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

ANNUAL REPORT 2015

CJIS

THE POWER TO CONNECT

The CJIS Division Annual Report 2015

"This annual report serves as a demonstration of our commitment to provide the best possible tools to help our partners fight crime and terrorism."

The FBI's **Criminal Justice Information Services (CJIS) Division** enjoyed a great year connecting with our partners as we worked to better serve them and to enhance the vital services we provide.

One way we improved our services was through the launch of a new Partner Relations and Outreach Unit (see page 4) to focus on our collaboration with our internal and external customers within law enforcement and criminal justice. Notably, this group, with counterparts at the Department of Justice, hosted a Tribal Engagement Conference in August 2015. The first of its kind, this conference brought together tribal law enforcement agency officials, CJIS service providers, and state CJIS System Officers to help connect tribal agencies to the services they need to better protect and serve their communities.

Another major undertaking of the CJIS Division in fiscal year (FY) 2015 was our work to make criminal justice records more complete and accurate by tracking down missing disposition information. We have made this a priority because, as I often say, we can have the best, most high-tech biometric identification tools, but once we connect biometrics with a name, inaccurate or incomplete information can prevent sound decisions from being made.

Finally, FY 2015 was an important year for our Uniform Crime Reporting Program as FBI Director James B. Comey personally engaged with the CJIS Division on our efforts toward modernizing national crime statistics to be more complete and timely. In addition, the Director is looking to the CJIS Division to establish a police "use-of-force" data collection. The scope and methodology for this data collection is being carefully developed in concert with the law enforcement stakeholders who will ultimately contribute and use this information.

In my role as Assistant Director, I have the privilege of traveling around the country to conferences and meetings to talk to our partners about CJIS Division services. I am always gratified to hear the many ways that our services are making a difference to investigators and officers, and how much respect our partners have for the CJIS employees who serve them.

This annual report represents just a portion of what we accomplished this year, but serves as a demonstration of our commitment to provide the best possible tools to help our partners fight crime and terrorism across our nation and around the world. We thank our many stakeholders for their collaboration with us and we look forward to the great things we can do together in 2016.

Stephen L. Morris

Assistant Director of the FBI's CJIS Division

Contents

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.

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.

Partner Relations and Outreach

Connecting you with the CJIS Division

CJIS Division executives created the **Partner Relations and Outreach Unit (PROU)** in March 2015 to build bridges, create new alliances, and strengthen and support existing relationships with the division's law enforcement and intelligence partners. PROU staff also promote internal collaboration on issues and enhancements that span the division's services. These efforts ensure consistent and clear communications involving CJIS Division enterprise services and ready assistance in the management of information-sharing strategies regarding those services.

The mission of the PROU is to maintain expertise and share information, at a high level, on the vast array of services offered through the CJIS Division to our law enforcement partners. The PROU aims to widen communication with our partners so they can gain a greater understanding of the resources and information available at the CJIS Division, as well as seek new information-sharing opportunities with current and future partners.

The PROU, in meeting its mission to enhance relationships with internal and external partners and improve their CJIS experience, collaborates with entities such as the Department of Justice's (DOJ's) Office of the Chief Information Officer, the FBI's Office of Partner Engagement and Private Sector, the FBI's Terrorist Screening Center, the Office of Management and Budget, as well as many others including both internal FBI and CJIS Division groups.

What does all this mean to a CJIS Division partner? It means the PROU is your first stop if:

- You are not sure what CJIS service you need or to whom you should speak with concerning that service.
- You need to request that a CJIS Division representative attend a conference or meeting.
- You want to share information about a new service or resource that may be available to the CJIS Division.
- You want to visit the CJIS Division to discuss enterprise services issues or new ideas.

In addition to being "information central" for the CJIS Division, the PROU maintains primary responsibility for the following two areas:

- CJIS Tribal Engagement Program, an effort to initiate collaboration between tribal and state law enforcement agencies regarding use of the CJIS Division's systems in daily operations; and
- The FBI Field/HQ Coordinator Programs, which designate a CJIS Coordinator in each of the 56 FBI field offices and applicable FBI Headquarters Divisions to help investigative personnel understand how to effectively use CJIS Division services in field intelligence and investigative situations.

To contact the PROU regarding any facet of CJIS Division systems or programs, e-mail PROU at: <PROU@ic.fbi.gov>.

PROU IN ACTION

The CJIS Tribal Engagement Program hosted the DOJ/CJIS Tribal Conference on August 19, 2015, in Tulsa, Oklahoma. The conference was held in conjunction with the CJIS Advisory Policy Board Working Groups to initiate collaboration between tribal and state law enforcement agencies regarding using CJIS Division

systems in their daily operations. Approximately 100 representatives from more than 80 federally recognized tribes attended the inaugural conference and received formal presentations from ten DOJ and FBI programs.

Representatives actively participated in workshops that discussed issues most important to the tribal law enforcement community and pertaining to the CJIS Division programs, (e.g., system access, federal and state authorities for fingerprinting).

Attendees received information about CJIS Division systems and established lines of communication to improve the CJIS Division's understanding of the issues that prevent some tribal law enforcement agencies from accessing or submitting data to CJIS Division systems.

Collaboration key to success: "We are all fighting the same fight"

Mary Kay MacNichol, CJIS Systems Officer for the New Hampshire State Police, believes in collaboration. In fact, one of her favorite quotes is from Vince Lombardi, "People who work together will win, whether it be against complex football defenses, or the problems of modern society." She views the CJIS Advisory Process, and the Advisory Policy Board (APB) on which she serves, as a great illustration of that kind of cooperation. One example from the last year that stands out to her was the DOJ/CJIS Tribal Outreach Conference in August 2015.

"Often, there is an assumption that everybody has access to the information they need," she said. "The tribal conference was an opportunity to take a step back, and see that some agencies don't have the same access." She said the conference helped her, as a leader on the APB, understand the issues and barriers that tribal agencies face.

MacNichol said she was encouraged by the participation from across the FBI and other DOJ entities to share information about funds available to help and how to get training and technology assistance. "Through these kinds of efforts, information sharing gaps will be eliminated in CJIS Division databases, which can only benefit all law enforcement and criminal justice agencies. We are all fighting the same fight to protect our homeland from violent criminals, both foreign and domestic terrorists, and anyone else out to cause harm to our communities."

She said efforts such as the tribal outreach, and the many system developments and enhancements that are occurring, make it an "exciting time" to be a part of the CJIS APB. "Great achievements are being made," she said. "And, through collaboration, law enforcement is helping to shape these achievements."

National Crime Information Center

Working to make this reliable information-sharing system even better

The **National Crime Information Center (NCIC)** is a computerized database of documented criminal justice information available to law enforcement nationwide. What began on January 27, 1967, with 95,000 records in five files has grown to more than 12.7 million active records in 21 files. In the system's first year, law enforcement agencies conducted 2 million queries. Today, the system handles about 12 million queries daily.

NCIC staff spent much of 2015 crisscrossing the United States asking law enforcement and criminal justice personnel for ideas and input into NCIC's upgrade, NCIC 3rd Generation, known as N3G.

In the largest user canvass in CJIS Division history, NCIC staff visited agencies in all 50 states and 3 territories from August 2014 to August 2015 and received more than 5,400 suggestions for enhancements. Nearly 500 agencies that use the NCIC—including 124 state-level agencies, 25 federal agencies, and 10 tribal agencies—provided input on modernizing the system. CJIS staff, along with the CJIS Advisory Policy Board, will review and refine those ideas to construct a plan to deliver improvements in the next few years.

Also in 2015, NCIC staff implemented eight enhancements to the current system. These enhancements ranged from giving agencies the ability to place identifying images of lost or stolen weapons into the NCIC to sharing NCIC information with the Department of Defense to better secure access to military bases.

Another highlight of the NCIC Program in 2015 was the creation of a tool that will resubmit a query automatically if a user desires. Called the "revetting tool," this feature gives NCIC users real-time information without the need to process the data daily. This tool was developed when staff discovered that some federal agencies repeatedly queried the NCIC with the same information, sometimes multiple times in a single day, and this was slowing down the system. Using the tool, an agency can place frequently queried records into an external table in the NCIC one time. The NCIC automatically searches those records daily and returns only matching information. This frees computer space on the NCIC system and saves agencies time by returning only matching information.

The progress made in 2015 serves as a strong foundation for the program's continued growth in 2016. In the coming year, NCIC staff will finalize a concept of operations, develop system requirements for the N3G, and expand the revetting tool to other federal agencies.

NCIC IN ACTION

On April 29, 2015, officers with the Elm Grove Police Department (EGPD) in Wisconsin noticed a minivan that kept circling through the small town and parking near a bank. The officers began to suspect wrongdoing, pulled over the minivan, and noticed a smell of marijuana. While officers were processing the four subjects from the minivan, individuals in a second vehicle came to bail them out. Officers contacted NCIC staff and requested an off-line search of license plates from the minivan and the second car. (An off-line search is a special technique that can be used to locate an item of property, determine the proximity of an individual to a crime scene, reveal if an inquiry was made on a particular individual, or confirm or discredit an alibi.) Occupants in the

second car allegedly had been involved in a check cashing scheme earlier in the day.

Within 4 hours, the EGPD took 10 people into custody. Eight of the individuals were charged with identity theft, and four of those individuals were charged with seven counts of receiving stolen property. In addition, the four occupants of the minivan were charged with possession of marijuana. One of the two vehicles queried in the off-line search had been rented but had been kept beyond its original contract and used outside of the terms of the rental agreement. Two vehicles, totaling more than $40,000 in value, and $4,000 in stolen cash, were recovered in connection with the case.

Since the first off-line request on April 29, the EGPD requested off-line searches on five additional vehicles involved in the case. The EGPD connected one of those vehicles to an open and unresolved fraud case from Colorado Springs, Colorado. To date, the group of suspects has been tied to at least $1 million worth of fraud and theft of payroll checks.

NCIC provides "critical, lifesaving information"

In the mid-80s, **Walt Neverman** was an NCIC dispatcher for the Wisconsin State Patrol working the night shift when a trooper called in a suspected DUI. The driver, who had three passengers in his vehicle, had no identification on him, but gave the trooper a name and date of birth. When Mr. Neverman entered this information into NCIC and Wisconsin state databases, no results were returned, including no driving record. The trooper approached the driver a second time and asked for a social security number. The driver complied, and a run of this information returned 10 arrest warrants, ranging from rape to abduction. The officer then called for backup, and when the passengers were each questioned, one, who had been sitting in the backseat, was found to have a sawed-off 30/30 rifle under his coat. The subject said he had intended to shoot the trooper on the trooper's second visit to the driver's window, but the gun had gotten caught on the coat. If the officer had not received the warrant information and called for backup before approaching the vehicle a third time, the subject may have had the opportunity to fire.

Walt Neverman now manages criminal justice services like NCIC for the state of Wisconsin in his role as director of the Crime Information Bureau for Wisconsin's Division of Law Enforcement Services, a part of the state's Department of Justice. The example from early in his career is one he cites when asked about the value of the NCIC system and the information it provides. "NCIC information is lifesaving for the police officer and the public," he said. "It is information that officers need every single day when they are in contact with the public—critical, lifesaving information."

As the NCIC program moves to a new development phase with N3G, Mr. Neverman is serving on the N3G Task Force that is a part of the CJIS Advisory Process. "The number of recommendations for new features and capabilities shows the great interest in what more NCIC could provide," he said. "I think we are just now opening our minds to options that are out there and the potential we have to make NCIC even more beneficial to the nation."

National Instant Criminal Background Check System

Ensuring the timely transfer of firearms to eligible gun buyers and preventing the transfer of firearms to those who are prohibited

On a rainy afternoon on March 30, 1981, then White House Press Secretary James Brady was shot during an assassination attempt on former President Ronald Reagan. Brady survived and went on to lobby for stricter regulations for the transfer of firearms and more sensible gun control laws. The result, the Brady Handgun Violence Prevention Act of 1993, spawned the **National Instant Criminal Background Check System (NICS)** housed at the CJIS Division.

Fast forward to 2015, and NICS—working with the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Justice; and local and state law enforcement agencies—continues to ensure the timely transfer of firearms to eligible gun buyers and to prevent the transfer of firearms to those who are prohibited.

One of the ways NICS staff keeps firearms out of the hands of ineligible individuals is through the use of the **NICS Index**, which contains information from local, state, tribal, and federal agencies of persons prohibited from receiving firearms under state or local law. The NICS Index contains prohibiting information that may not be in the National Crime Information Center (NCIC) or in the Interstate Identification Index (III).

The NICS Index contains more than 13.8 million records. From October 1, 2014, until September 30, 2015 , more than 1.3 million records were added to the NICS Index. An increase in the number of records in the NICS Index means quicker and more accurate turnaround times for the NICS Section, as well as for the customer and the gun dealer, also known as the federal firearms licensee (FFL).

One new facet of NICS is the dispositions of firearms. Beginning in 2015, when a law enforcement agency confiscates a firearm and then wishes to return it to the individual or a family member (for example, after an investigation has been completed), the agency can conduct a check of NICS (including the NICS Index) to ensure that the recipient is not prohibited from owning the weapon. Law enforcement agencies are not required to access NICS to return a weapon to its owner, and agencies are not permitted to use NICS for criminal investigative purposes. However, agencies in 31 states have received permission to conduct the checks. Agencies in 25 of those states have conducted such checks, processing more than 14,519 transactions.

The **NICS E-Check** program continues to grow. As of September 30, 2015, NICS E-Check usage accounted for approximately 58 percent of all transactions. The NICS E-Check enables FFLs to conduct unassisted NICS background checks for transfers of firearms via the Internet. The FFLs enter the prospective gun buyers' descriptive information directly into NICS and initiate the search process. This allows for more accurate searches based on the direct entry of descriptive data by the FFL, retrieval of NICS background check results 24/7 (including printing completed NICS background check search requests), availability of messages regarding NICS' operational status, and protection against identity theft for the customer.

The NICS Program has much to look forward to in 2016 with the implementation of the New NICS tentatively slated for January 2016. The New NICS will offer its internal and external users, FFLs, and other partners many enhanced features and benefits, such as increased system availability, additional automated features, and enhanced technology and performance.

NICS IN ACTION

On January 27, 2015, a NICS examiner processed a transaction for an FFL, a gun shop in Garland, Texas, for a long gun purchase. The NICS examiner identified a match based on descriptive data in the NCIC. The NICS examiner researched the transaction and determined that the NCIC entry contained a warrant issued on January 23 from a sheriff's office in Texas for aggravated assault with a weapon. The NICS examiner contacted the sheriff's office, which confirmed the active warrant. Based on the information received, the NICS examiner provided the FFL with the denial. Two hours later, the sheriff's office contacted the NICS examiner to request the subject's address. The sheriff's office had attempted to apprehend the individual at the FFL, but the individual had already left the store. The sheriff's office later advised the NICS Section that they had apprehended the subject.

National Data Exchange

Demonstrating capabilities and cultivating collaboration

In fiscal year 2015, the **National Data Exchange**, known as **N-DEx**, improved information-sharing capabilities for the criminal justice community by developing new partnerships, expanding existing collaborations, granting access to additional records, and delivering faster response times. N-DEx staff also promoted the system's capabilities by demonstrating its powerful tools for specific agencies' investigations and by celebrating law enforcement teams who successfully used N-DEx to solve cases.

Launched in 2008, N-DEx provides law enforcement personnel with a secure online environment where they can view and share valuable information such as incident and case reports; arrest, booking, and incarceration data; mug shots and booking photos; field contact and interview records; and supervised release, probation, and parole data. The advantage of N-DEx is that it removes jurisdictional and geographic limitations and allows local, state, tribal, and federal agencies to search, share, link, and analyze potential leads. N-DEX is also designed to boost sharing capabilities by connecting with other records management systems. These connections allow an N-DEx search to access other law enforcement systems' records and to expand the reach of N-DEx data and services.

Collaboration is key

Partnerships are a vital part of how N-DEx improves the convenience and value of its system. External partnerships between N-DEx and other information-sharing systems achieved major growth in 2015. By August 1, 2015, all six regions of the Regional Information Sharing Systems (RISS) Program were linked to N-DEx, forging a new level of service to the law enforcement community. Searches are expected to dramatically increase as a result of RISS service centers gaining a more direct path to N-DEx capabilities.

Law Enforcement Information Exchange (LInX) agencies are also being added to N-DEx as they join with regional LInX systems. Currently in the works is an N-DEx plan to partner with the International Justice and Public Safety Network (Nlets). This will give Nlets users streamlined access to N-DEx and enable N-DEx users to conduct simultaneous searches of Nlets.

Thanks to collaboration within the CJIS Division, N-DEx users can now query two of the FBI's major databases, the National Crime Information Center (NCIC) and the Interstate Identification Index (III). N-DEx will soon use the FBI's Next Generation Identification system to provide images of faces, scars, marks, and tattoos in its responses. Enhancements to N-DEx will also improve services provided internally to FBI investigators. For instance, N-DEx is in the preliminary phase of linking with the FBI's Data Integration and Visualization System, which further equips the FBI's analytical workforce to conduct information discovery and analysis. N-DEx staff are also engaged with the National Instant Criminal Background Check System (NICS) Section to ensure that NICS examiners have access to the N-DEx system information they need to perform timely and accurate gun checks.

Demonstrating the capabilities

To demonstrate the full capabilities and features of the system, N-DEx staff assisted the criminal justice community with several active case projects in 2015. Two FBI field offices provided information on cases that, when searched in N-DEx, produced additional leads that were previously unknown to investigators. In pilot projects, requests for NCIC off-line searches (checks of NCIC inactive records) were also queried through N-DEx. These searches generated many responses, providing requestors with actionable leads in

more than a dozen cases. In addition, N-DEx staff assisted several agencies with configuring large spreadsheets of data to search N-DEx using the batch query function. The batch queries simultaneously executed thousands of searches, resulting in significant time savings.

Celebrating success

In 2015, N-DEx staff presented multiple awards recognizing excellence in information sharing. The N-DEx Excellence Awards were presented at law enforcement conferences around the country to raise the visibility and awareness of the system within those states and to promote public safety through increased use of N-DEx.

N-DEx also established a new award, the N-DEx Success Story of the Year. The inaugural presentation of this award recognized the Maryland State Police and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). The investigation that warranted this honor occurred in 2012 when a Maryland State Highway Patrol (MSHP) officer conducted a traffic stop on a truck transporting three storage containers. An NCIC search of the vehicle and driver's information did not produce any red flags. The officer took the additional step of searching the name on each bill of lading through the LInX. Through the partnership between the systems, the search also generated a query of the N-DEx system. Within seconds, the N-DEx result indicated that an individual associated with one of the containers was the subject of an ongoing federal investigation. The MSHP officer allowed the vehicle to continue to its destination and, through subsequent collaboration with the ATF, intercepted the container's renter when he attempted to claim the contents. Agents found 3,000 cartons of counterfeit cigarettes; the owner was charged with and later convicted of multiple crimes, forfeiting more than $1.4 million in proceeds from his criminal activity.

Growing and improving

Entering fiscal year 2016, the N-DEx system continues to expand. Users can now search more than 500 million records, and that number grows daily. Response time to return results has improved, with 94 percent of responses being returned in less than 10 seconds. In 2015, N-DEx staff continued their efforts to demonstrate the power of N-DEx to the criminal justice community. As a result of those interactions, searches of the N-DEx system have increased by 25 percent to more than 315,000 per month.

N-DEX IN ACTION

On July 16, 2015, an active shooter targeted two military sites in Chattanooga, Tennessee: a joint armed forces recruiting center and a reserve and support location of the U.S. Navy and U.S. Marine Corps. Four Marines and a sailor were killed, and a Marine and a Chattanooga Police Department officer were wounded. The Naval Criminal Investigative Service (NCIS) Multiple Threat Alert Center received partial identity information for the shooter, who was killed in the incident. The partial identity information was used to conduct searches of the Department of Defense Data Exchange (D-DEx), which also generates queries of the LInX and N-DEx. The additional records provided identifying information on the shooter, his family, his vehicle, and his associations with Tennessee and Virginia. The subject had many possible combinations and spellings of his name, and the N-DEx known person result was instrumental in finding additional data. NCIS Special Agent/Division Chief Kris Peterson stated: "The FBI 'Known Person' record, developed by and available in N-DEx, really proved its worth in this case. NCIS, representing the D-DEx and LInX systems, is proud to be a strategic partner with the FBI and its N-DEx system in furtherance of law enforcement information sharing."

Law Enforcement Enterprise Portal

Providing information that is the currency of modern policing

The **Law Enforcement Enterprise Portal (LEEP)** has been successful in providing essential criminal justice information and resources to the law enforcement community for 20 years. The appreciation of these resources as critical tools of modern policing is clearly becoming a standard as the LEEP reached a high of 6,840,615 user hits in fiscal year (FY) 2015.

The array of services LEEP offers include access to programs within the CJIS Division, such as the National Data Exchange, as well as to programs from other agencies, like the federal Joint Automated Booking System—all through a single, convenient sign-on. Adding many tools to the officer's kit, LEEP allows customers to seamlessly access diverse services and sources of information.

Services enhanced in 2015

LEEP's **Virtual Command Centers (VCCs)** allow law enforcement officers in different locations to securely monitor and participate in the moving parts of high-profile events and law enforcement operations. During FY 2015, law enforcement used a total of 1,222 VCCs to organize and analyze law enforcement maneuvers.

The VCCs have been upgraded in order to better support large-scale arrests, search warrant services, and take-down operations. A new component, TRAX, gives users the ability to record and view suspect profiles and provides updated, real-time information that gives field agents a live look at how an operation is progressing. In addition, users now have the ability to upload their own documents and images into a VCC.

In 2015, LEEP began providing users with access to the CJIS Division's Law Enforcement Officers Killed and Assaulted Program's site and the National Instant Criminal Background Check System Electronic Check (for gun purchases). LEEP has also added a variety of other services, such as "Texas Mapping," a web mapping and reporting application that supplies visual representation of incident data; Cyber Shield Alliance, an FBI cybersecurity partnership developed to defend against cyber threats to law enforcement networks; and the National Domestic Communications Assistance Center, a hub of technical-knowledge management that facilitates sharing among agencies.

With the addition of the **Industry Law Enforcement Enterprise Portal (iLEEP),** many of the same resources that law enforcement count on are now provided to the private sector. Accessible via the Cyber Division's InfraGard Program, this new portal gives the FBI's private sector partners access to services that are critical to maintaining the nation's infrastructure. These services include Malware Investigator, an automated system that analyzes suspected malware samples; Cyberhood Watch, which shares cybersecurity and intrusion information; and iGuardian, in which users can report cyber intrusion incidents.

For services that do not yet meet the single sign-on requirements, LEEP has added a new feature called **"Partnered Links."** Examples of Partnered Links include the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) eTrace, the Case Explorer, the Critical Incident Planning and Mapping System, and the Transaction Records Analysis Center.

LEEP looking forward

In late 2015, VCCs began providing users with superior incident-management tools, including the ability to title and categorize incidents and assign multiple teams to collaborate on specific events within a VCC. Users will have

more control over project management during a live operation and will be able to use a new command center view of the events board for display on a large monitor.

Looking ahead to 2016, LEEP will add a new feature, with a social media feel, called **JusticeConnect**. This feature will allow users to find and communicate with subject matter experts, establish and join communities with people who have common interests, create blogs that allow them to present ideas and receive feedback, share files with colleagues, exchange ideas through online forums, and gather feedback from others through polls and surveys. Users will also be able to quickly view, manage, organize, and complete tasks through an activities application.

LEEP IN ACTION

On June 6, 2015, inmates Richard Matt and David Sweat, both serving time for murder, escaped from the Clinton Correctional Facility in New York. A VCC was quickly activated as the incident-management system for the manhunt that included the support of more than 500 law enforcement officers from local, state, and federal agencies. Leads, reports, and evidence were entered, tracked, and managed using the VCC, which eventually assisted law enforcement officials in locating Matt, who was shot and killed by Border Patrol Agents on June 22. Six days later, in a field two miles south of the Canadian border, a New York State Trooper spotted and shot Sweat. He survived and was placed under arrest. The VCC helped keep the vast amount of information and participants organized in this massive 3-week manhunt.

___

Another valuable law enforcement service managed by the LEEP program staff is the FBI's Repository for Individuals of Special Concern, or RISC, which provides a rapid, mobile biometric search of a limited repository of fingerprint records. This tool was key to a case on May 1, 2015, in which the Saginaw Police Department in Michigan responded to a call about a home invasion in progress. When officers arrived at the scene, they saw a

vehicle leaving at a high rate of speed. A pursuit ensued, and three subjects abandoned the vehicle, which was found to contain ski masks, gloves, and a can of gas. One of the subjects was caught quickly. A short time later, a local resident reported hearing two people arguing outside her residence and possibly trying to enter her home. Officers responded and located a subject who was covered in sweat and dirt and apparently suffering an asthma attack. The man refused to provide his name, but officers took him to the hospital to be treated. While there, the Michigan State Police scanned the subject's fingerprints using a Mobile Identification device. A hit was returned on the RISC but not on the state Automated Identification Fingerprint System. The man was wanted for a parole violation (intimidation) and burglary (home invasion). As a result of the RISC response, the subject was arrested. The third suspect eluded capture and remains at large.

Analyzing crime by the numbers

Established in 1930 to measure the level of crime in the nation, the FBI **Uniform Crime Reporting (UCR) Program** has been collecting crime data from law enforcement agencies using the Summary Reporting System (SRS) for 85 years. In an effort to bring crime data reporting up to date, FBI Director James B. Comey established the Crime Data Modernization project, a Director's Priority Initiative (DPI), to overhaul the UCR Program. The DPI aims to develop a methodology for collecting data on officer use of force, transition agencies using the SRS to the data-rich National Incident-Based Reporting System (NIBRS), and increase the level of participation in the UCR Program by the FBI and other federal agencies.

Data on officer use of force

As a primary component of the DPI, UCR staff is developing a data collection methodology for officer use of force. In his landmark speech "Hard Truths: Law Enforcement and Race" at Georgetown University in February 2015, Director Comey highlighted the need for data that track the number of incidents in which force is used by or against police, including nonfatal encounters. In Director Comey's words, "How can we address concerns about 'use of force?' How can we address concerns about officer-involved shootings, if we do not have a reliable grasp on the demographics and circumstances of those incidents? We simply must improve the way we collect and analyze data to see the true nature of what's happening in all of our communities."

A focus group that included law enforcement and criminal justice professionals and representatives from academia developed the initial proposal for the data collection, which includes definitions, scope, and exactly what data to gather. CJIS Division staff circulated the proposal to additional stakeholders and subject matter experts for feedback. In September, staff met with representatives from major law enforcement organizations to discuss moving forward with establishing the data collection.

Expansion of NIBRS and implementation of new offenses collected

As part of the DPI, CJIS staff worked with key stakeholder groups in fiscal year (FY) 2015 to form a consensus for the transition from the SRS to the NIBRS. This effort resulted in a joint letter of endorsement from the International Association of Chiefs of Police, the Major Cities Chiefs Association, the National Sheriffs' Association, and the Major County Sheriffs' Association.

In addition, UCR staff is working to implement collection of three new offenses and one new location code into NIBRS. The collection of crime data for the offenses of animal cruelty, hacking/computer invasion, and identity theft are set to begin on January 1, 2016. These new data elements will allow UCR Program staff to evaluate trends and associate information between multiple offenses. For example, UCR Program personnel will be able to cross-reference animal cruelty actions with other violent crimes to uncover possible connections between the crimes.

The UCR Program has paired the two new fraud offenses of hacking/computer invasion and identity theft with the newly implemented cyberspace location code. Until now, it has been difficult to identify and analyze crime that occurred over the Internet. With the implementation of the cyberspace location code, the UCR Program will have the ability to uniquely identify Internet crimes and analyze the information, potentially exposing new and emerging trends and hotspots for cyberspace-related crime.

Officer safety training and analysis

Attacks on law enforcement officers were an all too familiar occurrence in 2015. To help combat these troubling incidents, the UCR's Law Enforcement Officers Killed and Assaulted (LEOKA) Program staff presented Officer Safety and Awareness Training events to more than 1,700 law enforcement personnel from more than 450 agencies. LEOKA staff members also wrote several officer safety articles for online law enforcement publications, such as the *FBI Law Enforcement Bulletin* and *Police Chief Magazine*. Also in FY 2015, LEOKA Program staff began conducting an in-depth, strategic study focusing on the growing threat of ambushes. The study, *Ambushes and Unprovoked Attacks; Assaults on Our Nation's Law Enforcement Officers*, is currently in the interview stage. Once interviews of both officers and offenders are complete and the data analyzed, the LEOKA Program will release the study findings, which is expected to happen in 2016.

Outreach, promotion, and training

In April 2015, while training law enforcement agencies in Sacramento, California, on the accurate reporting of hate crime statistics, UCR staff met Dennis and Judy Shepard, the parents of Matthew Shepard. Matthew was a 21-year-old college student murdered in 1998 because he was gay. Matthew's death led Mr. and Mrs. Shepard to create the Matthew Shepard Foundation (a nonprofit organization created to raise awareness and promote acceptance). In addition, Matthew's death and the death of James Byrd, Jr., led to the Hate Crimes Prevention Act of 2009. Because of the influence that Matthew's death had on current hate crime reporting laws, the Shepards were invited to visit the CJIS Division campus in September to share Matthew's story and discuss the work of the Matthew Shepard Foundation.

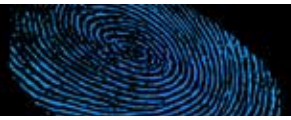
UCR IN ACTION

UCR Program staff released the annual *Crime in the United States* publication in fall 2015. Included, for the first time in program history, were FBI arrest data for the crimes of human trafficking, hate crime, and criminal computer intrusion. Expanding federal participation in the UCR Program began with this year's limited FBI data and will continue to grow with other federal participants in the coming years as part of the DPI.

—

On January 1, 2015, the UCR Program began collecting data for hate crimes with an anti-Arab bias motivation, as well as seven new religious-bias categories to be included in FY 2016's *Hate Crime Statistics* publication. Those new biases included anti-Buddhist, anti-Eastern Orthodox (e.g., Greek, Russian), anti-Hindu, anti-Jehovah's Witness, anti-Mormon, anti-Other Christian, and anti-Sikh.

Biometric Identification Services



Expanding opportunities for identification

During its first year of operation, the **Next Generation Identification (NGI)** system proved its value by expanding opportunities for law enforcement agencies, criminal justice agencies, and those working with protected populations to identify individuals. Most commonly known for checking fingerprints and names, the NGI and its associated services increased the scope of tools and technology including palm prints, latent prints (those lifted from crime scenes and improvised explosive devices), and face recognition. Following the transition of the Integrated Automated Fingerprint Identification System (IAFIS) to the NGI, biometric services staff provided support that was paramount to ensure limited impact to CJIS customers.

"Most commonly known for checking fingerprints and names, the NGI and its associated services increased the scope of tools and technology including palm prints, latent prints and face recognition."

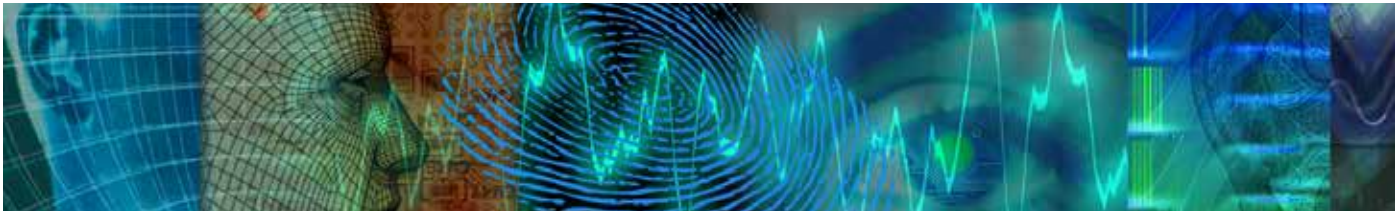
In addition to benefits from more accurate tenprint and latent print search algorithms, system users could also subscribe to the NGI's **Rap Back Service**. This feature allows authorized agencies to receive notification of criminal activity by individuals who hold positions of trust (e.g., educators, daycare workers) or who are under criminal justice supervision or investigation. This saves agencies time by eliminating the need to conduct periodic checks of designated populations and by offering immediate notification of these individuals' criminal activities.

On July 1, 2015, the Utah Bureau of Criminal Identification (a division of the Utah Department of Public Safety [DPS]) became the first participant in the Rap Back Program. As of September 30, 2015, the Utah DPS had 14,033 Rap Back subscriptions for active employees within its state. At that time, two Rap Back notifications had been returned for the agency's review.

As the FBI works with the CJIS Advisory Policy Board and the Compact Council to help agencies overcome legislative and technical constraints, it is providing testing environments to ensure field validation and successful operations of the Rap Back Service. The FBI anticipates the enrollment of six more states and four federal/regulatory agencies by the end of Fiscal Year (FY) 2016.

The **Interstate Photo System**, deployed as part of the NGI, enables law enforcement to search facial images against the FBI's national repository of criminal mugshots. These searches return investigative leads (not one-to-one identifications). To date, Michigan, Arkansas, and **FBI Facial Analysis, Comparison, and Evaluation (FACE) Services** (read more about FACE Services on next page) have connected to the Interstate Photo System with additional states and agencies currently testing connectivity. Going forward, there are plans to identify (and incorporate into operations) existing algorithms that would further improve the accuracy of automated searches of the NGI Interstate Photo System's repository.

In FY 2015, the **National Palm Print System** grew to more than 12.5 million prints, providing an additional resource for searching latent palm prints collected from crime scenes and disaster sites. In FY 2016, the FBI plans to electronically enter more than 20 million palm prints



maintained at the state level into the National Palm Print System.

Regarding latent prints, the NGI has also enabled latent searches of civil fingerprints associated with individuals' identification history summaries. In addition, it permitted secondary searches of civil submissions against the Unsolved Latent File (ULF), which contains more than 600,000 records. Each tenprint and palm print submission to the NGI is an opportunity to identify suspects linked to unidentified prints. For example, during FY 2015, a sample of ULF records that were previously searched against the legacy IAFIS and remained unsolved were selected to be reprocessed within the NGI. These searches resulted in the generation of 664 likely candidates, i.e., new investigative leads, for cases related to kidnapping, homicide, attempted bombing, and terrorist investigations.

Capitalizing on the new capabilities that the NGI provides its latent users, the biometric services staff developed the Cold Case Service during the FY. Enhancements to the Cold Case spectrum included the use of search capabilities such as face recognition to support FBI field offices and operational divisions during investigations.

FBI **FACE Services**, provided to FBI field office investigators, has grown exponentially since its launch in 2011 and is now available to all 56 FBI field offices and 11 legal attachés. In FY 2015, FACE Services received image search requests for 3,631 subjects that required biometric images specialists to perform 67,660 face searches and 6,679 text-based searches. As a result of those searches, FACE Services returned 2,354 investigative leads.

BIOMETRIC IDENTIFICATION SERVICES IN ACTION

On June 5, 2015, FACE Services received an image search request from a special agent (SA) assigned to the Pittsburgh Field Office (FO). The Violent Criminal Threat case dealt with a subject charged with Unlawful Flight to Avoid Prosecution-Crime of Violence from nearly 20 years ago. The subject had been found guilty of sexually molesting his three children over a 10-year period. After he failed to appear in court in April 1996, a warrant was issued for his arrest. However, he had evaded law enforcement ever since. To assist with the current investigation, the SA submitted a request form that contained two face photos, along with the subject's name, alias names, date and place of birth, and a Pennsylvania driver's license number.

When the photo search returned a likely candidate in a different state with a different name, additional information searches were performed tying the subject to a stolen identity in another state. On June 19, after tracking those leads and collaborating with agencies in different states, the SA in Pittsburgh reported that the subject was living in Muskogee, Oklahoma, and employed at a local department store. Hours after receiving the Pittsburgh FO's lead, task force members initiated physical surveillance of the subject and arrested him while he was at work, ending his 19-year evasion as a state and federal fugitive.

FBI Biometric Center of Excellence

Continuing to explore the "frontier" of biometric identification

In 2015, the **FBI Biometric Center of Excellence (BCOE)** engaged in projects that used face recognition to fight child exploitation, expanded the nation's repository of iris images, improved fingerprint capture techniques, and explored voice matching technologies. These and many other initiatives are part of the BCOE's efforts to foster collaboration, improve information sharing, and advance the adoption of biometric and identity management solutions across the law enforcement and national security communities. Since its inception in 2007, the BCOE has researched and developed software and conducted pilot projects to evaluate day-to-day operational applications and demonstrate biometric capabilities and concepts. The BCOE also manages biometric standards and development of specifications for the FBI.

Advances made in fiscal year 2015

This year, the BCOE worked with the FBI's Violent Crimes Against Children Unit (VCACU) to use face recognition technology with the Innocence Lost Database (ILD). The ILD is the first national child prostitution database designed to centralize information about victims and the activities and locations of suspects believed to be exploiting them. The BCOE demonstrated face recognition technology for the VCACU, conducting more than 26,000 searches of the VCACU's test data. The face recognition software, along with trained face examiners, made more than 60 matches. This led to the decision to integrate face recognition technology into the VCACU's new system.

The BCOE expanded its Iris Pilot program this year to include new users, and as a result, the repository grew to include more than 339,000 enrollees. The Iris Pilot was deployed in 2013 to establish a national iris image repository, analyze iris-recognition operations in a realistic environment, determine technical and operational best practices, and develop standards for iris capture and transmission. The BCOE will continue to develop the Iris Pilot by increasing the number of enrollees (therefore increasing the size of the searchable repository), expanding iris searches and enrollments to include additional criminal agencies throughout the United States, and enhancing the data quality—all to ensure the highest accuracy.

The BCOE also continued to encourage the development of technologies that match tattoos and symbols that may have significance in certain cases (in jurisdictions where their use is legally allowed). In collaboration with the National Institute of Standards and Technology (NIST), the BCOE sponsors the Tattoo Recognition Technology—Challenge (Tatt-C). The goal of Tatt-C is to assess technologies in image-based matching for tattoos and symbols and to determine which algorithms work best. In June 2015, the NIST hosted a Tattoo Recognition Technology—Challenge Workshop as part of a larger BCOE-sponsored challenge. The purpose of the workshop was to engage the research community to advance research and development in this area.

Biometrics on the horizon

The BCOE works with the criminal justice community, private industry, and the NIST to evaluate the utility and accuracy of "contactless devices." The current concept includes a contactless capture (e.g., photograph) in lieu of a scan taken of the fingerprints, which is expected to provide faster fingerprint capture, less image distortion, and the provision of more data than the traditional flat fingerprint capture method. Contactless fingerprint capture will result in more rapid prisoner bookings by providing quick, clean, fingerprint capture with little or no operator interaction. As this emerging technology develops, the BCOE will work with its partners to determine what additional values may

be added to agency operations using this type of fingerprint capture and then work to develop a certification process for such devices.

The BCOE is partnering with the NIST to launch a project to evaluate the performance of existing voice matching technologies. Exploring how well existing biometric technologies work to solve problems helps determine if, how, and under what conditions technologies may become useful tools for the criminal justice community. The BCOE will publish the findings of the evaluation and will provide stakeholders with factual performance data on voice products.

In addition to furthering fingerprint and voice recognition technologies, the BCOE is researching how aging facial features affect face recognition systems. Significant age differences between images of the same individual create a challenge for such systems. The BCOE has addressed the face aging problem within automated systems by establishing best practices for image capture and sponsoring research on the topic. For instance, automated tools that match faces are known to perform more accurately when using quality images of similar frontal poses. In the next year, the BCOE plans to find more representative test images and expand partnerships with researchers working in this field of study.

Data standards for biometrics

The BCOE administers the FBI Biometric Specifications (BioSpecs) Web site at <www.fbibiospecs.cjis.gov.> The Web site received 111,066 visitors this year alone. The FBI BioSpecs provides the most up-to-date information on biometric standards, certified products, software, and best practices required for the successful transmission of biometric data to the FBI's Next Generation Identification (NGI) System.

The CJIS Division receives more than 261,000 biometric transactions every day, and each transaction must comply with the Electronic Biometric Transmission Specification (EBTS). The EBTS, which provides guidelines for submission of fingerprint transactions and images to the NGI, is updated and maintained by the BCOE.

BCOE IN ACTION

The FBI averages more than 3,000 iris enrollees per week and has identified three deported criminal/aggravated felons through the Iris Pilot's search capabilities. In addition, the Iris Pilot identifications have yielded a 5.6 percent hit rate on one or more National Crime Information Center files, including 2.5 percent with outstanding want/warrants and 1.8 percent identified as sex offenders. For example, a correctional facility searched an inmate's iris images against the FBI's Iris Pilot before the subject's scheduled release. The Iris Pilot results provided information indicating the subject was wanted in another jurisdiction, preventing the subject from being released in error.

Global operations

Furthering information sharing worldwide

The CJIS Division's global operations are first and foremost about biometric information sharing and ensuring that sharing goes smoothly with our partners around the world. As part of these efforts the **Global Initiative Unit** acts as liaison for biometric services for FBI legal attachés overseas and promotes the **Foreign Biometric Exchange (FBE)** program.

This program's primary mission is to collect and share biometrics obtained from foreign law enforcement partners. The biometric records pertain to individuals of interest to the partner country, the United States, or the international law enforcement community. This includes individuals associated with or appropriately suspected of terrorist activity, egregious crimes, or transnational criminal activity. In fiscal year (FY) 2015, the CJIS Division collected 201,855 fingerprint records from foreign countries. Also, CJIS Division staff coordinated the signature of one memorandum of cooperation with a foreign government to participate in the FBE program.

Another area of global effort is the CJIS Division's work with the **Preventing and Combating Serious Crime (PCSC)** program agreements. These agreements represent an effort to enter into law enforcement information sharing agreements with the 38 Visa Waiver Program (VWP) countries. In addition to the VWP countries, the U.S. government has entered into PCSC agreements with other countries that aspire to be admitted into the VWP and understand the national security value of biometric information exchange to detect and combat terrorism and serious crime. The PCSC agreements require that each partner provide electronic query capability of the other's automated fingerprint identification system (AFIS) for criminal justice purposes.

Technical and operational implementation of the PCSC agreements is a joint effort between the FBI and Department of Homeland Security (DHS). The FBI and DHS work with the foreign partners to establish technical mechanisms for exchange of information, according to the authorities provided by the PCSC agreements. Currently, 41 countries have signed PCSC agreements and 26 of those countries are engaged in discussions to implement technical mechanisms to share information under the agreement.

The **CJIS Flyaway** program is a rapid deployment team whose members are prepared to deploy within 4 hours to support national and international special security events, critical incidents, mass arrest operations, sting operations, and other emergency operations with rapid identification services. Flyaway teams use electronic fingerprint capture devices and query FBI, Department of Defense, and DHS criminal fingerprint databases. In FY 2015, there were 14 flyway missions and a total of 388 subjects processed.

Another component of global operations is the **Mobile Biometric Application (MBA)/Quick Capture Platform (QCP)** program. Early in 2015, the CJIS Division conducted a pilot of the MBA program with FBI users. This fingerprint capture tool, which can be utilized on/with an FBI-issued smart phone or tablet, is new technology and quickly became a "game changer" when deployed. During the pilot, several of the test offices submitted success stories of wanted individuals being identified using the MBA. Users advised it gave them "an investigative advantage" and would "change law enforcement and undoubtedly save lives." The MBA and fingerprint scanner will enable FBI special agents and task force officers to quickly determine positive identification of suspected persons. The MBA program is an advancement of the highly successful QCP kits and makes it more conducive to conduct expeditious field operations.

The existing QCP devices, demonstrated in the photos at right, may soon be replaced with a Mobile Biometric Application tool used with a smart phone or tablet.

GLOBAL OPERATIONS IN ACTION

A subject sentenced to serve four years in a North Carolina prison for larceny escaped in 1974 and was at-large for more than 30 years. The FBI and the North Carolina Department of Public Safety located the subject through a collaborative investigation. When approached, the subject presented false identification information. An FBI agent obtained the subject's fingerprints and used the CJIS Division's QCP (CJIS' portable biometric system that allows investigators to collect, query, store, and submit fingerprints during operations anywhere in the field) to check the provided identification information. The QCP, which has the capability to quickly search millions of fingerprints from three government databases, including the FBI's Next Generation Identification system, allowed the agent to establish the subject's true identity and she was arrested.

Public Access Line

Central point of contact for tips from the public

The FBI's **Public Access Line (PAL)** serves as the central intake point for phone calls with information and tips the public wants to share with the FBI about criminal activities and threats to national security.

Since the PAL's inception in 2012, staff have received more than 1.3 million calls and have written more than 18,000 reports on pertinent information gathered. This also accounts for approximately 111,000 hours of work that the field division put to investigative uses rather than handling these phone calls as they had prior to the PAL.

The long-term goal, beginning in fiscal year 2016, is to develop and acquire the responsibility of e-Complaints into the PAL. E-Complaints will offer a centralized location within the CJIS Division for gathering and analyzing intelligence information from the Online Tips interface at <www.fbi.gov>. In addition, e-mails received from the public by FBI field offices will also be included in this process. Investigators and the public will benefit from this new service as it will provide additional access to the FBI through the PAL when reporting intelligence information.

PAL IN ACTION

On April 30, 2015, a PAL customer service representative (CSR) received a call from a distraught father who heard the police banging on the door of his residence. Rather than cooperate with law enforcement, the man barricaded himself inside. Further complicating matters, the father had his 5-year-old son barricaded inside the residence with him. The father called the PAL and demanded that the FBI tell the police to go away. While keeping the supervisory special agent (SSA) advised of the situation, the CSR calmed the father, which ultimately ensured the child's safety. In the meantime, the SSA worked with the FBI field office to conduct an orderly transition of the communication with the father from the PAL to agents on the scene. After almost 2 hours, the CSR transferred the call to the capable staff of the field office knowing that she had done all she could to resolve the situation and that it was in the hands of other experts. At this point, it was up to the FBI field office and the local police to work on a peaceful resolution. Approximately 2 hours later, the FBI field office advised PAL that the father had released his child and surrendered to authorities without further incident. The FBI field office thanked the CSR and PAL for a job well done.

—

In October 2014, a CSR in the PAL received a call from Peru. The caller made a complaint on behalf of her friend, who was the possible victim of crimes perpetrated in Peru by an individual the caller claimed traveled on multiple occasions from the New York area to Peru to engage in illicit conduct with the victim, who was then a minor. The caller also made follow-up conversations to the CSR, and the PAL sent a report about the complaint to the New York Division's Crimes Against Children (CAC) squad. After a few weeks of investigation, the CAC solidified probable cause and obtained arrest and search warrants. The subject was arrested, pled guilty to the charges, allocuted, and was sentenced to 10 years in federal prison for his crimes against an underage female.

CJIS Information Technology

Empowering the division, the Department of Justice, and our partners with vital services

CJIS Information Technology (IT) is not only the backbone of the vital services that the CJIS Division provides, but it is also a major player in the IT architecture of our parent agency, the Department of Justice (DOJ). In fiscal year (FY) 2015, the division realized significant milestones toward the DOJ's goal to consolidate its numerous data centers into just three by 2019. The FBI will operate and maintain two of those three data centers, with one located at the CJIS complex in Clarksburg, West Virginia, and the other, known as the Pocatello Information Technology Center (PITC) located in Pocatello, Idaho. Both locations are undergoing expansion of data center space, improvements to infrastructure, and implementation of plans for communicating with the third DOJ data center.

The DOJ's consolidation of its data centers, known as the Data Center Transition Initiative (DCTI), will optimize and standardize IT infrastructure, improve operational efficiency, and reduce the energy needs of the DOJ data centers. The CJIS Division helped with the DCTI by providing the DOJ with two operational Trusted Internet Connection points, as well as data storage and network infrastructure for the DOJ's unclassified domain. Once completed, the DCTI will establish CJIS as a disaster recovery site for the DOJ mainframe services operating at the PITC.

"People must be empowered with the right tools to be productive, innovative, and efficient."

As part of the data transition in FY 2015, the CJIS Division and the DOJ continued to install new mainframe hardware at the PITC, paving the way for the transfer of mainframe applications from the data center in Dallas, Texas. Similarly, installation of new mainframe hardware in the data center at the CJIS Division will allow the relocation of mainframe applications from a facility in Rockville, Maryland. These two consolidations allowed the DOJ to shutdown the data center in Dallas and will eventually lead to the shutdown of the Rockville site by FY 2017. Once completed, these moves will provide a more efficient use of the DOJ's data centers and reduce, or entirely eliminate, associated costs from space and hardware maintenance and procurement.

Justice Cloud Services

Another high profile component of CJIS Division IT is Justice Cloud Services. The Justice Cloud offers hosting, primary storage, and backup and archive services to DOJ entities and is on pace to replace 20 percent of the DOJ's compute environment. Another increase in compute capacity will occur when CJIS Division IT replaces out-of-date hardware which is slated for spring 2018. Costs associated with hosting on the Justice Cloud have decreased 2 years in a row, and the division projects another decrease in 2016. This confirms that the virtualization and standardization of IT systems/services is helping to decrease IT operating costs.

In the end, the CJIS Division, like every organization, is about its people. But, people must be empowered with the right tools to be productive, innovative, and efficient. CJIS IT provides that empowerment to the division, to the DOJ, and to the division's partners in the criminal justice community.

CJIS Advisory Policy Board

Collaborating from varying perspectives

Through the **CJIS Advisory Policy Board (APB)**, the CJIS Division seeks collaboration with law enforcement, criminal justice, and noncriminal justice communities. The different perspectives gained from this cooperation produce recommendations that are essential to the success and improvement of the CJIS Division's information-sharing systems and programs.

The APB, chartered under the provisions of the Federal Advisory Committee Act, consists of 35 representatives from criminal justice and national security agencies nationwide. The CJIS Advisory Process operates under a shared-management concept in which representatives of local, state, tribal, and federal system users provide guidance and direction regarding the criminal justice information systems and initiatives that are administered by the CJIS Division. The APB reviews and discusses general operational and technical policy proposals related to CJIS Division programs and makes recommendations to the FBI Director.

In fiscal year 2015, the APB addressed numerous topics and made several recommendations, some highlights of which are as follows:

- **National Crime Information Center (NCIC)**—The APB moved to add an image field to the NCIC Protection Order File, enabling officers to identify protected persons based on protection order photos. The board included a caveat asking CJIS staff to explore the need for a consent waiver to address privacy concerns. CJIS staff will add the image field during the development of the NCIC Third Generation.
- **CJIS Security**—The APB recommended adding the concept of *virtual escorting* to the *CJIS Security Policy*. Virtual escorting eliminates the need to assign authorized personnel to monitor unauthorized personnel performing remote system maintenance. Virtual escorting detects prohibited actions and immediately terminates the user's session without the need for a physical escort.
- **Identification Services**—The APB moved to allow identity history summaries located in the Next Generation Identification to contain DNA indicator information. This would inform criminal justice agencies outside of the state that collected the DNA of the presence of such information in any state DNA Indexing System.
- **Uniform Crime Reporting (UCR)**—The APB recommended the formation of a focus group to develop a plan to expand the National Incident-Based Reporting System (NIBRS) definition of Manslaughter by Negligence to include all non-operator fatalities resulting from an impaired operator of a vehicle or vessel. This recommendation was based, in part, on a proposal from the Association of State Uniform Crime Reporting Programs, with support from the National Sheriffs' Association and the International Association of Chiefs of Police. Currently the NIBRS user manual excludes such fatalities from its crime counts, and Manslaughter by Negligence (as currently defined) does not include Vehicular Manslaughter. Implementing the change will better define incidents of Vehicular Manslaughter by Negligence.

APB a "perfect example of practitioners coming together for the common good"

Chief Elaine Snow heads the police department in Rome, Georgia, and is one of the local agency representatives involved in the CJIS APB process. "Local agencies bring a different perspective from the state and federal agencies," she said. "It's great to have the opportunity to see what's happening with the recommendations that are made and share how changes may impact us at the local level. To be able to provide input and see how that input can shape a final decision is very rewarding."

Chief Snow believes APB discussions result in real-world services and tools that help officers on the street be safer and provide better protection for the citizens and communities they serve. "As a board, we are always striving for a good balance between protecting the privacy of citizens and having the information we need to protect them," she said. "In the discussions we have, it is important to hear all the options and opinions, but we all share a common goal to make the best decisions. This process is a perfect example of practitioners coming together for the common good."

Another component of the APB process that Chief Snow appreciates is the interest CJIS program managers and staff have in improving services. "Being asked 'how can we help you?' and 'how can we make this service better for you and your community?' is just something we do not typically hear," she said. "It's wonderful. The customer service provided across the division is genuine. There is a team approach of asking the questions and working together for solutions."

Virginia police chief and APB member says "use-of-force" data collection must be carefully considered

During 2015, FBI Director James B. Comey made clear his perspective that law enforcement needed reliable and timely data about incidents of use of force by police nationwide. In response, the CJIS Division has been working to define the scope and content of such a data collection that could be established as part of its effort to collect law enforcement statistics. **Douglas A. Middleton**, Chief of Police for Henrico County, Virginia, serves on the UCR Subcommittee of the CJIS APB. In the fall of 2015, the subcommittee reviewed information and recommendations from the APB's Working Groups about how to best collect police use-of-force data via the UCR Program. "The Henrico County Police Division is internationally accredited and we already collect this information," Chief Middleton said. "If the use-of-force data collection is established properly and circumspectly for the nation, there will be benefits to our communities, states, and the country."

Most important to Chief Middleton, however, is that the FBI and APB remain committed to the doing the "right thing" at every stage of developing the data collection. "We have a responsibility to those who work all hours of the day in all weather, who sacrifice time with their families, who deal with the frustration of trying to enforce the law in a bureaucratic system, and who are obligated to make split-second life and death decisions knowing they will be judged and critiqued for what they have done," he said. "These officers put their lives on the line every day to guarantee the safety of their community, not for a paycheck, but because they believe in what they are doing. We have a responsibility to them, and to those who have gone before them and made the ultimate sacrifice."

Compact Council

Enhancing safety while protecting privacy

The **National Crime Prevention and Privacy Compact Act of 1998 (Compact)** led to the creation of the 15-member Compact Council. The Compact Council establishes rules and procedures for using criminal history record information (CHRI) for noncriminal justice purposes (e.g., screening for employment or licensing).

In fiscal year 2015, the Compact Council continued to enhance public safety while respecting individuals' privacy through the following initiatives:

- The Compact Council approved the Bureau of Indian Affairs' (BIAs') proposal, issued on behalf of federally recognized tribes, to use the Fingerprint Submission Requirements Rule (Title 28, Code of Federal Regulations, Part 901), known as "Purpose Code X." This allows the BIA, during critical situations involving the temporary placement of children, to access the Interstate Identification Index (III) to conduct criminal history record checks with delayed fingerprint submissions of residents with whom the children will be placed. This provides a solution to those federally recognized tribes that would otherwise be unable to obtain timely criminal history information.

- Ohio became the 19th state to participate in the National Fingerprint File (NFF) program. This means that Ohio, like the other NFF participants, will no longer forward all its arrest fingerprint records and supporting documents to the CJIS Division, but will instead be responsible for maintaining all such documentation on its own. When a fingerprint-based background check submission produces a match in the III to an Ohio state-maintained record, the NGI will reach out to Ohio's criminal history repository, and Ohio will provide its criminal history record. NFF participation eliminates record duplication, enhances individual privacy protections, and helps protect our nation by supplying accurate and current criminal history record information.

- The Compact Council published a document titled, *National Fingerprint-Based Background Checks—Steps for Success*. This document helps educate lawmakers who are interested in drafting federal legislation that provides the best background check results. The document assists legislatures in understanding the best practices for obtaining a complete criminal history record check and emphasizes that any legislation dealing with criminal history should be consistent with the Compact. (This document is publicly available on the Council's Web site at <www.fbi.gov/about-us/cjis/cc/library/national-fingerprint-based-background-checks-steps-for-success>.)

The Compact Council, along with the CJIS Advisory Policy Board, embodies a collaborative spirit that results in the continued success of the CJIS Division's services.

Contributing to the successful implementation of the Compact

Dr. Natalie Chrastil, vice chairperson the Compact Council, says council members have a vital role in ensuring the appropriate use of criminal justice information for noncriminal justice purposes. Part of this work is helping states to ratify the Compact and, subsequently, participate in the National Fingerprint File, or NFF, program. NFF states increase efficiency, accuracy, and enhance the protection of individual's privacy in the national background check process.

Dr. Chrastil, who hails from Wyoming (already a Compact/NFF state), serves as Deputy Directory of the Wyoming Division of Criminal Investigation. She said the commitment on the part of the state to ratify the Compact and become an NFF state requires legislation be drafted and passed, along with many other steps that make it a lengthy, often multi-year, process. "One of the things we have learned from states who have gone through the process is that the Council needs to remain more involved," Dr. Chrastil said. "Turnover in staff and unfamiliarly with the steps needed are factors that can lengthen the process. We are developing a mentoring program where Compact Council officers have volunteered to partner with potential Compact states to help them." That assistance may involve meetings with key stakeholders, identifying necessary legislation, making on-site visits, and answering any questions that arise. "We believe the consistency and continuity of a mentor may make a difference in how successful the program can be."

Another key task the Compact Council does is track proposed national and state legislation that could potentially

impact the provisions of the Compact that enable criminal history background checks to protect vulnerable populations. Dr. Chrastil said a current strong partner in this effort has been the Government Affairs arm of nonprofit organization SEARCH, The National Consortium for Justice Information and Statistics. "Between this group and the FBI's attorneys, we have a good handle on what is being proposed and the effects it may have," Dr. Chrastil said. "It has been an excellent partnership."

Overall, she believes the Compact Council is in a busy and productive time. "We have lots of good energy on the Council," she said. "We have a good mix of members who have been with the Council for a while and have good historical knowledge, and some new ones who have fresh perspectives and are forward thinkers. It's an exciting time for us."

About the CJIS Division

The CJIS Division is divided into two branches. The **Operational Programs Branch**, led by **Deputy Assistant Director Randall C. Thysse**, includes many of the CJIS Division's crime reduction and terrorism prevention programs and initiatives, including the National Crime Information Center, the National Data Exchange, the Law Enforcement Enterprise Portal, the Biometric Center of Excellence, the Uniform Crime Reporting Program, and global outreach efforts. This branch also coordinates the CJIS Division's contract and administrative functions.

Randall C. Thysse

The **Information Services Branch**, led by **Deputy Assistant Director Jeremy M. Wiltz**, includes the development, enhancement and maintenance of the CJIS Division's vast information technology (IT) holdings that provide the backbone for all division services, as well as the division's cooperative IT efforts with the Department of Justice. The branch also administers the division's multimodal biometric identification services, the Next Generation Identification System, and the National Instant Criminal Background Check System.

Jeremy M. Wiltz

CJIS Advisory Process "critical to the success of CJIS services"

For 21 years, **Michael McDonald** wore the Delaware State Police Uniform. He retired in 1999, but has continued to serve the Delaware State Police in the civilian role of Director of Information Technology and Communications and CJIS Systems Officer. He also has been active with the CJIS Advisory Policy Board (APB) in that time, currently serving as vice chairperson. "Since I first started in law enforcement, the tools and technology available to officers is like night and day," he said. "Officers really appreciate having these additional capabilities in their toolkit."

Through Mr. McDonald's efforts, and because of the size and unique environment of statewide integrated criminal justice, Delaware criminal justice information systems have often been a "testing ground" for CJIS Division services and enhancements. "We are a small state with centralized systems," he said. "We are able to provide valuable feedback during development, and help with special projects." He cites the Delaware pilot of the National Data Exchange system in 2007 and 2008, and, recently, as a member of the Disposition Task Force, working with the CJIS Division on an initiative related to increasing the dispositions reported to the Next Generation Identification. "This kind of collaboration and analysis helps everyone," he said.

Mr. McDonald said the entire APB process enables law enforcement to embrace opportunities to provide needed services and enhancements with the input of the users. "It is true 'shared management,'" he said. "There is no other structure of shared management that can reach out to all those who have an interest in and who have an impact on national and international public safety, criminal justice, and homeland security issues. From the Working Groups to the Board itself, all agencies who participate in providing and using CJIS services are welcome and encouraged to be involved in the process and have their voices heard. It is critical to success of CJIS services."

Our Campus

Located in Clarksburg, West Virginia, the CJIS Division campus stretches across 986 acres of scenic foothills in the Appalachian Mountains. The main building, completed in 1995, contains 526,000 square feet of offices and a data center that hosts programs serving law enforcement and criminal justice agencies across the nation and around the world. These programs provide the criminal justice and intelligence communities with services such as fingerprint identification, face recognition services, the FBI's public tip hotline, firearm purchase background checks, law enforcement information sharing, and crime statistics.

In addition to the main facility, the campus includes a service center, a central power plant, a visitor's center, and a child development center. Each year, the campus is the site of a Fallen Law Enforcement Officers Memorial Ceremony and the FBI Jerry Dove Memorial 5K race, an event that celebrates the memory of FBI Special Agent and West Virginia native Jerry Dove, who was killed in the line of duty.

The CJIS Link (Link) keeps agencies informed about CJIS Division 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*.

Biometric Technology Center

New facility dedicated

Over the last year, work on a new Biometric Technology Center (BTC) building has neared completion. The BTC will accommodate approximately 1,400 personnel. On August 11, 2015, the CJIS Division welcomed dignitaries and members of the news media to the campus to formally dedicate the building. The new building will provide 300,000 square feet of office space for the CJIS Division's biometric services and 60,000 square feet for the Department of Defense's (DoD's) Biometric Identity Management Activity, bringing together the FBI's biometric services and the DoD's biometric identification holdings into one facility. The BTC will include a biotech laboratory where the Biometric Center of Excellence will host a variety of testing and evaluation activities in close coordination with academia and private industry. This will help ensure that the federal government remains on the forefront of biometric identification services.

Taking part in a dedication ceremony for the new BTC on August 11, 2015, are, from left, Don Salo, Director of the U.S. Army's Defense Forensics and Biometrics Agency; Brig. Gen. Mark Inch, who oversees the U.S. Army's criminal investigation command; U.S. Sen. Joe Manchin, D-W.Va.; Amy Hess, Executive Assistant Director of the FBI's Science and Technology Branch; the Rev. Hilarion Cann, CJIS chaplain; and Stephen L. Morris, Assistant Director of the CJIS Division.

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