

CJIS Division

2019 YEAR IN REVIEW

connect

identify

know

Progress and partnership highlighted in 2019

As the Assistant Director of the FBI's Criminal Justice Information Services (CJIS) Division, it is my honor to present the *CJIS Division 2019 Year in Review* publication. This document showcases the great work of our CJIS Division employees and contractors as we work to meet our mission to equip our partners with the criminal justice information needed to protect the United States while preserving civil liberties.

During fiscal year 2019, we continued to see benefits from our agile development approach and made significant progress in the areas of automation and use of the secure cloud, thereby strengthening our information technology services. Also during the year, we received tremendous support from our law enforcement partners for the transition to the National Incident-Based Reporting System and the participation in the National Use-of-Force Data Collection (see page 13 for more information). Both of these initiatives will result in more robust statistics for the nation and help guide law enforcement training. We continued to enhance our strong CJIS biometrics services. The ability to help our partners "connect, identify, and know" through biometrics is vital to preventing and fighting crime and terrorism.

As we recognize the innovation and achievements across our programs and services, we celebrate the 25th anniversary of our formal partnership with the law enforcement and criminal justice community through our CJIS Advisory Policy Board process. The success of the CJIS Division is grounded in collaboration with our partners. What we have accomplished together benefits the entire law enforcement and criminal justice communities. The safety of this nation and our citizens remains our top priority.



Michael D. DeLeon

Assistant Director of the FBI's CJIS Division



Contents

Celebrating 25 Years of CJIS APB and 50 years of partnership 2

Our Campus 4

NCIC: The 3rd Generation
System embarks on journey to modernize user experience 5

National Instant Criminal Background Check System
Resolving obstacles with innovative solutions 6

National Data Exchange
Adding resources, speeding up processes 8

Law Enforcement Enterprise Portal
Providing users a virtual gateway and collaboration tools. 12

Uniform Crime Reporting Program
First-of-its-kind data collection gets underway 13

Biometrics Services
Adding new tools to the biometrics toolbox 14

National Threat Operations Center
Always available, always ready to listen 16

Information Technology Services
Keeping CJIS technology a step ahead 17

National Crime Prevention and Privacy Compact Council
In safe hands: maintaining privacy and safety 19

FBI Citizens Academy
Sharing the FBI's mission and vision with our community 20

CJIS Division 2019 YEAR IN REVIEW



The *CJIS Link*

Follow CJIS all year long

Want to keep up with the CJIS Division?

Stay current on our division's programs and successes by following our news blog, the *CJIS Link*. Here, you'll learn about new initiatives at the CJIS Division, changes or enhancements to CJIS services, and success stories from investigations in which law enforcement agencies used CJIS programs or systems, and much more.



Scan the QR code with your smartphone or visit <https://www.fbi.gov/services/cjis/cjis-link> to learn more or to sign up for e-mail updates from the *CJIS Link*.



Celebrating 25 Years of CJIS APB and 50 years of partnership

For 25 years, the CJIS Advisory Policy Board (APB) has helped the CJIS Division adapt and expand its criminal justice information programs in order to maintain an edge in the fight against crime and terrorism. The FBI developed the CJIS APB to solicit guidance from the users of the CJIS Division's services. APB subcommittee and working group participants provide input concerning the development and operation of all of the CJIS Division's programs. The philosophy underlying the advisory process is one of shared management; that is, the FBI, along with federal, state, local, and tribal data providers and system users share responsibility for the operation and management of all the systems administered by the FBI for the benefit of the criminal justice community.

The APB's 25-year milestone is rooted in a history of collaboration spanning five decades. In 1969, the FBI established the National Crime Information Center (NCIC) Advisory Board to assist with management and governance over the NCIC System. Twenty years later, the FBI duplicated the successful shared-management philosophy within the Uniform Crime Reporting (UCR) program

and formed the UCR Data Providers Advisory Board. The NCIC and UCR boards were combined in 1994. At that time, the FBI established an overarching process, and the CJIS APB began to advise on the programs and services administered by the CJIS Division.

Since the CJIS APB formed 25 years ago, enhancements approved by the APB have ensured that longstanding services, such as NCIC checks and fingerprint identification, are effective and efficient. What began with governance of NCIC and UCR has expanded to include: Next Generation Identification, the National Data Exchange, the Law Enforcement Enterprise Portal, and the National



Since the CJIS APB formed 25 years ago, enhancements approved by the APB have ensured that longstanding services are effective and efficient.

Instant Criminal Background Check System. The most recent addition to the CJIS Division's lineup of services is the National Use-of-Force Data

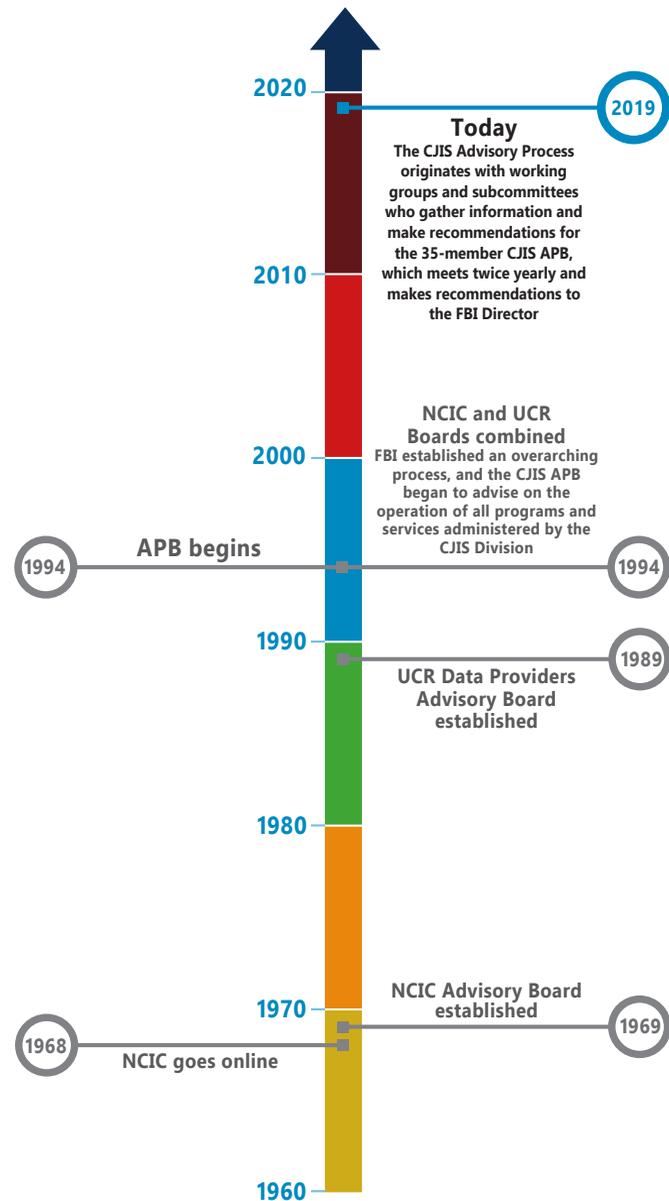
Collection. This service, like many others, was evaluated and approved through the thoughtful oversight and guidance of the CJIS APB.

The CJIS Advisory Process originates with working groups and subcommittees who gather information and make

recommendations to the 35-member CJIS APB, which is chartered by the Attorney General under the Federal Advisory Committee Act. The CJIS APB meets twice a year to review appropriate strategy, policy, technical, and operational issues. Its recommendations on national criminal justice information services are submitted to the FBI Director for final approval. (To date, the CJIS APB has provided more than 2,200 recommendations to the FBI Director.)

The CJIS APB and the CJIS Advisory Process is supported by the nation’s criminal justice community and includes active members from:

- State and local law enforcement agencies, representing all 50 states and the U.S. territories
- Federal law enforcement agencies
- Tribal law enforcement agencies
- Prosecutors
- The Judicial Branch
- National security agencies
- Correctional agencies
- American Probation and Parole Association
- International Association of Chiefs of Police
- Major Cities Chiefs Association
- Major County Sheriffs of America
- National District Attorneys Association
- National Sheriffs’ Association
- American Society of Crime Laboratory Directors
- Courts representative
- The Royal Canadian Mounted Police



Our Campus

Tucked in the rolling hills near Clarksburg, W.Va., is a diamond in the rough—the 990-acre campus known as the FBI’s CJIS Division. The grounds are the setting for two buildings that are the hub of the division: CJIS Main, a 528,000-square-foot office building and epicenter of criminal justice technology, and the Biometric Technology Center (BTC), a 360,000 square foot building dedicated to the analysis and advancement of biometrics, or human characteristics to aid identification. The CJIS complex also includes an FBI Police duty station, a service center, a central power plant, and a childcare facility.

In 2019, the CJIS Division underwent the typical renovations that a nearly 25-year-old installation needs. CJIS Main had 10 restrooms renovated throughout the building and a complete sidewalk replacement. At the property’s West Gate entrance, a canopy was built allowing the FBI Police to conduct more effective vehicle searches in all weather conditions. The future is looking bright for CJIS as new projects and upgrades are in the works for 2020, including a BTC lobby annex, the construction of the CJIS Square (a visitor-friendly area), and a 9/11 memorial.

There are plenty of break-time activities for CJIS employees on campus. They can enjoy a walk or run on the paths around the acreage or use their off time exercising in the 24-hour gyms located in both office buildings. On rainy or cold days, employees can enjoy lunch in cafeterias, or on a summer or fall day, they can eat at picnic tables on the patio.

The CJIS Division continues to offer annual events, such as Family Day and the Jerry Dove Memorial 5K Race, for its employees and family members, law enforcement colleagues, and the local community. The FBI Recreation Association held its annual softball tournament in July, bringing together teams from different states and law enforcement agencies for a fun-filled day

of friendly competition. Of special note this year, a white pine peace tree and memorial stone was dedicated on September 25 outside CJIS Main to symbolize peace and unity. It also reaffirmed a strong partnership between the FBI, our tribal law enforcement partners, and Native American communities.



The Peace Tree tradition is celebrated by the FBI and the CJIS Advisory Policy Board with tribal law enforcement. The Peace Tree serves as a reminder of the vital role tribal law enforcement agencies have in supporting public safety. Centuries ago, the Seneca, Cayuga, Onondaga, Oneida, and Mohawk Tribes cast aside intertribal conflict and united to become the Haudenosaunee (People of the Long House). They established a representative democratic government and memorialized the newly established peace by planting a white pine tree on the shore of Onondaga Lake in what is now New York State. The symbol of the Great Tree of Peace continues to serve as a reminder to Haudenosaunee people and others of the benefits of working together for the common good.

NCIC: The 3rd Generation

System embarks on journey to modernize user experience

It's no surprise that the National Crime Information Center (NCIC) continued its dependable, high-speed service to federal, state, local, and tribal agencies during fiscal year (FY) 2019. During that time, NCIC averaged 10,924,809 transactions per day, and the system responded to each of those requests in a fraction of a second. For NCIC, reliability is an asset. However, technology and varying needs from law enforcement mandate a need for change. Even with the upgrade of NCIC 2000 some 20 years ago, the appearance of NCIC information has looked much the same all five decades of its existence. But that is changing.

In November 2018, the FBI Director approved a recommendation from the CJIS Advisory Policy Board (APB) to adopt an Agile APB Process for the development of NCIC 3rd Generation (N3G). The



NCIC information has looked much the same all 5 decades of its existence. But that is changing.

Agile APB Process, simply put, charts a course for rapid delivery of the updated functions of the N3G Project.

In May 2019, NCIC began accepting National Information Exchange Model (NIEM) Extensible Markup Language, better known as XML, in its operational environment. This technological upgrade sets the scene for the N3G Project, which will enable users to customize an NCIC response for their specific purposes—making it easier to read and allowing users to incorporate information into their own information systems.

Looking ahead, NCIC plans to accept various file formats, as well as larger and higher resolution images. This stage of the N3G Project will also allow users to upload text documents and

Portable Document Format (PDF) files to NCIC records. This will enable agencies to upload copies of warrants or protection orders, for example.

In addition to improvements in collection and presentation, the system will begin transitioning users from the legacy File Transfer Protocol to the more automated and secure CJIS Electronic File Transfer Service (EFTS). The EFTS service will give users access to bulk-type NCIC extracts in a more secure environment while providing a platform that will more easily accept bulk data.

NCIC and young girl help apprehend kidnapper

On June 12, 2019, authorities in Lamar County, Mississippi, received a report that a man, believed to be under the influence of drugs, abducted his 6-year-old niece and stole a vehicle in Hattiesburg, Mississippi. Lamar County deputies searched for the suspect, the vehicle, and the girl throughout the night, but they were unable to locate any of them.

Just before noon on June 14, across the state line in Birmingham, Alabama, a concerned citizen called 911 to report a child wandering around with no adult supervision in the parking lot of a travel center off a local highway. Birmingham officers responded and found a young girl, who told them her name.

They ran a check of NCIC and determined she was a missing endangered juvenile out of Hattiesburg. With the girl's help, the officers located the suspect sleeping in a car parked nearby. The officers took the suspect into custody and returned the girl to her family.

National Instant Criminal Background Check System

Resolving obstacles with innovative solutions

In fiscal year (FY) 2019, the National Instant Criminal Background Check System (NICS) increased speed, efficiency, and accuracy of firearms checks through three major innovations: business process automation, the Fix NICS Act, and an initiative to directly collect vital court records.

With process automation, NICS software now performs certain tasks regarding firearm transactions, freeing staff to handle more complex cases. Since its launch in 1998, NICS has seen large increases in transaction volume, averaging 5.1 million annual federal transactions between 1999 and 2011. A new



Often, missing information in court records precludes staff from making on-the-spot decisions. The Fix NICS Act aims to improve NICS services.

average of 8.7 million each year from 2012 to 2019 was recorded.

This new automation feature allows staff to increase productivity and tackle rising

transaction volumes in a more time- and cost-effective way. As of August 2019, when reviewing criminal records matching potential firearms transferees, NICS software can automatically assess nearly 1,000 different criminal charges. This allows for the efficient routing of transactions so they may either be immediately resolved or sent to an examiner for further review. Around 2.7 million potential functions have been identified overall. NICS plans to continue building and testing these automations. The result on the other end of the transaction, firearm dealers are reaping the benefits of faster processing times for customers.

Missing dispositions on arrest records has long been the top obstacle for NICS staff. NICS strives to provide an immediate

determination of a person's eligibility to possess a firearm and/or explosives while the firearms dealer is still on the telephone or actively engaged in an online E-Check. In fact, the U.S. Attorney General (USAG) has mandated that NICS maintain an immediate determination rate of 90 percent. Often, missing information in arrest records precludes NICS staff from making timely decisions. The Fix NICS Act (which took effect in March 2018) aims to improve and increase the availability of information. The Act requires federal agencies to submit relevant records to the NICS and report certain record submission metrics to the USAG. An additional requirement is for the USAG to collaborate with states in the development of four-year plans which would help to address shortcomings in records reporting.

In FY2019, NICS worked closely with the Department of Justice in creating an implementation plan template for federal and state partners to help them identify and fix problems in their record-sharing procedures. To date, plans have been received from all 50 states as well as 70 federal agencies.

In addition, NICS began piloting a straightforward approach to obtaining missing records by contracting with services in the least responsive areas of the country. NICS provides a list of needed data to staff, who go directly to record-keeping facilities and obtain the information. Though still a pilot program, this approach seems to offer a promising solution to incomplete records.

NICS by the numbers

While accomplishing all this innovation, NICS staff managed to continue providing exemplary customer service.

In FY2019 NICS:

- Processed 27,487,818 total transactions (5.08 percent more than in the previous year).
- Denied 101,669 federal firearm transactions.
- Boasted a 90.08 percent immediate determination rate.
- Processed 81.96 percent of all federal NICS transactions online via the NICS E-Check.

NICS prevents fugitive from buying firearm

In 2019, a person attempted to purchase a long gun at a pawn shop in Texas. The NICS examiner could not make an immediate determination for eligibility because, while the person's criminal record showed arrests, the court records lacked dispositions for the charges. The examiner contacted the U.S. District Attorney regarding the charges and discovered the subject was wanted by the Drug Enforcement Administration (DEA). The collaboration among the NICS staff, the DEA, and the U. S. District Attorney's office led to the arrest of the subject, who is being held pending felony charges.



National Data Exchange

Adding resources, speeding up processes

Information sharing is crucial, and time is of the essence in law enforcement investigations. The National Data Exchange, or N-DEX, is getting faster at helping agencies link pertinent information to help solve their cases. In fiscal year (FY) 2019, N-DEX implemented a tool that automates the largest and most time-consuming tasks of the data integration process. Ninety percent of data extraction and analysis and 50 percent of data mapping were automated by the tool. As a result of this automation, the time it takes to integrate an agency's data into N-DEX was cut by half, allowing better information sharing between agencies.

Two hundred additional criminal justice agencies began contributing data to N-DEX in FY2019, increasing the total number of



N-DEX continues to help agencies connect the dots between information they have and the information in databases from other agencies.

contributors to more than 7,400 agencies in 44 states. In FY2019, the N-DEX System provided access to nearly 829 million records. Also, during

the FY, users performed nearly 17 million searches.

N-DEX continues to help agencies connect the dots between information they have and the information in databases from other agencies. Users also have the ability to perform batch searches, allowing a search of multiple items in a list, simultaneously. This enables continuous status monitoring of investigative targets, missing persons, and fugitives, as well as automated monitoring of high-risk, supervised populations. The batch search function was used in two major operations

with which N-DEX assisted. In Operation Safe Summer II, the connection of what appeared to be unrelated records led to the discovery of several missing children and wanted sex offenders. During the month-long Operation Independence Day, law enforcement arrested dozens of sex traffickers across the country and rescued more than 100 children.

Changes on the horizon

N-DEX is joining forces with the Law Enforcement Enterprise Portal to minimize the number of steps required to access the system, streamlining log on for thousands of N-DEX users.

The N-DEX database will soon be able to provide new services to federal and state agencies. Searches of N-DEX for firearms-related checks will soon be available, and federal agencies will be able to perform N-DEX searches as part of reinvestigations to ensure employees and contractors with federal security clearances are suitable to continue their employment with that agency.

From the technology perspective, N-DEX will continue its shift to cloud computing by storing its data, software, and applications on remote, secure servers. This will enhance collaboration capabilities and improve reporting and storage capabilities. The move will also aid future system growth. Completion of the move to the cloud is scheduled for April 2021.

N-DEX helps identify child predator and victims

A routine N-DEX system search led to federal charges for a Pennsylvania man and earned the 2019 N-DEX Success Story of the Year Award for the Wayland (Michigan) Police Department (WPD). A 12-year-old boy had encountered a man online who

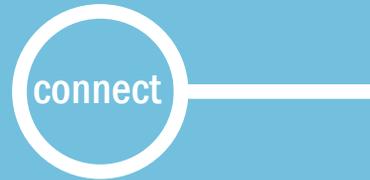
claimed to be a wealthy prince living in Beverly Hills, California; however, the man was actually unemployed and lived in Pennsylvania. An investigating officer with the WPD obtained a search warrant for the suspect's social media account information and Internet Protocol address, and he identified the suspect's possible name and address. The officer logged into N-DEx and searched the suspect's name and address, which helped establish probable cause for the search warrant on the suspect's residence in various police reports.

As a result of records found in N-DEx, the officer was able to obtain a search warrant for the suspect's residence, where investigators uncovered more than 1,000 suspected child porn images and identified additional suspected juvenile victims. The suspect was arrested and subsequently pleaded guilty to numerous federal charges.



From left to right: Michael D. DeLeon, CJIS Assistant Director; Barry J. Fagan, N-DEx Program Unit Chief; Wendy Easterbrook, Michigan State Police Department crime specialist; Chief Mark Garnsey, Wayland Police Department; Officer Mark Riemersma, Wayland Police Department; and Scott A. Rago, Global Law Enforcement Support Section Chief.

CJIS Division Fiscal Year 2019 by the Numbers



Biometric ID Services



77,471,369 Total number of criminal fingerprints in the repository.



69,153,149 Total number of fingerprint receipts/processed.

189,461 Average daily total of fingerprint receipts/processed.



38,487,078 Total number of criminal full face images used in comparisons. This includes 17,892,828 unique individuals.



16,023 Number of processed Facial Recognition Searches for active investigations.

Average Response Times



5 min 42 s
Criminal Fingerprint

17 min 19 s
Civil Fingerprint

40 min 43 s
Searches of the Interstate Photo System (mugshots)

National Crime Information Center



3,987,555,328 Total transactions.

10,924,809 Average daily transactions.



0.0128 s Average response time.



16,115,218 Total number of active records in the NCIC system.

National Data Exchange



16,633,813 Total number of N-DEX searches.



828,858,024 Total number of searchable records.



7,419 Total number of agencies in the United States contributing data to the N-DEX system.

identify

know

OUR MISSION To equip our partners with the criminal justice information they need to protect the United States while preserving civil liberties.

CJIS Information Technology



Committed to principles of Cloud Integration/Continuous Delivery to maximize staffing.



Implementing enhanced automation to optimize efficiency.

Operating all CJIS Systems an average of 99.85% of the time.



Divisionwide support of agile development planning and processes accommodating shifting priorities, workload changes, staffing changes, and customer needs.

National Threat Operations Center



540,307 Total number of tip calls received.



727,949 Total number of E-Tips received.



74,551 Total number of leads submitted to field offices.

National Instant Criminal Background Check System



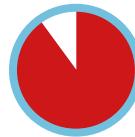
27,487,818

Total number of transactions processed (5.08 percent more than the previous year).



101,669

Total number of denied federal firearms transactions.



90.08 %

Immediate determination rate.



81.96 %

Percentage of federal NICS transactions processed online via the NICS E-check system.

Law Enforcement Enterprise Portal

Providing users a virtual gateway and collaboration tools

Revolutionizing its technology keeps the Law Enforcement Enterprise Portal (LEEP) in top shape. By modernizing current services and developing new enhancements and applications, LEEP continues to meet its users' needs and increase its user base.

LEEPs and bounds

In fiscal year (FY) 2019, LEEP continued to transform the way users access the system and its features. For those who use CJIS services via LEEP, the new CJIS Services Portlet is a quick way to view and select CJIS Services on the portal. Clicking the CJIS icon on the Services Preferences bar located on the LEEP homepage narrows the menu to CJIS services, such as the National Data Exchange and E-checks for gun purchase background checks. In addition, the JusticeConnect application, a real-time collaboration and communication tool for criminal justice, has a new chat feature that can be used simultaneously with other services on LEEP. Chat offers the ability to conduct business instantly and securely in various ways, such as group chats and file sharing.

LEEP continued to grow as CJIS staff added eight new services in FY2019, including the Symbols Affiliation Library, the VALOR Officer Safety and Wellness Program, and the Law Enforcement Officers Killed and Assaulted Program data collection. In all, 53 services are now on LEEP. While most users access LEEP's services by logging in with their LeepID Accounts, more agencies are opting to become Identity Providers (IdP). An IdP is an agency that provides single sign-on access to LEEP through their system via an icon or link on the agency's desktop. This year, Incident Management Analysis and Reporting System users within the U.S. Department of Interior as well as the Pima County Sheriff's Department

in Arizona became IdPs. This brings the number of agencies accessing LEEP in this way to 34. In addition to the increase in the number of services and IdPs, the average number of times users access LEEP has also increased to 856,000 instances per month.

Several developments are in the works for the coming year. Through technology and innovation in 2020, LEEP will provide a new software solution to automate the vetting and updating of LeepID Accounts allowing users to gain access much quicker. LEEP is also working toward a mobile application to make it easier for law enforcement to use LEEP in the field. LEEP's most popular service, the Virtual Command Center (VCC), will be enhanced to expand the usability of this platform during critical incidents and special events.

VCC tracks Medicare fraud takedown

LEEP's VCC played a role in bringing down one of the largest healthcare fraud schemes in U.S. history—Operation Brace Yourself. This \$1.2 billion dollar Medicare scheme spanned several continents and involved medical professionals, corporate executives, and owners of medical equipment companies who gave doctors kickbacks and bribes for prescribing unnecessary braces to thousands of unsuspecting elderly and disabled patients.

Twenty FBI field offices, 17 U.S. Attorneys Offices, representatives from Health and Human Services, and the Internal Revenue Service used LEEP's VCC to manage and track the operation nationwide. Twenty-four defendants were arrested and charge with allegedly laundering the proceeds through international shell companies and using the money to purchase exotic cars, yachts, and luxury real estate around the world.

Uniform Crime Reporting Program

First-of-its-kind data collection gets underway

Law enforcement officers face inherently dangerous situations on a daily basis. At times, they are required to use force in the course of their duties. In January 2019, the FBI launched an official, national mechanism to collect data on the incidents in which officers use force.

Growing and excelling

The National Use-of-Force Data Collection is the result of years of work and collaboration between the FBI and representatives at every level of law enforcement—federal, state, county, city, and tribal. The goal of the data collection is to offer a comprehensive view of the circumstances surrounding the use of force by law enforcement and to promote more informed conversations about the topic. To date, 3,654 agencies from several states provide the FBI with use-of-force data. Eight states have established deadlines to begin participating.

The National Use-of-Force Data Collection, however, wasn't the only collaborative effort that delivered in 2019. In April, staff in the Law Enforcement Officers Killed and Assaulted (LEOKA) Program released *Ambushes and Unprovoked Attacks: Assaults on Our Nation's Law Enforcement Officers*. A joint effort between LEOKA staff and researchers at West Virginia University, the 140-page study provides some explanations and insights into incidents in which offenders intentionally harmed officers during ambushes and unprovoked attacks. The report is a tool to help the law enforcement community better understand why these attacks occurred, the specific circumstances around the events, what some officers did to survive the attacks, and how those officers handled the aftermath.

Projects from previous years continued to flourish in 2019. The Crime Data Explorer, an online interface for UCR data, now includes expanded homicide data, supplemental property data, and arrest data, as well as access to master files that provide a variety of crime data from 1985 to 2016.



The Crime Data Explorer, an online interface for UCR data, now includes expanded homicide data, supplemental property data, and arrest data, as well as access to master files that provide a variety of crime data from 1985 to 2016.

In addition, the UCR Program staff continues work with our law enforcement partners to assist in their transition to the National Incident-Based Reporting System (NIBRS), a comprehensive

incident-based method of crime reporting. Currently, more than 8,300 agencies submit crime data via NIBRS, which accounts for 44 percent of UCR data contributors. Moreover, more than 4,000 additional agencies have committed to participate in the program by 2021.

The future of innovation rooted firmly in a distinguished past

UCR will celebrate its 90th birthday in 2020. Also ahead, in the summer of 2020, the UCR Program will launch the NIBRS Collection Application (NCA) through the Law Enforcement Enterprise Portal. The NCA will allow federal agencies that don't have their own collection systems to send crime data directly to the UCR program.

Biometrics Services

Adding new tools to the biometrics toolbox

The CJIS Division has long summarized its mission as enabling our law enforcement partners to connect, to identify, and to know. Nowhere is this undertaking more apparent than within our biometrics component. From helping revive cold cases to continuing to push forward on new frontiers of identification, CJIS Biometric Services brings information and technology to bear for our federal, state, local, and tribal partners.

Keeping our eyes on irises

In fiscal year (FY) 2019, CJIS continued to conduct identification searches submitted by participants in the FBI Iris Pilot and enroll subjects into the pilot repository. The iris, like a fingerprint, is comprised of distinct textures unique to each person. The pilot project has proven iris recognition to be a strong biometric resulting in quick and accurate identifications. With approximately 50,000 new iris enrollments as well as more than 2,000 iris identification searches per month, the pilot repository has grown to 1.1 million identity records and 3 million images. In December 2018, CJIS endorsed the establishment of a national iris recognition service based on the success of the FBI Iris Pilot.

Lending law enforcement a hand with palm prints

Forty-eight states, plus Washington, D.C., and the territories of Guam and Puerto Rico, have contributed palm prints to CJIS's National Palm Print System (NPPS). NPPS houses the palm prints of more than 18.9 million unique subjects derived from more than 38.5 million events (e.g., arrests, civil applications, etc.) which are available for nationwide investigative leads. At the projected growth rate, NPPS is set to contain the palm prints of more than 20 million unique subjects in FY2020.

Warming cold cases with new investigative leads

In 2011, the CJIS Division began phasing out the legacy Integrated Automated Fingerprint Identification System (IAFIS) and deployed the first increment of the Next Generation Identification (NGI) System. In May 2013, the NGI System deployed enhanced latent investigative services to provide law enforcement with new capabilities to identify persons of interest within unsolved investigations. Since then, CJIS has collaborated with law enforcement to provide support in searching unknown latent prints within the NGI System using a new matching algorithm and access to criminal and civil retained records. Law enforcement agencies in possession of latent prints that have never been searched against the legacy IAFIS or NGI System are encouraged to do so.



Law enforcement agencies in possession of latent prints that have never been searched in the legacy IAFIS or NGI System are encouraged to do so.

Latent prints previously searched and retained within the Unsolved Latent File (ULF) of the legacy IAFIS can be automatically

searched in the NGI System if requested by the law enforcement agency. This relaunch support is referred to as the ULF Project and to date has resulted in more than 5,000 new investigative leads in current and cold cases involving homicides, kidnappings, and other crimes. These efforts have been promoted to law enforcement through outreach and overviews provided during 20 conferences and biometric forums.

Helping identify mass shooting victims

The Mobile Biometric Application (MBA) is a smartphone application with a plug-in device that captures an individual's fingerprints and quickly determines the individual's identity. The number of FBI users of the MBA increased from 1,700 in FY2018 to 3,117 in FY2019.

Also in FY2019, CJIS received eight sets of fingerprints from the Dayton Police Department after the mass shooting in Dayton, Ohio, on August 4, 2019. CJIS staff processed the fingerprints through the NGI System and made three positive identifications.



National Threat Operations Center

Always available, always ready to listen

The National Threat Operations Center (NTOC) experienced major growth in fiscal year (FY) 2019 when it transitioned from a call center (the Public Access Line) to a full-fledged operations center with an expanded infrastructure. NTOC examines tips provided by the public, then reports the information to the appropriate FBI field office or law enforcement partner. With operations staff trained to deal with callers and electronic tips (E-Tips), and support staff assigned to monitor and plan processes and communications, as well as analyze and manage resources for maximum efficiency, NTOC is poised to handle and move information in an effective and efficient manner.

On duty 24 hours a day, 7 days a week, 365 days a year, during FY2019, NTOC:

- Received 540,307 calls.
- Received 727,949 E-Tips.
- Submitted 74,551 leads to field offices.

Of the tips in FY2019 that NTOC deemed actionable, 4 percent included threats to life. These tips, along with those involving potential terrorism, are routed to both the appropriate FBI field offices and state fusion/communication centers—which receive, analyze, and share threat-related information with federal, state, local, tribal, and private sector partners.

Recognizing the wealth of information contained in NTOC threat intake database, the system has been made available to all FBI field offices. Investigators and analysts throughout the Bureau can access the information to enhance their assessments and investigations, identify source information, and become aware of what issues the public has reported.

Looking forward, NTOC will continue to expand the CJIS Division Intelligence Program, housed in NTOC and designed to identify, manage, and share the division's intelligence products to the intelligence community. NTOC will incorporate its threat intake system data into a content warehouse that will connect with existing FBI assessments, investigations, and cases, giving FBI personnel access to relevant information needed to solve crime or mitigate threats.

NTOC call leads to federal prison for Anchorage man

In 2018, an Anchorage business owner contacted NTOC to report receiving threats of a mass shooting via text messages. The caller said a subject, who had moved to New York City, had used a text message thread to threaten to shoot, poison, and cut the subject's parents, two Anchorage Police Department officers and their families, and shoppers at a local business.

The FBI Anchorage Field Office (FO) was able to determine the subject's likely location in New York City. Anchorage collaborated with the FBI New York FO in the investigation and obtained an arrest warrant.

The suspect was indicted on eight counts of threatening interstate communications and extradited to Alaska. He was detained until his trial in October 2018, where a federal jury convicted him on all eight counts. On July 30, 2019, a U.S. District judge sentenced the offender to serve four years in federal prison followed by three years of supervised release.

Information Technology Services

Keeping CJIS technology a step ahead

Without the people and the framework of information technology (IT) at the CJIS Division, the FBI's law enforcement partners would be limited in their ability to collect and share the crucial data that officers need for their safety and for the protection of the public they serve. In the same vein, agencies depend upon the data contained in the CJIS systems for running background checks on individuals applying for jobs in positions of trust. Both law enforcement and non-law enforcement partners expect those checks to be accurate and timely. The CJIS IT team takes great pride in delivering reliable tools. They are tenacious in developing new software and applications, implementing enhancements, and keeping systems running at peak performance.

All systems go

During fiscal year (FY) 2019, the CJIS Division's systems were operational 99.85 percent of the time. The only exceptions to availability were 13 hours spread throughout the year when the systems were undergoing maintenance or when unscheduled outages occurred.

Every cloud has a silver lining

More and more CJIS systems are moving to the cloud, which increases available storage and resources. In FY2019, CJIS moved 80 percent of the Next Generation Identification System, as well as 76 percent of the National Data Exchange System's computing resources and 26 percent of its data to the cloud, eliminating the need for equipment and in-house storage. Another plus is all cloud storage and data movement is encrypted, which secures the data from malicious cyber activity. In the future, CJIS IT staff plans to migrate more CJIS systems to the cloud for better efficiencies.

Automating the future

In 2019, CJIS IT upgraded the National Threat Operations Center (NTOC) phone service, including call recording, voice to text, and automatic translation, which looks for threat words. Plans for NTOC upgrades continue. NTOC's threat identification procedures will be automated, which will allow better scoring of threat possibilities, resulting in information moving more quickly to



More and more CJIS systems are moving to the cloud, which increases available storage and resources.

FBI field offices for assignment. CJIS IT also worked on National Instant Background Check System (NICS)

automation this past year, providing technological analysis and machine learning that allows the systems to make certain decisions faster. The Electronic Departmental Order and Electronic Challenge (eChallenge) both use public facing sites to allow individuals requesting their own information from CJIS databases to quickly apply for and receive the answers to their requests. In addition, CJIS IT is assisting biometric services as they implement better facial recognition and new iris identification algorithms. This additional automation of CJIS systems means quicker and more accurate response times not only for the systems, but for law enforcement entities as well.

Adding to the CJIS IT team

With the increase in system enhancements comes an increase in the need for employees with the right IT skills. The CJIS Division is expanding efforts to recruit promising college students nearing graduation. CJIS IT staff is working closely with many schools

to generate interest in FBI jobs among students enrolled in engineering and computer-related fields. The CJIS Division will increase this outreach in the coming year. Currently, 20 IT staff members, specifically including women in CJIS IT, are participating

in the recruitment process, providing on-campus information booths and collecting résumés. CJIS IT plans to offer more recruitment events and locations that will allow more students to take full advantage of these opportunities.

Electronic Departmental Order (eDO) and the United States Postal Service (USPS) Pilot Project

Identity History Summary Requests made easy

The eDO system **reduces response times from 18 weeks to approximately a week**, including mailing time.

At this point, individuals who request a copy of their identity history summaries online are still *required to submit hardcopy fingerprint cards*. However, the rest of the process from the official request to receiving a response is performed electronically through the eDO's website.

Using the eDO website's online form, the public can

- Request a copy of their identity history summaries (or proof that one doesn't exist).
- Submit a challenge to their IdHSC.
- Request the reason their National Instant Criminal Background Check System (NICS) request was denied.
- Challenge (or "appeal") their NICS denial.



September 2018

FBI and the USPS begin a pilot project with two locations in the District of Columbia.

The pilot allows the public to submit fingerprints for IdHSC via eDO through biometric fingerprint scans at participating USPS Offices. Individuals who have their fingerprints scanned and submitted from post office locations via the pilot project **get a response in approximately 2 hours, as opposed to 18 weeks**.

Under the pilot, USPS provides the following services:

- Verification of individual's identity.
- Capture of fingerprints (live fingerprint scanning equipment installed at sites with USPS personnel trained to capture prints).
- Submission electronically to the FBI's NGI System via eDO.

Beginning in 2020
The USPS plans to expand this service to more locations.

2018



February 2018

FBI launches the eDO for Identity History Summary Checks (IdHSC).

2019



May 2019 Pilot expands

Number of locations in the pilot grows to 28 post offices in California, Illinois, Maryland, New Jersey, New York, Texas, Virginia, and the District of Columbia.



National Crime Prevention and Privacy Compact Council

In safe hands: maintaining privacy and safety

The National Crime Prevention and Privacy Compact (Compact) Council oversees the use of the Interstate Identification Index (III) in conducting national criminal history record checks for noncriminal justice purposes such as employment, licensing, or immigration and naturalization matters. In addition, the Compact Council continues to improve initiatives and outreach efforts aimed at increasing Compact ratification.

Since the Compact was enacted on October 9, 1998, the number of states that have ratified the Compact has continued to grow.

Since the Compact was enacted on October 9, 1998, the number of states that have ratified the Compact has continued to grow. Delaware, the most recent state added, ratified the Compact in fiscal year (FY) 2019. Today, the number of Compact states is 34, and 10 states/territories have signed a Memorandum of Understanding with the Compact Council.

This growth has led Compact Council leadership to pilot a new meeting structure. Going forward, two regional committees—eastern and western—will meet prior to the meetings of the Standards and Policy and Planning and Outreach Committees. The regional committees will review, discuss, and make recommendations to the appropriate Committees on various topics.

Enhancing policy to address illegible fingerprints

In FY2019, the Compact Council approved the FBI to expand the policy that removed the requirement for fingerprint submission with regard to double-amputee applicants. The expanded policy permits a name check without fingerprints for individuals who are permanently physically incapable of providing fingerprints due to amputation, illness, or injury affecting their hands or fingers.



FBI Citizens Academy

Sharing the FBI's mission and vision with our community

The FBI Citizens Academy Program increases public awareness about the FBI, its mission, its activities, and its people and also provides an avenue for the FBI to hear and respond to community issues and concerns. Each year, the CJIS Division hosts an FBI Citizens Academy in partnership with the Pittsburgh Field Office and Clarksburg Resident Agency.

Graduates from this program have formed an active FBI CJIS Citizens Academy Alumni Association while serving as

ambassadors of the FBI and participating in many community initiatives. For example, the FBI CJIS Citizens Academy Alumni Association coordinates the division's annual Jerry Dove Memorial 5K Race that honors the life and service of Special Agent Jerry Dove. Jerry Dove was a native of Charleston, W.Va., who died in the line of duty on April 11, 1986, in a gun battle with robbery suspects in Miami. The race attracts participation from individuals locally and from surrounding states.





Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV 26306

Scan the following QR codes with your smartphone or tablet to learn more about:

FBI's CJIS Division Online



The CJIS Division, or you can visit
<www.fbi.gov/services/cjis>.

Today's FBI



The Federal Bureau of Investigation,
or you can visit <www.fbi.gov>.