

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



CONNECT ▶ IDENTIFY ▶ KNOW

CJIS Division

2020 YEAR IN REVIEW

CJIS Division

2020 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 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*.

Contents

National Crime Information Center As reliable as it is responsive	4
National Instant Criminal Background Check System Meeting unprecedented volumes of transactions with improved processes	6
National Data Exchange N-DEx continues to advance for law enforcement and criminal justice benefit	8
Law Enforcement Enterprise Portal A virtual hub for law enforcement collaboration	10
Uniform Crime Reporting Program Summary Reporting System ends a good run	12
Biometric ID Services Expanding biometrics and their accessibility	14
National Threat Operations Center New technology and workflows make for more efficient processing	16
Information Technology Services Working through a global pandemic	18
CJIS Advisory Policy Board Working together to improve working together	19
National Crime Prevention and Privacy Compact Council Enhancing public safety, protecting privacy, and coordinating collaboration.	20
Our Campus	22

FBI's CJIS Division continues to make strides despite challenges

As I present this *CJIS Division 2020 Year in Review* publication, I reflect that no one could have anticipated what 2020 would bring. But at the Criminal Justice Information Services (CJIS) Division, we have managed to weather many storms and still advance programs and platforms and learn a lot along the way.

In fiscal year (FY) 2020, we made great strides on several fronts. Like many in the federal government and partner agencies, we learned how to effectively implement and manage remote work. With a strong remote work posture, CJIS maintained our 24/7 services/systems and was able to do planned system enhancements and development.

The CJIS Division also continued to support our stakeholder groups, the CJIS Advisory Policy Board (see page 19) and the Compact Council (see page 20). Although virtual meetings are not ideal, we demonstrated our commitment to established processes and successfully conducted business via virtual meetings.

The National Instant Criminal Background Check System (NICS) successfully managed unprecedented volumes in FY2020. NICS' staff successfully addressed incoming work that set several records (see page 6).

We were pleased to see increased participation in the National Use-of-Force Data Collection in 2020 (see page 12). More agencies participating will provide reliable, data-rich resources to assess the scope of law enforcement's use of force across the nation. Also in FY2020, we launched our National Iris Service (see page 14), and established the Law Enforcement Engagement Unit (LEEU). The LEEU aims to promote effective partnership and engagement with our federal, state, local, tribal, and global law enforcement partners; as well as FBI field offices. LEEU is committed to increasing awareness of criminal justice services, promoting consistent communications, and collaborating across CJIS business lines.

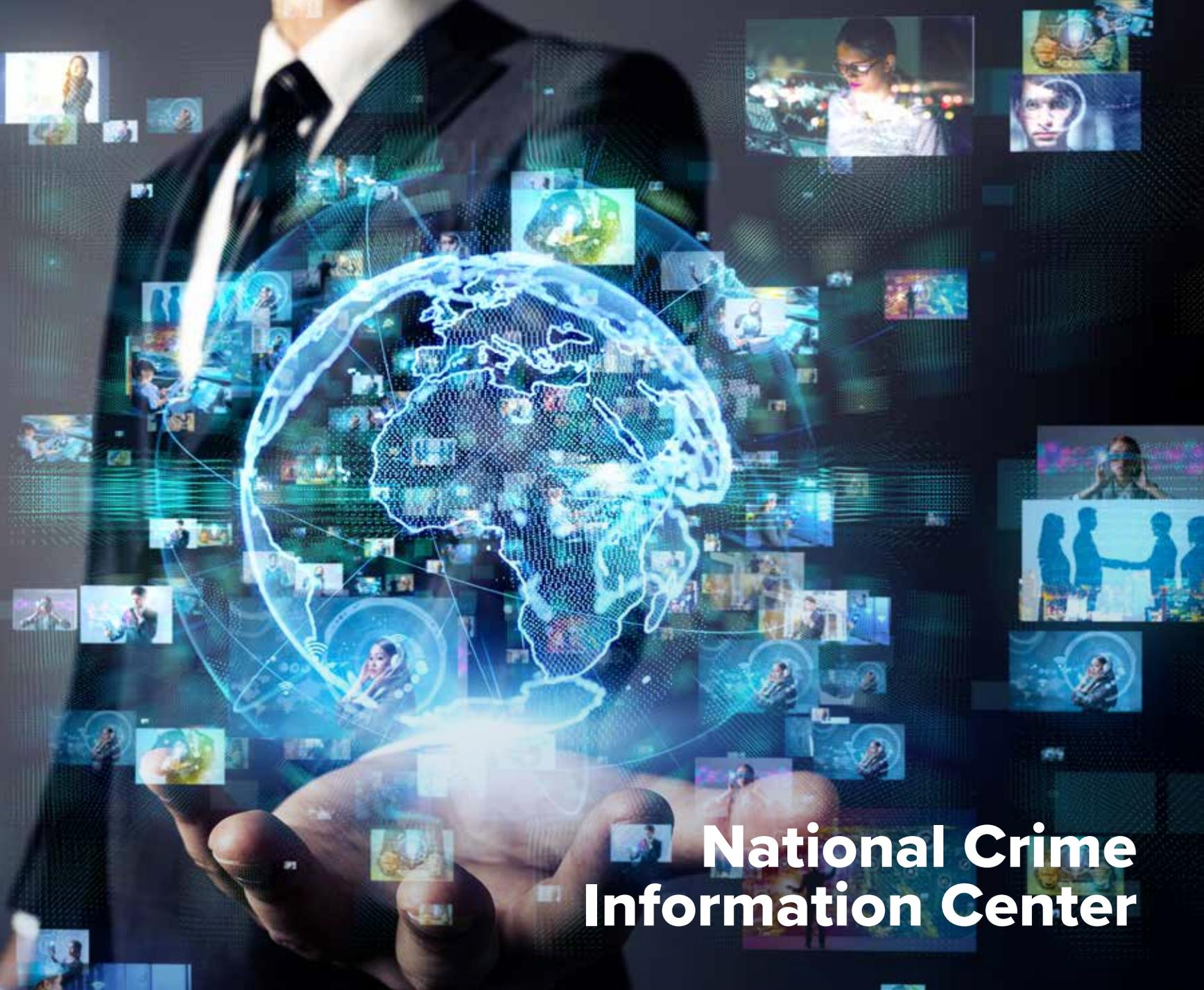
I am proud of the great work the CJIS Division accomplished in FY2020. The safety of our nation and our citizens remains our top priority. Despite the many challenges associated with the pandemic and civil unrest encountered in 2020, CJIS was able to meet the demands of our law enforcement, Department of Defense, U.S. intelligence community, and private sector partners. CJIS also upheld the FBI's responsibility to assist our allies and foreign partners with safeguarding their nations and citizens.



A handwritten signature in black ink, appearing to read "Michael D. DeLeon".

Michael D. DeLeon

*Assistant Director
of the FBI's CJIS Division*



National Crime Information Center

National Crime Information Center As reliable as it is responsive

During fiscal year (FY) 2020 the National Crime Information Center (NCIC) provided law enforcement partners with information at a record pace while continuing to improve, modernize, and expand the existing system. NCIC processed an average of 7,922,014 transactions a day and marked a new daily average response time record at an impressive 0.0044 seconds on May 9. The average response time to an NCIC query in FY2020 was 0.0069 seconds.

The NCIC Third Generation (N3G) project continued to focus on providing easier-to-read and customizable responses. This included a second version of its Extensible Markup Language (XML), which simplifies many of the complexities of NCIC data via the newest version of the National Information Exchange Model (NIEM) specification. In FY2020, two agencies successfully tested NIEM XML transactions.

N3G also added the Electronic File Transfer Service, known as EFTS, the newest method for sharing large electronic files in a secure fashion. This Web-based transmission improves the efficiency of retrieving files from NCIC and the Interstate Identification Index. The streamlined, user-friendly environment also allows users to access statistical reports, data extracts, and validation information, as well as to upload large files or to send batches of data, without size restrictions, back to NCIC.

Also, in FY2020, NCIC implemented an enhancement that creates a more efficient method for states to search the NCIC National Sex Offender Registry (NSOR) for criminal background checks of childcare staff members in accordance with the Child Care and Development Block Grant Act. This capability is also available to all NCIC users, allowing them to limit search results based on active non-suppressed NSOR records for investigative purposes and future authorized noncriminal justice purposes.

On deck next for NCIC

Next up for NCIC are two major enhancements to promote public and officer safety: the creation of a Blue Alert caveat and the creation of the Extreme Risk Protection Order (ERPO) File. With implementation scheduled for January 2021, the Blue Alert function will provide a warning to law enforcement to use extreme caution when approaching a vehicle or individual who has been identified as a threat to law enforcement. In addition, the ERPO File will allow officers to enter into NCIC and view the details of orders that temporarily restrict firearms from an individual who may present a danger to themselves or others. This file is scheduled to be made available to NCIC users in 2022.

NCIC identifies unhappy campers

On July 14, 2020, sheriff's deputies responded to a domestic disturbance incident at a campground. An NCIC query revealed that the individuals involved in the disturbance were wanted for abduction of their children when they failed to return the children to their legal guardian after a visit. The deputies placed the children in the care of the county department of Social Services and charged the pair with multiple counts of child abduction. One of the individuals was also charged with failing to appear in court on a charge of assault with a deadly weapon.



National Instant Criminal Background Check System

National Instant Criminal Background Check System

Meeting unprecedented volumes of transactions with improved processes

In fiscal year (FY) 2020, the National Instant Criminal Background Check System (NICS) experienced the impact of the COVID-19 pandemic, which was a catalyst for unprecedented volume of background checks and led to a modified work environment for NICS employees. The NICS staff had to adapt so they could process the record-breaking number of background checks while remaining healthy themselves.

A few weeks after COVID-19 was declared a pandemic, more than 80 percent of NICS' staff were sent home to work with the protocols, equipment, and technical assistance needed to remain effective. Since March 2020, NICS experienced 8 of its top 10 highest weeks ever and 5 of its top 10 highest days.

In FY2020, the total NICS transaction volume, including states that complete their own background checks, increased 34 percent from 2019 levels, ending the FY with a total of 36,731,704 checks.

During this unorthodox and busy time, the NICS Section staff processed 11,913,590 federal transactions; denied 176,411 federal firearm transactions; and handled 85.63 percent of all federal NICS transactions online via the NICS E-Check.

NICS rolls out new process to apply for appeals program

Despite the added challenges in FY2020, NICS rolled out a more convenient way for firearm purchasers to fill out forms to apply for inclusion in the Voluntary Appeal File (VAF). The VAF is a way for firearm purchasers, who are regularly delayed or denied due to either mistaken identity or incomplete records, to be vetted and issued a Personal Identification Number (PIN) to use when purchasing a firearm. The PIN allows NICS staff to access a person's fingerprint-based criminal history information and reconcile any identity or criminal record issues, allowing for a faster transaction.

Traditionally, a person applied for the VAF by filling out a paper form, getting a copy of their fingerprints, and mailing both to the NICS Section for processing. Results would also be returned via mail to the applicant. On June 1, NICS provided the eVAF on FBI.gov, which allows the forms to be completed and submitted online, saving mailing time and postage costs. By using eVAF, applicants receive status updates about their applications in real time and, if approved for inclusion in the VAF, will receive their PINs faster.

Automation benefits NICS and customers alike

Last year, NICS began using an automated process that allowed their system to perform certain tasks regarding firearm transactions, freeing staff to handle more complex cases. In FY2020, five percent of all background checks transferred to NICS received an automatic determination—never needing attention from NICS staff. Firearm dealers and purchasers alike are enjoying the benefits of faster processing times, and taxpayer dollars are saved on transactions that can be automatically processed.



National Data Exchange

National Data Exchange

N-DEX continues to advance for law enforcement and criminal justice benefit

In a challenging year, the National Data Exchange (N-DEX) System continues to thrive. In FY2020, the N-DEX System implemented “Use Code F,” which allows state criminal justice agencies to use the N-DEX System for background checks that are related to gun sales, and firearm licenses and permits. This capability gives authorized agencies another resource to search when conducting firearms-related background checks. In addition, federal agencies can now use N-DEX while conducting background investigations for federal security clearances, employment, and credentialing.

One outline for data submission, two programs

Agencies that submit N-DEX data via Extensible Markup Language, or XML, now need only one outline (known as an Information Exchange Package Documentation, or IEPD), to submit data to both N-DEX and the National Incident-Based Reporting System (NIBRS). This efficiency has been on the horizon for a while, and came to fruition in 2020. This new procedure streamlines submission methods and reduces the resources needed to provide information to these two CJIS systems.

A look toward the future

With nearly a 500-percent growth in distance learning offerings over the past two years, N-DEX staff is partnering with the National Sheriffs’ Association and the High Intensity Drug Trafficking Area program to further enhance N-DEX outreach efforts. Another area of expansion: N-DEX staff is working with the Law Enforcement Enterprise Portal, or LEEP, to transition to a live help desk available 24/7 for those with N-DEX System issues and questions.

The N-DEX System continues to shift toward cloud computing by storing its data, software, and applications on remote, secure servers. Using the cloud will enhance collaboration, improve reporting, and expand storage.

N-DEX assists in breaking money laundering, human trafficking, and drug transportation case

A special agent with the Office of the Inspector General of the U.S. Department of Housing and Urban Development (HUD) investigated an international money-laundering case that involved more than 100 subjects. A HUD employee suspected of laundering money was the original subject of the investigation.

The agent’s research confirmed that the employee was laundering money and funneling it to her boyfriend, who illicitly received millions of dollars. The pair was linked to an organized crime group with ties to money laundering, interstate human trafficking, drug transportation, and real estate fraud. The agent broke the case after using N-DEX to search phone numbers contained in the system’s records. His query returned police reports from around the country, mostly from the Las Vegas Metropolitan Police Department, that linked previously identified prostitution victims to the boyfriend. The victims provided crucial information about the operation’s key players, structure, and methods.

The nationwide money laundering organization included major cities, such as Chicago, Miami, Dallas, Las Vegas, and San Francisco. The agent was pleased with N-DEX’s results, saying, “N-DEX played a huge role in uncovering and identifying individuals involved in a multijurisdictional investigation. There are many times when I cannot find personally identifiable information but find it in N-DEX.”



**Law Enforcement
Enterprise Portal**

Law Enforcement Enterprise Portal

A virtual hub for law enforcement collaboration

The Law Enforcement Enterprise Portal (LEEP) supports criminal investigations across the country, providing safe and secure online services to law enforcement users. By staying modern and effective, LEEP continues to be a vital hub of resources for agencies to monitor and share information.

Rising to the challenges

LEEP provided tools to help law enforcement agencies meet the many challenges of 2020. Participation in JusticeConnect increased by 15,754 users in Fiscal Year (FY) 2020, and users created 166 new Communities of Interest to stay connected.

The LEEP team collaborated with the Strategic Information Operations Center (SIOC) to create a network using the Virtual Command Center (VCC) application for information sharing between FBI field offices. This enables SIOC and FBI executives to access critical information from one centralized source. So far, 42 of 56 FBI field offices are actively using this system, with more expected to enroll in the coming year. In addition, users leveraged the VCC application by creating 1,332 VCCs in FY2020 to track and share information about events.

To enrich LEEP's value, staff continually add more applications to expand users' virtual toolbelts. In FY 2020, LEEP began offering the Galton service that provides authorized agencies with the ability to enroll individuals in the Next Generation Identification (NGI) Rap Back service and view the results of their submissions. Since its launch, the Galton service has recorded more than 8,000 Rap Back enrollments, 600 Rap Back notifications, and 32,000 NGI responses.

Other new services include the National Incident-Based Reporting System (NIBRS) Collection Application (an interface for federal and tribal agencies to submit NIBRS data to the Uniform Crime Reporting Program); Relativity (for hosting records for joint cases with the Department of Justice's Criminal Division); and

the Digital Content Analysis Platform (provides tools and services that automate the processing and exploitation of unclassified and bulk or complex digital data). The total number of services available on LEEP is 62.

Beyond 2020

In addition to more field office involvement, the LEEP team is working with the FBI's Mobility Program Office to develop a communications interface for the VCC application. This interface will link radio communications, emails, text messages, and other communications needed in crisis situations.

LEEP plans to implement a new automated vetting feature for LeapID Accounts. This will give account holders a faster, more efficient process for gaining access. LEEP developers plan to boost the system's security software, which will simplify user access while more securely adopting web, mobile, and cloud technologies. It will balance usability and security by using risk-based access, single sign-on, integrated access management control, identity federation, and mobile multi-factor authentication.

Also coming, JusticeConnect users will have access to collaborative document editing, enhanced community analytics, and meeting capabilities in the JusticeConnect chat. LEEP will soon include a VCC mobile application for law enforcement.

Virtual tool proves useful in the year of COVID-19

Amid the COVID-19 pandemic, the LEEP team demonstrated its flexibility by providing increased online support to clients and developing and supplying virtual training for the users of LEEP, JusticeConnect, and the VCC service. Of the VCCs created in 2020, 32 were for sharing information about COVID19. This included a new use for VCCs: distributing information about the pandemic from the Centers for Disease Control. Some agencies used VCCs to help track incidents of officers exposed to COVID-19.



Uniform Crime Reporting Program

Uniform Crime Reporting Program Summary Reporting System ends a good run

During the past year, one of the Bureau's oldest programs, the Uniform Crime Reporting (UCR) Program, underwent major changes in preparation to end one data collection method and add others.

Out with the old, in with the NIBRS

The UCR Program will retire its Summary Reporting System on January 1, 2021, in favor of the more comprehensive National Incident-Based Reporting System (NIBRS). When used to its full potential, NIBRS identifies the location type of the crime, the type of offense committed, and the characteristics of its victims and perpetrators. With such detailed information, law enforcement can better understand the nature of crime and define the resources it needs to combat crime while using resources in the most efficient manner.

National Use-of-Force Data Collection marks first data release

The first release of data collected in the National Use-of-Force Data Collection was presented on July 27 via the Crime Data Explorer (CDE), a mobile-friendly application that allows users to query, view, and download crime data. The release of use-of-force participation data represented more than 5,000 federal, state, local, tribal, and college and university law enforcement agencies that submitted their data.

Another first: In September, UCR Program staff released the *Preliminary Uniform Crime Report, January-June, 2020* as the first quarterly publication of UCR data via the CDE. The commencement of quarterly reports aims to increase the timeliness of crime data releases.

Looking ahead, the Law Enforcement Suicide Data Collection Act was signed into law on June 16, 2020. The Act directs the FBI to collect and report statistics on suicides and attempted suicides within the law enforcement community. The collection is slated

to begin in July 2021, with the initial release of data to the public in June 2022.

New application eases data submission for federal and tribal agencies

On June 19, 2020, UCR Program staff launched the NIBRS Collection Application (NCA) in the Law Enforcement Enterprise Portal. The FBI developed the NCA to provide federal and tribal agencies the ability to easily submit NIBRS data to the UCR Program. The NCA, a no-cost NIBRS submission solution, allows federal agencies to comply with federal crime reporting guidelines. The NCA also reduces the amount of resources federal agencies need to submit and manage UCR data.

The NCA is an extension of the UCR Program and enables users to enter and submit NIBRS crime data directly to the UCR Program for processing, retention, and publication. Between the launch and September 2020, UCR staff trained personnel in more than 30 federal and tribal agencies to use the new application. Eight agencies have already obtained accounts and are using the application.



Biometric Services

Biometric ID Services

Expanding biometrics and their accessibility

The FBI has had a grasp on biometrics since it began administration of the national fingerprint registry in 1924. Biometric identification services are a rich and long legacy that reside in the CJIS Division. But being around a long time does not mean biometric ID services stay “status quo.” Staff at CJIS work hard to push biometric identification frontiers forward.

Seeing the benefit of iris identification

The Next Generation Identification (NGI) Iris Service deployed on September 29, 2020, seamlessly transitioning Iris Pilot users to full operational capacity. In fiscal year (FY) 2021 and beyond NGI Iris Service user base is expected to increase with expanded access to other law enforcement and criminal justice agencies. As the volume of irises enrolled in the NGI Iris Service repository increases, the search value will increase, benefiting users.

Adjudication processes, policy, and training will be developed to enable the use of the iris biometric for identification purposes. Ultimately, through the NGI Iris Service and the technical and procedural advancements made in support, the iris biometric may play a big role in the future of biometric identification.

Submitting fingerprints at the USPS

Thanks to the spirit of customer service at the CJIS Division, individuals who want a copy of their criminal history record can now take the first step in their request by visiting a participating U.S. Postal Service (USPS) location. Before releasing criminal history records, the FBI must be certain the person requesting the record is the same person shown on the record, and that’s done through fingerprint comparison. Previously, members of the public went to police departments, sheriff’s offices, or other government agencies to have their fingerprints manually taken with ink on a blank fingerprint card. Then, they mailed the fingerprint card to the FBI for analysis. Now, fingerprints can be electronically scanned and instantly submitted from select USPS locations. In

2018, the FBI and the USPS began a trial allowing members of the public to submit fingerprints through biometric scans captured at participating post offices. This new process reduced response times from more than 100 days to less than a week. During fiscal FY2020, CJIS worked with the USPS to expand the process. Now, more than 80 sites are equipped to scan and submit fingerprints.

Reporting back to agencies

Rap Back services allows government agencies to receive notification of new criminal activity by enrolled individuals who hold positions of trust (e.g., government employees, teachers, daycare workers). Law enforcement agencies also use the service to enroll individuals currently under an active criminal investigation or on active probation or parole. Four additional agencies began participation in Rap Back services in FY2020, bringing the total to 14 agencies.

Biometrics help shed light on sinister plot

A subject carrying a homemade bomb and a detonator that he had rigged to his cell phone was walking in a field toward his ex-girlfriend’s apartment complex. He apparently planned to bomb the complex. Instead, as he neared the complex, he detonated the bomb and killed himself. Authorities located a single fingertip at the grisly scene and analyzed it using the CJIS Division’s Mobile Biometric Application with a handheld device. The initial fingerprint search generated no hits. However, while investigating the incident, authorities discovered an abandoned rental vehicle near the scene containing a driver’s license. CJIS staff compared the unknown fingerprint from the explosion site to the prints on file for the individual who owned the driver’s license. The single finger matched a record, which allowed a positive identification of the suspect. Authorities searched the deceased suspect’s residence and discovered evidence of his intended plot to bomb the apartment building.



**National Threat
Operations Center**

National Threat Operations Center

New technology and workflows make for more efficient processing

Fiscal year 2020 brought significant updates to the National Threat Operations Center (NTOC), which receives threat information from around the globe and disseminates the information to the appropriate FBI field office or law enforcement agency for action. Working around the clock, 365 days a year, NTOC staff members:

- Received 650,434 calls.
- Processed 756,187 electronic tips (E-Tips).
- Submitted 4,782 threat-to-life leads to field offices/law enforcement partners.
- Published 113 intelligence products.

New algorithms that use machine learning, a form of artificial intelligence, now score and prioritize information based on historical data. These enhancements help NTOC staff members address threat-to-life and high-priority information promptly, which speeds the process of forwarding actionable information to the appropriate entity.

A new Social Media Exploitation Team addresses online threats to life from social media associated with unknown subjects, victims, and locations. The team conducts supplemental database searches and forwards the information to the correct agencies. The center has also established partnerships with social media outlets and both the FBI's Counterterrorism Watch program and Strategic Information Operations Center to facilitate the assessment of threats to life.

The CJIS Division's Intelligence Program, embedded within the National Threat Operations Section, identifies, manages, and reports valuable intelligence products within CJIS programs to the intelligence community and other FBI divisions.

NTOC is looking forward to the deployment of a redesigned Threat Intake Processing System that will use newer, more robust Web technologies to simplify the call intake process,

automate database searches, and unify the call and E-Tip review processes.

Most of the information submitted to NTOC are matters for state and local law enforcement. For that reason, NTOC is pursuing a connection to the Public Service Answering Point (PSAP) Registry of NENA: The 9-1-1 Association. This service provides 24x7 and administrative contact information for every PSAP Registry in the United States at any location, which will save precious time for NTOC staff handling local threats to life and emergencies.

NTOC call leads to rescue of human trafficking victim

In late 2018, an NTOC staff member received a call from a girl in the Philadelphia area who was whispering and crying uncontrollably. The caller said she was locked in a hotel bathroom with her captor asleep in the next room. She was being held against her will and was afraid for her life. The caller gave her name and approximate location then disconnected.

The staff member immediately drafted a threat-to-life lead while a supervisory special agent (SSA) called FBI-Philadelphia (FBI-PH). An SSA with FBI-PH called the local police department and spoke with a detective, who informed the SSA that the caller, a minor, had been missing for two months. The same day, the local child exploitation task force located the victim at an apartment and took her into protective custody without incident.

The task force arrested the subject in January 2019, and he entered a guilty plea in September 2019 to the federal charge of sex trafficking of a minor for prostitution purposes. In February 2020, the subject was sentenced to 66 months of imprisonment and 10 years of supervised release.

Information
Technology

Mobile
phone



Data

Communication

Computer

Business

**Information
Technology Services**

Information Technology Services

Working through a global pandemic

It almost goes without saying: 2020 was an unpredictable year in many ways. At the beginning of the fiscal year (FY) 2020, no one could have foreseen the COVID-19 pandemic happening, but the information technology (IT) team at CJIS answered the national health emergency brilliantly and kept the division's 2,500+ employees productive when most of the country was grinding to a halt. In rapid response to the unprecedented circumstances presented by COVID-19, IT staff enabled a remote work option to help CJIS employees stay efficient and safe. The serious health risks presented by the pandemic mandated that as many employees as possible vacate the CJIS campus to work from home. The IT team accomplished this daunting task in a matter of days. This effort required significant coordination among divisions and collaboration with other government agencies to allow CJIS employees to securely connect to CJIS networks from their homes. The initiative resulted in approximately 70 percent of CJIS staff continuing to deliver the same level of valuable services remotely as they would have while working on campus.

Reducing dropped calls

CJIS prioritized reducing the rate of dropped calls of the National Threat Operations Center (NTOC) as a key mission for FY2020. Over the past year, the CJIS IT team defined, refined, tested, and implemented automated tools to increase scoring accuracy and tip prioritization, which allowed for better use of resources for NTOC. The efforts, in collaboration with the business line, decreased the rate of dropped calls by nearly half, from 32 percent in FY2019 to 17 percent in FY2020.

The eyes have it

In FY2020, CJIS developed the iris workflow as the newest biometric mode of identification supported by Next Generation Identification. Despite a pandemic and many employees working remotely, the IT team, in great partnership with the business

lines, accomplished this landmark objective and iris identification capability that deployed in September.

Prioritizing 508 compliance

The FBI directed systems organizations to prioritize the 508 compliance of existing IT systems. Section 508 of the Rehabilitation Act dictates that federal agencies must make digital information accessible to citizens with disabilities particularly when the information is posted on the Internet, an intranet, or presented electronically in some other fashion. CJIS created an Accessibility Program Team to evaluate 508 requirements, establish a CJIS Implementation Roadmap, and produce a 508 compliance risk profile. The Implementation Roadmap was approved in December 2019 and is being implemented.

Making sure CJIS is always open for business

During FY2020, the CJIS Division's systems were operational 99.67 percent of the time. The only exceptions to availability were 15 hours spread throughout the year when the systems were undergoing maintenance.

CJIS Advisory Policy Board

Working together to improve working together



Chartered under the Federal Advisory Committee Act, the CJIS Advisory Policy Board (APB) provides the CJIS Division advice and guidance on strategy, policy, technical, and operational issues affecting CJIS Division Programs. They also make recommendations to the FBI Director regarding changes and improvements to these programs. This review and

recommendation process, which is known as the CJIS Advisory Process, serves as the cornerstone of the CJIS Division's shared management concept with federal, state, local, and tribal law enforcement.

With the challenges brought by the onset of the pandemic, the CJIS APB and CJIS staff rose to the challenge by using new methods of group communication, such as holding virtual meetings. These meetings helped the CJIS Division conduct business from remote locations while maintaining close communication with hundreds of participants in all 50 states, U.S. territories, and Canada.

During fiscal year 2020, the CJIS APB recommended the creation of a new file in the National Crime Information Center for individuals subject to Extreme Risk Protection Order (ERPO) laws. ERPO laws empower law enforcement and family members, and provide courts with the ability to temporarily remove an individual's access to firearms before that person can commit violence. Although the specific requirements vary among the many states, ERPO law generally make it illegal for respondents to purchase or possess firearms. The APB's recommendation will establish a new file to enter these orders into NCIC and to also collect authorized information about individuals who are subject to ERPO laws.

Finally, to help meet the challenges of 2020, CJIS APB Chairman Michael Lesko requested the reestablishment of the Public Safety Strategy (PSS) Subcommittee to ensure that the board stays strategically focused and abreast of topics most relevant to the communities CJIS serves.

Objectives of the PSS Subcommittee include:

- Providing guidance to the CJIS APB on topics spanning multiple systems or potentially influencing the CJIS enterprise.
- Proactively researching, identifying, and presenting items for strategic consideration by the CJIS APB.
- Developing efforts to strengthen the CJIS APB's relationship, communication, and interaction with major law enforcement associations and organizations.

National Crime Prevention and Privacy Compact Council

Enhancing public safety, protecting privacy, and coordinating collaboration



Created by law in 1998, the National Crime Prevention and Privacy Compact (Compact) Council governs the provision of information from criminal history records when accessed for noncriminal justice purposes, such as employment, licensing, immigration and naturalization, or adoption. The Compact Council and its committees

meet regularly to evaluate and make recommendations regarding the rules and procedures for effectively sharing relevant criminal history information.

Meetings restructured and conducted virtually

The structure of the Compact Council meetings was established when just a few states had ratified the Compact. Now, more than 20 years later, 34 states have ratified the Compact and have a seat at the table. As a result, the number of stakeholders involved in meetings has grown exponentially. To provide all participants the opportunity to review, discuss, and make recommendations, Compact Council leadership successfully piloted and approved the creation of two regional committees. The Eastern Regional Committee and the Western Regional Committee each meet separately to consider proposals and make their own recommendations to the Focused Committees, who in turn discuss and finalize a recommendation to the Compact Council.

Because of the COVID-19 pandemic, the Compact Council held its most recent council and committee meetings via a virtual platform. Although meeting over computers and mobile phones is not the preferred method to conduct business, it was an effective option to continue the important work of the Compact Council and to carry its momentum into 2021.

Meeting needs for noncriminal justice background checks during a global pandemic

As COVID-19 spread across the nation, access to noncriminal justice fingerprinting services was limited or unavailable. The lack of services hindered the ability for some states to fingerprint and perform background checks on critical positions. The Compact Council's executive committee and the FBI worked together to review rules and requirements to find legal options for states to continue to conduct background checks necessary to keep the public safe. It was determined that a proposal could be created pursuant to the Council's Fingerprint Submission Requirements rule that would permit preliminary name-checks to be conducted, with the delayed submission of fingerprints within a time frame specified by the Council.

Colorado and Oklahoma each worked with FBI staff to submit proposals to continue background checks without initially requiring a candidate's fingerprints. The Colorado proposal focused on criminal history record checks of individuals, including volunteers, being considered for healthcare and childcare positions in response to the pandemic. The Oklahoma proposal sought to use the preliminary name check and to expand a 15-day delay of fingerprint submissions already in place that allows the state to authorize temporary placement of children in foster care during emergency circumstances.



This is an artist's rendering of the new CJIS Square entrance to the Main facility on the CJIS campus

Our Campus

Our Campus

When people hear the words FBI, technology, and innovation, they tend to think of buzz and bustle. We have plenty of both at CJIS, but the nearly 1000-acre site of the FBI's largest division—one of four main FBI-owned sites—is a lush, wooded locale that belies the technology epicenter that sits in the middle of it. The bucolic, but secure, site provides a home to staff from four federal agencies and 12 FBI divisions. Two primary buildings serve as the base of operations: CJIS Main, a space with more than 500,000 square feet of offices that are the hub of federal criminal justice technology and information; and the Biometric Technology Center (BTC), a 470,000-square-foot structure that is the seat of both identification services and the advancement of biometrics—the science of human individualities that aid in identification.

Like the rest of the nation, CJIS has had to respond to the national health emergency that occurred when the COVID-19 pandemic began. Getting ahead of the spread and helping flatten the curve were uppermost in CJIS staff members' minds from March through this fiscal year. CJIS management, IT staff, and employees worked together to quickly and successfully send a large percentage of staff home to work remotely. This allowed social distancing and less exposure in CJIS buildings as well as fewer high-use areas that required constant, pristine cleaning for safety. Most importantly, it kept CJIS services efficient and available, while keeping CJIS staff, their families, and their communities safer.

Despite the challenges of maneuvering during a pandemic, maintenance and improvements are ongoing at the facility to keep it in top-notch shape. CJIS Main is more than 25 years old but getting the attention a great building deserves. A new entrance to CJIS Main is currently under construction. The project, known as CJIS Square, provides better access for visitors while reinforcing physical security of the building.



The CJIS Division campus has two large facilities: CJIS Main, the hub of federal criminal justice technology and information; and the Biometric Technology Center (BTC), home to both identification services and efforts toward advancement of biometrics.

The future is looking bright for CJIS as other new projects and upgrades are in the works for the coming year. These include a BTC lobby annex and a newly constructed Clarksburg Resident Agency. The Clarksburg Resident Agency, a component of the FBI's Pittsburgh Field Office, is being built on the CJIS campus.

Biometric ID Services



78,374,413

Total number of criminal fingerprints in the repository.

45,688,988

Total number of fingerprint receipts/processed.



124,833

Average daily total of fingerprint receipts/processed.



43,853,102

Total number of criminal full face images used in comparisons.

This includes 19,601,868 unique individuals.

18,262

Number of processed Facial Recognition Searches for active investigations.



Average Response Times

8 min 42 s

Criminal Fingerprint

34 min 59 s

Civil Fingerprint

31 min 8 s

Searches of the Interstate Photo System (mugshots)

Information Technology Services



CJIS Division's systems were operational 99.67 percent of the time. The only exceptions to availability were 15 hours spread throughout the year when the systems were undergoing maintenance.

National Instant Criminal Background Check System



36,731,704

Total number of transactions processed.
(34 percent increase from the previous year).



176,411

Total number of denied federal firearm transactions.



84.38%

Immediate determination rate.



85.63%

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

National Crime Information Center



7,922,014

Average daily transactions.



0.0069 s

Average response time.

National Threat Operations Center



650,434

Total number of calls received.



756,187

Total number of E-Tips processed.



43,368

Total number of leads submitted to field offices.



4,782

Total number of submitted threat-to-life leads to field offices/law enforcement partners.

National Data Exchange



19,840,420

Total Number of N-DEx searches.

Single = 7,793,650

Batch = 12,046,770



878,551,831

Total number of searchable records.

Stored Records = 540,820,918

Federated Records = 337,730,913



9,616

Total number of agencies in the United States contributing data to the N-DEx system.

CJIS Division

Fiscal Year 2020

By the Numbers



CONNECT ► IDENTIFY ► KNOW

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



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.