources for victims, information about legislation, and news pertaining to active shooter incidents.
- The RISC service page provides the RISC Implementation Guide, a map of participating states, and other pertinent information about the RISC. (The RISC provides a rapid, mobile biometric search of “high value” subjects—such as wanted persons with FBI numbers or National Sexual Offender Registry individuals—from various files within the NCIC.)
- The Virtual Academy is the FBI’s enterprise training system and provides the FBI’s criminal justice and intelligence partners with access to all FBI training.
- The Malware Investigator is an automated system that analyzes suspected malware samples and quickly returns technical information. It combines dynamic and static tools to assess how the samples interact within various types of host environments and allows users to correlate samples and collaborate with others to connect cyber events. The Malware Investigator is available to all LEEP users.



In 2014, the LEEP focused on highlighting two of its most used services—Virtual Command Centers (VCCs) and Special Interest Groups (SIGs). VCCs provide secure monitoring of high-profile events and law enforcement operations. SIGs serve as “communities” where personnel can access, share, or store data within particular groups. In the future, VCCs

and SIGs will be easier to find, as their respective icons will be added to allow users to access them more quickly and with fewer mouse clicks. Also, in 2014, a new tool, known as TRAX, was added to the VCC application. TRAX provides a way for tracking large numbers of arrests and search warrants.

With an eye to the future, the LEEP is adding an industry portal, iLEEP, for our partners in agriculture and food, banking and finance, energy, and other infrastructures. The iLEEP will partner with InfraGard; anyone with an InfraGard account will have access to the iLEEP. It is expected that services will include CyberHood Watch (which enables sharing of cybersecurity and intrusion information and includes access to iGuardian) and Malware Investigator.

Also in 2015, the LEEP is planning to implement a video conferencing tool, similar to a virtual meeting application, and to add services such as eLab, a laboratory information system which will provide evidence tracking capability; the Child Exploitation Tracking System, or CETS, a case management database of on-line child exploitation; and the National Domestic Communications Assistance Center, which will facilitate the sharing of electronic surveillance knowledge.

#### **LEEP IN ACTION**

On September 26, two Gwinnett County (Georgia) deputies were answering a suspicious person call. The subject of the call was apprehended, but he had no identification. A mobile ID unit was used to take the subject’s prints. Within two minutes the RISC response, in conjunction with the Georgia RapidID, revealed two active warrants: one for probation violation from the city of Duluth and one for a probation violation from the Gwinnett County Sheriff’s Department.

# Uniform Crime Reporting Program

*With expanding data collection, UCR continues to provide a national perspective of crime*

The **Uniform Crime Reporting (UCR) Program** has expanded in size, scope, and significance since its inception more than eight decades ago. With the participation of more than 18,000 agencies nationwide, the FBI's UCR Program provides crime statistics for use in law enforcement administration, operation, and management. These statistics are shared annually in four high-profile reports which include *Crime in the United States*, a comprehensive collection of crime offenses, clearances, arrests, and police employment information; *Hate Crime Statistics*, a report focused on bias-motivated crimes; *Law Enforcement Officers Killed and Assaulted (LEOKA)*, a statistical perspective detailing information on local, state, tribal, and federal law enforcement officers killed and assaulted in the line of duty; and NIBRS, a compilation of data from the National Incident-Based Reporting System.

## THE YEAR IN REVIEW

In fiscal year (FY) 2014, the FBI continued to modernize the UCR's crime data collection and reporting systems through the New UCR Project. Ongoing testing of the new system will ultimately improve its efficiency, usability, and sustainability. In addition, the UCR Program exceeded its initial goal (75 percent) of reducing paper submissions by seeing a 91.74 percent reduction of paper forms received.

Last year, the UCR Program began accepting data from agencies using an updated definition of rape. Prior to 2013, the UCR Program collected rape data in the Summary Reporting System as "forcible rape." The "legacy" definition included only rapes committed against women. The "revised" broader definition removed reference to gender.

In 2014, for the first time, *Crime in the United States* was prepared using data from both the revised and legacy definitions of rape.

Human Trafficking data will be published for the first time in 2014. The UCR Program began collecting this information in 2013 in order to comply with the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008.

Changes also took place in the UCR Program's Hate Crime data collection, which published for the first time data concerning gender and gender identity biases. The Hate Crime Statistics Program also broadened its collection to include an Anti-Arab bias motivation and seven additional religious bias motivations. The new religious bias types include Anti-Mormon, Anti-Jehovah's Witness, Anti-Eastern Orthodox, Anti-Other Christian, Anti-Buddhist, Anti-Hindu, and Anti-Sikh. The program is on track to begin data collection for these added biases in early 2015.

The UCR Program's LEOKA Program continued its collaborative efforts to offer safety education to law enforcement personnel. More than two decades ago, the LEOKA Program partnered with the FBI's Critical Incident Response Group and the Behavioral Research and Instruction Unit (BRIU), and is now working on their fourth special research project. This multi-year study focuses on felonious killings and assaults of law enforcement officers during ambush situations. The LEOKA/BRIU team identified approximately 80 ambush cases to be used for the research project. In FY 2014, team members interviewed 31 victim officers and 24 offenders involved in these incidents in

order to gain insight into ambush incidents. The findings from this study, *Ambushes and Unprovoked Attacks: Assaults on our Nation's Law Enforcement Officers*, will be available upon publication to law enforcement executives, officers, and trainers. In FY 2014, the LEOKA Program staff published 11 officer safety articles on the Law Enforcement Online "Highlights" page at <www.leo.gov>. Selected articles were also published monthly in a dedicated "Officer Survival Spotlight" section of the *FBI Law Enforcement Bulletin* (<www.leb.fbi.gov>) as well as the FBI National Academy Association's bi-monthly magazine, *The Associate*. With these publications, the LEOKA Program now reaches national and international audiences of more than 3.1 million people.

## UCR IN ACTION

James Young has been involved in law enforcement for 34 years: first, as a deputy sheriff in Maryland and currently as deputy director of the South Maryland Criminal Justice Academy. Mr. Young attended a LEOKA Officer Safety Awareness Training (OSAT) held at the Maryland Fire and Rescue Institute in College Park, Maryland. When the LEOKA instructor asked the class if anyone's agency had conducted foot pursuit training, only two hands went up, and Mr. Young's was not one of them. Mr. Young said the subject hit close to home for him because a close friend of his was killed in the line of duty during a foot pursuit. After attending the OSAT class, Mr. Young decided two things, (1) he was going to institute foot pursuit training at his academy, and (2) he was going to have the LEOKA Program train the entry level recruits in his agency. In the subsequent 2 years, his vision became a reality. Now, when asked who has completed foot pursuit training, 363 officers from 6 agencies in Maryland can raise their hands.

The image displays a collage of materials related to the FBI's Uniform Crime Reporting (UCR) program. At the top is a screenshot of the FBI's UCR website, featuring the FBI logo, navigation menus, and a section titled "Uniform Crime Reports". Below this is a circular logo for the UCR program. The main text on the website screenshot describes the UCR program's history and purpose, stating it was established in 1930 to provide reliable crime statistics for the nation. It also mentions that the program is supported by the FBI's UCR Program for more than 20 years.

Overlaid on the website screenshot are three reports:

- CRIME in the United States 2013**: A report titled "About Crime in the U.S. (CIUS)" which provides information by region, by state, by local agency, and by offense known to law enforcement. It includes sections for "Persons Arrested", "Police Employee Data", "Caution Against Ranking", "Hate Crime Statistics", and "Law Enforcement Officers Killed and Assaulted".
- 2013 Hate Crime Statistics**: A report titled "About Hate Crime Statistics, 2013" which provides information on hate crimes, including a table of statistics and a section on "Additional Data Collections".
- 2013 Law Enforcement Officers Killed & Assaulted**: A report titled "About Law Enforcement Officers Killed and Assaulted, 2013" which provides information on officers killed and assaulted, including a table of statistics and a section on "Additional Data Collections".

# Next Generation Identification

*Managing the world's largest repository of biometric and criminal history information*

The **Next Generation Identification (NGI) System**, which expanded and significantly enhanced the FBI's biometric identification capabilities, became fully operational near the end of fiscal year 2014, providing the criminal justice community with the world's largest and most efficient electronic repository of biometric and criminal history information. The NGI system replaced the Integrated Automated Fingerprint Identification System, which came online in 1999 and revolutionized the processing of fingerprints. The NGI system will further evolve law enforcement's use of biometrics for identification, investigative, and notification purposes.

Developed and implemented in incremental stages, NGI has provided many enhancements to automated fingerprint and latent searches over the past 4 years. For example, the Advanced Fingerprint Identification Technology, deployed in early 2011, increased automated fingerprint identification accuracy to 99.6 percent with its new algorithms. Late summer of 2011 introduced the capability for mobile fingerprint searches of the Repository for Individuals of Special Concern (RISC). The NGI RISC rapid search, with response times of less than 10 seconds, offers additional officer safety and situational awareness by providing on-scene access to a national repository of wanted persons, convicted sex offenders, and known or suspected terrorists.

As part of the increment deployed in the spring of 2013, latent print searches became three times more accurate (from 26 percent to 82 percent) with NGI's new algorithms, and reduced the number of searches required to access the entire gallery of fingerprint images. Also, additional types of fingerprint searches, including civil and RISC submissions,

are now run against the Unsolved Latent File. This has generated thousands of new leads that previously were not available. This increment also delivered the new National Palm Print System, providing the capability to receive palm prints and major case prints. The ability to search latent palm prints against a national repository of known palm prints has enormous potential to identify new leads and close cold cases, since a significant number of latent prints left behind at a crime scene are from the palm.

## THE YEAR IN REVIEW

On September 7, the final increment in the NGI's development achieved full functionality and added several important new services. The Rap Back service allows authorized agencies to receive notification of activity on individuals who hold positions of trust (e.g. school teachers, daycare workers) or who are under criminal justice supervision or investigation. As the NGI system went fully operational, the Interstate Photo System (IPS) was also introduced. The IPS, through Facial Recognition, now provides a way to search millions of criminals' photos—data the FBI has collected for decades—and generates a list of ranked candidates to be used as potential investigative leads by authorized agencies, adding another way biometrics can be used as an investigative tool. Another service, text-based searches for images of scars, marks, and tattoos, was also a part of the increment.

With all the improvements the NGI system has delivered for biometric identification in the last 4 years, one of its greatest achievements is the ability to add future biometric modalities. Up next is an internal exploration to develop a system capable of performing iris image enrollment

and recognition services. The Iris Pilot (IP) is evaluating technology in an operational setting while attempting to answer the challenges of using the technology in a large-scale law enforcement environment. The pilot has begun building a criminal iris repository which can be searched to provide identification responses. The pilot will also be used as a means for assessing best practices for iris image capture, iris camera specification requirements, specifications for iris image compression, and a review of new and existing iris image quality measurements.

### NGI IN ACTION

On February 9, 1997, the body of an unidentified female was found near a stream in a Midwestern state. The woman had been sexually assaulted and asphyxiated with a small black plastic bag. Authorities developed latent print evidence from the plastic bag and forwarded that evidence to their state Bureau of Investigation and to agencies in surrounding states to be searched against their Automated Fingerprint Identification Systems. No matches were found at that time. In February 2014, the latent fingerprints were resubmitted and searched against the NGI. This resulted in a new investigative lead and the arrest of a 36-year-old male who was not previously a suspect in the case.

On January 14, 1997, biometrics of an unknown deceased male, who had been found with gunshot wounds and whose body had been set on fire, were collected and searched, yielding no results. On March 15, 2014, the state's Bureau of Identification resubmitted the biometrics to the NGI, which returned possible candidates. As a result, an identification of the victim was made and law enforcement authorities are now investigating new clues concerning a suspect or a motive.



As Deputy Assistant Director of the Law Enforcement Support Division for the Texas Department of Public Safety, **Michael C. Lesko** has watched each increment of NGI bring improved biometric capabilities to the FBI's services. "One of the first things NGI brought to users was the increase in the quality of the algorithm used to match fingerprint submissions to prints in the system, which helped increase the accuracy of the searches we ran," he said. "There is also an increase in accuracy on the latent side, and we're seeing a lot more cases solved."

Of the services deployed with the latest increment of the system, Lesko said NGI's Rap Back will be of great benefit to users in Texas and around the country. "We have had state Rap Back in Texas for years," he said, "But if we had a subject, like a parolee, who went out of state and was arrested, we had to rely on the person to self-report this arrest. Now, the federal Rap Back will report that back for us." He said there will be similar advantages of Rap Back in its use for civil background checks as well.

Lesko said the use of other biometrics included in NGI that help generate case leads, such as face recognition, give investigators more information as they work to solve crimes. "Law enforcement is clamoring for these tools at the local level, and as multiple states start contributing to these kinds of centralized repositories, we will see these tools become more and more valuable."

The growing area of iris as a biometric identification modality is also on the horizon, with Texas participating in the iris pilot program with the CJIS Division. "We are seeing high interest in the use of iris recognition within the correctional community," Lesko said. "It is a fast biometric, more convenient than fingerprints for purposes such as ensuring accurate releases and even access to the commissary." He said innovations like iris show the potential of biometrics that haven't yet been fully explored. "I am sure there are even more benefits of these biometrics that we will realize in the future."

# Biometric Identification Services

## *Continuing to expand the biometric frontier*

In fiscal year (FY) 2014, the CJIS Division made significant improvements in many key areas of its biometric services. With a rich history, biometric services at the CJIS Division can be traced directly to the establishment of the Identification Division in 1924 as part of the Bureau of Identification (renamed precursor of the FBI) and has continued to expand the biometric frontier—right up to its accomplishments this past year.

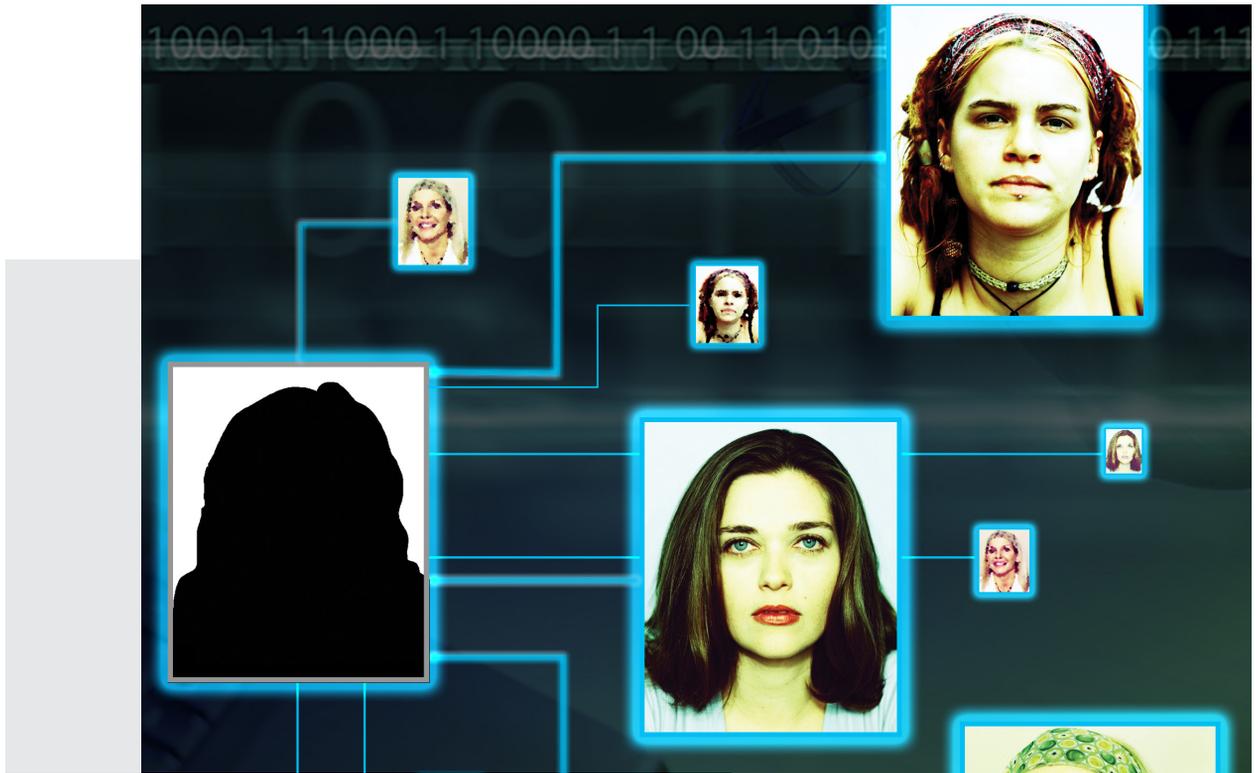
### **THE YEAR IN REVIEW**

On September 7, after over 15 years, a multitude of successes, and processing over 500 million transactions, the Integrated Automated Fingerprint Identification System (IAFIS) was fully replaced by the Next Generation Identification (NGI.) When it rolled out in 1999, the IAFIS provided automated tenprint and latent fingerprint searches, electronic image storage, and electronic exchanges of fingerprints and responses, as well as text-based searches based on descriptive information. Building on the foundation of the IAFIS, the NGI takes the FBI's biometric identification services and criminal history information to the next level. New capabilities include a national Rap Back service; the Interstate Photo System; text-based searches for images of scars, marks, and tattoos; fingerprint verification services; more complete and accurate identity records; and enhancements to the biometric identification repository.

In another area of biometric services, the capabilities of the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit continued to grow. The FACE Services Unit

currently accepts still images and surveillance video from FBI investigators and has the ability to search criminals' photos available through the NGI. Additional photo searches are also made possible by Memoranda of Understanding/Agreement with the Department of State, the Department of Defense's Biometrics Identity Management Agency, and 16 state Departments of Motor Vehicles. Since its inception, the FACE Services Unit has received facial photos from 54 field offices and 6 legal attachés in support of FBI cases.

On September 18, the CJIS biometric services staff completed the exhaustive process of leaving behind the era of physical storage of paper prints and digitized more than 35 million fingerprint cards that were stored in 1,031 filing cabinets. Before being scanned, the cards required extensive preparation work. Paperclips and staples were removed and recycled, rips were smoothed out and taped up, and some criminal cards needed to be placed in sequential order by FBI number. In addition to recycling the cards themselves, the empty cabinets were also recycled. This effort, which began in October 2012, eliminated the need to move the cabinets to the new Biometric Technology Center, located on the CJIS campus, when it opens in 2015.



### **BIOMETRIC SERVICES IN ACTION**

On July 16, an FBI field office investigator provided the FACE Services Unit with a photo search request containing three photos as part of a bank robbery investigation. A search of criminals' photos in the NGI resulted in a gallery of 50 potential candidates based on facial features. A biometric images specialist compared the images in the gallery to the three submitted photos and identified a likely candidate. An investigative lead containing the likely candidate was returned to the investigator on July 17, and subsequently a positive identification was made. The subject was arrested along with her partner, who was her father and whose criminal history included three convictions for bank robbery. Both are being held in federal custody.

# FBI Biometric Center of Excellence

## *Exploring new and enhanced biometrics*

The FBI's **Biometric Center of Excellence (BCOE)** has continued to explore and advance the use of new and enhanced biometric and identity management technologies for use in criminal justice and national security. The BCOE continued its collaboration with staff from the FBI's Laboratory Division and Operational Technology Division, as well as other law enforcement and intelligence agencies, members of academia, and partners in private industry in its mission to expand the use of biometrics.

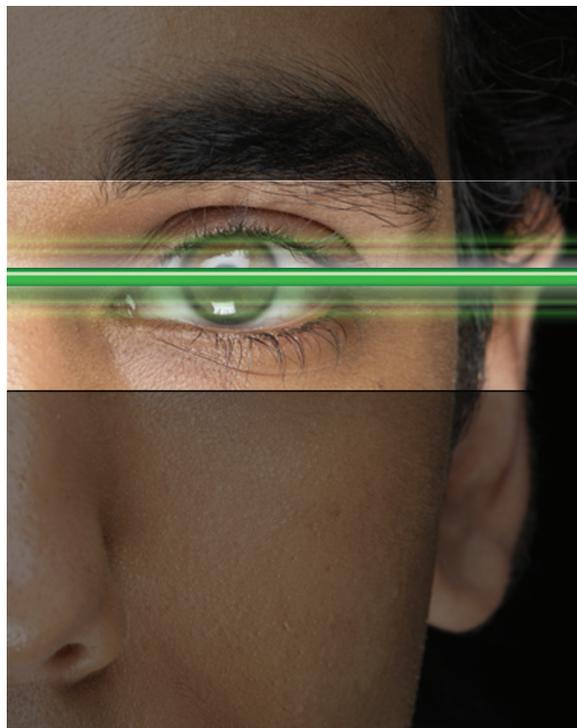
### **THE YEAR IN REVIEW**

During fiscal year (FY) 2014, the BCOE managed more than two dozen technical projects, such as defensive biometrics, facial recognition, and speaker recognition. In addition, the BCOE continues to be forward-thinking by addressing the scientific research needs in areas of biometric test data collection, product certification, as well as testing and evaluating of new and enhanced tools and technologies.

One of the BCOE-sponsored projects was the Fixed Location Surveillance Pilot (FLSP), which builds upon work previously sponsored by the Department of Defense for the Tactical Analysis of Video Imagery. The FLSP provides a new investigative capability through the development of software that can automatically detect, track, and log (e.g., time, date, and location) the presence of individuals who cross a camera's field of view prior to conducting facial recognition of those persons.

During FY 2014, BCOE employees also researched the use of periocular (area around the eye) features for biometric and forensic identification uses. The research revealed this

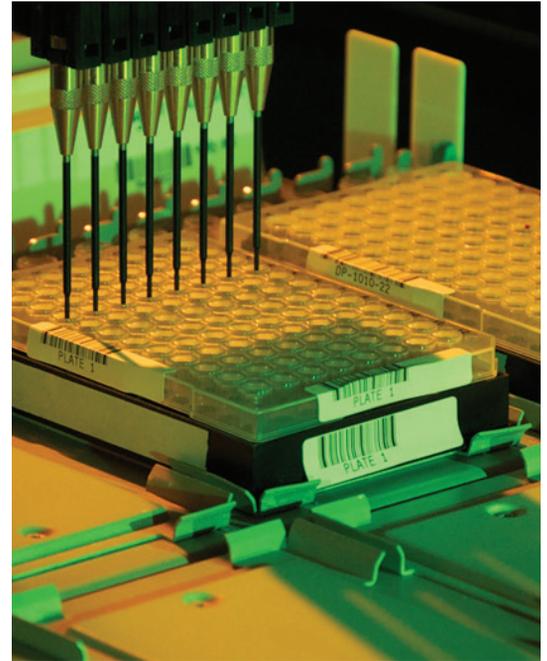
type of recognition may not be suitable in providing positive identifications (like fingerprints and DNA), but it does provide identity value that could be useful in investigative situations.



## BCOE IN ACTION

During FY 2014, the BCOE expanded biometric test data by collecting biometrics from individuals at the Twins Day Festival in Twinsburg, Ohio, for the fifth year in a row. The BCOE efforts this year marked the first time the FBI collected twins' audio and video data. The Twins Day Festival allowed the BCOE to not only collect information but to also collect large amounts of data from a unique sample of the population—twins and other multiple-birth siblings (such as triplets).

The BCOE ended the year by sharing biometric and identity management solutions with corporate, law enforcement, defense, and homeland security communities participating in the 2014 Global Identity Summit in Tampa, Florida. BCOE staff, along with representatives from throughout the FBI, exhibited various prototypes and capabilities from the Science and Technology Branch.



# CJIS Intelligence Program

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

The **CJIS Intelligence Program** provides identity intelligence products to intelligence groups at FBI field offices, and to the law enforcement, intelligence, and homeland security communities. The program also collects identity information and increases the sharing of such data among domestic and international partners. By gathering and analyzing biometric, biographic, and criminal history records from various sources, staff can merge resources to create a more complete view of a specific case or person of interest.

## **INTELLIGENCE PROGRAM IN ACTION**

The CJIS Intelligence Program expanded and enhanced its services in fiscal year 2014, including a new intelligence product that analyzes information from the FBI's National Instant Criminal Background Check System concerning individuals who were denied access to explosives. These denials were combined with criminal and intelligence data to conduct a cursory analysis of behavioral trends or patterns by prohibited individuals who attempted to access explosive materials. Many professionals in the law enforcement community have found the results valuable in their efforts to protect the public.



# Global Operations

## *Identifying criminals and terrorists across the globe*

The CJIS Division's global operations continued to support national and international law enforcement on the biometric front during fiscal year 2014. This included division staff collecting and updating identity information from domestic and international partners who support the Foreign Biometric Exchange (FBE). All of these biometric records were ingested into the Next Generation Identification's (NGI's) criminal master file and were made available to local, state, tribal, and federal law enforcement partners.

Other global efforts included progress made with the Preventing and

Combating Serious Crime (PCSC) initiative. PCSC agreements are forged with countries that are part of the Visa Waiver Program (VWP). Under the terms of the agreements, the United States and its VWP foreign partners conduct searches of one another's biometric databases in cases of serious criminal justice and terrorism investigations. Staff members and their partners at the Department of Homeland Security work with the VWP partners to find technical solutions for easier access of the databases. Currently, 44 countries have signed PCSC agreements, and 22 countries are currently engaged in discussions to implement such technology.

### **GLOBAL OPERATIONS IN ACTION**

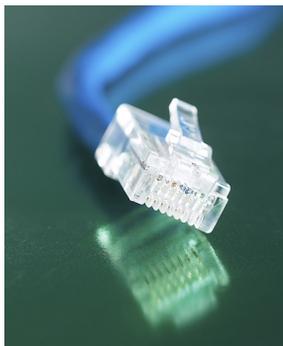
The CJIS Division's Quick Capture Platform (QCP) is a portable biometric system that allows investigators to



collect, store, and submit fingerprints during operations in the field—anywhere around the world. The QCP searches the NGI system, as well as identity databases from the Departments of Defense (Automated Biometric Identification System [ABIS]) and Homeland Security (IDENT). A subject was biometrically enrolled into the Department of Defense's (DoD's) ABIS in 2012 as a foreign national hire for base access in Afghanistan. The subject was later arrested in Uganda by FBI personnel as he attempted to pick up a drug shipment at the Entebbe airport. The FBI employee was able to positively identify the subject by using the QCP.

# Public Access Line

## *A single point of contact for crime tips*



In 2012, 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.

### **THE YEAR IN REVIEW**

With its staff dedicated to providing customer service 24 hours a day/7 days a week, the

PAL has developed a uniform process for handling telephone calls. As a result, the PAL currently enables FBI special agents in 28 field offices across the nation to focus on investigative duties rather than screen calls. The PAL has significantly improved how the FBI communicates with the public, and it is preparing to expand its services to receive and process Internet tips beginning in 2015.

### **PAL IN ACTION**

A PAL customer service representative (CSR) recently received a call from an individual who stated that he had knowledge of a bank robbery that might occur the next day in a Midwestern city. The caller stated that he had just left an individual who had said he was going to rob a bank and that the subject had been smoking marijuana. Initially, the CSR thought the caller did not appear to be credible as the caller seemed to be under the influence himself.

The CSR persuaded the caller to provide critical information about the subject. The caller provided the subject's name,

and the CSR conducted numerous FBI and open source data checks that provided no additional information.

The caller said the subject had traveled by train from California during the past week to meet some acquaintances, and that he (the caller) had paid for the subject's motel room. The subject told the caller that he was going to strap a bomb to himself, walk into a bank with a handgun, and hold an employee hostage. The caller indicated his conscience had prompted him to contact someone about the subject's plans.

Realizing the potential urgency of the information, the CSR worked outside of the normal process and immediately contacted the FBI field office. He provided the information he had obtained from the caller and noted that using the normal reporting process might have taken too long to enable the field office to take action in time to prevent the crime.

That evening, a special agent met with the caller and learned more about the subject, including the fact that the subject, a white supremacist and convicted felon, admitted to robbing a bank recently in California and assaulting a security guard.

Based on that information, and with the cooperation of the caller, the agent, with help from the local police, was able to safely arrest the subject at the hotel where the caller had left him. The decisive action and extra effort of the PAL's CSR was instrumental in the expeditious arrest of the subject—and in the resolution of the earlier bank robbery.

# CJIS Information Technology

*The backbone of the criminal justice services the CJIS Division provides*

Every day, the CJIS Division's Data Center processes millions of transactions across its information technology (IT) systems, ensuring quick response times that range from minutes, to fractions of seconds, for the vital criminal justice information services that the division provides.

In fiscal year 2014, the staff of the Information Technology Management Section (ITMS) completed dozens of system builds and enhancements in a way that minimized disruption to the division's 24/7/365 services. This included the major technical upgrade that was the full implementation of the Next Generation Identification system. The ITMS also supported other division programs in FY 2014, including the Law Enforcement Enterprise Portal, the New Uniform Crime Reporting system, and the New National Instant Criminal Background Check System, to name a few.

Two major technology initiatives that the CJIS Division has furthered this year include the **Department of Justice (DOJ) Data Center Consolidation Project** and **Justice Cloud Services**. The DOJ Data Center Consolidation Project was initiated in 2012 to coordinate the consolidation of the DOJ's many data centers into fewer, more efficient facilities. This effort aims to maximize the return on taxpayer investments in Government IT. In support of this project, the FBI and DOJ are working together to transform two existing FBI data centers, including the CJIS Division's Data Center, into FBI/DOJ-wide enterprise data centers.

One related component of this effort is already underway, with the CJIS Division offering Justice Cloud Services. The Justice Cloud offers an Infrastructure as a Service solution, providing an infrastructure on which systems/services operate. Core services include hosting, primary storage, and backup and archive services. Currently, the CJIS Division is offering its Justice Cloud services to DOJ entities.

Both of these initiatives are made possible by successful expansion of the division's **Common Operating Environment (COE)**. Enhancements to the COE's components, including its Common Compute Platform, disk storage and backup, and virtualization platform, have resulted in lower maintenance and overhead costs. These significant savings, shared by the division and the agencies for which the division hosts services, demonstrate innovation and good stewardship.



# CJIS Advisory Policy Board

## *Marking 20 years of collaboration*

The varying perspectives of the law enforcement, criminal justice, and authorized noncriminal justice agencies are integral to CJIS information-sharing systems. Through the **CJIS Advisory Policy Board (APB)** and the **National Crime Prevention and Privacy Compact Council (Compact Council)**, the CJIS Division seeks the input of these agencies to help manage its services. In addition, the **CJIS Field Coordinator Program** ensures that agents and investigators nationwide understand the services that CJIS systems offer. Together, these entities maximize the potential of the information available from CJIS systems and programs.

### **CJIS APB: Celebrating 20 Years of Collaboration**

Criminal justice officials from across the country comprise the intricate set of working groups and subcommittees that are represented on the CJIS APB. Through the CJIS Advisory Process, the APB vets strategy, policy, operational, and technical issues associated with CJIS services and ultimately makes formal recommendations to the FBI Director twice a year. Chartered under the provisions of the Federal Advisory Committee Act, the APB has been in existence for 20 years. Twenty-five years prior to that, the APB existed in the form of an advisory committee for the National Crime Information Center.

At its June 2014 meeting, the APB made several recommendations for approval, including the following:

- ***Revision of the CJIS Security Policy (CSP) for Mobile Devices.*** Basing new policy on what was written

in 2012 to define and address the use of mobile devices, the APB consolidated existing mobile security requirements (i.e., access, use, restrictions, and incident response) and presented new standards for smartphones and tablets.

- ***Creation of an Interstate Photo System (IPS) Policy and Implementation Guide.*** This guide provides direction for law enforcement on how to use the IPS to search for photos of missing persons, suspects, or criminals to assist law enforcement in solving crimes.
- ***Change to the Law Enforcement Officers Killed and Assaulted (LEOKA) Program.*** Previously, individuals who were killed in the line of duty while acting on behalf of a law enforcement agency but were not paid from governmental funds earmarked for sworn officers were not counted among the LEOKA statistics. The APB recommended that the LEOKA program should include previously uncounted individuals killed in the line of duty when a law enforcement agency whose officers meet the LEOKA criteria requests it.



A 48-year veteran of the Virginia State Police, **Captain Thomas W. Turner**, serves as commander of his agency's division of Criminal Justice Information Services. He has also been involved with FBI services for nearly 30 years, providing input for NCIC requirements in the early 1980s, becoming a part of the CJIS Advisory Policy Board at its official inception 20 years ago, and, most recently, serving as APB chairperson.

Turner said the APB has been integral part of the success of the many criminal justice information services provided by the FBI and shared by local, state, tribal, and federal agencies. "The APB shows that people can accomplish a lot when they work together," he said. "If we didn't have this process, data sharing would be severely limited."

In addition to the input that the FBI obtains for its systems through the APB, Turner said state agencies like his, and individual agencies, also benefit from sharing ideas through the process. "You have a cross section of experts who participate through various subcommittees and task forces," Turner said. "I'm amazed at how innovative these people are. They can come up with ideas that save time and resources. As stewards of the taxpayers' money, this helps us do the best we can with the funds we have."

Turner said it is a "privilege" to serve on the APB and to have been elected chairperson by his peers. "To be chosen to be their voice is an honor, because when it comes to criminal justice information services, the APB is the glue that holds things together."

# Compact Council and CJIS Field Coordinators

## *Working together toward common goals*

The **Compact Council** ensures that the use of criminal history record information (CHRI) used for authorized noncriminal justice purposes respects individuals' privacy and reflects the most accurate and current information available. The National Crime Prevention and Privacy Compact Act of 1998 (Compact Act) led to the establishment of the 15-member Council to regulate CHRI used for screenings for employment, licensing, and placement in positions of trust.

In fiscal year 2014, the Compact Council helped protect the privacy rights of individuals while increasing public safety through several initiatives.

- ***Continued efforts to increase states' participation in the National Fingerprint File (NFF) program.*** NFF participation eliminates record duplication, enhances individual privacy protections, and improves the accuracy, currency, and completeness of the CHRI provided. The Council supported NFF onsite assessments in New York and Maine during April 2014, opening dialogues regarding the technical and policy requirements for NFF implementation.
- ***Participated in numerous outreach and education efforts.*** As part of the National Defense Authorization Act Task Force, Council members provided a state perspective on the use of CHRI to close the gaps in conducting national security clearances through a series of meetings. Council members also collaborated with the National Consortium for Justice Information and Statistics in a panel briefing to inform judiciary staffers from the Senate and House of Representatives about the provisions of the Compact Act and the role of the Council.

- ***Increased the ease of information sharing.*** At the Council's request, the U.S. Department of Justice agreed to consider allowing multiple requests for fingerprint-based records to screen the same individual for more than one instance of licensing or employment as one official purpose, provided specific conditions are met. Therefore, when an individual works with children, the disabled, or the elderly in more than one capacity, authorized governmental agencies may share fingerprint-based CHRI, eliminating the need for an applicant to pay for multiple background checks.

### **CJIS Field Coordinator Program**

During 2014, the Field Office CJIS Subject Matter Expert Program was renamed the CJIS Field Coordinator Program. Each FBI field office has at least one CJIS Field Coordinator (FC), whose role is to inform field personnel on how to leverage CJIS services to support investigative and intelligence missions. CJIS FCs also serve as information points of contact for field office investigators, intelligence personnel, administrators, and CJIS Division staff. This year, among the continuing education opportunities, four speaker series events provided information on crisis assistance, CJIS intelligence products, and updates to Facial Analysis, Comparison, and Evaluation Services and Quick Capture Platform software. A CJIS FC conference is scheduled for 2015.

*"CJIS is very proactive to engage the field offices and keep them apprised of the latest capabilities."*

-Evaluation Comment from a CJIS Field Coordinator Speaker Series Event



**Dawn Peck** manages the Bureau of Criminal Identification for the Idaho State Police and serves as chairperson of the Council that administers the National Crime Prevention and Privacy Compact. She is proud of the work the Council does to ensure the privacy of citizens while also enabling authorized agencies to do civilian background checks for people placed in positions of trust, such as teachers and eldercare workers.

“The Compact Council epitomizes the ‘shared management’ approach,” she said. “Through collaboration, we are able to apply the policy for civilian background checks in a way that protects the privacy of individuals.” She recalls an example of the council’s work that made a big difference, the establishment of “Purpose Code X.” This purpose code can be used to do a name based check by law enforcement and social services agencies in emergency situations, such as placing children in protective care on short notice. For example, if a parent is arrested late at night and officers and social workers may want to authorize an extended family member to take children in for the night until Social Services can determine a more permanent placement. Officers can use this purpose code to run a background check for this purpose, which can help minimize trauma to children. The background check must be followed up with a fingerprint based check.

“This can also be extended to crisis situations where a disaster, such as a major hurricane, forces families to leave their homes and seek refuge in shelters with other evacuees,” she said. “In these cases, background checks for all those within a temporary shelter can give everyone some peace of mind.” Peck said being able to look at a critical need and address it through shared management and cooperation is the hallmark of the Council’s work. “We take this responsibility very seriously,” she said.

# Our Campus

*Where connections and identifications generate the power to know*



The CJIS Division campus stretches for nearly 1,000 acres across the scenic foothills of the Appalachian Mountains in north central West Virginia. The main building, completed in 1995, contains 526,000 square feet of offices and a state-of-the-art data center that hosts many programs serving law enforcement and criminal justice agencies across the nation. The campus also includes a service center, a central plant, a visitor's center, and a child care center.



*The CJIS Link (Link)* keeps agencies informed about CJIS services and benefits; showcases the successes of CJIS programs and systems; provides contact information; and alerts readers to new initiatives at the CJIS Division.

Scan the 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*.



Work continued in fiscal year 2014 on the newest addition to the CJIS Division's campus. The FBI's Biometrics Technology Center will house the CJIS Division's Biometric Services Section and the Department of Defense's (DoD's) Defense Forensics and Biometrics Agency. The new facility will contain 360,000 square feet of modern office space and serve as the home of the Biometric Center of Excellence. When completed in 2015, the structure will provide areas for training, conferences, and joint collaboration on projects related to biometric research.

The **CJIS MISSION:** 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.



### **DIRECTOR COMEY VISITS THE CJIS DIVISION**

On November 14, 2014, FBI Director James B. Comey visited the CJIS Division. In addition to speaking to employees, he also toured CJIS facilities and received briefings on division programs. In his comments, the Director described the services that the division provides as essential to the law enforcement and criminal justice communities. “What you do cannot be overstated,” he said. “This country would not be as safe a place if you did not do what you do here.”



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