



Minutes

Criminal Justice Information Services

Advisory Policy Board

June 9, 2021

Orlando, Florida

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>

Intentionally Left Blank



Criminal Justice Information Services

Advisory Policy Board

August 12, 2021

Mr. Nicky J. Megna
Federal Bureau of Investigation
CJIS Division
1000 Custer Hollow Road
Clarksburg, WV 26306

Dear Nicky:

I have reviewed the minutes and hereby certify that they accurately reflect the proceedings from the June 9, 2021 Criminal Justice Information Services Advisory Policy Board meeting.

Sincerely yours,

Sheriff Kathy H. Witt
Fayette County Sheriff's Office
Lexington, Kentucky
Chair, CJIS APB

Representing the interests of the local, state, federal, and tribal criminal justice community

Intentionally Left Blank

Criminal Justice Information Services (CJIS)
Advisory Policy Board
June 9, 2021
Orlando, Florida

Table of Contents

Item #1	Executive Briefings – CJIS Division Status.....	7
Item #2	Tribal Task Force Update	9
Item #3	Chairman’s Report on the Uniform Crime Reporting (UCR) Subcommittee.....	11
Item #4	Use-of-Force Update	27
Item #5	National Incident-Based Reporting System (NIBRS) Transition Update	29
Item #6	Chairman’s Report on the National Crime Information Center (NCIC) Subcommittee.....	30
Item #7	NCIC 3 rd Generation (N3G) Update	40
Item #8	Chairman’s Report on the National Data Exchange (N-DEx) Subcommittee.....	41
Item #9	Chairman’s Report on the Identification Services (IS) Subcommittee.....	43
Item #10	National Crime Prevention and Privacy Compact Council (Council) Report.....	53
Item #11	Chairman’s Report on the Security and Access (SA) Subcommittee.....	56
Item #12	Chairman’s Report on the Compliance Evaluation (CE) Subcommittee.....	59
Item #13	Chairman’s Report on the National Instant Criminal Background Check System (NICS) Subcommittee.....	64
Item #14	Chairman’s Report on the Public Safety Strategy (PSS) Subcommittee.....	66

Intentionally Left Blank

APPENDICES INDEX

Appendix A	APB Roll Call
Appendix B	APB Registered Attendees List
Appendix C	APB Meeting Agenda
Appendix D	APB Staff Papers
Appendix E	Item #1 Executive Briefing – CJIS Update
Appendix F	Item #3 Chairman’s Report on the Uniform Crime Reporting (UCR) Subcommittee
Appendix G	Item #4 Use of Force Update
Appendix H	Item #5 National Incident-Based Reporting System (NIBRS) Transition Update
Appendix I	Item #6 Chairman’s Report on the National Crime Information Center (NCIC) Subcommittee
Appendix J	Item #7 NCIC 3 rd Generation (N3G) Task Force Update
Appendix K	Item #8 Chairman’s Report on the National Data Exchange (N-DEX) Subcommittee
Appendix L	Item #9 Chairman’s Report on the Identification Services (IS) Subcommittee
Appendix M	Item #10 National Crime Prevention and Privacy Compact Council Report
Appendix N	Item #11 Chairman’s Report on the Security and Access (SA) Subcommittee
Appendix O	Item #13 Chairman’s Report on the National Instant Criminal Background Check System (NICS) Subcommittee

Appendix P	Item #14 Chairman's Report on the Public Safety Strategy (PSS) Subcommittee
Appendix Q	APB Item #2 Tribal Task Force Update
Appendix R	Acronym List
Appendix S	Fall 2020 APB Informational Topic Papers

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB) MEETING**

June 9, 2021
Orlando, FL

Meeting Report

Ms. Kathy Witt, Sheriff of Fayette County Kentucky, and the Federal Bureau of Investigation's (FBI's) CJIS APB Chair, called the meeting to order at 9:00 a.m., June 9, 2021, held in a blended manner with in-person and virtual attendees.

Mr. Nicky J. Megna, FBI, CJIS Division, and Designated Federal Officer (DFO) for the CJIS Advisory Process, welcomed everyone to the meeting and led the attendees in the Pledge of Allegiance.

Sheriff Witt thanked attendees for their participation and talked about what a historic day it was to be able to meet in person again. She discussed how the pandemic changed all our lives. She talked about how the global health pandemic collided with the racial justice global pandemic in America with the deaths of Breonna Taylor and George Floyd. She informed the members they were the gold standard and set the tone and the path forward for all law enforcement and criminal justice and the work they do will define the path forward.

Sheriff Witt provided housekeeping notes and proceeded with the roll call: *(See Appendix A for the Roll Call.)* Sheriff Witt welcomed Ms. Brenda Abaya and Sergeant Brian Parker as the newest official members of the CJIS APB. Ms. Abaya replaced Mr. Mike Lesko as a Western Working Group representative and Sergeant Parker replaced Lt. Colonel Scott Wilcox representing the Northeastern Working Group.

Chairman Witt then turned the meeting over to CJIS Assistant Director (AD), Michael Christman to introduce FBI Deputy Director (DD) Paul Abbate. Mr. Christman noted in February 2021, Director Christopher Wray named Paul M. Abbate as Deputy Director of the FBI. He oversees all FBI domestic and international investigative and intelligence activities. Mr. Abbate served as the Associate Deputy Director of the FBI, where he was responsible for the management of all FBI personnel, budget, administration, and infrastructure. Prior to that appointment, Mr. Abbate served as the Executive Assistant Director (EAD) of the Criminal Cyber and Response Services Branch where he oversaw all FBI criminal and cyber investigations worldwide, international operations, critical incident response, and victim assistance. He also served as the Assistant Director in Charge of the FBI's Washington Field Office for several years. Earlier in his career Mr. Abbate served in a variety of executive leadership roles to include Special Agent in Charge (SAC) of the FBI's Detroit Division, SAC of the Washington Field Office Counterterrorism Division and Section Chief (SC) in the Counterterrorism Division. As SC he provided oversight of all FBI's international terrorism investigations and counterterrorism operations external to the United States. Mr. Abbate also served in the Los Angeles Field Office as Assistant Special Agent in Charge for counterterrorism matters, overseeing the primary branch of the Los Angeles Joint Terrorism Task Force. He also served as the Assistant Section Chief in the Counterterrorism Division providing national level

oversite guidance over all U.S. based international terrorism investigations. Mr. Abbate received the Attorney General's Award for Exceptional Service alongside other team members during this time. He served as Supervisory Special Agent (SSA) within the Newark's Division Joint Terrorism Task Force from February 2006 to December 2009. During this time, he deployed to Afghanistan and served as the FBI Deputy On-Scene Commander leading FBI counterterrorism operations and personnel. In October of 2005, Mr. Abbate deployed to Iraq where he served as Senior FBI Liaison Officer to the U. S. Department of Defense (DOD) and lead a group of FBI personnel conducting counterterrorism operations. In December 2003, Mr. Abbate began his extensive leadership career as a SSA for the Counterterrorism Division in the Iraq Unit overseeing FBI counterterrorism operations and personnel deployments in Iraq. He began his FBI career as a Special Agent (SA) in March 1996, assigned to the New York City Field Office where he worked in the Criminal Division and served as a member of the Special Weapons and Tactics Team.

Mr. Abbate began by thanking the group and FBI staff for all their hard work in transforming the traditional "in-person" meetings into virtual options so they could continue to do their important work. Mr. Abbate talked about the current state of the FBI, and the threats and challenges they face, and how the APB's work makes a difference in the law enforcement community. He stated that counterterrorism is at the top, followed by counterintelligence and cyber, then violent crime, public corruption, civil rights, organized crime, and white-collar crime. Mr. Abbate stated they are concerned about the gun violence and gang violence plaguing so many of communities, along with the opioid crisis and child exploitation, but the FBI's looking hard at how they can intensify their impact in all those areas.

Mr. Abbate continued by noting counterterrorism remains the FBI's number one priority, even as the terrorism threat continues to change. The example he gave of that shift was the violence and destruction at the U.S. Capitol on January 6, 2021. There were peaceful protestors in D.C. but also criminal behavior that has no place in our democratic society to include assaults on 139 police officers. He assured the members they've been working day and night across the country to track down those responsible and hold them accountable.

Mr. Abbate continued to talk about the terrorist's space and the two types of threat actors that have posed the most lethal threat with the first being homegrown violent extremists who often act alone in the U.S., who are inspired by foreign terrorist organizations and their ideologies. Then there are the domestic terrorists who are racially or ethnically motivated and have been the most lethal threat in terms of impact and loss of life over the past several years. He stated that time and time again, would-be terrorists have been disrupted before they were able to strike, and those cases were driven by the frontline reporting and observations of our state and local partners.

Another topic Mr. Abbate discussed was maintaining lawful access to electronic evidence as technology continues to evolve. As end-to-end encryption proliferates across popular commercial products, the ability to obtain the evidence needed to investigate and prosecute all manner of crimes is steadily eroding. Mr. Abbate stated they will continue to talk to legislators, policymakers, and other leaders about the effects of this problem until a workable solution can be found. He stated we all want safe, secure, private data, and safe and secure communities, and he felt we could have both.

Mr. Abbate then talked about the importance of CJIS and the APB. He stated the CJIS APB helps keep the FBI in touch with 18,000 criminal justice agencies that own the data held within these systems. The data they provide leads to the success of CJIS programs like the National Crime Information Center (NCIC), National Data Exchange (N-DEx), Uniform Crime Reporting (UCR), and Next Generation Identification (NGI). The data helps to keep weapons out of the hands of people who shouldn't have them, solve cases, stop crime, and save lives. Over the past 25 years the APB has offered over 2,200 recommendations and the FBI has implemented 98 percent of them. Improvements to the way information about hate crimes is collected and how we alert law enforcement in real time about people with violent criminal histories have been made because of these recommendations. The APB continues to define the future of criminal justice information for our nation that includes new capabilities and data collections.

Mental health is a huge challenge currently facing the law enforcement community and is the reason the FBI and APB together, established the Law Enforcement Officer Suicide Data Collection (LESDC). This gives agencies a way to report law enforcement suicides and attempted suicides, so national statistics on these events can be compiled. Due to the APB's support, progress in National Incident-Based Reporting System (NIBRS) participation, Use-of-Force reporting, and biometric capabilities have been seen.

Mr. Abbate concluded by stating the APB is a perfect example of how the criminal justice community can collaborate to keep our citizens safe. The work to provide policy, operational, and technical guidance from the views of the groups represented is crucial to achieving their collective goal to improve, enhance, and modernize our criminal justice information systems and programs so we can better protect our law enforcement officers and those they serve.

Then, Sheriff Witt recognized the Working Group and Subcommittee chairs to include the following:

Mr. Joe Leon Guerrero, Western Working Group Chair
Ms. Renee Rigby, Northeastern Working Group Chair
Mr. Rick Stallings, Southern Working Group Chair
Mr. Tom Prevo, North Central Working Group Chair
Ms. Jennifer Armstrong, Federal Working Group Chair
Ms. Lynn Rolin, National Instant Criminal Background Check System (NICS) Subcommittee Chair
Ms. Carol Gibbs, N-DEx Subcommittee Chair, and APB member
Mr. Derek Veitenheimer, UCR Subcommittee Chair
Mr. Brian Wallace, NCIC Subcommittee Chair, and APB 2nd Vice Chair
Mr. Joe Dominic, Security and Access (SA) Subcommittee Chair
Captain Kyle Gibbs, Compliance Evaluation (CE) Subcommittee Chair, and APB member
Mr. Charles Schaeffer, Chair of the Public Safety Strategy (PSS) and Identification Services (IS) Subcommittees, and APB 1st Vice Chair

Mr. Megna introduced CJIS, Deputy Assistant Director (DAD), Information Services Branch, Ms. Kimberly DelGreco; Second Vice Chair, Mr. Brian Wallace; CJIS, DAD, Technical, Finance, and Logistics Branch, Mr. Brian Griffith; First Vice Chair, Mr. Charlie Schaeffer; CJIS, DAD, Operational Programs Branch, Mr. Greg Nelsen; EAD, Science and

Technology Branch (STB), Mr. Darrin Jones; CJIS, AD, Mr. Michael Christman; and APB Chair, Sheriff Kathy Witt. (*See Appendix B for a list of all attendees.*)

Sheriff Witt then turned the meeting over to SAC of the FBI Tampa Field Office, Michael McPherson for welcoming remarks. Mr. McPherson applauded the lifesaving recommendations the CJIS APB makes that help law enforcement work more collaboratively and strategically. He stated of the 56 field offices across the country the Tampa Field Office is the 18th largest and has a workforce of 200 special agents, 200 task force officers, and just over 200 support personnel. They service a population of over nine million people, but that didn't include the over 60 million visitors every year and that's why they depend on effective information sharing and strong law enforcement partnerships to do the job of protecting the public. The Tampa Field Office enjoys strong effective collaboration with the Orlando Police Department and the Orange County Sheriff's Office, and Mr. McPherson believed these successful partnerships have been enhanced due to the actions of the CJIS APB. The APB recognized the value of information sharing in law enforcement and its capacity to save lives and prevent crime. Currently the Florida Department of Law Enforcement (FDLE) is working with the FBI's CJIS Division to transition Florida to the NIBRS and will begin the certification process in July. On April 25, 2021 a call came into the National Threat Operations Center (NTOC) and threats were made to blow up a residence and the family. The NTOC operator immediately called the Tampa Field Office advising of the situation. Through the CJIS shared information systems it was determined the individual had violated several family protection orders. Because of the information that was shared, the individual was detained, and no harm was done. Mr. McPherson stated it was another example that sharing information does save lives. Mr. McPherson ended by commending the APB members for recognizing the value of these shared systems and thanked them for their hard work.

Next, Sheriff Witt introduced Ms. Denise Demps, Chief Deputy of the Orange County Sheriff's Office. Chief Deputy Demps thanked the CJIS APB for the invitation and welcomed them to Orlando. She noted she was very proud of her agency and how they've overcome all the challenges the past year due to the pandemic and how they've not only had to keep the members of their agency safe but also their community. She noted one of the things they've done to keep their community safe was to put together a medical response team to take care of special incidences where they knew there was a positive case of coronavirus. Chief Deputy Demps also talked about the civil unrest with the death of George Floyd. They had several days and nights of protesting and their team made sure no one was violated and there was minimal violence. She stated in spite of the hardships their agency continued to grow and implement new services to the community and one of those new services was a Behavior Response Unit that helps with not only the mentally ill in the community, but officers as well. Unfortunately, since some of the restrictions have been lifted, they've noticed a rise in gang violence according to Chief Deputy Demps. So, they created a task force which implemented intelligence gathering as well as investigative measures. Thanks to the sharing of information, that task force was able to take 78 firearms and 182 violent criminals off the street. Despite the pandemic and the civil unrest, the crime in Orange County has gone down by 18% and that was all thanks to what the APB is doing to ensure law enforcement can have access to the correct information, share the data, and access real time information.

Sheriff Witt then welcomed Deputy Chief Jose Velez of the Orlando Police Department to say a few words. Deputy Chief Velez thanked the APB members for allowing him to speak.

He noted the CJIS APB seeks advice and guidance of all the developmental operations of all CJIS programs and those who use them and everyone there had a shared goal of collaborating to benefit the criminal justice community. He relayed the Orlando Police Department's gratitude for the partnership with the FBI and the CJIS APB. Deputy Chief Velez stated Orlando Police Department remains committed to optimizing their services and keeping their officers and community safe.

Sheriff Witt then introduced Mr. Darrin Jones, EAD of the FBI's STB. Mr. Jones oversees the STB of the FBI, which includes the FBI Laboratory Division, the Operational Technology Division (OTD) and the CJIS Division. Mr. Jones hit the highlights of the STB, focusing on areas of significance to the APB. Mr. Jones stated the STB is the largest branch in the FBI with over 5,000 employees. STB's mission is to leverage science and technology to enhance operations and investigations. The Laboratory Division is home to traditional forensic sciences like latent, Deoxyribonucleic Acid (DNA), firearms, and tool marks, but it's also home to world class crime scene management reconstruction teams. The APB has been heavily involved with the Rapid DNA (R-DNA) Program for more than a decade, forming the CJIS APB R-DNA Task Force in 2010. Last August, the FBI completed all legislatively mandated tasks required by the R-DNA Act of 2017 and are now ready for the implementation of the R-DNA for qualifying arrestees at booking stations. This technology has the potential to substantially impact law enforcement operations across the country, quickly providing investigative leads to law enforcement while the arrestees are still in custody. This would not have been possible without the leadership and the work of the R-DNA Task Force.

Mr. Jones went on to talk about the Terrorist Explosive Device Analytic Center (TEDAC) located in Huntsville, Alabama. He stated it is the world's most sophisticated multi-national disciplinary facility conducting forensic analysis, technical exportation, and intelligence analysis on explosive materials, and improvised explosive devices through scientific and technical intelligence means. The TEDAC can determine how explosive devices were created, link improvised explosive devices from separate incidents, connect bombs to bomb makers, and rapidly share this critical information with our international and domestic law enforcement partners as well as the military and the intelligence communities. The FBI Laboratory Division is not just about conducting forensic examinations, it's also about advancing forensic science and encouraging and enforcing forensic discipline. Mr. Jones continued to touch on forensic discipline because he felt it was important, particularly today, as they work to address the erosion of the confidence and trust that exists between the public and law enforcement in many American cities. Mr. Jones quoted former FBI Director Hoover in saying that "the most effective weapon against crime is cooperation, and the efforts of all law enforcement agencies, with the support and understanding of the American people." Mr. Jones felt Mr. Hoover understood the importance of law enforcement maintaining the public trust and it's still true today regarding forensic sciences. Mr. Jones felt it's more critical to our future success as they employ new technologies in law enforcement. To help rebuild the confidence and further strengthen the forensic sciences foundations, the FBI Laboratory is leading international efforts to carefully study the reliability of forensic discipline. The current focus is on pattern evidence disciplines to include fingerprints, firearms, handwriting, and shoe prints to name a few. To ensure they have a robust representation across sections, the research projects in these areas involved hundreds of FBI examiners, examiners from other agencies as well as state crime labs across the nation and private sector examiners. Studies on fingerprints have produced more than

a dozen research papers as well as praise from the President's Council on Science and Technology and one of those research papers has been download over 60,000 times.

Mr. Jones continued to speak about integrity in data analysis. He feels we stand on a whole new era of data analytics through artificial intelligence (AI). Science fiction movie lines from just a few years ago are already starting to immerge as reality in the ways we aggregate, assimilate, and analyze data. He can easily envision a day when this data will serve as a basis for a probable cause judicial warrant and when that day arrives, we need to ensure we can not only present the data, but very granularly improve how we derive the data. He said as law enforcement executives, it's our obligation to ensure we are adhering to the highest standards of data science and we must strive to keep the civil liberties and privacy of the people we serve in mind and firmly engrained in our policies, processes, and procedures. EAD Jones felt there is much at risk and we must remain disciplined and transparent in both motive and process to build and maintain trust in our institutions, our processes, and our people.

Mr. Jones discussed facial recognition and he said there is a tremendous amount of misunderstanding surrounding how this technology is being used in law enforcement. He stated when the technology is used correctly, by well-trained individuals who adhere to established standards, it has proven to be a valuable tool for law enforcement, but when one law enforcement agency misuses the technology, it negatively affects us all.

Mr. Jones then briefed members on the OTD. He stated this is where they bend and stretch technology to help achieve their investigative mission. He stated there are approximately 1,500 technologists working across a wide range of disciplines such as physics, electrical and mechanical engineering, cryptography, digital forensics as well as computer network exporation. OTD employees often support high profile investigations which were born out of technical necessities, such as the need for better video analytics. In the 2013, after the Boston Marathon bombings the FBI was flooded with video and digital images from news crews and video surveillance cameras, which created an unprecedented challenge for the video technology. They received more than 13,000 images and over 2,000 videos within the first 72 hours. After they released images of the subjects, they received an additional 100,000 images and 10,000 videos. He stated even though they were able to identify the subjects, it was far from efficient and afterward they conducted a thorough investigation of their video analytic capabilities. It was clear improvements were needed. Their capabilities were put to the test seven years later and for the first time, the FBI was able to rapidly deploy a tip line for uploading images that worked remarkably well. Then again after the January 6, 2021 attack on the Capitol, they were able to quickly use the capability, efficiently view over 24,000 images and videos, and disseminate them to the field offices all over the country.

Mr. Jones talked about lawful access and how as a result of the implementation of the default warrant proof encryption, criminal and national security investigators are unable to access digital evidence even though they are lawfully authorized to do so. There have been lawful access bills introduced, but there's still a long way to go. He explained as law enforcement executives, they must know what they are and are not asking for. The tech industry has never been asked to hand over any decryption capability to law enforcement, but what they have asked is for industry to design, implement, secure and control, for themselves; the capability to decrypt information when presented with a lawful court order. The tech industry would have Americans believe this can't be done securely, but Mr. Jones said it is possible. He

stated the FBI is not opposed to strong encryption and supports and recommends the use of very strong, but responsibly managed encryption. The FBI is trying to identify easier ways to capture data on the lawful access encryption challenge, but it's difficult to quantify this challenge. Mr. Jones stated several months ago it was discussed adding new data fields within the NIBRS to capture lawful access data across all agencies. The UCR Subcommittee was not in support of believing it would be a financial burden to agencies, as well as the FBI, and would take a large amount of work and time and they needed a quick fix. The subcommittee recommended the use of a web-based interface like what is used to collect Use-of-Force data. He stressed we have to do a better job measuring lawful access and how it impacts our agencies so we can better inform our policy makers.

Mr. Jones closed by saying he believes the STB's role has never been more important as they continue to move together into this realm of technology.

Agenda items were then addressed. *(See Appendix C.)* Staff papers were distributed via e-mail to attendees prior to the meeting. *(See Appendix D.)*

APB Item #1 Executive Briefings

The topic was presented by CJIS AD Michael Christman. *(See Appendix E, PowerPoint.)* He expressed his excitement to be back at CJIS as the AD. His first APB meeting was in 2019 and seeing the process at work and what the CJIS Division does, helped him reshape his understanding of the FBI's relationship with law enforcement. He stated although this meeting was a blended meeting with in-person and virtual, it was still a positive step forward.

Mr. Christman began by talking about the pandemic's effect on the usage of some of the CJIS programs. Before the pandemic, the NCIC was running approximately 11 million transactions per day, but during the pandemic, it dipped down to around four to five million a day. There has been an increase from April of 2020 to April of 2021 and it's anticipated as travel increases and the economy picks up the numbers should continue to increase. The tenprint monthly processing also took a significant decrease between the civil and criminal fingerprint processing during the pandemic. Mr. Christman stated CJIS is optimistic as the numbers are beginning to increase as the economy and travel increase. The NICS was another big story during the pandemic. The election year and other events helped drive numbers up with eight out of the top ten highest days and nine of the top ten highest months in the history of the NICS program occurring in 2020 and 2021. A new high day record was set on March 17, 2021 with over 236,000 transactions. The highest month was March 2021 with 4.7 million. Great information technology (IT) and operations teamwork allowed the NICS to meet this demand and increase productivity through telework. The NTOC saw numbers remain steady through 2019 and 2020 but have seen a dramatic increase according to Mr. Christman. In FY 2020, the NTOC averaged about 3,500 tips per day to include telephone calls and electronic tips. Currently in 2021, they are averaging 6,000 tips per day. N-DEX searches seemed to hold steady during the pandemic. Typically, they average 5 million N-DEX searches a month and increased activity was from new users and contributors.

Mr. Christman then discussed a new partnership between the Law Enforcement Enterprise Portal (LEEP) and FirstNet which could open the door for new users to access law

enforcement data and services. The primary focus will be law enforcement, but it is believed there will be opportunities for first responders with a law enforcement nexus to gain access to LEEP resources that are specific to their mission.

He briefed the CJIS Division, with the support of the CJIS APB, is focusing efforts on the development of a file in the NCIC for Extreme Risk Protection Orders (ERPOs). As a direct result of an increase in mass shootings across the nation, states have passed red flag laws to combat gun violence. Red flag laws and ERPOs allows family members and law enforcement officers to petition courts to restrict an individual from possessing a firearm based on the belief they are a danger to themselves or others. He noted the CJIS APB approved the creation of a new NCIC ERPO file in December 2019 and prioritized its development above other NCIC enhancements due to the impact to officer and public safety. Mr. Christman expressed appreciation for the involvement of the CJIS APB and hoped a new file would be available by the fall 2022.

Mr. Christman then briefed the members on the NGI Iris Service and the continued work growing the iris image repository and user base. The iris repository consists of nearly 1.5 million enrollments, representing more than a million unique identities. This service provides an automated contactless method of identifying a subject if the subject's iris is enrolled in the repository. The NGI Iris Service continues to be valuable to correctional facilities when moving or releasing inmates with a response time of only 18 seconds. This service could also be used by law enforcement, court staff and probation and parole agencies. Mr. Christman informed the group that Arizona was the first state to become interoperable since launching full capability in September of 2020 with state, county, and local agencies in Arizona submitting iris images in March of 2021.

Mr. Christman briefed the members on the UCR Program. He mentioned the Use-of-Force and NIBRS initiatives are on track and the group would hear more later in the day. The US Attorney General tasked the Department of Justice (DOJ) with conducting a 30-day review on hate crime to strengthen the DOJ's enforcement efforts to address hate crime violence and discrimination across the nation. As part of the review a recommendation was made for the UCR Program to develop and draft a plan to release hate crime data on a more frequent basis. The CJIS Division recognized the importance of hate crime reporting and is committed to releasing this data in a timelier manner, possibly on a quarterly basis. The FBI UCR Program established a project team to include state UCR programs and executive board members, to conduct research and planning to implement this recommendation. Mr. Christman informed the group the FBI's Criminal Investigative Divisions Civil Rights Program is hosting conferences in 2021 to raise awareness of hate crime issues occurring across the nation and to educate law enforcement on the hate crime resources available at the federal level. There's been a lot of discussion from the DOJ and consumers of the UCR data about releasing data in a timelier manner. Currently the annual publications come out at the end of each following year. For calendar 2022, the FBI will work to release the annual publications earlier in the year. With releases being done on a quarterly basis it will allow the data to be released the same year it's collected. Mr. Christman noted to meet the deadline for more timely releases, we must all work together to optimize data submissions in order to provide transparency. Mr. Christman informed the members each annual release of Crime in the U. S., Hate Crime Statistics, Law Enforcement Officers Killed and Assaulted (LEOKA), and the NIBRS will be exclusively available on the

Crime Data Explorer (CDE), and all previously released publications will continue to be available on www.fbi.gov.

Mr. Christman mentioned the NTOCs dual-routing initiative. The volume of threat to life tips received by the NTOC continues to spike significantly. Many tips have no federal nexus, but each one must be looked at and handled appropriately. The NTOC personnel have visited all 56 FBI field offices to develop awareness around the NTOC mission and to identify law enforcement partners willing to except threat to life tips that don't have a federal nexus and as a result a dual-routing initiative has been established. The initiative includes establishing a dual-routing workflow to allow immediate dissemination of actionable, non-federal, threat-to-life tips to FBI field offices, state fusion center or state partners directly from the NTOC. Currently 25 field offices and 23 state fusion centers or state partners are participating in the dual-routing initiative.

One year ago, the Law Enforcement Engagement Unit (LEEU) was established, dedicated to sharing information about the CJIS Division and the CJIS programs and services with our law enforcement partners and FBI field offices. Mr. Christman stated despite the pandemic, it was a successful year for the LEEU as they conducted 40 Officer Safety Awareness training sessions to over 800 participants in 27 states. This is a great example of taking UCR data, such as the LEOKA data, analyzing it and presenting it to our law enforcement partners for appropriate action. This year the Tribal Engagement Program engaged with 42 tribes and supported several training events, virtual conferences, and task forces. LEEU staff also supported meetings of the new PSS Subcommittee and the LEEU writer-editors facilitated publication of CJIS-related articles in many law enforcement and criminal justice publications.

In closing, Mr. Christman thanked members for their participation and encouraged healthy debate that would lead to thoughtful decisions. He closed by thanking them for their commitment to public service.

APB Item #2 Tribal Task Force Update

This topic was presented by Mr. William Denke, Chief of the Sycuan Tribal Police Department in El Cajon, CA and Chair of the Tribal Task Force. *(See Appendix R, PowerPoint.)*

Mr. Denke advised that the Tribal Task Force is currently made up of 12 members with a very balanced representation of four tribal representatives, four state and/or local representatives, and four federal representatives. The task force last met in November 2020 and two additional virtual meetings were held in Fiscal Year 2020. Fiscal Year 2020 accomplishments included the establishment of a NIBRS Collection Application (NCA) which provides federal and tribal agencies the opportunity to submit NIBRS data to the UCR Program. The NCA is accessible via LEEP. The tribal NIBRS data submitted via the application is then forwarded to the Bureau of Indian Affairs (BIA) to ensure on time, accurate reporting. Mr. Denke said this is very important because the BIA requires tribal agencies that are contracted, commissioned, or deputized by the BIA to meet 30-day or monthly deadlines.

Next Mr. Denke briefed on the Tribal Access Program (TAP), commonly referred to as TAP, which was rolled out in 2016 as a solution by the DOJ for those verified tribal programs or agencies that needed access to CJIS programs which included hardware and software to allow for such access. As of the end of 2020, 98 Tribes have been accepted into this program. The DOJ is also deploying the TAP to several BIA locations that serve an additional 55 tribes. The number of tribes that will be served by TAP once their deployments have been completed will be a total of 153. Once this project is complete there will be over 500 tribal and federal agencies working on or with tribal reservations to access CJIS systems via TAP.

A “Dear Tribal Leader” letter was put together by the task force and was distributed to all 574 recognized tribes, hitting on the latent cascade of tribal submissions. The letter explained the cascade searches of biometric events against those unsolved latent files within the NGI system. This letter reflected on the tribe's option to decline participation if they wish.

The last accomplishment Mr. Denke touched on was the completion of the tribal video. Task force members will soon get to view it. The FBI went to the field to put this video together. It highlights six different tribes. The video highlights NGI, Law Enforcement Enterprise Portal (LEEP), NCIC, N-DEx, NICS, and UCR. Mr. Denke said he looks forward to viewing the video and getting it out to all the tribes in the very near future.

Mr. Denke mentioned tribal representation in the Advisory Process which includes a tribal representative on the APB, each of the regional working groups and a BIA Office of Justice Services representative on the Federal Working Group.

The task force next looks to focus on the study of tribal access to CJIS services. The task force is looking for partners to develop a study to determine tribal access on a state by state basis and the impediments that the tribes still have accessing CJIS systems through their respective states. The results of this study should provide the task force and the CJIS Tribal Engagement Program with solid information regarding the state of tribal access to CJIS systems with an effort to establish future CJIS initiatives to assist the tribes. The content on the survey has been completed and the survey is currently in the final approval process with CJIS. It will then be forwarded to the Office of Management and Budget (OMB) for final approval. It will then be sent to the 35 tribal CJIS System Officers (CSO).

The national Use of Force Data Collection is another task force initiative and along with the Tribal Engagement Program, they continue to increase awareness and tribal participation. There has been a slight increase in participation.

The task force continues to address issues regarding missing and murdered indigenous persons along with the Tribal Engagement Program they are increasing awareness of CJIS programs and services such as the Virtual Command Center which can be utilized as full case management.

Lastly, Mr. Denke mentioned the Tribal Engagement Program has met five different times with approximately 50 tribes. Another meeting with 12 tribes is scheduled to be held in late June

2021. The Tribal Engagement Program will continue to participate in tribal conference meetings as they become available.

APB Item #3 Chairman’s Report on the UCR Subcommittee

This topic was presented by Mr. Derek Veitenheimer, UCR State Program Manager, Wisconsin Department of Justice, and Chair of the UCR Subcommittee. *(See Appendix F, PowerPoint.)* He noted the subcommittee spent most of a full day discussing the issues and tried to understand the importance of improving the program with a focus on implementing changes as effectively and efficiently as possible. He acknowledged in many cases it is easier to add new data values than to define or add new data elements which change the structure of a new incident. This can be costly, as a result the subcommittee tried to maintain that awareness when recommending changes that would require cost. He then addressed the issues individually by the subcommittee.

UCR Issue #2 Beyond 2021 Initiative Update –NIBRS Data Elements

The purpose of this topic was to recommend proposed modifications to the NIBRS data collection recommended by the Beyond 2021 Task Force. There were 11 issues covered as follows:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

There were two options provided. Option A1: Add the ability to capture discharge of a firearm on the NIBRS Offense Segment. Option A2: No change.

The Northeastern, Southern, and Federal Working Groups motioned for Option A1. The North Central and Western Working Groups motioned for Option A2.

Mr. Veitenheimer noted the UCR Subcommittee considered the views expressed by the Association of State Uniform Crime Reporting Programs (ASUCRP) that opined the most effective way to address the issue was to add a new code to an already existing data element.

The UCR Subcommittee recommended a new option to the CJIS APB as follows: To add a new code to an existing data element such as Type of Weapon or Force Used with a priority of 3M.

Discussion: A member questioned if this would replace something that would be captured mandatorily. Further, if users put something in that field, would it replace data that could be used statistically somewhere else, or could there be multiple selections? Mr. Veitenheimer noted the plan was to allow for multiple selections of weapons of force.

APB RECOMMENDATION: The CJIS APB moved to add a new code to an existing data element such as Type of Weapon or Force Used. The priority should be 3M.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

There were two options provided. Option B1: Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment. Option B2: No change.

The North Central, Southern, and Federal Working Groups motioned for Option B1. The Western Working Group motioned for Option B2. The Northeastern Working Group motioned for a new option: Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment, with a caveat of not mandatory, and a priority of 3M.

Mr. Vietenheimer noted subcommittee members again agreed adding a new code to an existing data element would be the most efficient.

The UCR Subcommittee recommended a new option to add a new code to an existing data element such as Type of Criminal Activity with a priority of 3M.

Discussion: A member questioned with the addition of the new code if the entry would be mandatory or if multiple selections could be made. Mr. Veitenheimer noted the data element the new code was being added to is already mandatory for certain offenses, the code is just an addition choice, and that code may or may not apply. He noted it would not replace any current codes and multiple selections could be made where applicable.

APB RECOMMENDATION: The CJIS APB moved to add a new code to an existing data element such as Type of Criminal Activity. The priority should be 3M.

Issue C: Creation of a New Injury Code – Gunshot Wound to be Recorded on the NIBRS Victim Segment

There were two options provided. Option C1: Create a new NIBRS Injury Code of Gunshot Wound to be added on the NIBRS Victim Segment. If approved, the new Injury Codes would be as follows:

N = None
B = Apparent Broken Bones
G = Gunshot Wound
I = Possible Internal Injury
L = Severe Laceration
M = Apparent Minor Injury
O = Other Major Injury
T = Loss of Teeth
U = Unconsciousness

Option C2: No change.

Mr. Veitenheimer noted during discussions subcommittee members inquired if there was an option for more than one injury level to be entered into the victim segment and it was affirmed there was.

The UCR Subcommittee recommended Option C1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to create a new NIBRS Injury Code of Gunshot Wound to be added on the NIBRS Victim Segment. If approved, the new Injury Codes would be as follows:

N = None
B = Apparent Broken Bones

G = Gunshot Wound

I = Possible Internal Injury

L = Severe Laceration

M = Apparent Minor Injury

O = Other Major Injury

T = Loss of Teeth

U = Unconsciousness

The priority should be 3M.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

There were two options provided. Option D1: Add the ability to capture injury information for homicide victims within the NIBRS. Option D2: No change.

The Federal Working Group motioned for Option D1. The North Central and Western Working Groups motioned for Option D2. The Northeastern Working Group motioned for a new option: Add the ability to capture injury information for homicide victims within the NIBRS and add a new data value of “unknown” as an option. The Southern Working Group motioned for new option: To add the ability to capture injury information for deceased victims within the NIBRS.

Mr. Veitenheimer noted the subcommittee discussed this issue at great length. They concluded the intent was to understand the various types of injuries that victims of violence incur, including homicide victims.

Discussion: A member questioned if by limiting it to homicide victims if manslaughter victims would be left out and were there discussions to broaden the scope. Mr. Veitenheimer noted the idea was to allow for reporting specific injuries for homicide victims which could be easily accomplished by eliminating a validation change that would no longer block incidents that reported where a homicide was reported with injury type. He noted the conversation focused specifically on homicide victims noting there were not as many manslaughters by negligence or justifiable homicides. Members opined the value for reporting the information was significant enough to word as they did. They did discuss broadening the scope, however, there was concern that by opening the floodgates it could cause confusion. As a result, they tried to stay focused on homicides.

A member questioned if the subcommittee considered an attempted homicide that wasn't successful. Mr. Veitenheimer noted the subcommittee did but since attempted homicides are currently coded as aggravated assaults. The reporting of the injury type is mandatory for aggravated assaults so the information for those is already captured.

Mr. Veitenheimer further clarified this was not an attempt to address the process of agencies classifying a death as a homicide but rather to allow validation that currently blocks reporting the injury type for homicides.

A member inquired if they discussed accidental deaths or occupational deaths. Mr. Veitenheimer reiterated the subcommittee's conversation was specifically focused on allowing

homicide victims to be submitted with an injury type easily by the removal of the current validation preventing it.

The UCR Subcommittee recommended Option D1 as originally listed with a priority of 3M.

APB RECOMMENDATION: The APB moved to accept Option D1: Add the ability to capture injury information for homicide victims within the NIBRS. The priority should be 3M.

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

There were two options provided. Option E1: Create a new NIBRS Offense – Criminal Negligence. Option E2: No change.

The Northeastern, Southern, and Federal Working Groups motioned for Option E1 with a priority of 3M. The North Central and Western Working Groups motioned for Option E2.

Mr. Veitenheimer noted during subcommittee discussions members expressed concern with the addition of criminal negligence due to the variation in state laws, concern the vagueness would cause confusion, and the minimal return on value.

The UCR Subcommittee recommended Option E2.

APB RECOMMENDATION: The CJIS APB moved to make accept Option E2: No change.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

There were two options provided. Option F1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to expand the collection of NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS offenses. Option F2: No change.

The North Central, Southern, Western, and Federal Working Groups recommended Option F1 with a priority of 3M. The Northeastern Working Group recommended Option F2.

Mr. Veitenheimer noted Data Element 12 is currently restricted to a select number of offenses and the idea for this issue was to expand the collection to all NIBRS offenses. He noted the subcommittee considered the opinion of the ASUCRP, who were in favor of Option 1. However, noting criminal activity is not always relevant for all offenses such as driving under the influence, sports tampering, et cetera, so the UCR Program Office would still apply some restrictions where the offense would not have a criminal activity reported with them.

Discussion: A member noted currently there are offenses that the entry of a criminal activity code is mandatory. Would the expanded list of offenses proposed require the mandatory entry of criminal activity codes? Mr. Veitenheimer noted they would.

A member noted it could be confusing to say it was expanding with a caveat that some offenses would not be included but not be specific about what those are. Mr. Veitenheimer followed noting rather than listing out all the expanded offenses, the subcommittee decided to lean on the expertise of the UCR Program Office to determine what would apply and how to mitigate any potential issues whether through warnings or validations.

A member noted this would involve costs to reprogram and inquired if the subcommittee felt strongly enough about the importance to implement. Mr. Veitenheimer noted this would not involve adding a new data element but rather eliminating a validation in place that would prevent a code from being reported and therefore have a minimal impact.

The UCR Subcommittee recommended Option F1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to accept Option 1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to expand the collection of NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to all the NIBRS offenses. The priority should be 3M.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

There were two options provided. Option G1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include the additional values recommended by the Beyond 2021 Task Force. If approved values will be as follows:

O = Operating/Promoting/Assisting/**Abetting**
W = **Conspiracy**

Option G2: No change.

The North Central, Southern, Western, and Federal Working Groups recommended Option G1. The Southern Working Group assigned a priority of 4L. The others assigned a priority of 3M. The Northeastern Working Group recommended Option G2.

Mr. Veitenheimer noted the subcommittee saw value in adding conspiracy and clarifying language with abetting. The UCR Subcommittee recommended Option G1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to accept Option G1 – Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include the additional values recommended by the Beyond 2021 Task Force. If approved, the additional values will be as follows:

O = Operating/Promoting/Assisting/**Abetting**
W = **Conspiracy**

The priority should be 3M.

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

There were four options provided for this issue. Option H1: Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force and create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications. Option H2: Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force. Do not create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications. Option H3: Do not modify NIBRS Data Element 20 (Suspected Drug Type) but create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications. Option H4: No change.

Mr. Veitenheimer noted the members were appreciative of keeping the drug list current, as it is a frequent concern for the states.

The UCR Subcommittee recommended Option H1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to accept Option H1: Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force and create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications. The priority should be 3M.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

There were two options provided. Option I1: Modify NIBRS Data Element 22 (Type Drug Measurement) to reflect the changes recommended by the Beyond 2021 Task Force. Option I2: No change.

The UCR Subcommittee recommended Option I1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to accept Option I1: Modify NIBRS Data Element 22 (Type Drug Measurement) to reflect the changes recommended by the Beyond 2021 Task Force. The priority should be 3M.

Issue J: Modification to the FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

There were two options provided. Option J1: Modify the FBI UCR Program policy to allow for the conversion of NIBRS drug quantities to common units proposed by the Beyond 2021 Task Force. Option J2: No change.

The UCR Subcommittee recommended Option J1, with a priority of 3M.

Discussion: A member inquired if this change would create any compatibility issues between the old and new format. Mr. Veitenheimer noted it did not. It allows for the better categorization and reporting of the current drug units of measure. It's just a change to policy and methodology. No programming changes should be required.

A member questioned how this would affect historical data. For example, if the agency was using kilos before and now reports in pounds. Mr. Veitenheimer referred to Ms. Amanda Shaffer, UCR Program Office. Ms. Shaffer noted the conversions would be used for publication purposes and handled by the UCR Program. The files and units would still be available as originally submitted to the UCR Program for comparisons.

APB RECOMMENDATION: The CJIS APB moved to accept Option J1: Modify the FBI UCR Program policy to allow for the conversion of NIBRS drug quantities to common units proposed by the Beyond 2021 Task Force. The priority should be 3M.

Issue K: Additional Property Values of Utilities and Services and Intellectual Property

There were two options provided. Option K1: Add the data values of *Intellectual Property* and *Utilities and Services* to NIBRS Data Element 15 (Property Description). Option K2: No change.

The UCR Subcommittee recommended Option K1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to accept Option K1: Add the data values of Intellectual Property and Utilities and Services to NIBRS Data Element 15 (Property Description). The priority should be 3M.

UCR Issue #3 Beyond 2021 Update – Addition of Geolocation to the NIBRS

The purpose of this topic was to provide the recommendations of the Beyond 2021 Task Force for implementation of geolocation as a data point within the NIBRS. There were three options provided. Option 1: Pursue the addition of x/y/z (i.e., latitude/longitude) coordinates of the incident, but not address, to the NIBRS data collection. In order to implement this approach, the FBI UCR Program, and the FBI Office of the General Counsel will need to detail a method to collect incident to a geographic point while also providing a dissemination strategy that addresses the risks to privacy. Option 2: Pursue the collection of a geographic location of the incident through the indication of a small aggregate area, such as Census tract. Option 3: No change.

The North Central Working Group recommended Option 1, with a priority of 3M. The Northeastern and Western Working Groups recommended Option 2, with a priority of 3M. The Southern and Federal Working Groups recommended Option 3.

This topic was forwarded for consideration by the PSS Subcommittee. The PSS Subcommittee recommended Option 2. The UCR Subcommittee recommended Option 2, with a priority of 3M.

Mr. Veitenheimer noted during the discussion members voiced various concerns related to privacy, but believe it is a valuable addition for the NIBRS and requests to add the geographic information are received frequently. Members opined that listing longitude and latitude may be drilling down too far and result in the accidental release of private information specifically with regard to sex crimes, human trafficking, et cetera.

APB RECOMMENDATION: The CJIS APB moved to recommend Option 2: Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract. The priority should be 3M.

UCR Issue #4 Expansion of Location Data Values for the NIBRS Data Element (Location Type)

The purpose of this issue was to provide a proposal to implement changes and expansion to the Valid Data Values for NIBRS Data Element 9 (Location Type). There were three options provided. Option 1: Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the chart. The provided changes include a modification of existing Location Code 09 = Drug Store/Doctor’s Office/Hospital code to be separated into three individual Location Types: 09 = Drug Store/Pharmacy, 62 = Doctor’s Office, and 66 = Hospital. These changes will be effective immediately upon approval. Option 2: Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the chart. The provided changes include a modification of existing Location Code 09 = Drug Store/Doctor’s Office/Hospital code to be separated into three individual Location Types: 09 = Drug Store/Pharmacy, 62 = Doctor’s Office, and 66 = Hospital. The implementation will be included as part of the Beyond 2021 effort. All changes will be incorporated into the Beyond 2021 schedule accordingly. Option 3: No change.

The UCR Subcommittee recommended Option 2, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to recommend Option 2: Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the *Data Element 09 recommendations chart*. (Chart is provided below.) The provided changes include a modification of existing Location Code 09 = Drug Store/Doctor’s Office/Hospital Code to be separated into three individual Location Types: 09 = Drug Store/Pharmacy, 62 = Doctor’s Office, and 66 = Hospital. The implementation will be included as part of the Beyond 2021 effort. All changes will be incorporated into the Beyond 2021 schedule accordingly. The priority should be 3M.

CODE	VALID DATA VALUE	DESCRIPTOR	COMMENTS
9	Drug Store/Pharmacy	Store where the Food and Drug Administration-approved medicinal drugs are dispensed and sold.	Exists in NIBRS Technical Specification with other VDV's under same code.
59	Auto Salvage/Junkyard	Location where unusable vehicles or vehicle parts can be bought, sold, or	

		stored. a place where scrap is collected before being recycled or discarded.	
60	Carport/Garage/Driveway	An area around residential space not constituting a residential structure.	
61	Cemetery	An area set apart which contain graves, tombs or funeral urns.	
62	Doctor's Office	A medical facility in which one or more medical doctors, usually general practitioners, receive and treat patients.	
63	Gym/Fitness Club	Indoor club, building, or large room where people exercise or participate in indoor sporting activities to enhance physical fitness.	
64	Golf Course	Outdoor areas of land where golf is played.	
65	Hospital	An institution providing medical and surgical treatment and nursing care for sick or injured people	Routine, preventative, and scheduled care would be included in Doctor's Office. This would include urgent care facilities and inpatient behavioral health centers.
66	Library	Room or building containing collections of books, periodicals, software programs, films, or recorded music for people to read, borrow, or utilize as reference.	
67	Loan/Cash Advance/Check-Cashing Facility	Commercial business where individuals obtain financial services over the counter for a clear fee.	Specialty Store denotes "retail" element. These stores are not considered retail stores and are becoming more prevalent.
68	Marijuana Dispensary	Establishment primarily used for selling medical or recreational marijuana.	Specialty Store denotes "retail" element. These stores are not considered retail stores and are becoming more prevalent.
69	Marijuana Facility	Indoor or outdoor site used for the commercial production and harvesting of cannabis for recreational or medical use.	This is a facility for the manufacture of the product – not a sales facility.
70	Movie Theater	Venue where movies are shown for public entertainment.	
71	Museum	Building in which objects of historical, scientific, artistic, or cultural interest are stored and exhibited.	
72	Pawnshop	Commercial establishment for lending money in exchange for personal property which can be sold if the loan is not repaid by a predetermined time.	
73	Public Transportation	Buses, trains, subways, and other forms of transit which charge set fares, run on fixed rates, and are available to the public.	Incidents which happen on public modes of transportation cannot be considered a static location – need an option to distinguish this.
74	Tattoo Parlor	Place in which the primary function is professional tattooing.	

75	Zoo	Indoor or outdoor establishment, which maintains a collection of wild animals for study, conservation, or display to the public.	
----	-----	--	--

UCR Issue #5 Addition of Data Elements to the NIBRS for the Collection of Lawful Access Data

The purpose of this issue was to present options for adding Lawful Access data elements to the NIBRS data collection. There were two options provided. Option 1: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Option 2: No change.

The Southern, Western, and Federal Working Groups motioned for Option 1. The North Central Working Group motioned for Option 2. The Northeastern Working Group motioned for a New Option: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Caveat to create process to update the data values within data elements.

Mr. Veitenheimer turned the floor over to DFO Nick Megna who noted that Ms. Marybeth Paglino, Director, National Domestic Communications Assistance Center was in attendance. Then, Mr. Megna introduced Mr. Richard Littlehale, Assistant Director, Technology and Innovation Division, Tennessee Bureau of Investigation. Mr. Megna noted Mr. Littlehale is considered an expert on lawful access and has provided some guidance to the advisory process on the topic.

Mr. Littlehale noted he represented a small group of subject matter experts from various organizations. He chairs the Technology and Digital Evidence Committee of the Association of State Criminal Investigative Agencies, which works with the International Association of Chiefs of Police, Major City Chiefs, Major County Sheriffs, National Sheriffs and other organizations that have an interest in the issue. He noted all share the concern of federal partners that unregulated encryption is continuing to shrink access to digital evidence. He noted they agreed with Mr. Abbate and Mr. Jones that it is entirely achievable to create an exceptional access mechanism, a lawful access regime, that will mitigate the issue without an unacceptable trade-off to system security.

Mr. Littlehale stated going dark is the problem and lawful access the solution. He noted the problem is just as acute for the state and local law enforcement community. Those agencies are also having issues getting access to evidence on devices and evidence in motion, evidence in motion across networks, lawfully ordered electronic surveillance and things like that. He further noted state and local agencies are not necessarily as well-resourced as federal agencies.

He provided the following examples noting everyone hears about the big cases in the news, such as San Bernardino and Pensacola, and those are great examples. But for every one of those you hear about, you may not hear about many state and local cases, everything from Internet crimes against children, child predators on the Internet, people who victimize children who are not able to be captured, opiate pushers where communities struggling with the opiate

crisis are unable to get into a device so they can determine how to attribute responsibility for an overdose death. Cyber investigations that are frustrated. Threats of targeted violence that cannot be investigated. Drug trafficking organizations that go unaddressed. Domestic violence extremists who communicate in ways not accessible to law enforcement. These are all state and local problems every bit as much, if not more, than they are for federal partners. He noted he was speaking to the APB to ask for help.

Mr. Littlehale noted the Association of State Criminal Investigative Agencies Executive Board voted in support of the effort. He did not bring a specific recommendation as this is a work in progress. He opined however we are headed towards a solution that will ease the potential burden and result in providing meaningful data. The result would be for advocates in the policy process to be able to take evidence of the lawful access problem to policymakers and demonstrate the magnitude of harm it is causing to public safety so we can find a solution together.

Mr. Veitenheimer proceeded to brief the CJIS APB on the deliberations of the subcommittee regarding the topic. Members were concerned about the technical lift and constraints it could place on law enforcement agencies and the state UCR programs. The members understood the value of collecting the data but expressed concern of how early or quick the information could be collected and added to the NIBRS program, resulting in a potentially long delay of getting meaningful valuable data. With that, members suggested potentially having the FBI UCR Program create an application similar to the Use-of-Force application on the LEEP or the NCA that allows direct entry into a secure web form on the LEEP system.

A few members commented how important they thought collecting the data was and agreed setting up a separate portal from the NIBRS collection would potentially add access to the data quicker.

Mr. Jones expressed his thanks to the group for providing an alternative he believed was better than what was originally proposed. He noted he would be in touch for help moving forward.

The UCR Subcommittee recommended a New Motion: To have the UCR Program identify a collection mechanism outside of the NIBRS data file that leverages the UCR Program data collection infrastructure. The priority should be 3H.

APB RECOMMENDATION: The CJIS APB moved to have the UCR Program identify a collection mechanism outside of the NIBRS data file that leverages the UCR Program data collection infrastructure. The priority should be 3H.

UCR Issue #6 Expansion of Victim to Offender Relationship in the NIBRS Data Element 35

The purpose of this topic was to present a proposal for additions to the acceptable codes within NIBRS Data Element 35 to allow for new victim values with NIBRS. There were two issues addressed.

Issue A – Addition of “FP = Victim was Foster Parent” and “FC = Victim was Foster Child”

There were two options provided. Option A1: Create values “*FP = Victim was Foster Parent*” and “*FC = Victim was Foster Child*”. Option A2: No change.

The UCR Subcommittee recommended Option 1, with a priority of 3M.

APB RECOMMENDATION: The CJIS APB moved to accept Option A1: Create values “FP = Victim was Foster Parent” and “FC = Victim was Foster Child” and make allowable for the NIBRS Data Element 35. The priority should be 3M.

Issue B – Addition of “Co = Cohabitant (non-intimate relationship)”

There were two options provided. Option B1: Create value “CO = Cohabitant (non-intimate relationship)” and make allowable for NIBRS Data Element 35. Option B2: No change.

All the working groups motioned for Option B1. The North Central, Western, and Federal Working Groups assigned a priority of 3M. The Northeastern Working Group assigned a priority of 3H. The Southern Working Group assigned a priority of 4L.

Mr. Veitenheimer noted subcommittee members expressed concern limiting this definition to non-intimate relationships may cause confusion. There was a lot of discussion regarding how to add clarity

The UCR Subcommittee recommended a New Motion: Create value “CO = Cohabitant (non-intimate and non-family relationship)” and make allowable for NIBRS Data Element 35. The priority should be 3M.

Discussion: Two members questioned whether it was implied it was an “and” or an “an” situation. The example of cohabiting cousins was provided, where they were family but not intimate. Mr. Veitenheimer noted there are relationship codes that already exist to define those relationships. Subcommittee members made the additional to better specify what the idea behind cohabitant was, to provide an extra level of classification, saying non-intimate or non-family.

A member inquired if the program was drilling too far down to sub elements and wondered what the value was to that level of minutiae. Mr. Veitenheimer noted specifically in this case, there was a desire to better identify incidents where there were non-intimate people living together that resulted in a crime. There was concern by subcommittee members that not clarifying whether someone was living with a family member would add confusion, so they felt the need to certainly, as the working groups recommended, adding the cohabitant data value with just a greater level of specificity with the idea it would result in less confusion. He further stated subcommittee members try to give thoughtful consideration during deliberations to ensure return on value before making any recommendations.

A member opined you could have a family relationship by genetics, or you could have a family relationship by law. You could be married to someone, and they are part of your family, or you could not be married to them, but you are genetically related to them. This addition could cause more confusion than it helps. It was clear when it was just non-intimate in the original proposal. However, when we add non-family, if individuals are not genetically related, they might be legally related. For example, someone might have son-in-law that's not genetically related to them but cohabitates with them, so they are a family member. They are non-intimate. He was not sure that was going to help when the officer is standing there and asking these questions about victims and suspects. It's like, let's go down the list of what the possibilities are for your relationship. He noted maybe training could help but he didn't think it would be helpful to the investigating officer saying let's talk about your relationship.

Mr. Veitenheimer responded there was broad consensus from the working groups and the UCR Subcommittee to add cohabitant. The UCR Subcommittee was concerned about confusion. They attempted to provide clarity which resulted in more confusion. He noted he felt confident in the UCR Subcommittee's recommendation to add the cohabitant relationship code. He also noted he felt confident through training and the FBI's UCR Program clarifying details. The information could be added to better determine when that code is applicable. He advised he didn't want to get lost in the weeds and debate, the non-family part. If we agree cohabitant should be added, if that's the will of the APB, maybe we focus on that effort and rely on training from the FBI UCR program to clarify when and how that code is used.

One member opined he was in favor of adding the cohabitant. He noted assuming there are already categories for intimates and for those related by blood or marriage, rather than wait for the training to address it may make sense to just say non-intimate and non-family who are cohabitating?

Another member stated if you follow the definitions throughout the states with respect to particular protection orders, cohabitant means there's a sexual aspect. This may be an issue for a future topic paper. If roommate is not an option for a relationship, it certainly should be. He further opined that this is an "and" and not an "or" in the statement. He noted he was confident the UCR Program would make that abundantly clear in the manual, based on the conversation had at the meeting.

APB RECOMMENDATION: The CJIS APB moved to create value "CO = Cohabitant (non-intimate and non-family relationship)" and make allowable for the NIBRS Data Element 35. The priority should be 3M.

UCR Issue #7 Addition of a New Criminal Offense in Progress Data Element in the NIBRS

The purpose of this issue was to present a proposal to create a new data element to track criminal offenses in progress when a justifiable homicide takes place. There were three options provided. Option 1: Change the name of the Data Element 32 (Criminal Offense in Progress) with acceptable values for all crimes against persons and crimes against property offenses. This new data element would be mandated only when a justifiable homicide has taken place. Option 2: Create a new data element for "Criminal Offense in Progress" with acceptable values for all

crimes against persons and crimes against property offenses. This would include no changes to Data Element 32. This new data element would be mandated only when a justifiable homicide has taken place. Option 3: No change.

The Northeastern, Southern, Western, and Federal Working Groups recommended Option 1. The North Central Working Group recommended Option 3, no change.

The UCR Subcommittee recommended Option 3, no change, due to the value and the costs and time to implement the new offense.

Discussion: An APB member stated that determining whether a homicide was justifiable was a question of law and an investigator may have difficulty making that determination. An APB member responded that this determination is made when the person goes to court. Another member believed it would be reported perhaps when it goes through a grand jury or prosecution is declined.

APB RECOMMENDATION: The CJIS APB moved to accept Option 3: No change.

UCR Issue #8 Changes to Race Codes within the FBI UCR Program was handled by the PSS Subcommittee Chair Report.

UCR Issue #9 Beyond 2021 Initiative Update – Revision to the NIBRS Sex Offense Nomenclature

The purpose of this issue was to present the proposed modifications to the NIBRS data collection recommended by the Beyond 2021 Task Force. There were three issues addressed.

Issue A: Replacing the NIBRS Offense - “Fondling”

There were two options provided. Option A1: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

“Criminal Sexual Contact”

- The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.
- The forced touching by the victim of the actor’s clothed or unclothed body parts, without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.

Option A2: No change.

The Northeastern Working Group recommended Option A1, with a priority of 3M. The Western Working Group recommended a New Option: No change to the current definition of “fondling”. Replace the term “fondling” with “criminal sexual contact”, with a priority of 3M. The North Central Working Group motioned for a New Option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

“Criminal Sexual Contact includes the following:

- The intentional touching of the clothed or unclothed genitalia, anus, groin, breast, or buttocks of any person, without the consent of the victim.
- The forced touching by the victim of the actor’s clothed or unclothed genitalia, anus, groin, breast, or buttocks, without the consent of the victim.

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.” The priority was 3M.

The Southern and Federal Working Groups recommended a New Option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

““Criminal Sexual Contact includes the following:

- The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.
- The forces touching by the victim of the actor’s clothed or unclothed body parts, without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.” The priority was 3M.

The UCR Subcommittee recommended the New Option recommended by the Southern and Federal Working Groups.

Discussion: An APB member asked about the definition or intent of the word intoxication since it commonly refers to alcohol incapacitation, would this cover all forms of intoxication? Mr. Veitenheimer said it was intended to cover all forms of intoxication.

Issue A: Replacing the NIBRS Offense - “Fondling”

APB RECOMMENDATION: The CJIS APB moved to modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

“Criminal Sexual Contact”

- **The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.**

- **The forced touching by the victim of the actor’s clothed or unclothed body parts, without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.**

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.

The priority should be 3M.

Issue B: Updating the NIBRS Offense - “Incest”

There were four options provided for Issue B. Option B1: Modify the NIBRS offense “incest” definition to state: “Consensual intercourse between individuals related by blood within the degree that the individuals are prohibited based on state provision.” Option B2: Modify *incest* to be captured as a NIBRS Group B Offense with data captured as part of 90Z – All Other Offenses. Option B3: Discontinue collection of *incest* for national reporting. Option B4: No change.

The North Central, Southern, and Federal Working Groups motioned for Option B1. The North Central and Federal Working Groups assigned a priority of 3M. The Southern Working Group assigned a priority of 4M. The Northeast and Western Working Groups recommended Option B4.

The UCR Subcommittee recommended Option B4.

No discussion.

APB RECOMMENDATION: The CJIS APB moved to accept Option B4: No change.

Issue C: Modification of the NIBRS Offense – “Statutory Rape”

There were two options provided for Issue C. Option C1: Modify the NIBRS offense “*statutory rape*” definition to state: “*Consensual sexual intercourse with an individual who is under the age of majority but meets the state provisions for the age of consent.*” Option C2: No change.

The Northeastern, North Central, and Federal Working Groups recommended Option C1 with a priority of 3M. The Southern and Western Working Groups recommended Option C2.

The UCR Subcommittee recommended Option C2.

APB RECOMMENDATION: The CJIS APB moved to accept Option C2: No change.

UCR Issue #10 Creation of a NIBRS Offense Code Mapping Crosswalk Repository

The purpose of this issue was to present a proposal for the creation of a NIBRS offense code mapping crosswalk displaying state-level statute mapping to NIBRS offense definitions.

There were two options provided. Option 1: Create a NIBRS offense crosswalk repository hosted by the FBI UCR Program and maintained by state UCR programs containing state-level statute information crosswalked/mapped to NIBRS offense codes. Option 2: No change.

The Northeastern, North Central, Southern, and Federal Working Groups recommended Option 1. The Western Working Group recommended Option 2. The UCR Subcommittee recommended Option 1, with a priority of 3M.

Discussion: A member stated their UCR Program manager was concerned with this issue and believed offenses should be coded on what happened within the incident, not the statute the officer is charging them with. They also believed the level of burden placed on the state program managers to update and maintain this crosswalk is very high, especially if the program only has one person.

APB RECOMMENDATION: The CJIS APB moved to accept Option 1: Create a NIBRS offense crosswalk repository hosted by the FBI UCR Program and maintained by state UCR programs containing state-level statute information crosswalked/mapped to the NIBRS offense codes. The priority should be 3M.

UCR Issue #16 Summary of Recently Conducted UCR Quality Assurance Reviews (QAR)

The purpose of this issue was to present results of recently conducted UCR QARs. The details are provided in the staff paper provided as an addendum to the minutes.

APB RECOMMENDATION: The CJIS APB moved to authorize Letters of Interest be sent to each CSO and UCR Program manager as these reviews have been finalized.

APB Item #4 Use-of-Force Update

The topic was presented by Ms. Trudy Ford, Chief of the Global Law Enforcement Support Section (GLESS). *(See Appendix G, PowerPoint.)* Ms. Ford began her presentation by stating that at the request of and in coordination with law enforcement partners the FBI established the National Use-of-Force Data Collection. Data is gathered on law enforcement use of force incidents resulting in the death or serious bodily injury of a person as well as when a firearm is discharged by a law enforcement officer at or in the direction of a person. The goal is not to offer insight into single incidents but rather to gather a comprehensive view of circumstances, subjects, and officers involved in national use-of-force incidents nationwide. Participation will promote transparency and accountability between law enforcement officers and the communities they serve.

Ms. Ford briefed as of Monday, June 7, 2021 the participation rate was 49.5 percent for the 2021 matrix. The collection has continued to grow since its inception in 2019 while gaining new agencies daily who are submitting incident reports and zero reports. Thus far in 2021, they have surpassed the first two years of the collection. Ms. Ford was happy to announce that the first U. S. Territory submitted data to include specifically the Virgin Islands of St. Croix and St. Thomas. To be considered a participant, an agency must submit either a qualifying incident or submit a zero report.

In the 2020 matrix, the data collection reached a milestone of over 50 percent for law enforcement officers represented by the collection all made possible by the staff, the National Use-of-Force Task Force, as well as various other stakeholders. For the 40 percent publication for 2020 they met the OMB percent coverage threshold. Ms. Ford stated the threshold was also met for 2019 and 2021. The publication makes it possible to provide a narrative detailing the number of agencies participating, the list of agencies both enrolled and participating, the response percentages to include agencies that submitted a zero report, an incident report or those that didn't submit any data for a given month. The publications for 2019 and 2020 are currently available on the CDE.

Ms. Ford continued the third Use-of-Force data release is scheduled for July. Included in the data release will be an update or refresh the 2019 data, they will show where the 2020 data is over the 50 percent threshold for all federal, state, local, college/university, and tribal sworn law enforcement officers, and the first quarter of 2021 will be published. The information can be found on the CDE. They are anticipating the overall participation will grow to the mandated 60 percent threshold established by the OMB. Ultimately the goal is to reach the 80 percent threshold as at that point there are no conditions that apply to the information they can share or publish. They will be able to share the types of incidents reported, the number of incidents reported at the national, state, federal, and regional levels, the counts and types of resistance encountered, and the counts and types of force used.

More and more states are participating in the collection; however, the states want to manage the data being submitted to the FBI. States are passing legislation to mandate the data be collected which will help the participation grow. The total percent of sworn law enforcement officers is calculated by all the agencies within a state that submit to the collection thus the push to get the whole country to submit. The FBI continues to liaise with law enforcement officers, agencies, major organizations, legislative bodies, advocacy groups, criminologists, academia, criminal justice students, media outlets and the general public and all of this is being done through publications, conferences, and training to increase participation.

National Use-of-Force angular upgrades have also been implemented. The transition of going to the cloud-based system allowed the opportunity to develop new capabilities, enabled access to external users who can access the system through the LEEP and manage their data via dashboards. External stakeholders that have the administrator role can manage users within their area of responsibility and all users that have access can get tools such as frequently asked questions, tool tips, and the user guide. All dashboards are user role focused therefore you can only see what your user-role or account setting allows you to.

To put the data that is provided to the National Use-of-Force Data Collection into context it is important to see how often there is interaction with the public. The FBI is launching the Law Enforcement Public Contact Collection. This collection will be housed within the FBI UCR

Program. Its primary focus will be on the public contact that citizens have with law enforcement. The volume of the public contact will provide context to not only the National Use-of-Force Collection but also LEOKA. It will focus on three categories of contact: citizen calls for service, unit or officer-initiated contact, and court bailiff activities, as well as a wide range of contacts to include 911 calls as well as officer interventions, traffic stops, and judicial activities. Agencies submitting data will do so through the National Use-of-Force Data Collection portal and on an annual basis by a single transmission by each participating agency per year covering the entire year.

No discussion.

APB Item #5 NIBRS Transition Update

The topic was presented by Ms. Trudy Ford, Chief of the GLESS. *(See Appendix H, PowerPoint.)* Ms. Ford provided an update on the transition of the NIBRS. As of January 1, 2021, the FBI UCR Program transitioned to the NIBRS to provide the overall quality of crime data in an enhanced format as NIBRS captures details on each single crime incident to include information on victims, known offenders, relationships between victims and offenders, and property involving crimes as well as on separate offenses within the same incident. The Summary Reporting System (SRS) previously used a monthly aggregate tally. The NIBRS goes much deeper in providing the circumstances and context for crimes to also include the location, time of day, and whether an incident was cleared.

Ms. Ford continued that over the last six years the FBI UCR Program has been working diligently with law enforcement partners and various stakeholders to increase NIBRS participation. They expect the six non-certified states to become certified by the end of the year. As for federal agencies, currently 38 are reporting NIBRS, two agencies are in testing (Forest Service and Coast Guard), 30 additional agencies are working towards compliance, 20 agencies are in the process of obtaining NCA accounts and 11 agencies have not provided a contact to the FBI. There are 150 tribal agencies submitting via the NIBRS, 120 submitting via the NCA, and 30 via state programs.

Ms. Ford stated the areas of primary focus for the NIBRS continues to be communication, assistance and tracking. Assistance with communicating the transition is being provided in multiple formats by data integration specialist, subject matter experts, and free training.

Ms. Ford provided a breakdown of the current UCR Program certification counts. There are 18 states in full compliance, 26 states are partially participating, and six states and all territories are not NIBRS certified although all of them are working towards certification. Ms. Ford was pleased to announce that as of May 2021 Mississippi attained State UCR Program certification.

Ms. Ford then gave an overview of the NIBRS status map. She noted that California, Illinois, and Maryland are currently in the certification process. Florida has submitted NIBRS test data to initiate the certification process, and Alaska and New Mexico have begun the certification process.

Ms. Ford took a moment to acknowledge several people have shared concerns about the potential increase in crime statistics as a result of the transition to the NIBRS. Ms. Ford told the group when you are talking about the SRS and NIBRS it really is like talking about apples and oranges. The NIBRS captures more accurate information on offenses, the number of offenses per incident, the type of offenses, as well as more detailed information about the crimes. She noted that any increase is going to be the result of counting the crimes that were previously omitted using the hierarchy rule or the SRS. The FBI published a study on the effects of this change, and it found that violent crime reporting did increase three percent or more on average during the initial transition to NIBRS and she noted the study is available on the CDE.

The FBI and CJIS have continued to report the short-term impacts regarding the transition. It has been communicated to the law enforcement community, academia, and the public that all draw upon the information for multiple uses to include grant funding. The messaging has consistently anticipated the rises nationally with the implementation, but it is going to represent the true crime when it's happening as well as a temporary rise in crime because the bar is raising for everyone. Using multiple formats, multiple fronts on a regular and recurring basis since 2016, when the former FBI Director mandated the national conversion. They continue to communicate the benefits of the NIBRS transition and state the benefits far outweigh the temporary rise in violent crime rates.

Ms. Ford continued the FBI will slowly phase in changes to its trend methodology and incorporate NIBRS estimates into its data releases. Users will still be able to find trend information using data converted from the NIBRS to the SRS format to continue to support the availability of 20-year crime trends. In addition, any participating agency can request its data be specifically converted from NIBRS back to SRS to support their own long-term evaluations of crime trends.

The original purpose of the NCA was to provide federal and tribal agencies the ability to comply with the Uniform Federal Crime Reporting Act using a no cost NIBRS submission solution, however the NCA's functionality became more robust and became a viable option for non-transitioned states and local agencies to submit NIBRS. The NCA is an extension of the UCR system and enables users to directly enter and submit NIBRS crime data for processing, retention and publication. Everything is submitted through the internet and the NCA sends submissions directly into the UCR system from machine to machine. The NCA used established business rules to ensure valid submissions. To maximize participation, in December 2020 the CJIS Division AD requested the FBI UCR Program make the NCA available for non-transitioned state and local agencies to submit NIBRS data. Since that request the FBI UCR Program has worked diligently to message the availability, develop training tools, and assist with onboarding states and agencies that are interested in using the NCA.

No discussion.

APB Item #6 Chairman's Report on the NCIC Subcommittee

The topic was presented by Mr. Brian Wallace, Chief Civil Deputy, Operations Division Marion County Sheriff's Office, Salem, Oregon, and Chair of the NCIC Subcommittee. (*See Appendix I, PowerPoint.*)

The NCIC Subcommittee met virtually on April 19, 2021 and welcomed three new members. Mr. Tim Giesecke, FDLE, Ms. Leila McNeill, Idaho State Police, and Ms. Lisa Purinton, Alaska Department of Public Safety. Mr. Jeremy Hansford, Ohio State Highway Patrol is the new vice chair.

The NCIC Subcommittee addressed ten topics with 12 recommendations. Informational topics included updates on the following: NCIC 3rd Generation (N3G) Project, N3G Task Force, NCIC Electronic File Transfer System (EFTS) Migration, National Information Exchange Model (NIEM) Extensible Markup Language (XML) Presentation and Transformation Style Sheet, and the CJIS Division NCIC Status.

Next Mr. Wallace covered the action topics.

NCIC Issue #1 Proposal from the National Insurance Crime Bureau (NICB) to Modify the Memorandum of Understanding (MOU) with the FBI CJIS Division

In 1994, the APB granted access for the NICB to receive the NCIC vehicle file via a mirror image. Use of this information is regulated by an MOU between the FBI and NICB. This topic addressed a request from NICB to expand that authorized use of NCIC data to include self-insured entities that operate and manage a large fleet of vehicles. The NICB believed the proposal would mutually benefit the NICB and the law enforcement community. All five working groups and the NCIC Subcommittee moved to endorse Option 1.

APB RECOMMENDATION: The CJIS APB moved to expand the “Authorized Use” of NCIC data by the NICB to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations.

NCIC Issue #2 Modification of the Protection Person Date of Birth (PPB) Field Edits

The purpose of this topic was to present a proposal to modify the PPB field edits to allow for the current date to be entered. Entering protective person data is not mandatory when entering a protection order file record. However, if an agency elects to provide protected person data, the protected person name must be entered along with either the PPB, date of birth, or Social Security number. Recent analysis revealed the protected person date of birth could not be entered using the current date. The current field edits for PPB state and field must be a valid Gregorian date less than the date of entry. This proposal would make the PBB field consistent with other file records. All five working groups moved to endorse Option 1, as did the NCIC Subcommittee, with a priority of 3H.

APB RECOMMENDATION: The CJIS APB moved to modify the PPB Field edits to allow for the current date. Depending on technical feasibility, this enhancement may be implemented during the development of the N3G or post N3G initial operating capability. The priority should be 3H.

NCIC Issue #3 Creation of an ERPO File in the NCIC System

The purpose of this topic was to present the policy requirements established by the ERPO File Policy Group for records entered in the new NCIC ERPO File and introduce the ERPO file chapter of the *NCIC Operating Manual*. Mr. Wallace mentioned the CJIS APB had already approved the addition of an ERPO file in NCIC and gave it a priority over all NCIC enhancements, including the N3G. Mr. Wallace said as previously mentioned by the CJIS AD,

this file is important for officer and public safety. He encouraged CJIS System Agencies (CSAs) to take advantage of this file when it becomes available, expected delivery is in the fall of 2022.

Since approval of the file, the CJIS Division established an ERPO File Policy Group to develop policy regarding entry criteria and structural data elements. The ERPO Policy Group was comprised of peers with years of NCIC experience and knowledge of ERPO or red flag laws in their own or respective states. The group was led by former NCIC Subcommittee chair, Mr. Walt Neverman, Wisconsin DOJ who is now retired. Membership included APB chair, Sheriff Kathy Witt, APB member, Mr. Jeff Wallin, Vermont Department of Public Safety, Mr. Chuck Murphy, FDLE, and former members, Ms. Dalene Drum, Maryland Department of Public Safety, who was the founder of this topic, and lastly Mr. Ted DeRosa, previous APB member, from the Colorado Bureau of Investigation.

The group met very aggressively ten times in six months from May through October of 2020. Anywhere the group felt it prudent to mimic the policies and existing structure of the Protection Order file they did so to minimize development time and maximize on opportunities to keep the public safe. Mr. Wallace said it was a tremendous undertaking, and he appreciated their time and effort in bringing sound recommendations to the advisory process. Mr. Wallace recognized Mr. Zack Hartzell, FBI CJIS, and thanked him for his work on this issue.

Mr. Wallace also mentioned the upcoming five-year anniversary of the Orlando Pulse Nightclub mass shooting, the second largest mass shooting in U.S. history and then two years after that mass shooting, the Stoneman Douglas High School mass shooting took place in Parkland, Florida. These tragedies were the catalyst for Florida's red flag law which has been used well over 3,500 times since the Parkland incident. Mr. Wallace said he couldn't speculate if an ERPO File or law existed at the time of these shootings would have prevented these tragic events but believed it would have made it more difficult for these heinous acts to be committed.

Mr. Wallace said he would not be going into detail on all nine of the issues since the information was covered in the topic paper provided prior to the APB meeting.

The NCIC Subcommittee slightly modified the original option provided in the topic paper for Issue 3. The subcommittee did not want an automatic caution indicator entered for every ERPO since it is not consistent with other files, not even the violent person file has an automatic caution indicator. The subcommittee requested the indicator be entered manually if there are additional caution indicators that are necessary to alert law enforcement.

The NCIC Subcommittee also slightly modified the caveat provided in the topic paper for Issue 7 to make it more clear for law enforcement officers and dispatchers.

APB RECOMMENDATIONS:

Issue 1: Criteria for Entry

The CJIS APB moved to recommend Option 1: Accept the criteria for entry as recommended by the ERPO File Policy Group. Based on policy group deliberation, the final draft of the criteria for entry is recommended as follows (in *italics*):

1 Background

1.1 The Extreme Risk Protection Order (ERPO) File contains orders issued by a criminal or civil court for temporarily restricting an individual from purchasing or possessing a firearm, ammunition, or other related items, based on a finding that they may pose a significant danger of personal injury to themselves or others. The types of ERPOs and the information contained in them vary from state to state.

1.2 CRITERIA FOR ENTRY

Each record in the ERPO File must be supported by a court order (electronic or hard copy). ERPOs must meet the following criteria before an entry can be made into the file:

1. The ERPO includes a court finding that the named respondent of the order poses a significant danger of causing personal injury to themselves or others by having a firearm, ammunition, or other related items as set forth in state law, in their custody or control.

2. Reasonable notice and opportunity to be heard must be given to the person against whom the order is sought; or, in the case of ex parte orders, notice and opportunity must be provided within the time required by state laws, and in any event within reasonable time after the order is issued, sufficient to protect the respondent's due process rights.

Ex parte - without notice to the respondent or the opportunity of the respondent to be heard.

Please note: Ex Parte orders should be entered as temporary ERPO records.

3. The named petitioner in the ERPO is a criminal justice agency or an employee of a criminal justice agency who is statutorily authorized to serve in such capacity and must be doing so within the scope of his or her official duties (e.g., Law Enforcement Officer, States Attorney).

If the named petitioner is not a criminal justice agency or a statutorily authorized employee of a criminal justice agency (e.g., family member), the order must be issued by a court that is acting pursuant to its lawful authority to adjudicate criminal matters.

An ERPO may be entered based on the type of petitioner and/or the type of court proceeding under which the order is issued. The intention of the inclusion of the second half of the third criterion is to ensure agencies have an understanding that the two are not mutually exclusive. In addition, it is intended to clarify that if the petitioner is a family member, educator, co-worker, or other individual who is authorized under state law, but falls outside of the criminal justice community, the order must have been issued by a court

that judicially resolves criminal cases. Strictly civil orders with a non-criminal justice petitioner will not meet criteria.

Issue 2: Record Retention

The CJIS APB moved to recommend **Option 1: Accept the following recommendations from the ERPO File Policy Group regarding ERPO File record retention:**

1. The ERPO File Policy Group recommends that ERPO File records remain active until the record entering agency takes action to clear or cancel the record, or the expiration date has been reached.
2. The ERPO File Policy Group recommends that once ERPO File records are removed from active status they are no longer available in the on-line environment.
3. The ERPO File Policy Group recommends that policy be created to ensure agencies enter the accurate expiration date, as established by the issuing court, into the Date of Expiration (EXP) Field.

Issue 3: Message Key (MKE) Codes

The CJIS APB moved to accept the **New Option 3: To adopt the Western Working Group’s recommendation: Accept the Message Keys (MKEs) for entry, modification, removal, and inquiry of ERPO File records as recommended by the ERPO File Policy Group with the exception of the addition of the automatic caution indicator. (Updated table is included.) Add the caution indicator to the message key as is consistent with all other NCIC Person Files.**

The following chart provides a representation of the MKEs available in the ERPO File as recommended by the ERPO File Policy Group:

Message	MKE	Translation
Entry	ERO	EXTREME RISK PROTECTION ORDER
	ERO C	EXTREME RISK PROTECTION ORDER - CAUTION
	ETRO	TEMPORARY EXTREME RISK PROTECTION ORDER
	ETRO C	TEMPORARY EXTREME RISK PROTECTION ORDER - CAUTION
Modify	MRO	
	MTRO	
Cancel	XRO	
	XTRO	

Inquiry	QW	
	QWA	
	QWE	
	QWF	
	QWS	
	ZW	
	QWB	
	QWI	
	QV	
	ZV	
Clear	CRO	CLEAR RISK PROTECTION ORDER
	CTRO	CLEAR TEMPORARY RISK PROTECTION ORDER
Entry of Supplemental	ENRO	
Cancel Supplemental	XNRO	

Issue 4: Record Integrity

The CJIS APB moved to recommend **Option 1: Accept the following recommendations from the ERPO File Policy Group regarding the record integrity of ERPO File records:**

1. The ERPO File Policy Group recommends that the validation policy for ERPO File records is 60-90 days from entry and yearly thereafter.
2. The ERPO File Policy Group recommends that record-entering agencies will be responsible for conducting a second party check and all other requirements as outlined in the existing policy for record accuracy for ERPO File records.
3. The ERPO File Policy Group recommends ERPO File records must be entered immediately when the conditions for entry are met, not to exceed 3 days, upon receipt by the entering agency (unless documentation exists to support delayed entry). ERPO File records should be entered as soon as possible once the minimum amount of data required for entry (i.e., mandatory fields) and the appropriate record documentation are available.
4. The ERPO File Policy Group recommends that ERPO File records will be reviewed for record completeness as are all other NCIC records under the existing policy.
5. The ERPO File Policy Group recommends that the ERPO File be audited by the CJIS Audit Unit.
6. The ERPO File Policy Group recommends the following fields be critical for audit purposes: Name (NAM), EXP, Sex (SEX), Race (RAC), Date of Birth (DOB), Social

Security Number (SOC), FBI Number (FBI), Alias (AKA), Scars, Marks, Tattoos, and Other Characteristics (SMT), Miscellaneous (MIS), Caution and Medical Indicator (CMC), Miscellaneous Number (MNU), Operator's License Number (OLN) (data set), and License Plate Number (LIC) (data set).

7. The ERPO File Policy Group recommends that hit confirmation be required for ERPO File records.

Issue 5: ERPO File Fields

The CJIS APB moved to recommend Option 1: Accept the following recommendations from the ERPO File Policy Group regarding ERPO File fields:

1. The ERPO File Policy Group recommends the following fields be available at the time of record entry: Header (HDR), MKE, Originating Agency Identifier (ORI), NAM, SEX, RAC, Place of Birth (POB), DOB, (EXP), Height (HGT), Weight (WGT), Eye Color (EYE), Hair Color (HAI), FBI, Skin Tone (SKN), SMT, Fingerprint Classification (FPC), MNU, SOC, OLN, Operator's License State (OLS), Operator's License Year of Expiration (OLY), Date of Issue (ISD), Originating Agency Case Number (OCA) or Order Number (ORN), MIS, Notify Originating Agency (NOA), (LIC), License Plate State (LIS), License Plate Year of Expiration (LIY), License Plate Type (LIT), Vehicle Identification Number (VIN), Vehicle Year (VYR), Vehicle Make (VMA), Vehicle Model (VMO), Vehicle Style (VST), Vehicle Color (VCO), Court Identifier (CTI), Petitioner (PET), CMC, DNA Profile Indicator (DNA), DNA Location (DLO), Citizenship (CTZ), Ethnicity (ETN), Service Information (SVC), Service Date (SVD), Linking Agency Identifier (LKI), Linking Case Number (LKA), and State Identification Number (SID).
2. The ERPO File Policy Group recommends the following supplemental data fields be available in the ERPO File: AKA, DOB, SMT, MNU, SOC, OLN, OLS, OLY, LIC, LIS, LIY, LIT, VIN, VYR, VMA, VMO, VST, VCO, IMN, IMT, CMC, CTZ, and SID.
3. The ERPO File Policy Group recommends that the N3G Task Force consider the inclusion of address data in the NCIC ERPO File. Further, the fields, field character limitations, and conditions for the address data set available in the Wanted Person File should be mirrored in the new File. This would include the following fields: Street Number (SNU), Street Name (SNA), City Name (CTY), County (COU), State (STA), Zip Code (ZIP), Address Type (ADD), and Date of Documented Address (DDA).
4. The ERPO File Policy Group recommends that the following combination of fields be used to initiate transactions in the ERPO File: NAM and NIC, NIC and OCA, NAM and OCA, and NAM and ORN.
5. The ERPO File Policy Group recommends the following number of additional identifiers for supplemental entries in the ERPO File in the current and future (as recommended by the N3G Task Force and approved by the APB NCIC environments:

Field	Current	Future (N3G)
AKA	99	99
DOB	9	25
SMT	9	99
MNU	9	25
SOC	9	25
OLN (data set)	9	25
LIC (data set)	9	25
VIN (data set)	9	25
IMN (data set)	12	25
CMC	10	25
CTZ	9	25
SID	9	25

6. The ERPO File Policy Group recommends all current field lengths be consistent with other person files when the ERPO File is made available in the current NCIC environment.
7. The ERPO File Policy Group recommends the acceptance of increased field lengths (as recommended by the N3G Task Force and approved by the APB) for applicable fields in the ERPO File when N3G functionality is made available. The current and future field lengths are provided below:

Field	Current	Future (N3G)
NAM	30	50
MIS	500	1000
MNU	15	30
OCA	20	30
ORN (equivalent to PNO)	15	30

Issue 6: Codes

The CJIS APB moved to recommend Option 1: Accept the following recommendations from the ERPO File Policy Group pertaining to ERPO File MFCs:

1. The ERPO File Policy Group recommends all codes for fields being implemented in the ERPO File remain consistent with other NCIC person files when applicable.
2. The ERPO File Policy Group recommends that the PET and ORN Fields allow for a range of free-text data.
3. The ERPO File Policy Group recommends the addition of the following CMC codes in the ERPO File when N3G functionality is made available (as previously approved by the N3G Task Force and the APB): Blind, Deaf, Prior Law Enforcement Experience, Special Military Training, Behavioral Issues, Speech Impediment, and Universal Medical.
4. The ERPO File Policy Group recommends to adopt the recommendations of the N3G Task Force and create two separate fields for “cautions” and “medical conditions” in the ERPO File when N3G functionality is made available.

Issue 7: Indication of Firearm Prohibition

The CJIS APB moved to accept Option 1 as modified: Accept the ERPO File Policy Group’s recommendation to create a caveat to precede all ERPO File records responses in order to alert those reviewing record responses that the subject of record is prohibited from possessing a firearm; however, modify the caveat to the following:

******THE SUBJECT OF THIS RECORD IS PROHIBITED FROM RECEIVING OR POSSESSING A FIREARM. REFER TO THE MIS FIELD FOR ANY OTHER ADDITIONAL COURT ORDERED PROHIBITIONS******

Issue 8: MIS Field Requirements

The CJIS APB moved to accept the following:

Option 1: Accept the following recommendations from the ERPO File Policy Group pertaining to policy requirements for data to be entered into the MIS Field:

1. The ERPO File Policy Group recommends the following guidance be included in the appropriate location within the ERPO File section of the *NCIC Operating Manual* concerning the MIS Field:
 - Any data exceeding character limitations in NCIC fields should be entered into the MIS Field.
 - Specific details regarding cautions and medical conditions when CMC/Other is used should be entered into the MIS Field.
 - The edit table in the ERPO File section of the NCIC Operating Manual will indicate that if a non-conforming VIN is present, “SVIN” should be entered as the first four characters in the MIS Field.
2. The ERPO File Policy Group recommends policy be created to advise agencies to enter court information in the MIS Field if the CTI Field cannot be populated.
3. The ERPO File Policy Group recommends policy be created to advise agencies to enter conditions of which the subject of the ERPO File record must adhere (other than firearm restrictions) in the MIS Field.

Issue 9: ERPO File Placement in NCIC Hit Responses

CJIS APB moved to recommend Option 1: Accept the ERPO File Policy Group recommendation to modify the NCIC hit response hierarchy to the following:

- 1. Wanted Person**
- 2. Extreme Risk Protection Order**
- 3. Missing Person**
- 4. KST**
- 5. Gang**
- 6. Violent Person**
- 7. Sex Offender**
- 8. Supervised Release**
- 9. Immigration Violator**
- 10. Protection Order**
- 11. Identity Theft**
- 12. Protective Interest**
- 13. NICS Denied Transaction**

Sheriff Witt thanked Mr. Hartzell for his hard work and dedication on the ERPO File initiative. She said he showed tremendous leadership in leading the group through the mounds of data.

NCIC Issue #4 Sunset Date for File Transfer Protocol (FTP)

The purpose of this topic was to establish a community sunset date for the FTP to transfer large data files from NCIC. This is a transition from an older, less secure method to a newer, modern, secure method of transferring files. During the N3G user canvass, users requested a method for exchanging larger files within the CJIS Division. Transitioning to the EFTS, satisfies the ability to automate file retrieval.

The N3G Task Force set a notional date of September 30, 2022 as the sunset date for FTP. There are a significant number of users using EFTS today, and it is suggested the establishment of that firm sunset date for FTP be set for December 31, 2021. This would meet the needs of the users and improve the CJIS Division's security posture. The CJIS Information Security Officer (ISO) has made several notifications to states already. EFTS is applicable to NCIC only. The NCIC Subcommittee discussed the time frame for notification, and whether it would be too late for users to meet the newly proposed sunset date of December 2021 since the APB and the FBI Director approvals may not come until August or September of 2021. Many states have already made the change, and others are coming on board soon. The CJIS ISO will continue their efforts and help states quickly transition. Four working groups moved to endorse Option 1, along with the SA and NCIC Subcommittees.

APB RECOMMENDATION: The CJIS APB moved to accept Option 1: Recommend an FTP sunset date of December 31, 2021.

NCIC Issue #10 COVID-19 Guidance

The purpose of this topic was to obtain feedback on the NCIC guidance provided at the beginning of the pandemic and determine a path moving forward. The following

recommendations were provided to the NCIC user community at the beginning of the COVID-19 pandemic.

1. Terminal Operator and User Training, Testing, and Recertification

Guidance was to adhere to the NCIC training policies if capable. If unable to adhere, NCIC training policies were temporarily suspended.

2. Wanted Person Entries

Guidance was to enter the correct Extradition (EXL) code; however, if the entering agency had potential concerns on complying with the EXL code listed, it was recommended to add the standard language NATIONAL EMERGENCY/COVID-19 in the MIS Field.

3. Hit Confirmation and Locate Procedures

Guidance was to continue confirming hits on all NCIC records. For warrants, if extradition was not going to occur, it was recommended to not place a locate with No Extradition (NOEX) so the second locate of NOEX did not cause the record to be removed from NCIC.

4. Validation Procedures

Guidance was to continue validating records to the full extent possible and ensure all available database checks take place so the NCIC records are accurate and up to date. Additionally, automatic purging of NCIC records was suspended for online validations.

The NCIC Subcommittee recommended discontinuing terminal operator and user training, testing, and recertification COVID-19 guidance limitations. The remaining guidance will continue.

This topic was accepted as information only.

A member asked about the information only topic regarding the NIEM XML Presentation and Transformation Style Sheet Update as to whether any funding would be available to transition from the socket to the style sheet. Mr. Todd Commodore, FBI CJIS, NCIC Policy and Operations Unit (NOPU), responded that funding hasn't been identified to help the states transition but some other things have been done. The transformation style sheet will help CSAs support their legacy users who are not ready to go to NIEM. Mr. Commodore said the NOPU as well as CJIS IT staff are available to assist states with the transition.

APB Item #7 N3G Task Force Update

This topic was presented by Mr. Jeffrey Wallin, Director of the Vermont Crime Information Center, Vermont Department of Public Safety, and chair of the N3G Task Force. *(See Appendix J, PowerPoint.)*

Mr. Wallin provided a brief update on the work of the task force made up of a group of federal, state, and local members working together on the N3G project. Mr. Wallin thanked both previous and current members for the time put in on this critical project. The N3G Task Force effectively met virtually over the last 14 to 15 months. They extensively reviewed white papers to provide effective recommendations. The task force continues to review and discuss policy

group recommendations. They have dispositioned 63 percent of the nearly 50 recommendations and requirements that were approved by the APB for further exploration. A total of 188 items have been approved by the task force and forwarded to CJIS technical staff for exploration and development. Active policy groups include the Warrant, Response/Notification, and Record Integrity. The Blue Alert, MKE, Supplemental, Offline Search, Gang and Missing/Unidentified Policy Groups have concluded. Future policy groups include Training, and Advanced Search and Codes. They will be meeting soon. Mr. Wallin said he sincerely appreciated those willing to help with the policy groups. Sheriff Witt thanked Mr. Wallin for his leadership on the N3G Task Force.

This topic was accepted as information only.

APB Item #8 Chairman's Report on the N-DEx Subcommittee

The topic was presented by Ms. Carol Gibbs, Chief of the Program Administration Bureau, Illinois State Police, and Chair of the N-DEX Subcommittee. *(See Appendix K, PowerPoint.)* The N-DEX Subcommittee met virtually on April 23, 2021. The agenda included four issues and one ad hoc topic items.

N-DEx Issue #1 N-DEx Program Office Update

The Data Sharing Services Unit (DSSU) presented an update on program activities. The subcommittee was briefed on N-DEX System participation, N-DEX System technical updates and enhancements, distance learning opportunities, and the N-DEX Success Story Program.

With regard to system participation, there are 7,687 states participating, 30 states participating at the state level, 555 million records stored in the N-DEX, 343 million records available via federation, and 1.5 million monthly searches.

Ms. Gibbs then briefed on regional participation. All Law Enforcement Information Exchange (LInX) regions except fed LInX are connected. Also connected are all Regional Information Sharing System (RISS), centers and 29 High Intensity Drug Trafficking Areas.

Ms. Gibbs advised the primary technical update and enhancement was the completion of Information Exchange Package Documentation 4.0, including functionality for search and retrieve, subscribe and notify, and batch search counts. She noted the UCR Program is in the process of developing a cadence for implementing NIBRS changes that considers time for vetting through the process and technical changes that would be valuable to both UCR and the N-DEX. The UCR Program Office plans to deliver an information paper through the fall 2021 working group process. Some upcoming completed technical completions with regard to N-DEX are completion of cloud migration, search engine update, and an automated test case for the nonoperational environment.

Next, she briefed on distance learning opportunities. From the beginning of 2021 through the end of March, there were 47 outreach sessions with approximately 1,400 attendees.

Lastly, she briefed on the N-DEx Success Story of the Year and the Excellence and Information Sharing award winners.

This topic was accepted as information only.

N-DEx Issue #2 The N-DEx System to Obtain More Images from the NGI System

This topic was addressed in APB Item #6, IS Issue #9.

N-DEx Issue #3 Explore the Ability to Query the Search History of the N-DEx System

The purpose of this issue was to explore a query of the search history in the N-DEx System. Ms. Gibbs noted there are already some features within the current functionality of N-DEx where an individual could subscribe to a notification of future searches if a search involved person or property of interest to the authorized user. This proposal involves the Program Office exploring the ability to query what has already occurred, the transaction query logs. The Program Office indicated their work would not be just a technical assessment. They felt it also needed to have some policy consideration for things such as acceptable use, limits on the query, how the request would come in, either directly to the Program Office or through the CJIS Systems Officer (CSO); other limitations or concerns about dissemination and whether certain data elements should be suppressed.

Two options were provided for consideration. Option 1: Explore the implementation of a query of the search history by DSSU staff of the N-DEx System and report the results to the working groups and Option 2: No change. All five working groups and the N-DEx Subcommittee accepted Option 1 as written.

No discussion.

APB RECOMMENDATION: The CJIS APB moved to recommend Option 1: Explore the implementation of a query of the search history by DSSU staff of the N-DEx System and report the results to the working groups.

N-DEx Issue #4 Fiscal Year 2020 Audit Results Summary

Ms. Gibbs advised the FY 2019 and 2020 audit results were presented by the audit unit. She noted the two highest findings were acceptable use and incorrect use code, often stemming from self-queries, and some of the incorrect use codes were the result of a firearms code prior to the rollout of use code F for the states. She advised the group to refer to Informational Topic K for more details regarding the N-DEx audits.

No discussion. This topic was accepted as information only.

Ad-Hoc Topic Using Derived ORIs to Address Law Enforcement Information Sharing Gaps Within the N-DEx System

Ms. Gibbs stated the N-DEx Subcommittee looked at the evolution of the N-DEx Program and its data sharing rules. During the last full round of Advisory Process meetings, the Program Office, the N-DEx Subcommittee, and the working groups considered the various categories of data within the N-DEx System and the information sharing rules set by the data contributor for sharing and dissemination. At the onset of the N-DEx Program, the data sharing rules were determined by the construct of the authorized agency's ORI. Through the evolution of the N-DEx, originally Law Enforcement National Data Exchange, it became open to criminal justice. Recently, it has been identified that agencies that fit within the definition of criminal justice but have subunits with law enforcement authority may have an ORI designation that impacts what data is disseminated to them. The subcommittee created an action item for the PROGRAM OFFICE to initiate a task force to address this topic and report the recommendation back to the subcommittee.

No discussion. This topic was accepted as information only.

APB Item #9 Chairman's Report on the IS Subcommittee

The report was presented by Mr. Charles Schaeffer, Director, FDLE, Tallahassee, Florida, and Chair of the IS Subcommittee. **(See Appendix L, PowerPoint.)** The IS Subcommittee is responsible for biometrics, criminal histories, and how they are created with the various modalities of identification.

IS Issue #1 Miscellaneous Action Items Update

Mr. Schaeffer stated the subcommittee along with FBI IS DFO Mr. Gary Stroupe and FBI IS scribe Ms. Brandi Meighan keep track of items discussed within the meetings and there are usually numerous action items. The IS Subcommittee reviews those action items every time they meet to determine if they have been completed or what the next steps are.

No discussion. This topic was accepted as information only.

IS Issue #2 Identification Services Coordination Group (ISCG) Update

The ISCG Task Force is a unique task force that falls under the IS Subcommittee. The ISCG is led by Ms. Beth Owens, Ohio Bureau of Criminal Investigation and Identification. The ISCG focuses on the different modalities of identification. Mr. Schaeffer then gave an update on the Facial Analysis, Comparison, and Evaluation (FACE) System. FACE technology has been a great success in helping officers on the street. FBI CJIS DAD Kimberly Del Greco has testified in front of Congress regarding the privacy concerns surrounding facial recognition. Mr. Schaeffer explained while many know this is a useful technology, we need to find the place where law enforcement is comfortable using it.

Mr. Schaeffer then briefed on the work being done on iris services. The Iris Service has come a long way. He noted there would be topics later in the subcommittee where members would discuss further use cases. Mr. Schaeffer stated he believes iris has a place in our society for investigative and identification purposes.

No discussion. This topic was accepted as information only.

IS Issue #3 Consideration of Additional Use Cases for the NGI Iris Services

The topic provided background information on the current and future intended uses of the NGI Iris Service and a request by the CJIS Division for feedback/recommendations regarding how it could expand the scope of the NGI Iris Service to better serve the needs of the criminal justice community. There have been many successes with the use of the Iris Service and the accuracy behind it. Technology and the ability to capture an iris has evolved. This can be done at a distance and the quality of the image has significantly improved. This has helped with movement in correctional facilities and proven to be more efficient than using fingerprints. This process is also contactless. The Iris Program looked to the APB for endorsement to expand the NGI Iris Service for identification validation and identification purposes.

Two options were presented for consideration.

Option 1:

Endorse the expansion of the NGI Iris Service for the following use cases:

1. Identification Validation
 - a. Incarceration - to enhance the security and accuracy of other prison processes such as prisoner ingress and egress procedures and movement within the facility
 - b. Supervised Release – to aid in the management and verification of identities in the Probation and Parole Systems.
 - c. Court System - to validate the identity of individuals as they traverse the courts' processes.
2. Identification
 - a. Law Enforcement - to work with all CSOs and state agencies to navigate the programming requirements necessary to participate in the NGI Iris Service for enrollments to grow the iris repository, for searches to capitalize on the service, and to develop mobile iris capabilities for the law enforcement community.
 - b. Homeland Security - to pursue the integration of Department of Homeland Security (DHS) agencies for authorized IIDS uses of the NGI Iris Service.

Option 2:

Make no change at this time to the current NGI Iris System use cases.

All five working groups and the IS Subcommittee accepted Option 1 as presented in the topic paper. The working groups recommended a priority of 3M. The IS Subcommittee recommended a priority of 3H.

APB RECOMMENDATION #36: The CJIS APB moved to endorse the expansion of the NGI Iris Service for the following use cases:

1. Identification Validation

- a. Incarceration—to enhance the security and accuracy of other prison processes such as prisoner ingress and egress procedures and movement within the facility.**
- b. Supervised Release—to aid in the management and verification of identities in the Probation and Parole Systems.**
- c. Court System—to validate the identity of individuals as they traverse the courts' processes.**

2. Identification

- a. Law Enforcement—to work with all CSOs and state agencies to navigate the programming requirements necessary to participate in the NGI Iris Service for enrollments to grow the iris repository, for searches to capitalize on the service, and to develop mobile iris capabilities for the law enforcement community.**
- b. Homeland Security—to pursue the integration of DHS agencies for authorized Iris Image Identification Search uses of the NGI Iris Service.**

The priority should be 3H.

IS Issue #4 NGI Iris Service Search upon Enrollment Enhancement

The purpose of the topic was to obtain CJIS APB endorsement for searching iris images during the iris image enrollment process. Cite and release and a notice to appear have become a problem. More often, a person who commits a crime is not booked and due to that, they are cited and fingerprinted. The fingerprint is sent to the court and when a person fails to appear, law enforcement then does not know who they are because the fingerprint did not go anywhere. The idea of a mobile fingerprint then became a topic of discussion but did not gain traction for many years due to the cost of the device. An idea was then brought forth to capture mobile iris's and attach those images to the notice to appear. This would cut down on the time it takes for the officer on the street to fingerprint the subject as well as creating a contactless option that would also capture the person's face. If the subject fails to appear, then iris images would be on file as well as a picture of the subject. Due to the accuracy the Iris Service has proven to have, Mr. Schaeffer urged the CJIS APB to consider allowing this modality to add to the criminal master file.

With the accuracy of iris, we can establish a record with their iris images and fingerprint them at the court. If the subject is convicted of the crime, the fingerprints can then be captured. This method of capturing a mugshot and iris images will be much easier and more efficient for the officers on the street. There is also less chance of damage caused to the iris unlike the common occurrence of people altering their fingerprints by damaging them to prevent law enforcement from identifying them. Mr. Schaeffer stressed the value of considering using the iris modality in a mobile setting to establish a record and conclude with fingerprints at the court level if convicted.

No discussion.

Two options were provided for consideration.

Option 1

Endorse the enrollment validation process, as proposed. Iris images submitted for enrollment will be searched against iris images already enrolled in the repository. If the iris images do not pass validation, return the new Status/Error Field notification message of:

Manual Review - Enrollment

A search of the submitted iris enrollment requires CJIS to adjudicate the results. The iris images were not enrolled.

This validation process will have an analysis component if an anomaly is discovered through the NGI search. In this instance, collaboration with the submitting agency of the iris and the current tenprint record (or records) hit upon will be necessary.

Option 2

Make no change.

All five working groups and the IS Subcommittee accepted Option 1 as presented in the topic paper with a priority of 3M.

APB RECOMMENDATION #37: The CJIS APB moved to endorse the enrollment validation process as proposed. Iris images submitted for enrollment will be searched against iris images already enrolled in the repository. If the iris images do not pass validation, return the new Status/Error Field notification message of:

Manual Review - Enrollment

A search of the submitted iris enrollment requires CJIS to adjudicate the results. The iris images were not enrolled.

This validation process will have an analysis component if an anomaly is discovered through the NGI search. In this instance, collaboration with the submitting agency of the iris and the current tenprint record (or records) hit upon will be necessary.

The priority should be 3M.

IS Issue #5 Update to 2019 Topic “Driver’s License Numbers (DLN) in the NGI System

The purpose of this topic was to discuss methods for capturing DLNs in the NGI System. The information should also be available on the criminal history record shared via the Interstate Identification Index (III). This request would allow the DLN to be recorded in the repository. Mr. Schaeffer stated they could either create a new field to capture the DLN, create two new fields to capture the state and DLN, or utilize the Miscellaneous Number field. The IS Subcommittee, after reviewing the working group and Compact Council recommendations,

endorsed Option 3, as the field already existed. This option did not require reprogramming fingerprinting systems to accept a new data element. Mr. Schaeffer stated there could be some value in the future for splitting them out from a data perspective and suggested this be done in XML when/if that time comes as it is more cost effective. Mr. Schaeffer explained Option 3 would allow for the entry of the DLN to be an optional field.

Discussion: A member asked if they could leave the option on the table to reconsider this when states are fully transferred to XML. Mr. Schaeffer stated that would be the most logical thing to do because you can change an XML scheme easily as opposed to electronic biometric transmission specification (EBTS). If we were to move to XML for fingerprint transactions and other modalities such as iris or FACE, XML can be easily incorporated. A member asked if the format included in Option 3 would easily be converted if the transition to XML would take place. Mr. Schaeffer explained it would be the job of the Joint Task Force on Rap Sheet Standardization (JTF) to take that data and convert it to XML, however, it can be parsed. A member asked if Option 3 is passed, would the format include the dash, i.e. DL-state then the license number. Mr. Schaeffer confirmed the format would be exactly as is written in Option 3. A member stated the Compact Council also ended with Option 3 after much discussion.

The following options were provided for consideration.

Option One: Create a new DLN field in the NGI System to submit the DLN. An additional EBTS field must be created to capture the DLN for EBTS types of transactions (TOTs).

Option Two: Create an OLN, OLS, and OLY field in the NGI System to collect DLN in a manner consistent with the NCIC. Additional EBTS fields must be created to capture the DLN in the OLN, OLS, and OLY fields for EBTS TOTs.

Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-.

Option Four: Make no change.

The Federal, North Central and Northeastern Working Groups accepted Option Two, Priority 3M. The Southern and Western Working Groups accepted Option Three with the Southern Working Group recommending a priority of 4H, and the Western Working Group recommending a priority of 3M.

APB RECOMMENDATION #38: The CJIS APB moved to recommend Option 3: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-.

The priority should be 3M.

IS Issue #6 Posting Federal Dispositions to Multiple Dates of Arrest

In December 2013, the FBI's APB recommended a procedure to cross-reference federal disposition data to multiple related dates of arrest in the NGI System. An update was provided as well as a request for guidance to determine if this procedure should be continued. For many years, the states reported dispositions differently than the federal agencies. The purpose of this topic was to ask the federal agencies to report dispositions the way the state agencies report currently. Mr. Schaeffer stated the reality is the accuracy that we thought we would get with the federal agencies way of reporting was not successful. The main issue was with having numerous arresting agencies reporting the crime, however, only one agency who was in charge of the prosecution posting the disposition. This has caused a major problem with disposition rates at the federal level.

Discussion: A member stated this topic went through the Compact process as non-criminal agencies receive these rap sheets and struggle to piece the dispositions together. The Compact also discussed when a record is expunged, agencies with the disposition are expunging the records. However, the other agencies are not submitting expungements. Therefore, you have an arrest that tells you to refer to another arrest that has already been expunged. The Compact decided not to make a recommendation to the APB as it was more of an APB issue than a Compact issue. A member asked if this would fix historical data in III or would this change only take affect after it is approved. Ms. Paula Zirkle, FBI CJIS Division, explained this change would be day one and forward. Ms. Zirkle did state there is a way to manually go back and correct the records, but it will not be automated.

Two options were provided for consideration. Option 1: Continue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest and Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

The Federal, Northeastern and Southern Working Groups recommended Option 2. The North Central and Western Working Groups recommended Option 1. The IS Subcommittee recommended Option 2 with one-member abstaining. The NICS Subcommittee accepted the topic as information only.

APB RECOMMENDATION #39: The CJIS APB moved to recommend Option 2: Discontinue the current procedures of cross-referencing federal disposition data to multiple related dates of arrest.

IS Issue #7 Update on the Interstate Identification Index (III) Delete Record Cycle (DRC) and Modify Record Cycle (MRC) MKE Development

The purpose of this topic was to provide an update on the development of the III DRC and MRC MKE as it enhances the CJIS APB recommendation from 2006. Mr. Schaeffer explained the MKEs, simply put, are used if you want to modify or delete a record. The MKEs are in various stages of being developed and they are currently working on the tool for removing an arrest cycle from a criminal history. A work group has been formed at the FBI CJIS Division to look at the requirements for modifying an arrest cycle through a MKE. Mr. Schaeffer

expressed it is important for states that are not a part of the Compact as those states still must modify and maintain records to include dispositions, etc. Mr. Schaeffer encouraged non-Compact states to consider making the transition and expressed hopes that the DRC and MRC will be available within an 18-months to two-year timeframe.

No discussion. This topic was accepted as information only.

IS Issue #8 Unknown and Known Deceased Searches of the DHS's Automated Biometric Identification System (IDENT) and the DOD's Automated Biometric Identification System (ABIS)

The purpose of this topic was to provide the fingerprint images from Unknown Deceased and Known Deceased (deceased) tenprint transactions to the DHS's IDENT and the DOD's ABIS to discover identity information for this important population. Mr. Schaeffer explained this would be helpful to states when trying to identify a deceased person who could have been prior military or an immigrant that came through a border crossing on a work visa. There are currently 16 states that receive this information. The other 34 states will be required to program their systems to receive this data.

Considering the advantages and disadvantages discussed for providing deceased transactions to the DHS IDENT and the DOD ABIS, the following three options were provided for consideration:

- Option 1: No change. Deceased tenprint transactions will not be provided to the DHS IDENT or the DOD ABIS unless an agency makes a specific request of the Special Processing Center.
- Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.
- Option 3: Utilize the Name of Designated Repository field to allow contributors to choose when to search the DHS IDENT and/or the DOD ABIS with deceased tenprint transactions. The requesting agency will need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DOD ABIS response.

All five working groups accepted Option 2 with the Federal, Northeastern, Southern and Western Working Groups recommending a priority of 3M. The IS Subcommittee recommended Option 2, with a priority of 3H.

APB RECOMMENDATION #40: The CJIS APB moved to recommend Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DOD's ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS's IDENT and/or DOD's ABIS response.

The priority should be 3H.

IS Issue #9 The N-DEx System to obtain more images from the NGI System

The purpose of this topic was to present a proposal to enable criminal justice and law enforcement users to obtain additional NGI images via the N-DEx System. All five working groups did approve to expand the sharing of images with N-DEx as well as the IS Subcommittee.

Two options were provided for consideration. Option 1: Expand sharing from NGI to provide access for the N-DEx System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number and Option 2: No change.

All five working groups accepted Option 1. The Federal, North Central, and Western Working Groups recommended a priority of 3M. The IS Subcommittee recommended Option 1, with a priority of 3M.

No discussion.

APB RECOMMENDATION #41: The CJIS APB moved to recommend Option 1: Expand sharing from NGI to provide access for the N-DEx System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number. The priority should be 3M.

IS Issue #10 JTF on Rap Sheet Standardization Update

The JTF on Rap Sheet Standardization is led by Ms. Leila McNeill, Idaho State Police. Ms. McNeill noted there are 13 states not using the standardized rap sheet, JTF 4.0. The JTF 4.0 is being upgraded and modified in hopes the 13 states can migrate towards utilizing it. Mr. Schaeffer stated the key is to get away from teletype and use XML as well as applying style sheets. Mr. Schaeffer explained rap sheets that are more readable will be more useful to the law enforcement community.

No discussion. This topic was accepted as information only.

IS Issue #11 R-DNA Update

The purpose of this topic was to provide an update on the FBI Booking Station R-DNA Initiative. Mr. Schaeffer explained the driving motivation by the FBI to use R-DNA was to assist in cold cases. The law enforcement community then expressed interest in using it at crime scenes. The next step is to determine the use cases to know how we make R-DNA work at a crime scene. The R-DNA Task Force was reconstituted and currently looking at the use of R-DNA at crime scenes. This task is being led by Mr. Thomas Callaghan, FBI STB. Mr. Schaeffer stated there will be many customers, i.e. police departments and detectives, who will want this device. The task force will continue to provide updates on how to move forward with R-DNA at crime scenes.

No discussion. This topic was accepted as information only.

IS Issue #12 NGI System Purpose Code F Responses vs Purpose Code C Responses

The purpose of this topic was to provide an explanation of Purpose Codes F and C and how responses could differ with the use of each. Purpose Code F is used for the NICS Section and POC states for firearm check purposes. When running a Purpose Code F, states respond to the transaction with a rap sheet. Mr. Schaeffer explained there is a disconnect as some states respond differently with Purpose Code F versus Purpose Code C. Purpose Code C is for criminal justice purposes. Some states do not currently share sealed information for Purpose Code F. Mr. Schaeffer asked the states who currently do this to reconsider why they do this. Mr. Schaeffer noted in the world we live in; we have people who are buying guns. There is a high increase in gun sales and if we are not getting the information to determine whether an individual should have a gun or not, it is a problem. As a law enforcement agency, you can run a Purpose Code C, however, many agencies do not run it when doing a firearm's check. When states do not send sealed information on a rap sheets results in bad decisions when it comes to firearm check determinations.

No discussion. This topic was accepted as information only.

IS Issue #13 Update on the FBI's Manual Fingerprint and Name Check Services

The purpose of this topic was to provide an update on the FBI's manual fingerprint and name check services. Ninety-three percent of the time fingerprints go through the NGI System without issue and seven percent of the time they need manual intervention due to fingers being out of sequence or there are palms and fingers that do not match. The FBI asked to do the sequencing check ahead of time, it will reduce the amount of work needed to push the prints into the NGI. Mr. Schaeffer explained it boils down to training and getting the law enforcement officers that are doing the prints to check at the beginning of the process. This would save the state and the FBI seven percent of the work that goes into managing those prints.

There was also discussion during the IS Subcommittee regarding unknown deceased prints. The FBI is still processing fingerprint requests for unknown deceased people. The IS Subcommittee discussed ways to improve this process. Mr. Schaeffer recommended using two fingers instead of rolling tenprints on a deceased person. Using rapid identification works well however you cannot do this nationally. There has been conversation regarding searching the entire criminal master file with the Repository for Individuals of Special Concern as it is the only repository of individuals with special concern we are not currently searching the entire repository. The capability of doing this is currently being looked at.

No discussion. This topic was accepted as information only.

IS Issue #14 Criminal History Update

The purpose of this topic was to provide an update on criminal history record information initiatives, including dispositions, missing arrests, pseudo-pointer records, and functional record support. There is a major issue with disposing arrests as only 67 percent of cases in the repository have dispositions and only 50 percent of the state repository has dispositions. Mr. Schaeffer explained not having dispositions on records affects a variety of things:

employment, firearm checks, etc. A Disposition Task Force has been created to look at these issues and hopefully leverage technology as a solution.

Purpose Code I is used for employment purposes, and there are currently numerous states who do not respond. Mr. Schaeffer expressed the importance of responding to Purpose Code I and provided an example of a sexual offender moving states and applying for a job within a school. It is imperative that states respond to the Purpose Code I when running a background check for employment as there could become instances where a registered sexual offender is receiving employment in a school, etc. While this is a Compact Council issue, Mr. Schaeffer stated it should also be an APB issue as the CJIS APB is made up of CSO's responsible for maintaining the repositories. The Compact Council are consumers and cannot force states to change anything. Mr. Schaeffer expressed the importance for CSO's to know whether they are responding and if they aren't, to figure out why. States need to be responding to Purpose Code I, so we can continue to keep the children and the elderly safe.

Purpose Code S is used to provide security clearances. States who are not responding to Purpose Code S are allowing people from their states to receive security clearances when they shouldn't.

Purpose Code X is used in exigent circumstances such as national disasters and/or global pandemics. Mr. Schaeffer urged states to respond not responding could result in similar situations discussed with Purpose Code I. Mr. Schaeffer explained this is the reality of not doing the right thing and for states to think about why they are not responding.

No discussion. This topic was accepted as information only.

IS Issue #15 Identification for Firearm Sales (IFFS)

The purpose of this topic was to provide an overview and update of the IFFS program. The IFFS program allows federal partners to make the correct decision when determining if an individual can possess and/or buy a firearm. When an IFFS flag occurs, the examiner working the background check does not have to review the record. If the IFFS response is a valid match, it is an automatic deny and no research needs to be conducted. With high volumes of gun sales, this is very beneficial to the NICS Section as they only have three days to make a final determination before the firearms dealer can legally transfer the firearm. Mr. Schaeffer encouraged states to make sure they are doing this to the best of their ability to prevent further gun violence.

No discussion. This topic was accepted as information only.

IS Issue #16 The NGI System Interstate Photo System (IPS) Update and IPS Policy and Implementation Guide Revisions

The purpose of this topic was to provide information regarding the importance of enrolling type 10 (photos and scars, marks, and tattoos) records into the NGI IPS; the impact of face coverings on face recognition searches and the guidelines for conducting face recognition searches of the NGI IPS. In addition, the topic provided a status on the progress of updating the *NGI IPS Policy and Implementation Guide*. The IPS has been a major success. IPS currently

has 103 million mugshots at the national level and 50 million of those are searchable. Mr. Schaeffer explained you can search IPS without state level assistance. There are caveats to this and encouraged states to work with their CSOs. Mr. Schaeffer also encouraged CSOs to take this to the local level and show agencies how NGI is maturing and the success of IPS.

No discussion. This topic was accepted as information only.

IS Issue #17 Biometric Interoperability Update

The purpose of this topic was to provide the NGI System users with information regarding the expanded implementation of interoperability between the DOJ, FBI's CJIS Division, the DHS's IDENT, and the DOD's ABIS. With this interoperability, states are able to search the IDENT system. Mr. Schaeffer explained this has been a successful tool, especially during an immigration debate. This system allows for agencies to make a better decision.

No discussion. This topic was accepted as information only.

IS Issue #18 Programs Research and Standards Unit Update on Contactless Fingerprint Collection Studies

The purpose of this topic was to summarize the recent activities related to the study of contactless fingerprint matching capability with legacy contact prints and status on certification of contactless collection devices. Research is ongoing in regard to contactless fingerprinting. The FBI is currently in the process of collecting and accepting contactless fingerprints for civil and criminal processing. The National Institute of Standards and Technology (NIST) and the FBI's Biometric Support Section continue to test and will update as research continues.

No discussion. This topic was accepted as information only.

AdHoc Issue Data Protection Strategy

The FBI and states continue to work with DHS to determine how they are currently protecting our data. While this process differs from the *CJIS Security Policy*, there is a strategy in place that is very similar. There are requirements to protecting the data and audits are conducted. The requirements for the data protection strategy are currently being reviewed. Mr. Schaeffer stated trust has been built over time with these strategies that were put in place. The hope is to come back with a revised data strategy that is not as arduous as it has been in the past for DHS.

No discussion. This topic was accepted as information only.

APB Item #10 National Crime Prevention and Privacy Compact Council (Council) Report

This topic was presented by Ms. Leslie Moore, Director of the Kansas Bureau of Investigation in Topeka and Chair of the Compact Council. (*See Appendix M, PowerPoint.*)

Ms. Moore advised the Compact Council continues to work with the states that are exploring Compact ratification. She reminded the group the Compact ratification video is a

resource located on the Compact Council's website at www.fbi.gov/CompactCouncil. In addition, the Compact mentorship program pairs representatives from non-Compact states with representatives from Compact states to assist them through the process. She encouraged non-Compact states to contact her if they would like to learn more about Compact ratification. She stated ratifying the Compact brings states closer to providing the most comprehensive criminal history record for noncriminal justice requests. This is achieved by participation in the National Fingerprint File (NFF) Program which places the management and responsibility for the effective control, collection, maintenance, and dissemination of state criminal history files solely on the state. NFF participation results in enhanced individual privacy protection and better security for the nation's most vulnerable populations. Currently, 20 states participate in the NFF program, and Vermont is scheduled to become the first alternate NFF state on June 16, 2021. The alternate NFF concept was approved by the Council in May 2016 and provides Compact states an opportunity to join the NFF program with less programming than is required for the traditional NFF states. Several other states are moving forward with NFF implementation, either late this year or early 2022.

During the November 2020 Council meeting, a proposal was submitted by the Transportation Security Administration (TSA) to expand the NGI system message literals associated with the L0008 reject code into two separate and distinct codes. Currently, the L0008 reject code is applied systematically when the NGI system cannot locate a potential biometric match due to the image quality. In 2018, modification was made to the L0008 message literal to enhance the name check process, specifically to tell the contributor that the biometric candidates were found and to resubmit a new set of fingerprints for comparison purposes. As such, when a noncriminal justice agency receives the message literal indicating candidates were found, it can take advantage of the name check service after receiving two fingerprint quality rejects. If the L0008 message does not indicate candidates were found after two fingerprint-based attempts, the noncriminal justice agency recognizes that a name check is unnecessary. To assist with the automation and streamlining purposes, the TSA requested separating the L0008 reject codes associated with the message literals into two separate and distinct codes. One, the L0008 code when there are biometric candidates, and two, a new code if there are no biometric candidates.

The TSA also requested that the new quality reject code include a very specific message literal to remove the ambiguity about whether a manual name check should be requested. This topic was also presented to the APB, as the initial concept would have impacted both noncriminal and criminal justice submissions. During the November 2020 meeting, the Compact Council recommended more time to be given to the research of this issue and for the results to go back through the Compact Council process again. The APB recommended the same. Given the reason behind this request was to assist the noncriminal justice name check service when two fingerprint-based submissions had been rejected due to quality, the first change to this topic was to limit the changes to only the noncriminal justice types of transactions, thereby eliminating the impact to the criminal justice community. The second change was to consider the feedback provided by the Compact Council's committees and modify the recommendation after additional discussions, research, and work with the TSA. The topic was presented again during the spring 2021 meetings. The Compact Council ultimately moved for no change and to leave the current L0008 message literals as for noncriminal justice purposes.

Due to the unavailability or limited availability of noncriminal justice fingerprint services resulting from the coronavirus, the FBI CJIS Division received numerous inquiries regarding the use of the Council's fingerprint submission requirements rule, often referred to as Purpose Code X. During the November 2020 meeting, the Council moved for the use of two proposals to allow for III name checks allowed by the delayed submission of fingerprints during the coronavirus pandemic. The Compact Council approved a submission time frame of as soon as possible, but no later than 180 calendar days during the coronavirus pandemic, or 90 calendar days from the expiration of the state's emergency declaration, whichever occurred first. The Oklahoma proposal was for the emergency placement of children in exigent circumstances. The Colorado proposal was for the sole purpose of conducting criminal history record checks of individuals to include volunteers for limited critical positions as defined by the state in response to the coronavirus pandemic, as specifically identified in a state statute previously approved pursuant to Public Law 92-544. Some examples of that would be for healthcare workers or childcare workers. As done with the past Purpose Code X proposals, the Compact Council reviewed the draft notices for publication in the Federal Register. The Compact Council approved the draft notices, and the proposals will be included in the Federal Register as attachments should they be used for precedence for future events.

As the states' NFF falls under the Compact Council's purview, the Compact Council continues to focus on increased participation in the NFF by Compact party states. This topic highlighted the NFF implementation plans submitted by the required 14 states. During the focused committee meetings in March, the Planning and Outreach (PO) Committee reviewed the status of each state's plans and made recommendations to assist states in joining the NFF program. The Compact Council approved the PO Committee recommendations and to have the NFF mentors reach out to the non-NFF party states without a target implementation date to see what assistance may be needed. The Council also approved a recommendation to conduct a virtual NFF information sharing symposium to answer frequently asked NFF questions.

During the Compact Council meeting, they also discussed topics being presented via the Advisory Process that required the input and awareness of the noncriminal justice community.

She noted on September 30th, 2021, five state Compact Officer positions in the Compact Council will be vacated due to expiring terms. Those states include Alaska, Kansas, Montana, Oklahoma, and Tennessee. Pursuant to section 6.1 6 of the Council's Bylaws, dated November 5th, 2020, the FBI Compact Officer conducted an election via email. The at-large Compact Officers, effective October 1, 2021, are Mr. Michael Christman, FBI; Ms. Jennifer Reich, California DOJ; Mr. Jason Henry, DHS; Ms. Carol Gibbs, Illinois State Police; and Ms. Denise Matthews, Georgia Department of Community Health.

She reported the fall 2021 round of Compact Council meetings is scheduled to be held virtually. The regional committee meetings are tentatively scheduled for August 3-5, 2021. The Standards and Policy and PO Committee meetings are tentatively scheduled for September 21-23, 2021. The Sanctions Committee meeting is tentatively scheduled for November 2, 2021, and the Compact Council meeting to be held on November 3-4, 2021. Topics pertaining to noncriminal issues for the Compact Council's consideration can be

submitted via the Compact Council's website. Topic suggestions may also be forwarded to the FBI Compact Officer, Ms. Chasity Anderson.

This topic was accepted as information only.

APB Item #11 Chairman's Report on the SA Subcommittee

This topic was presented by Mr. Joe Dominic, California DOJ and Chair of the SA Subcommittee, and Ms. Cindy Johnston, FBI, CJIS Division. (*See Appendix N, PowerPoint.*)

Mr. Joe Dominic, California Department of Justice, stepped in as Chair of the SA Subcommittee upon the retirement of Mr. Brad Truitt. Due to technical difficulties during Mr. Dominic's presentation via Microsoft TEAMS, Ms. Cindy Johnston provided the SA Subcommittee update. The SA Subcommittee met on April 22, 2021 and the agenda included two action and three information issues with one motion for APB approval.

SA Issue #1 Fiscal Year 2020 Audit Results Summary

The audit time frame was October 1, 2019 through March 31, 2020. The number of audits was significantly reduced due to the pandemic. There were 84 criminal justice agencies and 57 non-criminal justice agencies audited. The top three areas of noncompliance for the criminal justice agencies were management control agreements, event logging, and security addendums. The top three areas of noncompliance for the non-criminal justice agencies were outsourcing, event logging, and personally owned information systems.

SA Issue #2 CJIS Security Policy (CSP) Modernization Task Force (MTF) Update

The CSP MTF was established in September 2020 to align the CSP with the modern technology standards. It was designed to establish small groups to address specific topics. The first group established was the Data Categorization Task Force, chaired by Mr. Bill Phillips, International Justice and Public Safety Network. The MTF's primary task was to review the eighteen NIST 800-53 Moderate Control Families and align them with the CSP. The first two areas to be reviewed were the Identification and Authentication and the Media Protection Control Families. Recommendations from those reviews will be presented to the APB for input during the fall 2021 round of advisory process meetings.

SA Issue #3 Criminal Justice Data Categorization

This was an action paper relating to the Criminal Justice Data Categorization. The purpose of the paper was to provide methodology and recommendations on the appropriate security categorization for criminal justice information (CJI) as defined in the CSP. Within the policy, CJI refers to all FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions. There is additional information provided in Section 4 of the CSP.

Arriving at an impact level was a key factor that will drive the work of the MTF going forward. This recommendation was not made lightly and sets the tone for how protection of data will relate to security requirements and underpins the future direction the CSP MTF will take in their review of the CSP.

Ms. Johnston introduced Mr. Phillips, who discussed how the categorization was conducted. He explained they were tasked to identify the categorization for CJI. He ensured there was a clear definition of what they were to accomplish and that was to use the existing definitions for CJI and not to redefine it. Membership consisted of local, state, and federal agencies, in addition to assistance from FBI staff. Essentially, they looked at the information processed and determined if it was appropriately categorized, next security controls were selected from that categorization, and then those security controls were implemented around the systems that process, store, and transmit that type of information. Due to technical difficulties, Mr. Phillips was unable to finish his presentation and Ms. Johnston took over for him.

Ms. Johnston recapped the information. Basically, when framing security around repositories of information, it's important to understand the impact to the data if confidentiality, integrity, and availability are lost. The data was looked at from a user community perspective and how they would interpret the impact levels. From this assessment the Data Categorization Task Force settled on a moderate impact level. Ms. Johnston advised they could choose Option 1 to accept the Data Categorization Task Force's recommendation for CJI to be categorized as moderate for confidentiality, integrity and availability, or they could choose Option 2 which was to make a recommendation to categorize it as low or high. Ms. Johnston shared that the SA Subcommittee and all five regional working groups selected Option 1 to categorize the data as moderate.

The following options were presented for consideration:

Option 1: Accept the Data Categorization Task Force's recommendation for criminal justice information to be categorized as MODERATE for confidentiality, integrity, and availability.

Option 2: Motion for criminal justice information to be categorized as a _____ impact for confidentiality, integrity, and availability.

All five working groups and the SA Subcommittee accepted Option 1.

Discussion: Mr. Megna asked the CJIS ISO, Mr. Chris Weatherly, if he believed the working groups and subcommittee's decision was the right way to go? Mr. Weatherly agreed with the decision and explained what they weren't able to hear from Mr. Phillips was the amount of work the Data Categorization Task Force put forth. They wanted to get the security requirements correct and right sized for the type of information being protected. After several weeks of meetings spent on this arduous task, they settled on a recommendation of a moderate impact level and that was right where they needed to be.

A member asked from an auditor's perspective, does that mean that they want to lower the impact or responsibility of a state's requirement to protect the data from their site and will they be changing compliance findings, evaluations, and steps to make sure states get back into compliance once information was lost. Mr. Weatherly answered he didn't know that it would lower or raise it, but it would be right sized based upon the impact to confidentiality, integrity, and availability. The wording will be changed within the CSP. Mr. Weatherly said he is constantly asked for a crosswalk between *NIST 800-53* and the CSP. Once the policy is modernized, a crosswalk won't be needed. Supplemental guidance or discussion will be included under each control, as well as an auditor's guide to show how an agency would meet compliance of that requirement. The member followed up by asking if this would help

noncriminal justice agencies in their struggle to protect the data. Mr. Weatherly explained this was actually to modernize the policy. The current policy was published in 2012. It had nine iterations and this will update it with modern technology and modern data protection strategies. The member then asked if it would be in layman's terms for the non-criminal justice agencies because it was a huge training curve for them. Mr. Weatherly said one thing they added was the discussion under each information assurance requirement demonstrating how to meet those requirements. There will be an auditor's guide demonstrating further what to look for and lay out explicitly how to meet each requirement. Another member asked if they would have an overlay for *NIST 800-53*. Mr. Weatherly replied, through the task force meetings, it was determined agencies prefer to have all the requirements in one document.

Mr. Maury Mitchell, the CSP MTF Chair, reiterated the data categorization was the foundation for the remainder of the work needed to modernize the *CSP*. The foundation was tied into the *NIST* research that applies to most of the federal data and the way it was used at the federal level. They are trying to parallel this to the way the *CSP* works with the states. Mr. Mitchell applauded Mr. Phillips and the task force on the phenomenal job overviewing the policy and making the determination to use moderate. There was a lot of effort involved mapping security controls from *NIST* and applying them to the *CSP*. With eighteen different security controls, they have initiated two sub task forces to begin work on the modernization. They have been working closely with Mr. Bill Fisher at NIST to put together a great product.

A member did not have any concerns with the definition or decision but referenced an earlier discussion concerning the Court Task Force and their opinion of the *CSP*. The Office of State Court Administrators and the Conference of Supreme Court Justices has been loud and clear about the existing policy. If the courts didn't agree then the member wasn't sure they could move forward on this. Mr. Megna said they could socialize this with the courts, but in the interest of moving forward they would need to consider the best way to handle it. The member agreed but felt it would need to be addressed or all the efforts from the task force, ISO, and ISO Program would be wasted if the courts make everything a public record. In agreement with the Data Categorization Task Force, working groups, subcommittee and ISO's recommendation, a motion was made to accept Option 1 as written.

APB RECOMMENDATION: The CJIS APB moved to recommend Option 1: Motion to accept the Data Categorization's Task Force's recommendation for criminal justice information to be categorized as MODERATE for confidentiality, integrity, and availability.

SA Issue #4 Interpretive Guidance Task Force (IGTF) Update

The IGTF was formed to make recommendations because of inconsistencies with personnel background checks and how they were handled in the virtual cloud environment across the CJIS user community. The IGTF has worked in collaboration with the SA Subcommittee, MTF, and the APB Executive Committee. A topic paper will be prepared for the fall 2021 Working Groups.

SA Issue #5 Sunset Date for FTP

Ms. Johnston concluded her presentation with the Sunset Date for FTP. Both the NCIC and SA Subcommittees had the opportunity to make recommendations on this topic and the final recommendation was presented earlier in the NCIC Chairman's report.

APB Item #12 Chairman's Report on the CE Subcommittee

The topic was presented by Captain B. Kyle Gibbs, Service Bureau Commander at the Stillwater, Oklahoma Police Department and Chair of the CE Subcommittee. He advised the CE Subcommittee met virtually on June 3, 2021 to review the audit findings and updates from 54 agencies which represent about 122 component audits spanning 2010 to 2020. Captain Gibbs then presented the findings:

Administrative Office of the United States Courts – 2018

NCIC – Follow-up to CSO

Alabama – 2016

IT – Closure to Governor

Alabama – 2019

NCIC, IT, NGI – Follow-up to CSO

Alaska – 2017

IT – Follow-up to CSA Head

Arizona – 2020

NCIC, National Sex Offender Registry (NSOR), IT, NGI – Follow-up to CSO

NICS – Commendation to CSO

N-DEx – Closure to CSO

Colorado – 2018

IT – Follow-up to CSO

Connecticut – 2017

IT – Follow-up to CSO

NGI – Follow-up to Repository POC

Delaware – 2019

IT, NICS – Closure to CSO

Florida – 2018

NSOR – Follow-up to CSO

IT – Closure for local level findings/Hold in abeyance for court level findings

Georgia – 2019

NSOR, NICS – Follow-up to CSO

N-DEx – Commendation to CSO
NCIC, IT – Closure to CSO

Guam – 2018
NSOR – Closure to CSO

Idaho – 2017
IT – Follow-up to CSA Head

Illinois – 2015, 2018
NCIC, NSOR – Email Follow-up to CSO

Illinois – 2018
IT – Follow-up to CSO
NGI – Closure to CSO

Iowa – 2018
NSOR – Follow-up to CSO
IT – Closure to CSA Head

Kansas – 2018
IT – Email Follow-up to CSO

Kentucky – 2019
NSOR – Closure to CSO

Louisiana – 2017
NSOR – Follow-up to CSA Head

Louisiana – 2020 POINT OF CONTACT
NCIC, NSOR, IT – Follow-up to CSO
NICS – Commendation to CSO
N-DEx, NGI – Closure to CSO

Maine – 2010, 2013, 2016, 2019
NCIC – Email Follow-up to CSO

Maine – 2019
NGI – Follow-up to CSO
NSOR – Closure to CSO

Maryland – 2017
IT – Closure to CSA Head

Massachusetts – 2017
NCIC, NSOR – Follow-up to Governor (elevation)
NICS – Follow-up to CSA Head

IT – Closure to CSA Head

Massachusetts State Identification Bureau – 2017

IT, NGI – Follow-up to Repository Point of Contact (POC)

Michigan – 2019

NGI – Follow-up to CSO

NSOR, IT – Call/Close or Follow-up to CSO

Minnesota – 2015

IT – Follow-up to Governor

Minnesota – 2018

IT – Follow-up to CSA Head

Mississippi

NGI – Follow-up to CSO

NSOR – Closure to CSO

Missouri – 2018

NCIC, NSOR – Follow-up to CSA Head

Montana – 2014

IT – Follow-up to Attorney General

Montana – 2017

NSOR – Follow-up to CSA Head

IT – Closure to CSA Head

Nlets

IT – Commendation to POC

Nebraska – 2019

IT, NICS – Follow-up to CSO

Nevada – 2017

IT – Email Follow-up to CSO

New Hampshire – 2018

NCIC, IT, N-DEx, NGI – Follow-up to CSO

New Jersey – 2019

NCIC, IT – Follow-up to CSO

NSOR – Closure to CSO

New Mexico – 2016

IT – Follow-up to Governor

New Mexico – 2019

NCIC, IT, NICS – Follow-up to CSO

NGI – Closure to CSO

New York – 2014

NCIC, NSOR, IT – Follow-up to Governor

New York – 2018

NCIC, NSOR, IT – Follow-up to CSO

New York SIB – 2018

IT – Closure to POC

North Carolina – 2016

IT – Follow-up to Governor

North Carolina – 2019

IT – Follow-up to CSO

North Dakota – 2019

NGI – Follow-up to CSO

Office of Biometric Identity Management – 2019

IT – Closure to POC

Ohio Bureau of Criminal Investigation – 2017

NICS – Follow-up to Superintendent

IT – Closure to Superintendent

Oklahoma – 2019

NSOR, IT – Follow-up to CSO

Oklahoma State Identification Bureau – 2019

IT – Commendation to CSO

Oregon – 2015

NSOR – Call/Close or Email Follow-up to CSO

Oregon – 2018

IT – Call/Close or Email Follow-up to CSO

NSOR – Call/Close or Email Follow-up to CSO

Puerto Rico – 2013, 2015

NCIC – Follow-up to Governor

Puerto Rico – 2019

NCIC, IT – Follow-up to CSO

Rhode Island – 2017

IT – Closure to CSA Head

Rhode Island Repository – 2017

IT – Follow-up to Attorney General

South Carolina – 2013, 2017

IT – Email Follow-up to CSO

South Carolina – 2017

NSOR, IT – Follow-up to CSA Head

South Dakota – 2019

NSOR, IT, NICS – Closure to CSO

South Dakota State Identification Bureau – 2019

NGI – Follow-up to POC

Tennessee – 2019

IT – Follow-up to CSO

Texas – 2019

NSOR – Follow-up to CSO

Transportation Security Administration – 2019

IT – Closure to CSO

United States Air Force Office of Special Investigation – 2018

NCIC, IT – Closure to CSO

United States Customs and Border Protection – 2019

IT – Closure to CSO

United States Immigration and Customs Enforcement – 2019

NCIC, IT, NICS, N-DEx – Commendation to CSO

United States Virgin Islands – 2019

NSOR, IT – Follow-up to CSO

Vermont – 2019

IT, NGI – Follow-up to CSO

NSOR – Closure to CSO

Virginia – 2015, 2018
NSOR – Email Follow-up to CSO

Washington – 2018
IT – Follow-up to CSO

West Virginia – 2018
NCIC – Follow-up to CSO

Western Identification Network – 2020
IT – Commendation to POC

Wisconsin – 2018
IT – Follow-up to CSO

No discussion.

APB RECOMMENDATION: The CJIS APB moved to accept all audit findings as presented.

APB Item #13 Chairman’s Report on the NICS Subcommittee

The topic was presented by Ms. Lynn Rolin, Program Coordinator, IT CJIS Liaison, South Carolina Law Enforcement Division, Columbia, South Carolina. *(See Appendix O, PowerPoint.)*

Ms. Rolin briefed that most of the informational topics covered by the NICS Subcommittee on April 22, 2021, had already been addressed prior to this presentation. She thanked Mr. Schaeffer for the information he provided on Purpose Code F, IFFS, and federal arrests and said this information was very helpful to NICS and the user community.

Ms. Rolin applauded the NICS Section for their quick response to the COVID-19 pandemic and the phenomenal job of processing a record number of background checks. She said she was proud to represent the NICS Section. She mentioned the annual report from the CAU on the overall trends as they relate to NICS audits. Audits were severely impacted by COVID-19. The CAU conducted six NICS audits from October 2019 to March 2020 and have now resumed onsite audits. Ms. Rolin then presented the NICS action topic.

NICS Issue #7 Additional DOB Requirements for NICS Indices Entry

A matching NICS Indices hit to a prospective firearm transferee or firearm permit applicant allows the user to render an immediate denial determination as all NICS Indices information is validated by the contributor as prohibiting prior to their submission. This prevalidation, in turn, provides greater efficiency by eliminating the user's need to conduct additional research to determine if the information is prohibiting for the firearm transfer or receipt of a firearm permit. The NICS will currently accept partial DOBs in the NICS Indices entry. A NICS Indices hit with the partial DOB may make it difficult for a NICS user receiving the hit to determine if the individual in the NICS indices hit is a match with their subject.

The purpose of this topic was to provide options for additional DOB requirements for a NICS Indices entry when a partial DOB is present. As recommended by the APB and approved by the Director, beginning October 1, 2019, populating the DOB and middle name fields became required if the source documentation maintained by the contributor contained that information. For the DOB, a contributor must include the DOB listed in the source documentation or one that can be linked to the individual. If the contributor has a qualified individual for entry in the NICS Indices but only has a partial DOB, such as 04/00/1944, the entry can be completed with this DOB even without an additional descriptor such as a SOC or MNU.

However, if no DOB is contained within the source documentation and no additional descriptors exist, the contributor should not create an arbitrary partial DOB to complete the entry process. Of the over 23 million records in the NICS Indices, about 2,500 contain a partial DOB. Although this is a small percentage of entries, when a hit occurs on the NICS Indices with a partial DOB, it may be very difficult to determine if the individual is a descriptive match with the hit, especially if the name provided is an exact match with the hit. On several occasions state partners have expressed concern and frustration over the lack of or incomplete biographical descriptors in the NICS indices. Therefore, it's imperative that the complete DOB be provided with each NICS indices entry. The following options were presented for consideration.

Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message.

Option 2: With this option, the NICS will be programmed to accept a partial DOB for a NICS Indices entry, only if an additional descriptor is included, e.g., SOC or MNU. If a contributor attempts to enter a partial DOB without an additional descriptor, they will receive a reject message.

Option 3: No change. Partial DOB will continue to be accepted by the NICS.

Note: If Options 1 or 2 are approved, the NICS Section will complete the system enhancement. There should be no impact for the states, only awareness of the additional requirement. The system enhancement necessary to implement the change will be assigned a priority and categorized.

Four of the five working groups accepted Option 1. The Southern Working Group accepted Option 2. The NICS Subcommittee accepted Option 1.

Discussion: A member asked if entries in the indices that do not contain a DOB would remain once this change is made. The response was yes. Another member asked if this change would impact "John Doe" protective orders entered by the protective order registries. Ms. Jill Montgomery, FBI CJIS, NICS Section, said it would have an impact, if they do not provide a complete DOB, they will no longer be able to be entered.

APB RECOMMENDATION: The CJIS APB moved to recommend Option 1: The NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message.

Ms. Rolin then briefed on the informational topic regarding Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) denials. Both the FBI, NICS and ATF share denial information. Representative from the ATF explained the ATF's Denial Enforcement and NICS Intelligence (DENI) Branch reviews and researches NICS denials daily. The DENI Branch sends denied transactions to ATF field offices for further investigation and shares denial data with state fusion centers. The DENI Branch also responds to inquiries and concerns regarding the NICS and works diligently to identify illegal firearms trafficking and other criminal trends. In 2019, the ATF DENI Branch started transmitting denial data monthly to the state fusion centers. In March 2021, the ATF DENI Branch automated the state fusion center reports and started transmitting denial data to them on a weekly basis. All cases not sent to the ATF field offices for further investigation are shared with the fusion centers for state action as they see fit. The CJIS Division began sharing NICS denial information with 56 FBI field offices in 2010 via a monthly spreadsheet. Much of the data was outdated before it reached the field offices, as information is returned, and denials are overturned on a regular basis. In 2019 the process was modernized and NICS now shares denial information daily, so the field offices have the most current denial information. Five years of NICS denial data, both federal and state, is contained within these reports.

Ms. Rolin mentioned the upcoming NICS User Conference to be held virtually with three sessions taking place in July, August, and September. She said the agenda has some great topics and she encouraged people to sign up for one of the sessions.

She also mentioned the Fix NICS Peer-to-Peer Session held June 1, 2021 and thanked those who participated. She encouraged users to upload their reports, if their state allows it, so everyone can see what each state is doing and garner ideas of how to improve these reports.

Ms. Rolin closed by thanking Sheriff Witt for her many years of service to the NICS Subcommittee noting they served alongside each other for nine years. Ms. Rolin said she thoroughly enjoyed her collaboration, friendship and mentorship and looked forward to continuing their work together.

APB Item #14 Chairman's Report on the PSS Subcommittee

The topic was presented by Mr. Charles Schaeffer, Director, Criminal Justice Information Services, FDLE, Tallahassee, Florida, and Chair of the PSS Subcommittee. (*See Appendix P, PowerPoint.*) Mr. Schaeffer covered the action topics first.

PSS Issue #4 Recommendation for Changes to Sex Codes within UCR

Mr. Schaeffer briefed that this topic was first brought to the working groups and the UCR Subcommittee during the fall 2020 round of meetings. There were several different opinions and

the UCR Subcommittee decided to refer this topic to the PSS Subcommittee. The following options were presented for consideration.

Option 1 – The UCR Program should allow sex code selections of M for male, F for female, X for non-binary, or U for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity American Psychological Association [(APA) 2008].

Option 2 – The UCR Program should resolve sex and gender in two phases.

Phase 1: The UCR Program should allow sex code selection of M for male, F for female, X for non-binary, or U for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008). Phase 1 may be immediately implemented.

Phase 2: The UCR Program should implement a new data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined) or U for unknown/unspecified are allowed. Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts to the law enforcement community at one time due to the nations ongoing transition to NIBRS.

Option 3 – The UCR Program should allow sex code selection of M for male, F for female, X for non-binary, man (code to be determined), woman (code to be determined), transgender male (code to be determined), transgender female (code to be determined), or U for unknown/unspecified. These code selections capture gender expression and gender identity together.

Option 4 – The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy.

Option 5 – No change.

There was a lot of discussion by the subcommittee about the difference between biology and psychology and after deliberation, the PSS Subcommittee came up with an Option 6 which would implement a third sex code of U for unidentified. The PSS also recommended a phased approach to be respectful of someone's desire to not reveal their sex code. This provides a way to capture the information now and address gender identity issues in the future. If you end up with several gender identifies in the sex code it would throw the algorithms off and the discussion and debate centered around if a change was made in one system, how would it be captured in all other impacted systems.

Discussion: A member asked if approved, when Phase II ends, would it change the sex code to biological sex or would it keep the field name the same? Mr. Schaeffer said they will need to study this more to answer the question.

APB RECOMMENDATION: The CJIS APB moved to recommend New Option 6: The UCR Program should resolve sex and gender in two phases.

Phase 1: The UCR Program should implement a third sex code category of for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy.

Phase 2: The UCR Program should implement a new optional data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined) or U for unknown/unspecified are allowed. Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts to the law enforcement community at one time due to the nation's ongoing transition to NIBRS.

The priority should be 3M.

PSS Issue #7 Changes to Race Codes within the FBI UCR Program

The purpose of this topic was to present a proposal for changes to the race code data element within FBI UCR Program data collections to allow for multiple race code choices within race code data elements. The following options were presented in the topic paper.

Option 1: Change the NIBRS race category to allow for multiple selections for the arrestee, offender, and victim segments.

Option 2: No change.

The Federal and Southern Working Groups recommended Option 1. The North Central and Northeastern Working Groups recommended Option 2. The Western Working Group recommended the topic be referred to the PSS Subcommittee for further exploration with no change until that was completed. The UCR Subcommittee moved to accept the Western Working Group's recommendation. The PSS Subcommittee opted for no change with the following action item: CJIS to develop a strategic plan on how to reconcile race, sex, and gender codes across CJIS Systems with other relevant fields as practical and establish goals in harmonizing CJIS services when it comes to specific data elements. More work will be done and this topic will come back to the process at a later time.

Discussion: A member expressed they were good with the action item but questioned why they addressed the previous topic regarding sex codes instead of incorporating into the action item for this topic. Mr. Schaeffer said they moved forward on the sex code recommendation because Department of Motor Vehicles are allowing the use of unidentified, but they are currently not allowing the use of multiracial. Sheriff Witt recommended the APB accept the action item as recommended by the PSS Subcommittee and there were no objections.

Action Item: CJIS to develop a strategic plan on how to reconcile race, sex, and gender codes across CJIS Systems with other relevant fields as practical and establish goals in harmonizing CJIS services when it comes to specific data elements.

Mr. Schaeffer closed by thanking Ms. Kim Lough, DFO of the PSS Subcommittee for her work.

Closing Remarks

Sheriff Witt noted it was a long but productive day of history making decisions. She was honored to play a part alongside the APB members in moving the country forward. Sheriff Witt congratulated Mr. Megna on 25 years of service with the FBI. She then turned to Mr. Megna to provide closing remarks.

Mr. Megna thanked Sheriff Witt for acknowledging his service and offered thanks to her for chairing the meeting. Mr. Megna also thanked Ms. Cindy Johnston, DFO of the SA Subcommittee for the great job in taking over the SA Chairman's report due to technical difficulties during Mr. Dominic's presentation. Mr. Megna then provided the fall 2021 meeting dates. The working group meetings will be held August 16-20, 2021. The subcommittees will be held October 4-8, 2021. The APB meeting will be held December 7-9, 2021. The fall working groups will be held virtually and the others will be determined once the fiscal year budget is determined. He noted the blended meeting presented some technical challenges with some room for improvement but overall, it was a good meeting. He thanked everyone for their patience. Sheriff Witt closed by thanking everyone and wished them safe travels.

Intentionally Left Blank

CJIS Advisory Process Board (APB) Meeting
June 9, 2021
9:00 a.m. (EDT)
Roll Call

APB Members:

X	Sheriff Kathy Witt, <i>Chair</i>	In-Person	Fayette County, KY Sheriff's Office <i>Representing the Southern Working Group</i>
X	Mr. Charles I. Schaeffer, <i>Second Vice Chair</i>	In-Person	Florida Department of Law Enforcement <i>Representing the Southern Working Group</i>
X	Mr. Brian Wallace, <i>First Vice Chair</i>	In-Person	Marion County, OR Sheriff's Office <i>Representing the Western Working Group</i>
X	Ms. Brenda Abaya	Virtual	Hawaii Criminal Justice Data Center <i>Representing the Western Working Group</i>
X	Chief William G. Brooks, III	In-Person	Norwood, MA Police Department <i>Representing the International Association of Chiefs of Police</i>
X	Mr. Michael M. Brown	In-Person	National Sheriffs' Association <i>Representing the National Sheriffs' Association</i>
X	Mr. Kevin C. Cockrell	In-Person	Montgomery County, KY Attorney <i>Representing the National District Attorneys Association</i>
X	Ms. Keri Brady	Virtual	National Targeting Center, U.S. Department of Homeland Security <i>Proxy for Mr. Donald Conroy</i> <i>Representing the National Security Sector</i>
X	Chief Dwayne D. "Rusty" Cooper	In-Person	Kingman, AZ Police Department <i>Representing the Western Working Group</i>

X	Ms. Veronica S. Cunningham	In-Person	America Probation and Parole Association <i>Representing the American Probation and Parole Association</i>
X	Chief William J. Denke	Virtual	Sycuan Tribal Police Department <i>Representing Tribal Law Enforcement</i>
X	Ms. Carol Gibbs	Virtual	Illinois State Police <i>Representing the North Central Working Group</i>
X	Captain B. Kyle Gibbs	In-Person	Stillwater, OK Police Department <i>Representing the Southern Working Group</i>
X	Mr. Jeremy Hansford	Virtual	Ohio State Highway Patrol <i>Representing the North Central Working Group</i>
X	Ms. Shelly Holzerland	Virtual	Dodge County, Nebraska 911 <i>Representing the North Central Working Group</i>
X	Mr. Bruce T. Houlihan	Virtual	Orange County, CA Crime Laboratory <i>Representing the American Society of Crime Laboratory Directors</i>
X	Mr. Donald Hull	In-Person	Stowe, Vermont Police Department <i>Representing the Northeastern Working Group</i>
X	Ms. Versie Jones	In-Person	Connecticut State Police <i>Proxy for Mr. Darryl Hayes</i> <i>Representing the Northeastern Working Group</i>
X	Ms. Lynda G. Lovette	Virtual	Baltimore City, MD Police Department <i>Representing the Southern Working Group</i>
X	Ms. Amy Mancuso	In-Person	South Dakota Department of Public Safety <i>Representing the North Central Working Group</i>

X	Ms. Leila McNeill	Virtual	Idaho State Police <i>Representing the Western Working Group</i>
X	Mr. Maury Mitchell	In-Person	Alabama Law Enforcement Agency <i>Representing the Southern Working Group</i>
X	Ms. Kathryn M. Monfreda	Virtual	Alaska Department of Public Safety <i>Representing the Western Working Group</i>
X	Ms. Leslie Moore	In-Person	Kansas Bureau of Investigation <i>Representing the Compact Council</i>
X	Mr. J. Kent Oberkrom	In-Person	Henry County, Missouri Sheriff's Office <i>Representing the North Central Working Group</i>
X	Sergeant Brian Parker	In-Person	New Hampshire State Police <i>Representing the Northeastern Working Group</i>
X	Mr. Scott G. Patterson	Virtual	Talbot County, MD State's Attorney <i>Representing the Prosecutorial Sector</i>
X	Mr. Brian Pittack	In-Person	Office of Biometric Identity Management U.S. Department of Homeland Security <i>Representing the Federal Working Group</i>
X	Mr. Corey R. Steel	Virtual	State Court Administrator Nebraska Supreme Court <i>Representing the Conference of Chief Justices</i>
X	Ms. Sonya Thompson	Virtual	Federal Bureau of Prisons <i>Representing the Correctional Sector</i>
X	Mr. Jeffrey Wallin	In-Person	Vermont Department of Public Safety <i>Representing the Northeastern Working Group</i>

X	Honorable Nathan E. White	In-Person	American Judges Association <i>Representing the Judicial Sector</i>
X	Sheriff Anthony Wickersham	Virtual	Macomb County, MI Sheriff's Office <i>Representing the Major County Sheriffs of America</i>

First	Last	Agency
Brenda	Abaya	Hawaii Criminal Justice Data Center
Paul	Abbate	Federal Bureau of Investigation
Yusuf	Abdul-Salaam	ECS
Melissa	Abel	Federal Bureau of Investigation
Kevin	Ahearn	GDIT
Peter	Ahearn	Ahearn Consulting
Constantine	Alex	Federal Bureau of Investigation
Mark	Allen	Federal Bureau of Investigation
Jim	Anderson	Washington State Patrol
Cathy	Arbaugh	Federal Bureau of Investigation
Natalie	Argabrite	Federal Bureau of Investigation
Jennifer A.	Armstrong	U.S. Marshals Service
Janine	Arnold	Federal Bureau of Investigation
Gail	Azaroff	Plural Sight
Heela	Aziz	U.S. Immigration and Customs Enforcement
Melanie	Bailey	Charlotte County Sheriff's Office
Thomas	Baker	Baker Associates International Associates
Tonya	Barnes	Federal Bureau of Investigation
Steven	Barnes	Federal Bureau of Investigation
Charles	Barnett	IntelliWare, Inc.
Diane	Bartell	Minnesota Bureau of Criminal Apprehension
Brian	Bear	Accenture
Mitch	Beemer	Kansas Bureau of Investigation
Eric	Berkowitz	Guidehouse, LLP
Joe	Bianco	Buchanan& Edwards
Olivia	Blackburn	DMI, LLC
Mark	Blackman	Imageware
Amy C.	Blasher	Federal Bureau of Investigation
Kenneth	Blue	Tennessee Bureau of Investigation
Liz	Bodell	ServiceNow
Kaitlyn	Bodkin	Federal Bureau of Investigation
Susan	Bogucki	Gigamon
Jay	Bokulic	VMware, Inc.
Katherine	Bond	Federal Bureau of Investigation
Laura	Boufford	Google
Janice	Bradford	Department of Maryland State Police
Keri	Brady	Department of Homeland Security
Joseph	Brandon	IDEMIA National Security Solutions
Dion	Bright	Federal Bureau of Investigation
Lestyn	Bright	Federal Bureau of Investigation
William G.	Brooks, III	Norwood Police Department
John	Broome	Clearshark
Kyle	Brown	Arkansas Crime Information Center AR DPS
Tracy	Brown	Noblis
Michael M.	Brown	National Sheriffs' Association
James	Buckley, Jr.	CPI

First	Last	Agency
Julie	Bumgardner	Federal Bureau of Investigation
Kaylah	Burt	Virginia Department of State Police
Frank	Campbell	Highland Strategies, LLC
Shiloh	Cantu	Tyler Technologies
Mark	Carvelli	Federal Bureau of Investigation
William	Casey	TSCTI
Alvaro	Castillo	Deloitte Services
Christopher	Casto	Federal Bureau of Investigation
Kayla	Celaya	United States Marshal Service
Christopher	Chan	Google
Christopher	Chaney	US DOJ of Office of Tribal Justice
William	Chase	EnProVera, Inc.
Valerie	Chase-Robert	MuleSoft, LLC
Michael	Christman	Federal Bureau of Investigation
Timothy	Chung	Arizona Department of Public Safety
Jennifer	Clark	Inquiries Screening
Anthony	Clayton	CIO Federal IT
Ryan	Clemm	Federal Bureau of Investigation/Mitre
Linda	Click	Federal Bureau of Investigation
Denise	Coates	Federal Bureau of Investigation
Charles	Coats, Jr.	South Carolina Law Enforcement
Brandon	Cobb	Kentucky State Police
Celeste	Cochran	Federal Bureau of Investigation
Kevin C.	Cockrell	Montgomery County Attorney
Jeremy	Cohn	Red Hat
Shirley	Collins	The Rehancement Group
Todd	Commodore	Federal Bureau of Investigation
Mary Ellen	Condon	Condon Associates, LLC
Dwayne D. "Rusty"	Cooper	Kingman Police Department
Jason	Corder	Federal Bureau of Investigation
Joseph	Courtesy	JCour-Consulting, LLC
Latarshia	Crawford-Jones	Steampunk
Holden	Cross	FBI CJIS
April	Cross	Florida Department of Law Enforcement
Jeff	Cullen	Wyoming Division of Criminal Investigation
Jimmie	Culley	DFSC Biometric Operations Directorate
Veronica S.	Cunningham	American Probation and Parole Association
Rebecca	David	Oregon State Police
Stacey	Davis	Federal Bureau of Investigation
Diana	Davison	Federal Bureau of Investigation
Dennis	DeBacco	SEARCH
Frank	deBraga	Nevada Department of Public Safety
Kimberly	Del Greco	Federal Bureau of Investigation
Sammy	DeMarco	Federal Bureau of Investigation
William	Denke	Sycuan Tribal Police Department
Karen	DeSimone	NTT DATA Federal Services, Inc.

First	Last	Agency
Alicia	Dewitt	South Carolina Law Enforcement Division
Adam	Dickerson	VMWare, Inc.
Lorie	Doll	Federal Bureau of Investigation
Joe	Dominic	California Department of Justice
Gregory	Donewar	Federal Bureau of Investigation-Contractor
Jack	Donohue	Retired NYPD/Previous APB Chair
David	Donovan	Booz Allen Hamilton
Gena	Dowell	Federal Bureau of Investigation
Randal	Doyle	U.S. Army Crime Records Center
Anissa	Drabish	Federal Bureau of Investigation
Donald	Dudley	MPD
Fredia	Dunn	Louisiana Commission on Law Enforcement
James	Dunn	Federal Bureau of Investigation
Brian	Edgell	Federal Bureau of Investigation
Mohamed	Elansary	Buchanan & Edwards
Angela	Elliott	Federal Bureau of Investigation
Brent	Ellsworth	Federal Bureau of Investigation
Kate	Evans	CT DESPP
Scarlett	Everly	Federal Bureau of Investigation
Mark	Ewing	National Background Check, Inc.
Stephen	Exley	Amazon Web Services
Pamela	Faber	Federal Bureau of Investigation
Patrick	Fagan	Motorola Solutions
June	Fahey	Federal Bureau of Investigation
Michelle	Farris	Texas Department of Public Safety
Amber	Fazzini	Federal Bureau of Investigation
David	Fazzini	Federal Bureau of Investigation
Jackie	Fendrock	Accenture Federal Services
Jeffrey	Fisher	Federal Bureau of Investigation
David	Flannigan	Missouri State Highway Patrol
Amy	Fleming	Federal Bureau of Investigation
Steven	Flowers	Axon Enterprise
Trudy Lou	Ford	Federal Bureau of Investigation
Jennifer	Francis	Federal Bureau of Investigation
Joseph	Friend	Department of Justice
Lisa	Fritsch	Agile5 Technologies
Peter	Fritsch	Agile5 Technologies, Inc./FBI
Terry	Fromson	Women's Law Project
Jacquelyn	Gabriel	ThermoFisher Scientific
Gerard	Gallant	Amazon Web Services (AWS)
Luis	Garcia	Cisco
Cole	Garrett	Federal Bureau of Investigation
JoAnn	Garrison	Federal Bureau of Investigation
Courtney	Gatlin	Red Hat
Ashley	Gerken	Federal Bureau of Investigation
James	Gerst	Federal Bureau of Investigation

First	Last	Agency
Carol A.	Gibbs	Illinois State Police
B. Kyle	Gibbs	Stillwater Police Department
Neal	Gieselman	NCTC
Natalie	Goff	Federal Bureau of Investigation
Becki	Goggins	SEARCH
Nichole	Gohman	Peraton
Kristi	Gordon	Florida Department of Law Enforcement
Mary	Gostel	Tygart Technology, Inc.
Todd	Graham	AnaVation, LLC
Jill	Grant	Federal Bureau of Investigation
Brandon	Gray	IDEMIA
Scott	Gray	Gray Analytics
Robert	Greeves	National Criminal Justice Association
Brian	Griffith	Federal Bureau of Investigation
Deanna	Griffith	Federal Bureau of Investigation
Jennifer	Grimes	Federal Bureau of Investigation
Shelly	Guerreo	ThermoFisher Scientific
Michael	Haas	DOJ Office of the Chief Information Officer
Darla	Hackworth	Colorado Bureau of Investigation
Harry	Halden	IDEMIA
Christian	Hall	Salient CRGT
Daniel	Hall	Illinois State Police
Patricia	Hanning	Federal Bureau of Investigation
Jeremy	Hansford	Ohio State Highway Patrol
Penny	Harker	Federal Bureau of Investigation
Nicholas	Harris	Oregon State Police
Charity	Harris	Federal Bureau of Investigation
Cortney	Harris	Federal Bureau of Investigation
Zachary	Hartzell	Federal Bureau of Investigation
Michael	Hash	IDEMIA
Daryl	Haug	Lexis Nexis Special Services Inc.
Beverly	Hawkins	Federal Bureau of Investigation
Kim	Hayhurst	Federal Bureau of Investigation
Cherie	Henry	SentinelOne
Patrick	Henry	ManTech
Dreama	Hewitt	Federal Bureau of Investigation
Tracy	Hicks	Federal Bureau of Investigation
Dina	Hitch	Splunk
Joey	Hixenbaugh	Federal Bureau of Investigation
Lisa	Hodgson	Federal Bureau of Investigation
Caitlin	Hoebeke	Amazon Web Servies
Laura	Holder	USCIS
Shelly	Holzerland	Fremont/Dodge County 911
Bruce T.	Houlihan	Orange County Crime Laboratory American Society of Crime Lab Directors
John	Howell	Federal Bureau of Investigation
Donald B.	Hull	Stowe Police Department

First	Last	Agency
Mike	Hulme	Unisys
Ted	Hunt	Federal Bureau of Investigation
Rachel	Hurst	Federal Bureau of Investigation
Doug	Ingros	Contractor Dutch Ridge Consulting Group, LLC
Danny	Jackson	Louisiana Sheriff's Association
Joy	Jarrett	Federal Bureau of Investigation
Michael	Jefferson	Federal Bureau of Investigation
Tyler	Jeffords	Cisco Systems
Cynthia	Johnston	Federal Bureau of Investigation
Versie	Jones	CT State Police
David	Jones	Federal Bureau of Investigation
Darrin	Jones	Federal Bureau of Investigation
Rebecca	Kanin	Octo
Brittany	Karlen	Federal Bureau of Investigation
Robert	Keener	Federal Bureau of Investigation
Camden	Keener	Federal Bureau of Investigation
Gary	Kelley	Federal Bureau of Investigation
David	Kennedy	Florida Department of Law Enforcement
Dale	King	Tennessee Bureau of Investigation
Charles	Klebe	Federal Bureau of Investigation
Chris	Kleinman	Splunk
Lora	Klingensmith	Federal Bureau of investigation
Krista	Koch	Federal Bureau of Investigation
Thomas	Kohler	Full Visibility, LLC
Chris	Kovac	Los Angeles County Sheriff's Department
Thomas	Krall, Jr.	CGI Federal
Drew	Kudrick	Clearshark
Michael	Kuhla	Tableau
Karen	Lamb	New Hampshire State Police
Rebecca	Lambert	Federal Bureau of Investigation
Brian	Lamont	INTEGRITYOne Partners
Scott	Lamoreux	Dorrean, LLC
Brent	Lane	Dell Technologies
Sandra	Layman	Federal Bureau of Investigation
Robin	Layton	Mississippi Department of Public Safety
Thomas	Lee	Octo Consulting Group
Thomas	Lehosit	Federal Bureau of Investigation
Charles	Lemley	Federal Bureau of Investigation
Joseph J.	Leon Guerrero	Guam Judicial Center
Elliott	Leshner	Federal Bureau of Investigation
Mike	Lesko	NEC America
Brian	Lester	Paradyme Management
Steve	Lewis	Qmulos LLC
Brett	Lincoln	Federal Bureau of Investigation
Denise	Lindsey	ECS
Karen	Lissy	SEARCH

First	Last	Agency
Bonnie	Locke	Nlets
Crystal	Lockhart	Georgia Bureau of Investigation
Brad	Long	Datamaxx Applied Technologies, Inc.
James	Loudermilk, II	James Loudermilk Services
Kimberly	Lough	Federal Bureau of Investigation
Katie	Loughran	IntelliWare Systems
Lynda G.	Lovette	Baltimore City Police Department
Benjamin	Lowther	Federal Bureau of Investigation
Jordan	Lowthert	Federal Bureau of Investigation
Nicole	Lubich	Nevada Department of Public Safety
Veronica	Luna	Arizona Department of Public Safety
Alyson	Lunetta	California DOJ
Steve	Ly	ServiceNow
Kirk	Macchiavello	ZolonTech, Inc.
Leo	Makowski	Salesforce
Ben	Mallory	Grant Thornton Public Sector, LLC
Amy	Mancuso	South Dakota Department of Public Safety
Amber	Mann	Federal Bureau of Investigation
Raymond	Mansi	Nevada Department of Public Safety
Stephanie	Manson	Federal Bureau of Investigation
Briana	Marino	Federal Bureau of Investigation
William	Marosy	Dutch Ridge Consulting Group, LLC
Lonnie	Martinez	U.S. Postal Inspector Service
Sherrie	Masden	ES Metro Safe 9-1-1 Communications
Chandler	Maskal	ImageWare
Cara	Matheny	Federal Bureau of Investigation
Jeff	Matthews	OffenderWatch
James	Maurer	Aware, Inc.
Robert	May	IJIS Institute
Charles	Mays	Federal Bureau of Investigation
Andrea	McCarthy	HARP, LLC
Caroline	McClendon	Federal Bureau of Investigation
Marla	McDonald	Federal Bureau of Investigation
Sean	McElroy	Kace Company
Christopher	McIntosh	Federal Bureau of Investigation
Paul	McInturff	Federal Bureau of Investigation
Michael	McIntyre	Federal Bureau of Investigation
William G.	McKinsey	Federal Bureau of Investigation
Jan	McNally	Nebraska Crime Commission
Leila	McNeill	Idaho State Police
Michelle	Meder	Federal Bureau of Investigation
Aimee	Medonos	AnaVation, LLC
Nick	Megna	Federal Bureau of Investigation
Brandi	Meighan	Federal Bureau of Investigation
Matthew	Melton	Amazon Web Service
Amy	Messier	Vermont Crime Information Center

First	Last	Agency
Roger	Miller	Paradyne Management Inc.
Roberta	Miller	Federal Bureau of Investigation
Maury	Mitchell	Alabama Law Enforcement Agency
Kelly	Moan	New York Police Department
Kathryn M.	Monfreda	Alaska Department of Public Safety
Jill	Montgomery	Federal Bureau of Investigation
Michael	Moore	Beadle County State's Attorney
Michelle	Moore	South Carolina Law Enforcement Division
Nichole	Moore	Diverse Computing, Inc.
Leslie	Moore	Kansas Bureau of Investigation
Stephen	Morris	IBM
Holly	Morris	Federal Bureau of Investigation
Beverly	Morris	Federal Bureau of Investigation
Brian	Mortweet	NTT Data
Deborah	Mullens	Federal Bureau of Investigation
Charles	Murphy	Florida Department of Law Enforcement
Scott	Myers	Federal Bureau of Investigation
A.J.	Naddell	Imageware
Steve	Nash	Aware
Kristi	Naternicola	Federal Bureau of Investigation
Greg	Nelsen	Federal Bureau of Investigation
Larry	Newton	Kentucky State Police
Apollo	Nguyen	Google, LLC
Nicholas	Nguyen	i3, LLC
Christy	Nichols	Federal Bureau of Investigation
Kevin	Nugent	Axiologue Solutions
Cherish	Nunez	Michigan State Police
J. Kent	Oberkrom	Henry County Sheriff's Office
Brandon	Ohrns	Larimer County Sheriff's Office
Paul	Oliver	Federal Bureau of Investigation
Paulina	Orlikowski	Metro Star, Inc.
Beth	Owens	Ohio Attorney General BCI&I
Richard	Page	Federal Bureau of Investigation
Marybeth	Paglino	Federal Bureau of Investigation
Brian H.	Parker	New Hampshire State Police
Kim	Parsons	Federal Bureau of Investigation
Jay	Patkar	Mule Soft
Zenia	Patrick	Federal Bureau of Investigation
Scott G.	Patterson	Talbot County State's Attorney
Darrin	Paul	Federal Bureau of Investigation
Todd	Pearl	Paterson Police Department
Chris	Peek	Versaterm
Andrew	Pelletz	Noblis
Louis	Penn, Jr.	U.S. Immigration and Customs Enforcement
Alan	Peto	Las Vegas Metropolitan Police Department
Wyatt	Pettengill	Idemia

First	Last	Agency
Emily	Philip	Colorado Bureau of Investigation
Tammy	Phillips	Federal Bureau of Investigation
Bill	Phillips	Nlets
Chris	Piehota	Searchlight Cyber, LLC
Brian	Pittack	Office of Biometric Identity Management - DHS
Jillana	Plybon	Federal Bureau of Investigation
Jennifer	Plyler	DOD DCSA
Kim	Portik	Canyon State Reporting
Deborah	Post	Federal Bureau of Investigation
Shane	Powers	National Security Solutions
Akshai	Prakash	Red Hat
Thomas R.	Prevo	Nebraska State Patrol
Leslie	Prichard	E-INFOSOL, LLC
Matthew	Procter	Pegasystems
Charles	Prouty	General Dynamics IT
Lisa	Purinton	Alaska Department of Public Safety
Cary	Quinn	Thompson Reuters Special Services
Scott	Rago	Federal Bureau of Investigation
Kevin	Reid	Fusion Technology, LLC
Robyn	Richards	DHS/USCIS/Office of Fingerprint Liaison
Brian	Richardson	Maximus
John R.	Richter	Federal Bureau of Investigation
Dorothy	Riddle	Federal Bureau of Investigation
Renee	Rigby	Delaware State Police
Diana	Riley	Maryland State Police
Gabriel	Rios	Arizona Department of Public Safety
David	Roberts	SEARCH Group, Inc
Mark Jason	Roberts	Jacobs
Cody	Robinson	Federal Bureau of Investigation
Melinda	Rogers	DOJ Office of the Chief Information Officer
Evelyn "Lynn"	Rolin	South Carolina Law Enforcement Division
Megan	Root	Federal Bureau of Investigation
Allen	Rothbaum	Department of the Interior
Patricia	Russo	VMware
Derek	Sabatini	Los Angeles County Sheriff's Department
Flor Yesonia	Sandoval	USCIS/IRIS/IIMD
Julius	Santa Colombo	Federal Bureau of Investigation
Donnie	Sawin	CPI/Wilton Police Department NH
Charles I.	Schaeffer	Florida Department of Law Enforcement
Shelley	Scott	Louisiana State Police
Gary	Seder	Montana DOJ/DCI
Bryan	Sell	Federal Bureau of Investigation
Amanda	Shaffer	Federal Bureau of Investigation
Amanda	Shaffer	Federal Bureau of Investigation
Julianne	Shaffer	Federal Bureau of Investigation
Anil	Sharma	IBM

First	Last	Agency
Roger	Shaw	Federal Bureau of Investigation
Angela	Sheppard	Federal Bureau of Investigation
Monica	Shillingburg	Federal Bureau of Investigation
Marsha	Shockey	Federal Bureau of Investigation
Linda	Shriver	Federal Bureau of Investigation
Kate	Silhol	Nlets
Amanda	Silva	Nevada Department of Public Safety
Loretta	Simmons	Federal Bureau of Investigation
Elizabeth	Skinner	Federal Bureau of Investigation
Joan	Smith	Washington Association of Sheriff's and Police Chiefs
Samuel	Smith	Transportation Security Administration
Valerie	Smith	FBI Contractor
Danielle	Smith	Federal Bureau of Investigation
Jeff	Solomom	Secure Community Network
Douglas	Sprouse	Federal Bureau of Investigation
Rick	Stallings	Arkansas Crime Information Center
Robin	Stark-Nutter	Federal Bureau of Investigation
Corey R.	Steel	Nebraska State Court Administrator
Gary	Stroupe	Federal Bureau of Investigation
Carrie	Supko	Peraton
B. Scott	Swann	RankOne Computing
Erik	Swanson	BAE Systems
Richard	Swearingen	Florida Department of Law Enforcement
Edward	Talbert	IMTAS
Mark	Tanner	GDIT
William	Tatun	Diverse Computing
Don	Taylor	Peraton
Betsy	Taylor	Federal Bureau of Investigation
Barbara	Taylor	Federal Bureau of Investigation
Nicole	Tennant	Federal Bureau of Investigation
David	Tetrick	Federal Bureau of Investigation
James	Thatcher	National Background Check, Inc.
Sonya	Thompson	Federal Bureau of Prisons
Jeffrey	Tichinel	Federal Bureau of Investigation
Nikolay	Todorov	Federal Bureau of Investigation
John	Toothman	Federal Bureau of Investigation
Scott	Tousley	Splunk
John "Jay"	Town	Gray Analytics
Carol	Tracy	Women's Law Project
James	Travelstead	Federal Bureau of Investigation
R. Scott	Trent	Federal Bureau of Investigation
Antonio	Trindade	Dev Technology Group
Amaha	Tsegays	ECS
Garnet	Tucker	Federal Bureau of Investigation
Robert	Turnbaugh	Buchanan & Edwards
Keon	Turner	Virginia Department of State Police

First	Last	Agency
Tom	Turner	Virginia State Police
Brett	Van Anne	Idaho State Police
Angela	Vandergrift	Federal Bureau of Investigation
Melanie	Veilleux	Arizona Department of Public Safety
Derek	Veitenheimer	Wisconsin Department of Justice
Carey	Vereen	CACI, Inc.
Paul	Wagner	Federal Bureau of Investigation
Michael	Walker	John Jay College of Criminal Justice
Mary	Walker	Federal Bureau of Investigation
Brian	Wallace	Marion County Sheriff's Office
Jeffrey	Wallin	Vermont Department of Public Safety
Guy	Walton	Counterthreat Analysis Mitigation Ops, LLC
Ralph	Ward	Arkansas Crime Information Center - DPS
Dale	Watson	Booz Allen Hamilton
John "Chris"	Weatherly	Federal Bureau of Investigation
Jason	Webster	Department Of Homeland Security
Kellie	Weir	USCIS
Rhonda	Westbrook	Georgia Bureau of Investigation
Alicia	Wetzel	Federal Bureau of Investigation
Charlotte	Whitacre	First Responder Network Authority
Nathan E.	White, Jr.	American Judges Association
Patricia	Whitfield	Oregon State Police
Anthony	Wickersham	Macomb County Sheriff
Missy	Willett	Red Hat
Ida	Williams	Maryland State Police
Jackie	Williford	Imageware
Greg	Willmore	Utah Department of Public Safety
Renita	Wilson	IMTAS
Melissa	Winesburg	IJIS Institute
Michelle	Wingate	GuidePoint Security
Kathy	Witt	Office of the Fayette County Sheriff
Glenn	Wood	Oracle National Security Group
Joseph	Wright	Federal Bureau of Investigation
Michael	Yates	Federal Bureau of Investigation
John	Yearty	Peak Performance Solutions
Theodore	Yoneda	Federal Bureau of Investigation
Christi	Yost	Federal Bureau of Investigation
Richard	Zak	Microsoft
Paula	Zirkle	Federal Bureau of Investigation

**Criminal Justice Information Services (CJIS)
Advisory Policy Board (APB)
June 9, 2021
Orlando, Florida
Final Agenda**

Wednesday, June 9, 2021
9:00 a.m.

Board Convenes

Mr. Nicky J. Megna
Designated Federal Officer (DFO)
CJIS Division
Federal Bureau of Investigation

Roll Call

Sheriff Kathy Witt
APB Chair
Fayette County Sheriff's Office
Lexington, KY

Introduction of Attendees and Special Guests

Sheriff Witt

Welcoming Remarks

Mr. Michael F. McPherson
Special Agent in Charge – Tampa Field Office
Federal Bureau of Investigation

Chief Deputy Denise Demps
Orange County Sheriff's Office

Deputy Chief Jose Velez
Orlando Police Department

*No staff paper.

CJIS Advisory Policy Board
Wednesday, June 9, 2021

Item #1*

FBI Executive Briefings

Mr. Paul M. Abbate
Deputy Director
Federal Bureau of Investigation
Washington, D.C.

Science and Technology Branch Update
Mr. Darrin E. Jones
Executive Assistant Director
Federal Bureau of Investigation
Washington, D.C.

CJIS Division Update
Mr. Michael A. Christman
Assistant Director
Federal Bureau of Investigation
Clarksburg, WV

Item #2*

Tribal Task Force Update – Chair

Mr. William Denke
Chief
Sycuan Tribal Police Department
El Cajon, CA

Break

Item #3

Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee

Mr. Derek Veitenheimer - **Chair**
Wisconsin Department of Justice
Madison, WI

Lunch

*No staff paper.

CJIS Advisory Policy Board
Wednesday, June 9, 2021

Item #4*
Use of Force Update

Ms. Trudy Ford
Global Law Enforcement Support Section Chief
CJIS Division
Federal Bureau of Investigation

Item #5*
National Incident-Based Reporting System Transition Update

Ms. Ford

Item #6
Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

Mr. Brian Wallace - **Chair**
Chief Civil Deputy
Operations Division
Marion County Sheriff's Office
Salem, OR

Item #7*
NCIC 3rd Generation (N3G) Task Force Update

Mr. Jeffrey Wallin - **Chair**
Director
Vermont Crime Information Center
Vermont Department of Public Safety
Waterbury, VT

Break

Item #8
Chairman's Report on the National Data Exchange (N-DEx) Subcommittee

Ms. Carol A. Gibbs - **Chair**
Illinois State Police
Springfield, IL

*No staff paper.

CJIS Advisory Policy Board
Wednesday, June 9, 2021

Item #9

Chairman's Report on the Identification Services (IS) Subcommittee

Mr. Charles Schaeffer – **Chair**
Director
Criminal Justice Information Services
Florida Department of Law Enforcement
Tallahassee, FL

Item #10*

National Crime Prevention and Privacy Compact Council Report

Ms. Leslie Moore - **Chair**
Director
Information Services Division
Kansas Bureau of Investigation
Topeka, KS

Item #11

Chairman's Report on the Security and Access (SA) Subcommittee

Mr. Joseph Dominic - **Chair**
Criminal Justice Information Services
California Department of Justice
Sacramento, CA

Item #12*

Chairman's Report on the Compliance Evaluation (CE) Subcommittee

Captain Kyle Gibbs - **Chair**
Services Bureau Commander
Stillwater Police Department
Stillwater, OK

*No staff paper.

CJIS Advisory Policy Board
Wednesday, June 9, 2021

Item #13

**Chairman's Report on the National Instant Criminal Background Check System (NICS)
Subcommittee**

Ms. Lynn Rolin - **Chair**
Program Coordinator
Information Technology CJIS Liaison
South Carolina Law Enforcement Division
Columbia, SC

Item #14*

Chairman's Report on the Public Safety Strategy (PSS) Subcommittee
Mr. Schaeffer

Other Business

Adjourn

*No staff paper.

Intentionally Left Blank

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FL**

STAFF PAPER

APB ITEM #3

Report on the Uniform Crime Reporting (UCR) Subcommittee

UCR ISSUE #1* (*Info T*)
UCR Status Report

UCR ISSUE #2
Beyond 2021 Initiative Update – National Incident-Based Reporting System (NIBRS) Data Elements

UCR ISSUE #3
Beyond 2021 Update - Addition of Geolocation to NIBRS

UCR ISSUE #4
Expansion of Location Data Values within NIBRS Data Element 9 (Location Type)

UCR ISSUE #5
Addition of Data Elements to the NIBRS for the Collection of Lawful Access Data

UCR ISSUE #6
Expansion of Victim to Offender Relationship in NIBRS Data Element 35

UCR ISSUE #7
Addition of a New Criminal Offense in Progress Data Element in the NIBRS

UCR ISSUE #8 (*See APB Item #14, PSS Issue #7*)
Changes to Race Codes within the FBI UCR Program

UCR ISSUE #9
Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

UCR ISSUE #10
Creation of a NIBRS Offense Code Mapping Crosswalk Repository

UCR ISSUE #11**
Law Enforcement Suicide Data Collection Update

* Delivered with the information only staff papers
** No staff paper

UCR ISSUE #12

National Use-of-Force Data Collection Update

UCR ISSUE #13

Status of the NIBRS Transition

UCR ISSUE #14*

Beyond 2021 Task Force Update

UCR ISSUE #15* (*Info K*)

Fiscal Year 2020 Audit Results Summary

UCR ISSUE #16

Summary of Recently Conducted QAR Reviews

* Delivered with the information only staff papers

** No staff paper

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #2

Beyond 2021 Initiative Update – National Incident-Based Reporting System (NIBRS) Data Elements

PURPOSE

To present the proposed modifications to the NIBRS data collection recommended by the Beyond 2021 Task Force

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the Beyond 2021 Task Force recommended enhancements to NIBRS data and recommend a priority for these enhancements.

BACKGROUND

The Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program is working with stakeholders to create enhancements to crime data after the January 1, 2021 transition from a summary-based data collection to a NIBRS data collection. In 2019, the FBI UCR Program formed the Beyond 2021 Task Force to assist in the creation of the FBI UCR Program roadmap after the NIBRS transition is complete. The Beyond 2021 Task Force's purpose is to engage the stakeholder community through the Criminal Justice Information Services (CJIS) APB process. The FBI UCR Program is achieving this through the Beyond 2021 Task Force and its supporting Subject Matter Expert (SME) groups. The SME groups are charged with creating proposals for consideration by the Beyond 2021 Task Force that ensure the value of FBI UCR Program data are realized by all data submitters and consumers. The Beyond 2021 Task Force has developed actions and topics of interest for the purposes of review and prioritization within the UCR Subcommittee based on the proposals of the SME groups.

DISCUSSION AND ANALYSIS

The FBI UCR Program began using the NIBRS in 1989 to capture additional details within an incident to provide enhanced analytical value. Through the NIBRS, law enforcement agencies report on each offense and arrest within 28 offense categories consisting of 71 specific crimes, classified as Group A offenses, which are considered more serious offenses such as murder, rape, robbery. For each Group A offense, law enforcement collects administrative, offense, property, victim, offender, and arrestee information. In addition, law enforcement submits arrest data for 13 Group B offenses (less serious offenses such as loitering or driving under the influence). Law enforcement agencies use data elements and data values to report incident information to the FBI UCR Program. A data element is the smallest named item of data that conveys meaningful information or condenses a lengthy description into a short code. The NIBRS contains 58 data elements within each segment for a Group A and Group B incident report to describe the details of each component of an offense.

The information collected by law enforcement agencies evolves to meet the needs of the time, and NIBRS data is a by-product of law enforcement agencies' records management systems (RMS). As law enforcement evolves, so must offense codes and the data elements associated with those offenses. Through the work of the Beyond 2021 Task Force and its supporting SME groups, areas for enhancement within NIBRS offenses and the data elements collected when a law enforcement agency reports an offense to the FBI UCR Program have been identified. The goal of the recommended modifications below is to provide additional context surrounding incidents known to law enforcement, to assist the law enforcement, the research community, and the public when discussing crime data. The Beyond 2021 Task Force recommended modifications included for review can add value to crime data and assist law enforcement agencies across the nation in enhancing policies and procedures while providing a national overview of law enforcement data.

Specifically, the following recommended changes or additions will be discussed in this paper:

- Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment
- Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment
- Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment
- Expansion of Data – Collection of Injury Information on Homicide Victims
- Creation of a New NIBRS Offense – Criminal Negligence
- Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12)
- Modification of Data Element – Suspected Drug Type (Data Element 20)
- Modification of Data Element – Type Drug Measurement (Data Element 22)
- Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units
- Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Updates to Weapon Information Collected

Data Element 13 (Type Weapon/Force Involved) allows law enforcement agencies to indicate up to three types of weapons or force (or no weapons or force if applicable) used by an offender for certain offenses.¹ SME group members focused their discussion on providing additional detail to offenses and the weapons involved, specifically firearms. The Beyond 2021 Task Force and the supporting SME groups concurred on the value of expanding on the data collected beyond the use of a firearm during an incident in order to more fully assess and quantify additional dimensions to crimes associated with firearms. As this additional weapon information will be submitted for a subset of offenses, the enhancements associated with collecting additional weapon information should be collected as part of the NIBRS Offense Segment to ensure the information is associated with the offense. Additional information about the weapons involved in an offense and how those weapons are used when an incident occurs will provide additional context to incidents and provide additional information that can be analyzed to provide more information on crimes involving firearms.

Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

NIBRS allows law enforcement agencies to provide the type of weapon used, but agencies cannot specify how the weapon was used. For example, a law enforcement agency can report a firearm was used in the commission of a crime, but it is unknown whether the firearm was brandished, used as a blunt object, or discharged. The Beyond 2021 Task Force recommends adding the ability to collect firearm discharge information as a new data element within the NIBRS Offense Segment. The Task Force proposes the definition of discharge of a firearm as the following:

“Includes the intentional, unintentional, accidental, or negligent discharge of a firearm during the commission of a criminal incident, or to advance a criminal incident. Discharge requires the deliberate or unintentional pulling of a trigger or other action that result in the discharge of the weapon.”

When capturing firearm discharge information, law enforcement agencies will only capture information recorded as a criminal incident, within an RMS. The FBI UCR Program will provide direction to law enforcement on incidents of “shots fired.” Not all incidents require an incident report; therefore, these incidents will not be expected to be submitted to the NIBRS. However, if a “shots fired” incident requires an incident report based on agency protocol, the incident will be submitted for inclusion in NIBRS data as a weapon law violation and firearm discharge information will be collected.

¹ These offenses include Murder and Nonnegligent Manslaughter, Negligent Manslaughter, Justifiable Homicide, Kidnapping/Abduction, Rape, Sodomy, Sexual Assault with an Object, Fondling, Robbery, Aggravated Assault, Simple Assault, Extortion/Blackmail, and Weapon Law Violations.

Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

In addition to collecting information on whether the firearm used in an incident was discharged, the Beyond 2021 Task Force recommends adding an additional data element to record if the firearm used in the commission of an offense was stolen. If known to law enforcement, additional information on whether a firearm was stolen can be obtained by accessing the National Crime Information Center (NCIC) Gun File or potentially local records. The NCIC Gun File contains records of stolen weapons, recovered (abandoned, seized, or found) weapons, lost or missing weapons, or weapons that have been used in the commission of a felony. Law enforcement officers access the NCIC files when investigating an incident. If a weapon was used and has been logged in the NCIC Gun File or local records as stolen, law enforcement will be able to include this information in incident records within the agency records management system and the data submitted to the FBI UCR Program.

Firearm information may not be readily available to law enforcement. If a firearm was stolen and was not reported to law enforcement, or the information was not added to the NCIC Gun File for some reason (for example, due to an unknown serial number), then the weapon would not be in the NCIC Gun File. It would be the responsibility of the FBI UCR Program to provide guidance and message to data consumers that the information reported regarding stolen firearms within NIBRS is dependent upon whether the weapon was reported to law enforcement as stolen and its subsequent inclusion in the NCIC Gun File or local records, which can lead to underreporting of stolen weapon information.

Updates to Injury Information Collected

The NIBRS Victim Segment collects information including age, sex, and race of the victim of an offense. Law enforcement agencies are required to provide at least one victim for each NIBRS offense and can enter information for up to 999 victims per incident. When law enforcement agencies enter victim information using code I = Individual, and the NIBRS Offense Code falls within a specific set of offenses (Kidnapping/Abduction, Rape, Sodomy, Sexual Assault with an Object, Fondling, Aggravated Assault, Simple Assault, Extortion/Blackmail, Human Trafficking, Commercial Sex Acts, Involuntary Servitude), the law enforcement agency must enter information in Data Element 33 = Type Injury selecting one of the following categories:

- N = None
- B = Apparent Broken Bones
- I = Possible Internal Injury
- L = Severe Laceration
- M = Apparent Minor Injury
- O = Other Major Injury
- T = Loss of Teeth
- U = Unconsciousness

Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Currently within NIBRS, law enforcement agencies cannot report if the victim of an offense suffered a GSW. If the victim of an offense suffers a GSW, it is collected within the injury codes available, like internal injury or other major injury; however, GSW is not easily evident with the current NIBRS reporting methods. GSW is an option for injury information collected within the FBI UCR Program data collections of the Law Enforcement Officers Killed and Assaulted and the National Use-of-Force data collections. To provide uniformity across all FBI UCR Program data collections, the Beyond 2021 Task Force recommends adding a new injury code of G = Gunshot Wound on the NIBRS Victim Segment.

The new injury code of G = Gunshot Wound also would include incidents involving grazing or minor injuries received when the firearm was discharged. Adding the ability to report GSW as an injury code allows law enforcement agencies to provide additional insight into an incident. Specifically calling out GSW provides the ability for data users to determine the injuries incurred with a given incident and can provide researchers and law enforcement with additional information to use when analyzing crime data.

Collection of Injury Information on Homicide Victims

When entering victim information for a homicide offense, mandatory fields include victim age, sex, race, and the relationship to offender. Current UCR policy does not allow for the reporting of victim injury information. As previously noted, victim injury information is mandatory when entering information on nine NIBRS offenses; homicide is not a NIBRS offense requiring victim injury information.

The Beyond 2021 Task Force recommends adding the ability to collect injury information on homicide victims within NIBRS to provide additional context to homicide incidents. Law enforcement agencies would be required to ascertain injury information through evidence obtained or observed during the initial investigation and not rely on additional case information or manner of death obtained through court or medical records or a coroner's report.

Creation of a New NIBRS Offense – Criminal Negligence

The FBI UCR Program leveraged the Beyond 2021 Task Force to review the potential impact of implementing recommendations from the National Academy of Sciences – Modernizing Crime Statistics Study (NAS) to alleviate any potential gaps in crime reporting. An area of concern within the NAS was the inability for law enforcement agencies to capture in additional information related to offenses involving criminal negligence including situations of persons under care. Currently, offenses that fall into the category of Criminal Negligence are reported as either 90F – Family Offense, Nonviolent or 90Z – All Other Offenses depending on the circumstances surrounding the incident.

The Beyond 2021 Task Force recommends the addition of a new NIBRS category of Criminal Negligence. Law enforcement agencies will use the new NIBRS category to capture additional

offenses not specified within current NIBRS offenses such as elder abuse due to neglect, parental neglect and abandonment, and other criminally negligent acts that lead to the injury of a victim. Offenses that would fall within this category include acts of negligence in which the offender is aware of but ignores the risk to the victim. For instances of Criminal Negligence, the offender must have knowledge, or awareness, that the conduct will result in harm of the victim. Examples of incidents falling into the category of Criminal Negligence are elder abuse due to neglect, distracted driving resulting in injury, abandonment resulting in injury. The suggested definition for the new offense Criminal Negligence is derived from the Model Penal Code, which was developed as a guideline to standardize criminal law procedures. A potential definition is as follows:

Criminal Negligence – Causing substantial harm to another person through negligence. This includes instances in which an individual participates in an act that can cause substantial and unjustifiable harm to the victim.

Modification of Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS Offenses

Data Element 12 (Type Criminal Activity/Gang Information) indicates the criminal activity/gang involvement of the offenders of 18 NIBRS offenses. When reporting on any of these 18 offenses, law enforcement agencies can enter up to 3 data values of activity for the offense including:

- A = Simple/Gross Neglect (unintentionally, intentionally, or knowingly failing to provide food, water, shelter, veterinary care, hoarding, etc.) (*Only Animal Cruelty*)
- B = Buying/Receiving
- C = Cultivating/Manufacturing/Publishing (i.e., production of any type)
- D = Distributing/Selling
- E = Exploiting Children
- F = Organized Abuse (Dog Fighting and Cock Fighting) (*Only Animal Cruelty*)
- G = Other Gang (only violent crimes)
- I = Intentional Abuse or Torture (tormenting, mutilating, maiming, poisoning, or abandonment) (*Only Animal Cruelty*)
- J = Juvenile Gang (membership is predominantly juvenile [under 18 years of age])
- N = None/Unknown (mutually Exclusive)
- O = Operating/Promoting/Assisting
- P = Possessing/Concealing
- S = Animal Sexual Abuse (Bestiality) (*Only Animal Cruelty*)
- T = Transporting/Transmitting/Importing
- U = Using/Consuming

Law enforcement agencies also use this data element to describe the type, or lack of an offender's gang activity for eleven NIBRS offenses² while the remaining seven offenses³ allow

² Murder and Nonnegligent Manslaughter, Negligent Manslaughter, Kidnapping/Abduction, Robbery, Rape, Sodomy, Sexual Assault with an Object, Fondling, Aggravated Assault, Simple Assault, Intimidation

³ Counterfeiting/Forgery, Stolen Property Offenses, Drug/Narcotic Violations, Drug Equipment Violations, Gambling Equipment Violations, Pornography/Obscene Material, Weapon Law Information

for the reporting of the type of criminal activity. During discussions with the Beyond 2021 Task Force, members found value in expanding the values represented within Data Element 12 (Type Criminal Activity/Gang Information) and expanding the use of Data Element 12 (Type Criminal Activity/Gang Information) for use with all NIBRS offenses.

The Beyond 2021 Task Force recommends that Data Element 12 (Type Criminal Activity/Gang Information) should be available for all NIBRS offenses. The recommendation stems from the desire to collect as much information on each incident as feasible to add context to an incident. Adding the ability to capture Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS offenses provides an additional data point for review during analyses of crimes.

Modification of Data Element 12 (Type Criminal Activity/Gang Information) to Include Additional Values

Current UCR policy indicates that crimes that involve either “aiding/abetting” or “conspiracy” must be reported as an arrestee-only record under the category of *All Other Offenses*. In order to capture more complete information on criminal incidents involving these two potential types of criminal activity, the Beyond 2021 Task Force recommends that UCR policy allow for the reporting of the substantive offense connected to the incident. In addition, offenses involving aiding/abetting and conspiracy will be identified with the additional data values on NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include the following:

- A = Simple/Gross Neglect (unintentionally, intentionally, or knowingly failing to provide food, water, shelter, veterinary care, hoarding, etc.) (*Only Animal Cruelty*)
- B = Buying/Receiving
- C = Cultivating/Manufacturing/Publishing (i.e., production of any type)
- D = Distributing/Selling
- E = Exploiting Children
- F = Organized Abuse (Dog Fighting and Cock Fighting) (*Only Animal Cruelty*)
- G = Other Gang (only violent crimes)
- I = Intentional Abuse or Torture (tormenting, mutilating, maiming, poisoning, or abandonment) (*Only Animal Cruelty*)
- J = Juvenile Gang (membership is predominantly juvenile [under 18 years of age])
- N = None/Unknown (mutually Exclusive)
- O = Operating/Promoting/Assisting/**Abetting**
- P = Possessing/Concealing
- S = Animal Sexual Abuse (Bestiality) (*Only Animal Cruelty*)
- T = Transporting/Transmitting/Importing
- U = Using/Consuming
- W = Conspiracy**

Expansion of NIBRS Data Elements – Collecting Additional Drug Information

The Beyond 2021 Task Force reviewed the information collected within NIBRS drug incidents with two main objectives:

- Update NIBRS drug information to ensure the data collected is relevant and valuable to law enforcement.

- Ensure the data collected aligns with the inclusion of federal drug offenses.

To ensure the data is relevant, valuable, and uniform, the Beyond 2021 Task Force included representatives from the Drug Enforcement Administration (DEA) in SME group discussions regarding the drug information collected and reported by the FBI UCR Program. Based on these discussions, the Beyond 2021 Task Force makes the following recommendations to enhance the NIBRS drug information.

Modification of Data Element 20 (Suspected Drug Type)

Data Element 20 (Suspected Drug Type) identifies the types of drugs or narcotics seized in a drug case. Law enforcement agencies can report up to three types of drugs or narcotics per incident. The current data values available for entry are:

- A = Crack Cocaine
- B = Cocaine (all forms except Crack)
- C = Hashish
- D = Heroin
- E = Marijuana
- F = Morphine
- G = Opium
- H= Other Narcotics: Codeine; Demerol; Dihydromorphinone or Dilaudid; Hydrocodone or Percodan; Methadone; Pentazocine; Propoxyphene or Darvon; etc.
- I = LSD
- J = PCP
- K = Other Hallucinogens: BMDA or White Acid; DMT; MDMA; Mescaline or Peyote; Psilocybin; STP; Spice; Dronabinol; Marinol; etc.
- L = Amphetamines/Methamphetamines (includes Methcathinone)
- M = Other Stimulants: Adipex, Fastine, and Ionamin (Derivatives of Phentermine); Benzedrine; Didrex; Khat; Bath Salts; Methylphenidate or Ritalin; Phenmetrazine; Tenuate; etc.
- N = Barbiturates
- O = Other Depressants: Glutethimide or Doriden, Methaqualone or Quaalude, or Talwin; etc.
- P = Other Drugs: Antidepressants (Elavil, Triavil, Tofranil, etc.) Aromatic Hydrocarbons; Tranquilizers (Chlor diazepoxide or Librium, Diazepam or Valium, etc.); Steroids; etc.
- U = Unknown Type Drug
- X = Over 3 Types

Discussions with the Beyond 2021 Task Force focused on updating the NIBRS drug type information to ensure the data collected meets the needs of modern law enforcement and aligns with the data collected by the DEA to ensure uniformity amongst law enforcement agencies submitting data. The existing list of drug types has not been substantively updated since the NIBRS data collection was established in the late 1980s. To align with modern policing the suggested modifications include substances not previously included in the NIBRS suspected

drug values and expanding certain drug categories to include additional drug type information. Suggested additions to Data Element 20 (Suspected Drug Type) include the following:

- Amphetamine
- Benzodiazepine
- Cannabis/Marijuana
- Miscellaneous Depressants
- Fentanyl (and its generics)
- GHB/GBL/BD (and GHB Analogues)
- Hashish and Synthetic Cannabinoids
- Miscellaneous Hallucinogens
- Cocaine, Crack, etc.
- LSD
- Methamphetamine
- Heroin
- Oxycodone and other Licit Opioids
- Precursor Chemicals
- Khat and other Cathinones
- Steroids
- MDA/MDMA/MDE, ‘Ecstasy’
- Other Drug Types
- Unknown Drug Types
- Over 3 Drug Types

In addition to the modified substances collected, the Beyond 2021 Task Force recommends the FBI UCR Program collaborate with stakeholders to develop a process and schedule for assessing the NIBRS drug types for potential future modifications. Creating a schedule to reassess the drug types collected ensures the data collected is relevant and provides value to all stakeholders. In addition to regular updates to the list of drug types, the FBI UCR Program will provide a means to crosswalk older codes and categories to revised codes and categories to ensure that analytical utility will be maintained.

Modification of Data Element 22 (Type Drug Measurement)

Law enforcement agencies use Data Element 22 (Type Drug Measurement) to indicate the type of measurement used in quantifying drugs and narcotics seized in a drug case. Data Element 22 (Type Drug Measurement) can contain up to three entries that should correlate with the data values reported for Data Element 20 (Suspected Drug Type). Law enforcement agencies must enter data using these values:

<i>Weight</i>	<i>Capacity</i>	<i>Units</i>
GM = Gram KG = Kilogram OZ = Ounce LB = Pound	ML = Milliliter LT = Liter FO = Fluid Ounce GL = Gallon	DU = Dosage Unit (Number of capsules/pills/Tablets, etc. NP = Number of Plants (ex. Marijuana Plants)

As with Data Element 20 (Suspected Drug Type), the Beyond 2021 Task Force recommends modifying Data Element 22 (Type Drug Measurement) to ensure the data collected is relevant to modern policing and aligns with the information law enforcement is capturing within records management systems. The recommended modifications to data Element 22 (Type Drug Measurement) include:

<i>Weight</i>	<i>Capacity</i>	<i>Units</i>
MG = Milligram GM = Gram KG = Kilogram OZ = Ounce LB = Pound TN = Ton MT = Metric Ton	ML = Milliliter LT = Liter FO = Fluid Ounce GL = Gallon	DU = Dosage Unit PC = Pills, Capsules, etc. NP = Number of Plants (ex. Marijuana Plants) O = Other

Modification to FBI UCR Policy – Allowing Drug Quantities to be Converted to Common Units

To ensure consistency and continuity of data, the FBI UCR Program has historically converted specific data. For instance, the FBI UCR Program converts NIBRS data to historical Summary views. As part of the discussions on NIBRS drug information, the Beyond 2021 Task Force consulted with DEA staff to obtain information on how drug offense information is collected at a national level. Based on this research, the Beyond 2021 Task Force is recommending converging drug measures to common measures for publication and analytical purposes to ensure consistency within the data. The FBI UCR Program will use conversion tables established by the DEA as a reference for data users. Depending on the drug measurement type, the below common measures are recommended:

- Measures of mass/weight = grams
- Measures of volume/capacity = millimeters
- Measures of quantity = dosage units

Creation of New NIBRS Property Values – *Utilities and Services and Intellectual Property*

Data Element 15 (Property Description) allows law enforcement agencies to provide information on the type and value of property involved in incidents. Within NIBRS, law enforcement agencies can select from 82 potential data values when entering property information. During its analysis of the NAS study, the Beyond 2021 Task Force identified potential enhancements for the NIBRS Data Element 15 (Property Description) – *Intellectual Property* and *Utilities and Services*.

Based on review of the recommendations from the NAS, the addition of the property values *Intellectual Property* and *Utilities and Services* can provide additional information to stakeholders regarding crimes against property. Adding two new data values can provide additional insight to crimes across the nation, as these property values are often recorded within

the *O = Other* data value. Through conversations with SME group members, it was determined additional detail can alleviate overuse of the *O = Other* data value, and provide additional context surrounding property crimes.

IMPACT

The enhancements to NIBRS recommended by the Beyond 2021 Task Force will require technological and documentation enhancements for the FBI UCR Program as well as for state UCR programs. The FBI UCR Program will be required to add the ability to capture the additional data elements and adjust NIBRS business rules to ensure high-quality data outputs. State UCR programs also will be required to reprogram RMSs to capture the new data values. The FBI UCR Program also will be required to update all documentation, including the *NIBRS Technical Specification*, the *NIBRS User Manual*, and the *NIBRS XML Developer's Guide* to reflect the enhancements. In addition, audit and training processes will require modifications to accommodate the changes.

Proposed Timeline

The FBI UCR Program anticipates beginning implementation of the listed changes upon recommendation by the CJIS APB and approval by the FBI Director. While the FBI UCR Program is cognizant of the work within each state to meet the January 1, 2021, deadline for the NIBRS transition, there is a desire to implement all changes as soon as feasible to ensure the information is relevant to law enforcement and the stakeholder communities. Upon approval of the modifications, the FBI UCR Program will work to communicate enhancement implementation dates with all stakeholders. The FBI UCR Program will begin implementing any approved enhancements during calendar year 2022, with implementation for states beginning in calendar year 2023.

OPTIONS

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Option A1 – Add the ability to capture discharge of a firearm on the NIBRS Offense Segment.

Option A2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Option B1 – Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment.

Option B2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Option C1 – Create a new NIBRS injury code of Gunshot Wound to be added on the NIBRS Victim Segment. If approved, the new injury codes will be as follows:

- N = None
- B = Apparent Broken Bones
- G = Gunshot Wound**
- I = Possible Internal Injury
- L = Severe Laceration
- M = Apparent Minor Injury
- O = Other Major Injury
- T = Loss of Teeth
- U = Unconsciousness

Option C2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Option D1 – Add the ability to capture injury information for homicide victims within NIBRS.

Option D2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Option E1 – Create a new NIBRS Offense of *Criminal Negligence* to capture offenses not specified within current NIBRS offense definitions.

Option E2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Option F1 – Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to expand the collection of NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS offenses.

Option F2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Option G1 – Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include the additional values recommended by the Beyond 2021 Task Force. If approved, the additional values will be as follows:

- O = Operating/Promoting/Assisting/**Abetting**
- W = Conspiracy**

Option G2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Option H1 – Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force and create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.

Option H2 – Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force. Do not create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.

Option H3 – Do not modify NIBRS Data Element 20 (Suspected Drug Type) but create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.

Option H4 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Option I1 – Modify NIBRS Data Element 22 (Type Drug Measurement) to reflect the changes recommended by the Beyond 2021 Task Force.

Option I2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Option J1 – Modify FBI UCR Program policy to allow for the conversion of NIBRS drug quantities to common units proposed by the Beyond 2021 Task Force.

Option J2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Option K1 – Add the data values of *Intellectual Property* and *Utilities and Services* to NIBRS Data Element 15 (Property Description).

Option K2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Motion: To accept Option A1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Motion: To accept Option B1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Motion: To accept Option D1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Motion: To accept Option E1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Motion: To accept Option F1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Motion: To accept Option G1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Motion: To accept Option H1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Motion: To accept Option I1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Motion: To accept Option J1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Motion: To accept Option K1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Motion: To accept Option A2: No change. Consider updating the existing type of weapon/force used values to break out more specific firearm discharge values.
Action: Motion carried.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Motion: To accept Option B1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Motion: To accept Option D2: No change.
Action: Motion carried.

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Motion: To accept Option E2: No change.
Action: Motion carried.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Motion: To accept Option F1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Motion: To accept Option G1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Motion: To accept Option H1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Motion: To accept Option I1 as presented in the topic paper.
Priority 3M.
Action: Motion carried.

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Motion: To accept Option J1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Motion: To accept Option K1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Motion: To accept Option A1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Motion: To accept a New Option: Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment. Caveat of not mandatory. Priority 3M.

Action: Motion carried.

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Motion: To accept New Option: Add the ability to capture injury information for homicide victims within NIBRS. Caveat adding unknown. Priority 3M.

Action: Motion carried.

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Motion: To accept Option E1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Motion: To accept Option F2: No change.

Action: Motion carried.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Motion: To accept Option G2: No change.

Action: Motion carried.

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Motion: To accept Option H1 as presented in the topic paper. Priority 3H.

Action: Motion carried.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Motion: To accept Option I1 as presented in the topic paper. Priority 3H.

Action: Motion carried.

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Motion: To accept Option J1 as presented in the topic paper. Priority 3H.

Action: Motion carried.

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services and Intellectual Property*

Motion: To accept Option K1 as presented in the topic paper. Priority 3H.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Motion: To accept Option A1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Motion: To accept Option B1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Motion: To accept Option C1 as presented in the topic paper. Priority 3M

Action: Motion carried.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Motion: To accept new option: Add the ability to capture injury information for deceased victims within NIBRS. Priority 3M.

Action: Motion carried. Three nays, 1 abstain

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Motion: To accept Option E1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Motion: To accept Option F1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Motion: To accept Option G1 as presented in the topic paper. Priority 4L

Action: Motion carried.

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Motion: To accept Option H1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Motion: To accept Option I1 as presented in the topic paper. Priority 4M.

Action: Motion carried.

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Motion: To accept Option J1 as presented in the topic paper. Priority 4M.

Action: Motion carried.

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Motion: To accept Option K1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Motion: To accept Option A2: No change.

Action: Motion carried.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Motion: To accept Option B2: No change.

Action: Motion carried.

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Motion: To accept Option D2: No change.

Action: Motion carried. 1 Nay.

Issue E: Creation of a new NIBRS Offense – Criminal Negligence

Motion: To accept Option E2: No change.

Action: Motion carried.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Motion: To accept Option F1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Motion: To accept Option G1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue H: Modification of Data Element – Suggested Drug Type (Data Element 20)

Motion: To accept Option H1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Motion: To accept Option I1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Motion: To accept Option J1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Motion: To accept Option K1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SPRING 2021 UCR SUBCOMMITTEE ACTIONS:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Motion: To accept a New Option: Add a new code to an existing data element such as type of weapon for force used. Priority 3M.

Action: Motion carried. 3 Nays.

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Motion: To accept a New Option: Add a new code to an existing data element such as Type of Criminal Activity. Priority 3M.

Action: Motion carried. 1 Nay.

Issue C: Creation of a New Injury Code – Gunshot Wound (GSW) to be Recorded on the NIBRS Victim Segment

Motion: To accept Option C1 as presented in the topic paper. Priority 3M

Action: Motion carried.

Issue D: Expansion of Data – Collection of Injury Information on Homicide Victims

Motion: To accept Option D1: Add the ability to capture injury information for homicide victims within NIBRS. Priority 3M.

Action: Motion carried. 2 abstained.

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Motion: To accept Option E2: No change.

Action: Motion carried.

Issue F: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses

Motion: To accept Option F1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Motion: To accept Option G1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Motion: To accept Option H1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Motion: To accept Option I1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Motion: To accept Option J1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue K: Expansion of Data – Additional Property Values of *Utilities and Services* and *Intellectual Property*

Motion: To accept Option K1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #3

Beyond 2021 Update – Addition of Geolocation to the National Incident-Based Reporting System (NIBRS)

PURPOSE

Provide the recommendations of the Beyond 2021 Task Force for the implementation of geolocation as a data point within the NIBRS.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the approaches to integrate geolocation into the NIBRS data collection and provide a recommendation.

BACKGROUND

The Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program is working with stakeholders to create enhancements to crime data after the January 1, 2021 transition from a summary-based data collection to a NIBRS data collection. In 2019, the FBI UCR Program formed the Beyond 2021 Task Force to assist in the creation of the FBI UCR Program roadmap after the NIBRS transition is complete. The Beyond 2021 Task Force's purpose is to engage the stakeholder community through the Criminal Justice Information Services (CJIS) APB process. The FBI UCR Program is achieving this through the Beyond 2021 Task Force and its supporting Subject Matter Expert (SME) groups. The SME groups are charged with creating proposals for consideration by the Beyond 2021 Task Force that ensure the value of FBI UCR Program data are realized by all data submitters and consumers. The Beyond 2021 Task Force will develop actions and topics of interest for the purposes of review and prioritization within the UCR Subcommittee based on the proposals of the SME groups.

Calls for the addition of geolocation to NIBRS

While the addition of geolocation to the NIBRS incident has been brought forward by various entities since early implementation of NIBRS, the most recent example was from the National Academies of Sciences, Engineering, and Medicine Panel on Modernizing the Nation’s Crime Statistics (hereafter referred to as the Modernization Panel). During its tenure from 2013 to 2018, the Modernization Panel reviewed the data collected by the UCR Program as detailed in its charge and provided substantive and methodological recommendations for improvement. The Modernization Panel published its findings in two reports outlining a series of possible additions and improvements to the NIBRS data collection. The Beyond 2021 Task Force reviewed many of these recommendations to assess their potential value.

As part of the recommendations for new additions for NIBRS, the Modernization Panel requested the addition of incident geographic location as “ideally an appropriately anonymized latitude/longitude pair; otherwise, a geocode to some small-area geography such as census block or tract.”¹

DISCUSSION AND ANALYSIS

Many law enforcement agencies already publish crime incident information on agency websites or share it through open data portals, which set high expectations for the level of granularity for geolocation. The Law Enforcement Information Technology Standards Council (LEITSC) includes functional specifications for geolocation data to be captured on calls for service data, incident reporting data, and analytical data.² The functional requirements encourage the management of a master location file that includes possible addresses, range of addresses, or x/y/z (or latitude/longitude) coordinates. Mapping data to a point typically provides the most granular data available for geolocation of law enforcement data. As indicated by the Modernization Panel recommendation, an alternative to collecting point geographic data would be to associate the NIBRS incident with a smaller geographic area than the law enforcement jurisdiction.

Analytical Utility of Point Data

Law enforcement agencies perform geographic analysis on their own locally stored data in order to provide tactical and strategic insight into crime patterns and trends. The questions answered by geographic analysis range from tactical information that can lead to the arrest of an individual responsible for a series of crimes, to strategic resource questions related to the management of personnel and patrol areas. Based upon the 2016 Law Enforcement Management and

¹ National Academies of Sciences, Engineering, and Medicine. (2016) *Modernizing Crime Statistics: Report 1: Defining and Classifying Crime*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/23492>, p. 134.

² LEITSC (2003) *Standard Functional Specifications for Law Enforcement Records Management Systems (RMS)*. Downloaded on 11/2/2020, https://it.ojp.gov/documents/LEITSC_Law_Enforcement_RMS_Systems.pdf.

Administrative Statistics survey,³ about 45 percent of agencies had computerized crime analysis and mapping capabilities.

Beyond their own internal uses of geographic and crime data, many agencies provide this information to the communities they serve. Approximately 30 percent of agencies with a website provided the public with the ability to access crime statistics directly.⁴ While published resources generally acknowledge that there is a risk to privacy with the publication of mapped crime data, there is not an existing consensus regarding how to manage those concerns.^{5,6,7,8} In addition to providing geocoded crime data on their own websites, law enforcement agencies have also begun making operational data available through open data initiatives, such as the Police Data Initiative managed by the Police Foundation.⁹ Due to its operational nature, the law enforcement data published on public-facing open data websites may have differing ways of managing privacy issues connected to the dissemination of point data that diverge from the concerns of statistical use of law enforcement data as managed by the FBI UCR Program.

Risks to privacy

The details currently collected in the NIBRS incident include information on persons associated with the incident. These include victims, offenders, and arrestees. Within these person records, it may be possible to use the geographic location to discover the identity of these individuals. The potential discovery of identity could include special populations of individuals who have legal protections associated with the release of identifying information—for example, juvenile offenders. In addition, there could be concerns regarding the sensitive disclosure of victimization (such as victims of sex offenses) or disclosures that could potentially result in harm to individuals, as would be the case for informants or undercover personnel. In order to move forward with the proposal to add a method to collect geolocation that allows for the benefits of point location (latitude/longitude or x/y/z coordinates), the FBI Office of the General Counsel and the FBI UCR Program will need to include methods to minimize the potential risk of disclosure of an individual's identity. The geolocation that will be captured through this initiative will be the geolocation associated with the initial incident report. Any subsequent

³ United States Department of Justice (USDOJ). Office of Justice Programs (OJP). Bureau of Justice Statistics (BJS). Law Enforcement Management and Administrative Statistics (LEMAS), 2016. ICPSR37323-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [producer and distributor], 2020.

⁴ USDOJ. OJP. BJS. LEMAS, 2016. ICPSR37323-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [producer and distributor], 2020.

⁵ Harries, K. D. (1995). *Mapping crime: Principle and practice*. US Department of Justice, Office of Justice Programs, National Institute of Justice, Crime Mapping Research Center.

⁶ Leipnik, M. R., & Albert, D. P. (Eds.). (2002). *GIS in law enforcement: Implementation issues and case studies*. CRC Press.

⁷ Armstrong, M. P., & Ruggles, A. J. (2005). Geographic information technologies and personal privacy. *Cartographica: The International Journal for Geographic Information and Geovisualization*, 40(4), 63-73.

⁸ Kerski, J. J. GS-04-Location Privacy. Downloaded on 11/9/2020.

https://www.researchgate.net/profile/Joseph_Kerski/publication/308667976_Location_Privacy/links/584afcc308aecb6bd8c12731/Location-Privacy.pdf

⁹ <https://www.policedatainitiative.org/>

location information gathered by law enforcement (such as analysis of computer or handheld devices) will not be reported through NIBRS.

Publication and dissemination strategy will be key to mitigating the risks to privacy. Some of the options currently under review by the FBI would be that point data could be published with limited information. For example, only offense information, but no victim or offender information. The information regarding persons on a NIBRS incident could be presented in an aggregate format such as Census tract.¹⁰ If geolocation data is published in an aggregate format, the FBI is considering disseminating the most granular data under a restricted use dataset managed by a user agreement.

IMPACT

If the FBI moves forward with the addition of point location to the NIBRS incident, a suitable geographic coordinate system (for example, NAD83) will need to be selected for the technical specifications associated with point geographic data. Contributing agencies will need to transform geographic data into a single standard geographic coordinate system to ensure uniformity on a national scale. This transformation process would include geocoding incident-level data from address to a point location, and the state UCR Programs will need to assume responsibility for performing the address geocoding process. Geocoding relies upon a significant amount of local knowledge to resolve data quality issues associated with geocoding failures where the address is not clearly assigned to the correct point location and is best resolved at the most local level possible. If point geocoding is selected as the preferred option, consideration will be given to how the UCR Program should aggregate the data for publication and whether the UCR Program should pursue the release of the point data to vetted users under certain restrictions.

Point data provides for the most flexibility in terms of the types of spatial or geographic analysis that can be performed with it. However, point data has the highest potential for privacy impact.

An alternative to point geographic data that provides a higher level of privacy protections is geocoding NIBRS incident data to a small aggregate geographic area. Currently, UCR data can only be geographically attributed to the area assigned to the jurisdiction of the law enforcement agency. For example, the UCR data for a municipal law enforcement agency would be assigned to the geographic extent of the city it serves. One potential alternative is to identify areas that are smaller than the jurisdiction, but not as precise as the point location. Assigning the incident information to an aggregate area could introduce an aggregation effect (similar to what can sometimes be observed with “gerrymandering”) that might limit the types of analysis available to those using the data. In order to mitigate some of that potential impact to analytical utility, the proposed small area for this option would be the Census tract. The Census tract is a stable geographic area that provides for the best alignment of existing smaller areas for joining crime data with common correlates of crime from an approximately homogeneous population. If

¹⁰ Census tracts are small, relatively permanent statistical subdivisions of a county, which are uniquely numbered in each county with a numerical code.

<https://www2.census.gov/geo/pdfs/education/CensusTracts.pdf>

geocoding to a Census tract is the preferred option, the state UCR Program will need to be able to aggregate point data to a Census tract or work with agencies to assign incidents to a Census tract.

Regardless of the method selected, the FBI UCR Program will also be required to update all documentation, including the *NIBRS Technical Specification*, the *NIBRS User Manual*, the *NIBRS XML (Extensible Markup Language) Developer's Guide*, and the *NIBRS XML IEPD (Information Exchange Package Documentation)*.

Proposed Timeline

The FBI UCR Program proposes the implementation of geolocation in the NIBRS incident by no later than January 2023. This proposed implementation date allows the FBI UCR Program to present this recommendation through the Spring 2021 APB process for recommendation of approval by the FBI Director and conduct any additional analysis necessary prior to implementation. This start date also provides the FBI UCR Program with sufficient time to communicate with the Office of Management and Budget, the FBI Office of the General Counsel, and the stakeholder community.

OPTIONS

Option 1 – Pursue the addition of x/y/z (i.e., latitude/longitude) coordinates of the incident, but not address, to the NIBRS data collection. In order to implement this approach, the FBI UCR Program and the FBI Office of the General Counsel will need to detail a method to collect incident to a geographic point while also providing a dissemination strategy that addresses the risks to privacy.

Option 2 – Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract.

Option 3 – No change

RECOMMENDATION

The FBI UCR Program recommends the addition of geolocation to the NIBRS incident. Assuming privacy risks can be addressed by the FBI Office of the General Counsel, the FBI UCR Program recommends the collection of point geolocation on the NIBRS incident captured as x/y/z (i.e., latitude/longitude) coordinates. The final policy for the collection of this data will also address situations where there is an indeterminate geolocation (such as sometimes occurs with cyber offenses). The FBI UCR Program would appreciate input regarding the possible use of user agreements to manage the release of point-level data as a restricted use dataset.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 3: No change.
Action: Motion carried. 2 opposed

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: Pursue the addition of x/y/z (i.e., latitude/longitude) coordinates of the incident, but not address, to the NIBRS data collection. In order to implement this approach, the FBI UCR Program and the FBI Office of the General Counsel will need to detail a method to collect incident to a geographic point while also providing a dissemination strategy that addresses the risks to privacy. Priority 3M.
Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 2: Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract. Priority 3M.
Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 3: No change.
Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2: Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract.
Action: Motion carried.

SPRING 2021 SUBCOMMITTEE ACTIONS:

UCR SUBCOMMITTEE ACTION:

Motion: To accept Option 2: Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract. Priority 3M.
Action: Motion carried. 1 Nay/2 Abstain.

PSS SUBCOMMITTEE ACTION:

Motion: To accept Option 2: Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract.
Action: Motion carried. 2 Nays.

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #4

Expansion of Location Data Values within National Incident-Based Reporting System (NIBRS) Data Element 9 (Location Type)

PURPOSE

Present proposal to implement changes and expansion to the Valid Data Values for NIBRS Data Element 9 (Location Type).

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Respectfully request the review and approval of the proposed expansion, and modifications, to the NIBRS Data Element 9 (Location Type).

BACKGROUND

Implemented to improve the overall quality of crime data collected by law enforcement, NIBRS captures details on each single crime incident—as well as on separate offenses within the same incident—including information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in crimes. NIBRS goes much deeper because of its ability to provide circumstances and context for crimes like location, time of day, and whether the incident was cleared.

When reporting an incident to the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program, the “location type” is used to indicate the type of location where each offense took place; however, only one location type may be entered for each NIBRS offense. To ensure accurate and consistent reporting within the NIBRS, every effort has been made to ensure applicable selections for all data elements are available to submitters. Currently, there are 58 Valid Data Values (VDVs) for Data Element 9 (Location Type). If more than one of the data values associated with a data element could apply to the situation, agencies are instructed to use the most specific one applicable to the incident. Because the geographic location of an incident

is not always the same as the functional location of the incident, the FBI UCR Program relies on the law enforcement agency (LEA) to report the most appropriate location type.

DISCUSSION AND ANALYSIS

The FBI UCR Program strives to provide many possible options which could exist within the data elements collected in a NIBRS incident. Recent events have provided additional suggestions for Data Element 9 (Location Type).

Without any Geographic Information System coordinate, or postal address data field(s) collected in the NIBRS, the “Location Type” is a key mandatory data element for law enforcement (federal, state, county, city, university and college, and tribal agencies). The location type allows a LEA to most accurately report the location where crimes in their jurisdiction are physically located. More exact crime location options could provide enhanced accuracy and assist criminal justice agencies in creating user-friendly data visualization projects and publicly available crime trend analyses. Further differentiation of location types would also maximize the granularity of NIBRS data, especially as it becomes the national standard for 18,000 law enforcement agencies and their records management systems. For example, a more comprehensive snapshot of an incident could be depicted with a location of Marijuana Dispensary than with the location of a Specialty Store. While each would be appropriate, an entry of Marijuana Dispensary would provide more valuable insight than an entry of Specialty Store. While the use of Data Value 25=Other/Unknown can be used to denote location data not otherwise specified, additional options could diminish vagueness and provide useful context to local/state crime analysts, criminologists, and citizen consumers.

Based upon NIBRS training to sworn officers, fulfilling public data requests, and completing crime data analysis, the Missouri UCR Program recently identified a concern in the location code options for a reportable incident. The FBI UCR Program found a large majority of location types, in which crimes most frequently occur, are currently reported either under a different, loosely associated location type, or under the generic “25=OTHER UNKNOWN” category. As the NIBRS is dedicated to reflecting accurate data elements of an incident, a recommendation to expand Data Element 9 (Location Type) has been requested. The following table reflects suggestions made by the Missouri UCR Program manager, as well as additional descriptors and coding. The recommendation has been made to amend the existing NIBRS Data Element 9 (Location Type) to include:

CODE	VALID DATA VALUE	DESCRIPTOR	COMMENTS
9	Drug Store/Pharmacy	Store where the Food and Drug Administration approved medicinal drugs are dispensed and sold.	Exists in NIBRS Technical Specification with other VDV's under same code.
59	Auto Salvage/Junkyard	Location where unusable vehicles or vehicle parts can be bought, sold, or stored. a place where scrap is collected before being recycled or discarded.	
60	Carport/Garage/Driveway	An area around residential space not constituting a residential structure.	

61	Cemetery	An area set apart which contain graves, tombs or funeral urns.	
62	Doctor's Office	A medical facility in which one or more medical doctors, usually general practitioners, receive and treat patients.	
63	Gym/Fitness Club	Indoor club, building, or large room where people exercise or participate in indoor sporting activities to enhance physical fitness.	
64	Golf Course	Outdoor areas of land where golf is played.	
65	Hospital	An institution providing medical and surgical treatment and nursing care for sick or injured people	Routine, preventative, and scheduled care would be included in Doctor's Office. This would include urgent care facilities and inpatient behavioral health centers.
66	Library	Room or building containing collections of books, periodicals, software programs, films, or recorded music for people to read, borrow, or utilize as reference.	
67	Loan/Cash Advance/Check Cashing Facility	Commercial business where individuals obtain financial services over the counter for a clear fee.	Specialty Store denotes "retail" element. These stores are not considered retail stores and are becoming more prevalent.
68	Marijuana Dispensary	Establishment primarily used for selling medical or recreational marijuana.	Specialty Store denotes "retail" element. These stores are not considered retail stores and are becoming more prevalent.
69	Marijuana Facility	Indoor or outdoor site used for the commercial production and harvesting of cannabis for recreational or medical use.	This is a facility for the manufacture of the product – not a sales facility.
70	Movie Theater	Venue where movies are shown for public entertainment.	
71	Museum	Building in which objects of historical, scientific, artistic, or cultural interest are stored and exhibited.	
72	Pawnshop	Commercial establishment for lending money in exchange for personal property which can be sold if the loan is not repaid by a predetermined time.	
73	Public Transportation	Busses, trains, subways, and other forms of transit which charge set fares, run on fixed rates, and are available to the public.	Incidents which happen on public modes of transportation cannot be considered a static location – need an option to distinguish this.
74	Tattoo Parlor	Place in which the primary function is professional tattooing.	
75	Zoo	Indoor or outdoor establishment, which maintains a collection of wild animals	

		for study, conservation, or display to the public.	
--	--	--	--

When considering the inclusion of these modifications and additional location codes, the FBI UCR Program must consider the ability of state UCR Programs to make system changes due to limited resources, capability to retain local agencies and personnel, and the means of the UCR Program to recreate and disseminate reporting information. The FBI UCR Program must also consider the impact to direct-contributing law enforcement agencies.

OPTIONS

The FBI UCR Program suggests the following options for consideration:

Option 1 – Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the chart. The provided changes include a modification of existing Location Code 09=Drug Store/Doctor’s Office/Hospital code to be separated into three individual Location Types: 09=Drug Store/Pharmacy, 62=Doctor’s Office, and 66=Hospital. These changes will be effective immediately upon approval.

Option 2 – Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the chart. The provided changes include a modification of existing Location Code 09=Drug Store/Doctor’s Office/Hospital code to be separated into three individual Location Types: 09=Drug Store/Pharmacy, 62=Doctor’s Office, and 66=Hospital. The implementation will be included as part of the Beyond 2021 effort. All changes will be incorporated into the Beyond 2021 schedule accordingly.

Option 3 – No change

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: __ (enter High, Medium, or Low).

RECOMMENDATION

The FBI UCR Program proposes Option 2 to implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type). The implementation will be made in accordance with the Beyond 2021 project efforts by no later than January 2023. This proposed implementation date allows the FBI UCR Program to present this recommendation through the full Spring 2021 APB Process, acquire Director approval, and conduct any additional analysis necessary prior to implementation. The proposed start date allows a year for states and agencies to implement the changes and, provides the FBI UCR Program with sufficient time to communicate with the Office of Management and Budget, the FBI Office of the General Counsel, and the stakeholder community.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 2 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 2 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 2 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 2 as presented in the topic paper. Priority 4M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Motion: To accept Option 2 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #5

Addition of Data Elements to the National Incident-Based Reporting System (NIBRS) for the Collection of Lawful Access Data

PURPOSE

Present options for adding Lawful Access data elements to the NIBRS data collection.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to agmu@leo.gov

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information included in this paper and choose an option regarding the addition of Lawful Access specific data elements to the NIBRS data collection.

BACKGROUND

Recently, society has experienced a fundamental shift in the communications and personal data device industries resulting in increased encryption of electronic information. The increased use of encryption results in law enforcement's inability, in criminal and national security investigations, to obtain needed evidence and intelligence pursuant to lawfully obtained access. The ability of law enforcement to access and collect information pursuant to legal authority and lawfully obtained access, in support of justice and public safety, is being impacted by segments of industry that design, develop, and deploy services and technologies with strong encryption. The increased use of strong encryption inhibits law enforcement's ability to lawfully access data on electronic devices and platforms. In response to law enforcement's description of these challenges to law makers, Congress routinely requests a quantitative assessment. In other words, they want to know how bad the problem is. However, a uniform, nationally representative count of these occurrences does not currently exist.

The effects of strong encryption on law enforcement investigations can be broken down into the following categories:

- Data at Rest – Inability to access the plain text of data stored on a commercial consumer device or system (or cloud) due to encryption (e.g., mobile devices/phones, encrypted hard drives, or thumb drives).
- Data in Motion – Inability to access the plain text of data in transit (intercepted) due to impenetrable encryption (e.g., Services such as WhatsApp, Signal, Telegram or others).
- Non-compliant Providers – No apparent technical means of assisting law enforcement, or processes that result in significant or indefinite delays to accessing potential evidence for investigations

Past efforts to collect quantitative and qualitative data on lawful access challenges have presented several issues. In 2016, the FBI, in coordination with law enforcement associations, began a statistical collection asking law enforcement agencies to submit data related to a variety of lawful access impediments. However, since approximately 2018, the statistical collection has ceased to provide useful statistical data. In April 2020, the FBI Office of Partner Engagement initiated an effort to survey National Law Enforcement Telecommunication System agencies regarding encounters with encryption, but only received a small number of responses. The FBI and other federal, state, and local law enforcement continue to collect qualitative case examples that highlight lawful access challenges, but these are very resource intensive and are often un-releasable until after adjudication – sometimes years later.

Organizations representing federal, state, and local prosecutors, chiefs, sheriffs, and officers, and the Association of State Criminal Investigative Agencies have sent numerous jointly authored letters to lawmakers in support of varying pieces of proposed legislation to combat this issue. The FBI has been speaking publicly about this issue since 2009, and as recently as December 2019, the International Association of Chiefs of Police adopted a resolution for the *Worldwide Call for Legislation and/or Appropriate Regulation That Mandates Encryption Implementation Regimes That Maintain Reasonable Security of Communications and Stored Data, yet Permit Lawful Access by Law Enforcement Pursuant to the Rule of Law*.

In September 2020, representatives from the FBI’s National Domestic Communications Assistance Center presented the topic of Lawful Access to the CJIS APB Executive Committee, followed by presentations to the Uniform Crime Reporting (UCR) and Public Safety Strategy Subcommittees. The UCR Subcommittee recommended that a subject matter expert (SME) group be formed to explore how best to capture this information within the FBI’s UCR Program. With the existing data sharing infrastructure and an advisory board made up of data contributors, the FBI UCR Program is well positioned to support the collection of this emerging data need.

ANALYSIS

Following the recommendation from the UCR Subcommittee, the FBI established a Lawful Access SME Group comprised of representatives from all levels of law enforcement (federal, state, local) and the CJIS APB, as well as the Association of State Criminal Investigative Agencies. The focus of the group was to assist with the analysis and finalization of a topic paper to present options for adding the collection of lawful access data to the NIBRS data collection.

Before developing options for consideration, the SME group focused on building the case for this collection by ensuring the problem was clearly defined, as well as the potential outcomes or value to be realized once this data has been collected. Over several months, the group met formally on three occasions as well as numerous individual engagements to ensure the paper was able to clearly define the “what”, “why”, and “how” for the addition of this data to NIBRS.

The SME group settled on the following outcomes as to “why” to collect this data from contributors at all levels of law enforcement;

- Determine the level of impact that this problem is having on all levels of law enforcement and provide the information to lawmakers and the public.
- Quantify the potential impact to investigations due to the continued encounters with encrypted devices/transmissions.
- Provide metrics on occurrences and examples of impact to law makers in the attempt to generate legislation to combat this lack of lawful access.
- Enable the changing of laws to combat this issue, potentially saving lives, preventing crimes, reducing victimization, and exonerating the innocent.

Although it is clear through discussion with SME group members that encounters with encrypted stored data devices and/or communications applications are frequent and becoming more frequent, it remains unclear at what level, if any, these encounters are being tracked and measured at each law enforcement agency. It is anticipated that the technical implementation of the ability to collect lawful access information will need to be accomplished in conjunction with the definition of and changes to law enforcement agency business processes and policies to support the reporting and collection of this information. The SME group considered these impacts as it decided which data points to collect, and where in the NIBRS submission to collect them to maximize the value and potential additional utility of the data.

DISCUSSION AND IMPACTS

The Lawful Access SME Group determined that adding three data elements to both the victim and offender segments of the NIBRS submission was the best possible solution for data collection. Additional options for collecting lawful access at the administrative and offense segments were discussed, but it was determined these segments would miss the ability to associate an inaccessible encrypted device with a victim (such as a murder victim with an encrypted phone) or an offender. The SME group concluded adding new data elements to the victim and offender segments provided the best insight into the lawful access issues and a greater ability to associate encryption encounters with offenses, victims, and offenders.

Adding three data elements to both the Victim and Offender Segments of the NIBRS data collection

This option will add three data elements to both the Victim and Offender Segments of the NIBRS data collection. The first data element would indicate if encryption was encountered with a yes/no response option. The second and third data elements would indicate on which type of medium the encryption was encountered.

DATA ELEMENT (DE) XX – Encryption Encountered

- Yes
- No
- N/A

DE YY – If DE XX is yes, select the stored data device involved (select all that apply):

- iPhone
- Android
- Hard Drive
- Removeable Media
- Other
- None

DE ZZ – If DE XX is yes, select the communications applications involved (select all that apply):

- WhatsApp
- Apple iMessage
- Apple FaceTime
- Facebook Messenger
- Signal App
- Telegram App
- Snap Chat
- Other
- None

Benefits of adding data elements to the victim and offender segments:

- Indicates if the encryption encountered was associated to a Victim or Offender.
- Allows for association of the offense to the encryption encountered.
- New data elements and associated data values to address congressional requests for quantitative assessment.
- Enables further analysis of types of crime, details of the incident, and outcomes associated with encryption encounters.
- Victim perspective is also useful for advocacy groups.

Disadvantages of adding three data elements to NIBRS:

- Implementation time (18 to 24 months, possibly longer).
- Medium-High Impact - Complexity of business rules to address victim and offender information. (Example: Will the collection be limited to individual victim types?)

OPTIONS FOR COLLECTING LAWFUL ACCESS DATA

Option 1 – Add three data elements to both the Victim and Offender Segments of the NIBRS data collection.

Option 2 – No change.

RECOMMENDATIONS

The FBI and the Lawful Access SME Group propose Option 1 – Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. The impact to participating data providers implementing this option is anticipated to be medium-high based on the need for system and business process changes and additions. Option 1 maximizes the value of this new data by both addressing congressional requests for quantitative assessment and enabling further analysis of types of crime, details of the incident, and outcomes associated with encryption encounters.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 2: No change.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept a New Option: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Caveat to create process to update the data values within data elements.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Priority 3M.

Action: Motion carried. 3 Nays.

Action Item: Request the UCR Program clearly define data element DE XX - Encryption Encountered. Consider changing description to Encryption Resistance.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Motion: To accept a New Option: To have the UCR Program identify a collection mechanism outside of the NIBRS data file that leverages the UCR Program data collection infrastructure. Priority 3H.

Action: Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #6

Expansion of Victim to Offender Relationship in National Incident-Based Reporting System (NIBRS) Data Element 35

PURPOSE

To present a proposal for additions to the acceptable codes within NIBRS Data Element 35 to allow for new victim values with NIBRS

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the additional victim codes for NIBRS Data Element 35

BACKGROUND

The Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program received a request from a state UCR Program manager to develop additional values for NIBRS Data Element 35. Data Element 35 reports the relationship of the victim to the offender in incidents involving crime against persons or property. There were two changes recommended to the FBI UCR Program involving Data Element 35, and each proposed change will be addressed separately within this paper.

Issue A: Addition of “FP=Victim was Foster Parent” and “FC=Victim was Foster Child”

A crime committed by a foster parent against his/her child may be reasonably reported by a local Law Enforcement Agency (LEA) to have NIBRS victim-to-offender relationship of “CH=Victim was Child,” “OF=Victim was other family member,” or “OK=Victim was Otherwise Known.” Similarly, a crime committed by a foster child against his/her foster parent may be reasonably reported by a local LEA to have a NIBRS Victim-to-Offender relationship of “PA=Victim was Parent,” “OF=Victim was other family member,” or “OK=Victim was Otherwise Known.”

Issue B: Addition of “CO=Cohabitant (non-intimate relationship)

At the discretion of a law enforcement agency and taking the possible living arrangement and structures into consideration, a violent or property crime committed by one roommate against another could be reported in NIBRS as a Victim-to-Offender type of “OK=Victim was Otherwise Known,” “AQ=Victim was Acquaintance,” “FR=Victim was Friend,” or “NE=Victim was Neighbor”.

DISCUSSION AND ANALYSIS

Issue A

Within NIBRS, “OK=Victim was Otherwise Known” is the current option for NIBRS Data Element 35 in the scenario of a foster child/parent victim. However, this code does not accurately reflect the relationship between a foster parent and foster child. A description value for Foster Child and Foster Parent would allow the FBI UCR program to utilize the granularity within NIBRS to ensure proper interpretation of this scenario within the victim segment. It also creates collection uniformity in relation to other NIBRS values such as “SP=Victim was Stepparent,” “SC=Victim was Stepchild,” “SS=Victim was Stepsibling.” States may also consider crimes against foster children and foster parents as domestic related. Some states use NIBRS Data Element 35 responses to filter out domestic-related incidents. These states, such as Missouri, do not consider “OK=Victim was Otherwise Known” to indicate domestic-related incidents.

Solution - Create values of “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” for Data Element 35.

In creating this additional value to track a dissimilar attribute from others present in Data Element 35, there is a need to provide a solution for how this value will be mapped to the Summary Reporting System (SRS) when NIBRS conversion takes place. Based on the nature of this relationship, the most appropriate solution would be to map “FP” and “FC” to the Summary Homicide Report value of “Other-Known to Victim” in SRS.

Issue B

It is important to maximize use of the granularity of NIBRS data, especially as it becomes the national standard for 18,000 LEAs and their record management systems. While the values of “OK=Victim was Otherwise Known,” “AQ=Victim was Acquaintance,” “FR=Victim was Friend,” or “NE=Victim was Neighbor” do vaguely reflect the relationship between roommates or housemates living together, it does not take advantage of the collection capabilities present in NIBRS.

Solution - Create a value of “CO=Cohabitant (non-intimate relationship) for Data Element 35.

Based on the nature of this relationship, the most appropriate solution would be to also map CO=Cohabitant (non-intimate partner) to “Other-Known to Victim” for the purpose of NIBRS conversion.

IMPACT

State UCR Programs would have to incorporate the new “FP”, “FC”, and “CO” data values into Data Element 35 of their state NIBRS repositories, as well as share the new code titles, code number/letters, definitions, and implementation data with their local law enforcement submitters.

OPTIONS

Issue A

Option A1 – Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35.

Option A2 – No Change

Issue B

Option B1 – Create value “CO=Cohabitant (non-intimate relationship) and make allowable for NIBRS Data Element 35.

Option B2 – No Change

RECOMMENDATION

The FBI UCR Program recommends option A1 and B1.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Issue A

Motion: To accept Option A1: Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

Issue B

Motion: To accept Option B1: Create value “CO=Cohabitant (non-intimate relationship) and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Issue A

Motion: To accept Option A1: Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

Issue B

Motion: To accept Option B1: Create value “CO=Cohabitant (non-intimate relationship) and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Issue A

Motion: To accept Option 1: Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. Priority 3H.

Action: Motion carried.

Issue B

Motion: To accept Option 1: Create value “CO=Cohabitant (non-intimate relationship) and make allowable for NIBRS Data Element 35. Priority 3H.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Issue A

Motion: To accept Option A1: Create values “FP= Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. Priority 4M.

Action: Motion carried.

Issue B

Motion: To accept Option B1: Create value “CO=Cohabitant (non-intimate relationship) and make allowable for NIBRS Data Element 35. Priority 4L.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Issue A

Motion: To accept Option A1: Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

Issue B

Motion: To accept Option B1: Create value “CO=Cohabitant (non-intimate relationship) and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

SPRING 2021 UCR SUBCOMMITTEE ACTIONS:

Issue A

Motion: To accept Option A1: Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion carried.

Issue B

Motion 2: To accept a New Option: Create value “CO=Cohabitant (non-intimate/nonfamily relationship) and make allowable for NIBRS Data Element 35. Priority 3M.

Action: Motion Carries. 1 Abstain.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #7

Addition of a New Criminal Offense in Progress Data Element in the National Incident-Based Reporting System (NIBRS)

PURPOSE

To present a proposal to create a new data element to track criminal offenses in progress when a justifiable homicide takes place.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the creation of a new data element to track criminal offenses in progress when a justifiable homicide takes place.

BACKGROUND

The Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program received a request from a state UCR program manager concerning the ability of NIBRS data to track the criminal offense in progress during the event of a justifiable homicide. Pursuant to the NIBRS Technical Specification (v2019.2.1) and Error 266, “when a justifiable homicide is reported, no other offense may be reported in the Group A Incident Report. These should be submitted on another Group A Incident Report.” This means justifiable homicides by officers or citizens are required to be separate in NIBRS from the criminal offense that resulted in the justifiable homicide. In addition, while Data Element 32 (additional justifiable homicide circumstances) provides some explanation of the underlying event, it does not include the ability to report the actual offense being committed at the time of officer or citizen intervention, such as murder, rape, sodomy, sexual assault with an object, robbery, aggravated assault, or kidnapping.

DISCUSSION AND ANALYSIS

Due to the justifiable homicide and underlying criminal offense being separated by NIBRS incident numbers, the situational context of the events leading up to the justifiable homicide are lost for the national and state-level research, crime analysis, and public safety reports.

While such correlations are currently available in the Summary Reporting System (SRS), there is no linkage in NIBRS between a justifiable homicide and the crime occurring at the time such grave action is taken by an officer or citizen acting in self-defense. With the participation in the FBI National Use-of-Force Data Collection being a voluntary local agency-by-agency decision, the law enforcement community needs a standardized mechanism to study which offenses (and additional victim/offender/weapon/location demographics) tend to lead to justifiable homicides.

In response to this dilemma, it is recommended an additional data element be created for NIBRS that will allow for Law Enforcement Agencies to connect the criminal offense that was in progress (regardless of whether that offense was attempted or completed) to the event of a justifiable homicide. It is recommended the NIBRS Data Element 32 be restructured to allow for a second element to collect this information. This would take the form of the following:

- Data Element 32A (Additional Justifiable Homicide Circumstances)
- Data Element 32B (Criminal Offense in Progress)

Data Element 32A would retain the same acceptable data values currently listed. Data Element 32B would be coded to allow acceptable values for all crimes against persons and crimes against property offenses.

The National Use-of-Force Data Collection currently collects data on incidents of law enforcement uses of force in the line of duty. This includes instances of justifiable homicide. When an agency reports a justifiable homicide to the National Use-of-Force Data Collection, they have the option of reporting the criminal offense in progress at the time of the officer's or civilian's action. The National Use-of-Force Data Collection also allows participating agencies to link NIBRS incident numbers to a use-of-force incident. If an agency reported a justifiable homicide to the National Use-of-Force Data Collection and reported the criminal offense in progress when the justifiable homicide took place in a NIBRS incident, then the NIBRS incident number could be listed on the Use-of-Force report to link the two incidents for further reference.

IMPACT

State UCR Programs would have to implement the NIBRS Technical Specifications change to their repositories, as well as provide technical guidance and a planned implementation date to all local law enforcement partners and associated vendors.

OPTIONS

Option 1 – Change the name of Data Element 32 to “Data Element 32A” and create a new data element of 32B (Criminal Offense in Progress) with acceptable values for all crimes against

persons and crimes against property offenses. This new data element would be mandated only when a justifiable homicide has taken place.

Option 2 – Create a new data element for “Criminal Offense in Progress” with acceptable values for all crimes against persons and crimes against property offenses. This would include no changes to Data Element 32. This new data element would be mandated only when a justifiable homicide has taken place.

Option 3 – No change.

RECOMMENDATION

The FBI UCR Program recommends option 1, which will require the least amount of burden on UCR contributors and maximize data collection efficiency.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 3: No change.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Motion: To accept Option 3: No change.

Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #9

Beyond 2021 Initiative Update – Revision to National Incident-Based Reporting System (NIBRS) Sex Offense Nomenclature

PURPOSE

To present the proposed modifications to the NIBRS data collection recommended by the Beyond 2021 Task Force.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the Beyond 2021 Task Force recommended enhancements to NIBRS data and recommend a priority for these enhancements.

BACKGROUND

In April 2019, the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program received a Criminal Justice Information Services (CJIS) APB process topic request to examine the NIBRS sex offense definitions. Citing inconsistencies between the verbiage and collection methods of the Summary Reporting System (SRS) and NIBRS data collections, the request included suggested enhancements to ensure no data is lost with the January 1, 2021, transition to NIBRS. The request included the below modifications:

- Replace the NIBRS rape definition with the 2012 revised SRS rape definition.
- Discontinue the categories of “sodomy” and “sexual assault with an object.”
- Replace the term “fondling” with “unwanted sexual contact.”
- Replace “incest” and “statutory rape” with more appropriate terms.
- Create an additional category of “other sex crimes.”

This request was received as the FBI UCR Program was initiating the Beyond 2021 Initiative, a collaborative effort with stakeholders creating enhancements to crime data after the

January 1, 2021, transition from a summary-based data collection to a NIBRS data collection. The Beyond 2021 Task Force's purpose is to engage the stakeholder community through the CJIS APB process. The FBI UCR Program is achieving this through the Beyond 2021 Task Force and supporting Subject Matter Expert (SME) groups. The Beyond 2021 Task Force is responsible for creating the FBI UCR Program roadmap after the NIBRS transition. The SME groups are charged with creating proposals for consideration by the Beyond 2021 Task Force that ensure the value of FBI UCR Program data are realized by all data submitters and consumers. Due to the timing, the request to review NIBRS sex offense nomenclature was added as a point of focus for the Beyond 2021 Task Force.

This topic was first presented to the CJIS APB Working Groups during the Spring 2020 meetings and to the UCR Subcommittee during the Fall 2020 meetings. During these meetings, it was recommended the FBI UCR Program move forward with the proposal to replace the NIBRS rape definition with the 2012 revised rape definition, which alleviates the necessity to collect the categories of "sodomy" and "sexual assault with an object." In addition, there is no desire to create an additional "other sex crimes category." However, the FBI UCR Program was requested to explore the most appropriate terminology to replace the terms "fondling," "incest," and "statutory rape."

DISCUSSION AND ANALYSIS

Issue A: Replacing the NIBRS offense – "Fondling"

Within NIBRS, *fondling* is defined as:

"The touching of the private body parts of another person for the purpose of sexual gratification without the consent of the victim, including instances where the victim is incapable of giving consent because of his/her age or because of his/her temporary or permanent mental or physical incapacity."

The original request suggests a replacement term of "*unwanted sexual contact*," citing the term "fondling" is not often viewed as a crime, and "*unwanted sexual contact*" clearly illustrates a forcible sex offense. However, during the Fall 2020 meeting, UCR Subcommittee members recommended the amendment of the term "*fondling*" to "*criminal sexual contact*," tasking the FBI UCR Program with determining an appropriate definition for the offense. The goal of the Beyond 2021 Task Force is to provide clarity for law enforcement agencies submitting sex offense data. Through discussions with the Beyond 2021 Task Force and the supporting SME group, the below definition is recommended as an update to the NIBRS offense of *fondling*:

Criminal Sexual Contact includes the following:

- *The intentional touching of the clothed or unclothed genitalia, anus, groin, breast or buttocks of any person by the actor's clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*
- *The forced touching by the victim of the actor's clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

It is important to note that the proposed definition does not allow law enforcement officers to report contact in which the offender uses any body part not specified within the definition including touching with the hand.

Issue B: Updating the NIBRS offense – “Incest”

For NIBRS purposes, *incest* is defined as:

“Sexual relations between persons who are related to each other within the degrees wherein marriage is prohibited by law.”

For UCR purposes, *Incest* is a non-forcible offense; if through law enforcement investigation it is determined force is involved, law enforcement agencies are directed to record the offense as one of the forcible NIBRS sex offenses. The state statutes for the offense of *incest* vary across states and jurisdictions. Law enforcement agencies report the offense of *incest* if it is determined the individuals involved are related within the degree of prohibition established at a state level. In many cases, since *incest* is a state-level crime between two consenting individuals both individuals are charged with the offense *incest* as seen below:

Victim						Offender			
Victim Count	Age	Sex	Race	Ethnicity	Relationship	Age	Sex	Race	Relationship
1	43	F	B	U	N	63	M	B	1CH 2VO
2	63	M	B	N	R	43	F	B	1VO 2PA
1	26	F	W	U	N	28	F	W	1SB 2VO
2	28	F	W	U	N	26	F	W	1VO 2SB

With a focus on ensuring value and high-quality data outputs, the Beyond 2021 Task Force and supporting SME group determined two potential options for modifying the NIBRS sex offense of *incest*:

- Modification of the NIBRS definition to reflect the offenses collected within the NIBRS offense code.
- Discontinuation the collection of *incest* for national reporting.

The first option is the modification of the NIBRS definition for *incest*. The goal in the modification is to ensure clarity in reporting of the offense to the FBI UCR Program. The recommended definition of *incest* is:

“Consensual sexual intercourse between individuals related by blood within the degree that the individuals are prohibited based on state provision.”

Two additional options include the discontinuation of the NIBRS offense *incest which can be accomplished by:*

- Report *incest* offenses using NIBRS offense code 90Z – All Other Offenses.
- Do not report *incest* offenses for national reporting purposes.

Collecting *incest* as 90Z – All Other Offenses will require a reclassification of the offense from a NIBRS Group A offense to a Group B offense. With this reclassification additional details of the offense, including the victim to offender relationship will not be captured. The second option is the discontinuation of any reporting of *incest* offenses to the FBI UCR Program. Law enforcement agencies will continue to capture information on these offenses, but state UCR programs will not map the offense to a NIBRS offense code and report the information for national reporting purposes.

Issue C: Modification of NIBRS Offense – “Statutory Rape”

For NIBRS purposes, *statutory rape* is defined as:

“Sexual intercourse with a person who is under the statutory age of consent.”

Like *incest*, the NIBRS offense *statutory rape* is considered a consensual act with the defining factor being the age of the individuals involved. Current definitions of rape account for situations where an individual is under the age of consent. For a *statutory rape* incident to be reported to the FBI UCR Program the individuals involved must fall within the age ranges for consent as determined by each state. When reporting offenses of *statutory rape*, law enforcement agencies can report both individuals as offenders or can opt to report the older individual as the offender. Examples of how these incidents are reported to the FBI UCR Program are below:

Victim						Offender			
Victim Count	Age	Sex	Race	Ethnicity	Relationship	Age	Sex	Race	Relationship
1	14	F	W	N	R	14	F	W	1VO 2BG
2	15	M	W	N	R	15	M	W	1BG 2VO
1	14	F	B	N	R	16	M	W	1BG
1	14	F	B	H	R	17	M	B	1BG
2	14	F	W	N	R	17	M	W	1AQ
3	15	M	W	N	R	18	F	A	1BG
1	14	F	W	N	N	16	M	W	1BG

Through conversations with the Beyond 2021 Task Force and supporting SME group, it was determined questions surrounding the offense of *statutory rape* arise based on the current NIBRS definition. Value and clarity will be added if the definition clearly articulates what constitutes *statutory rape* for national reporting purposes. Clarification on the definition will not only benefit local law enforcement agencies, but will better align the offense to college and university law enforcement agencies reporting based on Clery Act standards. The Beyond 2021 Task Force recommends modification of the NIBRS *statutory rape* definition to:

“Consensual sexual intercourse with an individual who is under the state age of majority but meets the state provisions for the age of consent.”

IMPACT

The modifications to the NIBRS sex offense nomenclature recommended by the Beyond 2021 Task Force will require technological and documentation enhancements for the FBI UCR Program as well as for state UCR programs. State UCR programs will be required to ensure all information reported meets the updates standards outlined in the FBI UCR Program documentation. The FBI UCR Program also will be required to update all documentation, including the *NIBRS Technical Specification*, the *NIBRS User Manual*, and the *NIBRS XML Developer’s Guide* to reflect the enhancements. In addition, audit and training processes will require modifications to accommodate the changes.

Proposed Timeline

The FBI UCR Program anticipates beginning implementation of the listed changes upon formal recommendation by the CJIS APB and approval by the FBI Director. While the FBI UCR Program is cognizant of the work within each state to meet the January 1, 2021, deadline for the NIBRS transition, there is a desire to implement changes to the NIBRS sex offense nomenclature as soon as feasible. Implementation ensures the information is relevant to the law enforcement and the stakeholder communities. The FBI UCR Program will begin implementing any approved enhancements during calendar year 2022, with implementation for states beginning in calendar year 2023, or at a date determined in the CJIS APB recommendation.

OPTIONS

Issue A: Replacing the NIBRS offense – “Fondling”

Option A1 – Modify the NIBRS offense “*fondling*” to “*criminal sexual contact*” with the below definition:

Criminal Sexual Contact includes the following:

- *The intentional touching of the clothed or unclothed genitalia, anus, groin, breast or buttocks of any person by the actor’s clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*
- *The forced touching by the victim of the actor’s clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

Option A2 – No change.

Issue B: Updating the NIBRS offense – “Incest”

Option B1 – Modify the NIBRS offense “incest” definition to state:

“Consensual intercourse between individuals related by blood within the degree that the individuals are prohibited based on state provision.”

Option B2 – Modify *incest* to be captured as a NIBRS Group B Offense with data captured as part of 90Z- All Other Offenses.

Option B3 – Discontinue collection of *incest* for national reporting.

Option B4 – No change.

Issue C: Modification of NIBRS Offense – “Statutory Rape”

Option C1 – Modify the NIBRS offense “statutory rape” definition to state:

“Consensual sexual intercourse with an individual who is under the age of majority but meets the state provisions for the age of consent.”

Option C2 – No change.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Issue A: Replacing the NIBRS offense – “Fondling”

Motion: To accept a new option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

Criminal Sexual Contact includes the following:

- *The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*
- *The forced touching by the victim of the actor’s clothed or unclothed body parts, without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

Priority 3M.

Action: Motion carried.

Issue B: Updating the NIBRS offense – “Incest”

Motion: To accept Option B1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue C: Modification of NIBRS Offense – “Statutory Rape”

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Issue A: Replacing the NIBRS offense – “Fondling”

Motion: To accept New Option A3: Modify the NIBRS offense “*fondling*” to “*criminal sexual contact*” with the below definition *Criminal Sexual Contact includes the following:*

- *The intentional touching of the clothed or unclothed genitalia, anus, groin, breast or buttocks of any person, without the consent of the victim.*
- *The forced touching by the victim of the actor’s clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

Priority 3M.

Action: Motion carried.

Issue B: Updating the NIBRS offense – “Incest”

Motion: To accept Option B1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue C: Modification of NIBRS Offense – “Statutory Rape”

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Issue A: Replacing the NIBRS offense – “Fondling”

Motion: To accept Option A1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue B: Updating the NIBRS offense – “Incest”

Motion: To accept Option B4: No change.

Action: Motion carried.

Issue C: Modification to NIBRS Offense – “Statutory Rape”

Motion: To accept Option C1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Issue A: Replacing the NIBRS offense – “Fondling”

Motion: To accept new option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

Criminal Sexual Contact includes the following:

- *The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*
- *The forced touching by the victim of the actor’s clothed or unclothed body parts, without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

Priority 3M.

Action: Motion carried.

Issue B: Updating the NIBRS offense – “Incest”

Motion: To accept Option B1 as presented in the topic paper. Priority 4M.

Action: Motion carried.

Issue C: Modification of the NIBRS offense – “Statutory Rape”

Motion: To accept Option C2: No change.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Issue A: Replacing the NIBRS offense – “Fondling”

Motion: To accept a New Option: No change to the current definition of “fondling”. Replace the term “fondling” with “criminal sexual contact”.

Action: Motion carried.

Issue B: Updating the NIBRS offense – “Incest”

Motion: To accept Option B4: No change.

Action: Motion carried. 1 Nay.

Issue C: Modification of NIBRS Offense – “Statutory Rape”

Motion: To accept Option C2: No change.

Action: Motion carried.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Issue A: Replacing the NIBRS offense – “Fondling”

Motion: Motion to accept New Option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

Criminal Sexual Contact

-The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.

-The forced touching by the victim of the actor's clothed or unclothed body parts, without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.

-This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation

Priority 3M

Action: Motion carried. 1 Abstained.

Issue B: Updating the NIBRS offense – “Incest”

Motion: To accept Option B4: No change.

Action: Motion carried. 3 Nays.

Issue C: Modification of NIBRS Offense – “Statutory Rape”

Motion: To accept Option C2: No change.

Action: Motion carried. 1 Abstained.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #10

Creation of a National Incident-Based Reporting System (NIBRS) Offense Code Mapping Crosswalk Repository

PURPOSE

To present a proposal for the creation of a NIBRS Offense Code Mapping crosswalk displaying state-level statute mapping to NIBRS offense definitions.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the creation of a NIBRS Offense Code Crosswalk, propose the best method for implementation, and recommend a priority for this enhancement.

BACKGROUND

The Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program is working with stakeholders to create enhancements to crime data after the January 1, 2021, transition from a summary-based data collection to a NIBRS data collection. In 2019, the FBI UCR Program formed the Beyond 2021 Task Force to assist in the creation of the FBI UCR Program roadmap after the NIBRS transition is complete. The Beyond 2021 Task Force's purpose is to engage the stakeholder community through the Criminal Justice Information Services (CJIS) APB process. The FBI UCR Program is achieving this through the Beyond 2021 Task Force and supporting Subject Matter Expert (SME) groups. The Beyond 2021 Task Force is responsible for creating the FBI UCR Program roadmap after the NIBRS transition. The SME groups are charged with creating proposals for consideration by the Beyond 2021 Task Force that ensure the value of FBI UCR Program data are realized by all data submitters and consumers. The Beyond 2021 Task Force will develop actions and topics of interest for the purposes of review and prioritization within the UCR Subcommittee based on the proposals of the SME groups.

DISCUSSION AND ANALYSIS

To fulfill the FBI UCR Program's mission, it must produce a nationwide view of crime statistics, based on state statute level data, which can at times be problematic. State statutes define crimes according to specific situations whereas the definitions of the offenses captured within NIBRS are generic to allow the capture of as many state offenses as possible. Data contributors must map state statutes to specific NIBRS offenses to submit data to the FBI UCR Program for inclusion in national data releases. Mapping is an extended translation process that correlates criminal offenses with varying state codes and titles to NIBRS offense definitions. The mapping of state statutes helps achieve the common language of the FBI UCR Program that is necessary for national views of crime data.

As part of the Beyond 2021 Initiative, FBI UCR Program staff created a SME group focused on enhancing NIBRS offense definitions. The NIBRS Offense Definitions SME group discussed the near-term resource of a NIBRS offense code crosswalk hosted by the FBI UCR Program. Since states base their criminal statutes on common-law definitions, many offense codes directly align with a corresponding NIBRS offense classification, or easily fit within one offense category. However, based on definitions, some criminal state statutes do not map to the same NIBRS offense classification as they do within the state. As an example, some state statutes require law enforcement agencies to record thefts from motor vehicles as burglaries, but for NIBRS purposes, these incidents must be mapped to larcenies. In addition, some NIBRS offenses may not have corresponding state statutes. For example, many states do not have statutes for embezzlement, but must map applicable state statutes to those NIBRS offense classifications based on NIBRS definitions.

The goal of a NIBRS offense code crosswalk is to enhance uniformity among state UCR programs. This crosswalk can be used as a tool for the FBI UCR Program to provide guidance on incidents that do not clearly fit within NIBRS offense definitions as well as for state UCR programs to share information on how specific state statutes are mapped to NIBRS offense classifications. The NIBRS Offense Definitions SME group members believe the ability for state UCR Programs to upload how state statutes are mapped to NIBRS offense codes will be a useful reference with utility for all state UCR program managers to compare offenses across states, identify discrepancies and gaps within crime data, and improve uniformity within the national data collection. Since every state statute must be mapped to a NIBRS offense definition to help ensure uniformity and consistency of data across the nation, the FBI UCR Program has actively engaged with stakeholders to ensure an effort has been made to appropriately map state statutes. Creating a location in which data contributors can house and update NIBRS offense-mapping information will provide a valuable resource to the FBI UCR Program, and data contributors. It will provide a central location for state mapping information to be shared and reviewed by data contributors and consumers.

To assess the feasibility of establishing this repository, the FBI UCR Program surveyed state UCR program managers to determine if any states use a NIBRS statute crosswalk. Out of the 50 state UCR programs canvassed, 24 responded stating they maintain a NIBRS offense crosswalk, six do not currently maintain a NIBRS offense crosswalk, and 20 did not respond. Based on the

information collected, it was determined if this repository is established, the FBI UCR Program could receive data from at least 24 states.

Ensuring Quality Information

As with all FBI UCR Program data presented in a public forum, the FBI UCR Program will be required to establish policies governing the storage and use of the data presented within the NIBRS offense crosswalk. To create appropriate policies, the FBI UCR Program will coordinate with the Office of Management and Budget, the Office of the General Counsel, and stakeholders to ensure all established policies align with federal and state policies for maintaining state-level information by a federal entity.

The FBI UCR Program will provide guidelines and expectations for maintaining the data housed within the repository, to include guidance on versioning of information uploaded and notating when state-submitted information has been updated. In addition, NIBRS Offense Definitions SME members propose the creation and establishment of policy for handling requests or comments on state-owned information. Through discussion it was determined the FBI UCR Program should not be responsible for handling state-specific requests regarding statutes, and a policy will be created within the repository guidelines establishing methods to communicate such requests with state points of contact. This policy will also include information outlining how the FBI UCR Program will collaborate with state UCR programs to ensure feedback and questions are routed to the appropriate state UCR programs for review and response.

To ensure the success of a NIBRS offense repository, the Offense Definitions SME group recommends delineating the responsibilities of FBI UCR Program staff and the state UCR programs submitting data. Participation in the NIBRS offense crosswalk repository will be voluntary, and state UCR programs will have the option to contribute and reference statutes and NIBRS offense codes. State UCR programs choosing to participate will be responsible for managing all state-level information within the repository. It will be the state UCR program's responsibility to upload, update, validate, and audit their state's information. State UCR programs must also ensure information is properly versioned so users viewing the information can differentiate between versions, and all updates and maintenance revisions are clearly documented. In addition, if a state UCR program opts to no longer supply data to the repository, it is the responsibility of the state to communicate that decision to the FBI UCR Program and delete its data. State UCR programs will also be able to include state-specific statutes that fall outside the NIBRS parameters. The Offense Definitions SME group suggested adding these additional data points to aid the understanding of data that law enforcement agencies across the nation are collecting by mandate or due to its perceived or realized value for decision-making.

The table below summarizes roles and responsibilities of the FBI UCR Program and those state UCR programs participating in data sharing through this repository.

Task	Assigned to FBI UCR Program	Assigned to State UCR Program
Create and maintain the interface for a NIBRS offense crosswalk repository.	X	
Establish guidelines for NIBRS Crosswalk Repository participation.	X	
Establish rules for maintaining the data within the NIBRS Crosswalk Repository.	X	
Document the guidelines for housing and protecting data within the NIBRS Crosswalk Repository.	X	
Create a secure dashboard interface allowing the ability to upload NIBRS statute information.	X	
Create and support a public interface for information sharing.	X	
Collaborate to establish guidelines for how feedback and questions from repository users will be answered.	X	X
Upload, update, validate, and audit state-level data.		X
Ensure all state-level data is versioned and meets FBI UCR Program requirements.		X

In addition, the NIBRS Offense Definition SME group discussed who should have access to this tool. Based on the Offense Definitions SME group’s feedback, the repository should be available through a publicly accessible location to ensure information is widely available to all stakeholders. While the main audience for a NIBRS repository is expected to be state UCR program managers, other groups such as the public, Statistical Analysis Centers, special interest groups, and the media are also potential data consumers who could have an interest in the information.

IMPACT

If approved, the creation of a NIBRS offense crosswalk repository will impact both the FBI UCR Program and state UCR programs. The FBI UCR Program will be required to create a mechanism for state UCR programs to securely upload state-level data and for data users to access the information. In addition, the FBI UCR Program will be required to create documentation outlining the requirements for participation in the NIBRS Crosswalk Repository. Participating state UCR programs will be required to maintain their state-level information within the repository if they choose to participate.

Since NIBRS Offense Definitions SME group discussions request such a repository be available to the public, two separate interfaces must be established. The FBI UCR Program must ensure participating state UCR programs have access to a secure dashboard interface allowing the ability to upload and update NIBRS statute information while supporting a public interface for information sharing across stakeholder communities. Since this repository will be publicly available, it is imperative the NIBRS offense crosswalk repository is properly maintained, with

established mechanisms for state UCR programs to submit data through a secure interface and a public interface for all data consumers.

The creation of a NIBRS offense crosswalk repository will positively impact the FBI UCR Program, state UCR programs, and data consumers. A NIBRS offense crosswalk repository will provide the opportunity for data users to view and compare state-level information from a central location with clearly established maintenance guidelines. Other benefits of the creation of a NIBRS offense code repository include enhancing the understanding of NIBRS data and providing insight to the information collected at a state and national level. Creation of this tool will also provide the FBI UCR Program to conduct additional analysis on state statute mapping and identify potential gaps in offenses, allowing the FBI UCR Program to create recommendations for future enhancements to NIBRS data.

Proposed Timeline

The FBI UCR Program proposes the implementation of a NIBRS offense crosswalk repository no later than January 2023. This proposed implementation date allows the FBI UCR Program to present this recommendation through the Spring 2021 APB Process for recommendation of approval by the FBI Director and conduct of any additional analysis necessary prior to implementation. This start date also provides the FBI UCR Program with sufficient time to communicate with OMB, OGC, and the stakeholder community.

OPTIONS

Option 1: Create a NIBRS offense crosswalk repository hosted by the FBI UCR Program and maintained by state UCR programs containing state-level statute information crosswalked/mapped to NIBRS offense codes.

Option 2: No change.

RECOMMENDATION

The FBI UCR Program recommends the creation of a NIBRS offense crosswalk repository to be created and hosted by the FBI UCR Program.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2: No change.

Action: Motion carried.

SPRING 2021 UCR SUBCOMMITTEE ACTIONS:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried. 1 Abstained.

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #12

National Use-of-Force Data Collection Update

PURPOSE

The purpose of this paper is to provide an update on the National Use-of-Force Data Collection, and to provide information on publication of data.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

BACKGROUND

Police-involved shootings and use of force have long been topics of national discussion, but high-profile cases in which subjects died have heightened public awareness of these issues. However, the opportunity to study use-of-force incidents was hindered by the lack of enough data to compile nationwide statistics. In response to this, representatives from major law enforcement organizations and federal, state, local, tribal, and college/university agencies requested the FBI establish a National Use-of-Force Data Collection, as no national collection existed. The Federal Bureau of Investigation (FBI) launched the National Use-of-Force Data Collection on January 1, 2019.

This voluntary program gathers data on law enforcement use-of-force incidents, which result in the death or serious bodily injury of a person, as well as the discharge of a firearm at or in the direction of a person. The definition of serious bodily injury is based, in part, upon Title 18, United States Code, Section 2246 (4). The term “serious bodily injury” means “bodily injury that involves a substantial risk of death, unconsciousness, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental faculty.” The goal of the resulting statistics is not to offer insight into single use-of-force incidents, but to provide an aggregate view of the incidents reported and the circumstances, subjects, and officers involved.

The publication strategy for the National Use-of-Force Data Collection is based upon the Terms of Clearance, which were agreed upon with the Office of Management and Budget. Publication is tied to achieving specific milestones related to the coverage of the collection, as measured by the number of sworn officers employed by the law enforcement agency. The FBI is required to

adhere to terms of clearance for publishing use-of-force data at the 40, 60, and 80 percent participation thresholds. The terms of clearance present the quality standards necessary for dissemination of the data. In addition, the terms of clearance provide guidance on the publishable data elements at each threshold and how those data elements are represented, i.e., percentages, ratios, lists, or counts.

Publication

On July 27, 2020, the inaugural publication was released. Agencies submitting 2019 data represented 41 percent of all federal, state, local, tribal, college/university sworn law enforcement officers. The publication can be found on the FBI's Crime Data Explorer (CDE) at <https://crime-data-explorer.fr.cloud.gov/officers/national/united-states/uof>. The 2019 data publication included agencies that submitted zero reports or incidents occurring between January 1, 2019, and December 31, 2019.

The 40 percent publication focused on the following:

- Narrative detailing the number of agencies participating in the collection.
- List of agencies both enrolled and/or participating in the collection.
- Response percentages, to include agencies that submitted a zero report, agencies that submitted an incident report, and agencies that did not submit data for a given month.

The second publication released on November 9, 2020, represented 42 percent of all federal, state, local, tribal, college/university sworn law enforcement officers. The publication displayed the same data on CDE as the 2019, 40 percent publication. No updates were made to the 2019 data, just the 2020 data. The 2020 data is based on the information agencies provided to the FBI for incidents and zero reports that occurred in the time period of January 1, 2020 to August 31, 2020. The FBI will continue to collect 2020 data for future publications.

The FBI Uniform Crime Reporting Program plans to continue producing publications that further enhance the understanding of the data, including counts.

Future Publications

It is imperative the FBI reaches the mandated 60 and 80 percent participation thresholds, as each threshold allows the ability to publish a more comprehensive view of the data elements, within the use of force incidents, at the national, regional, and state level. At 60 percent coverage, the data collection will publish percentages and lists at the national and regional levels for the following data elements: type of incident, reason for initial contact, type of force applied, and whether resistance was encountered. At 80 percent coverage, the publication has no conditions that apply to the publication.

Once published, the data will provide a transparent and comprehensive view of use of force incidents in the communities the agencies serve, and also provide data to law enforcement officers to enhance training initiatives within departments.

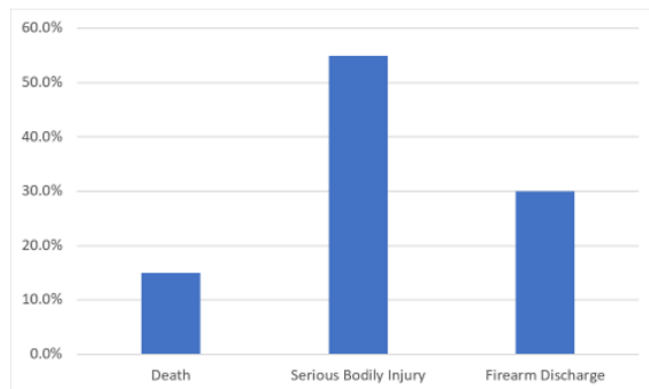
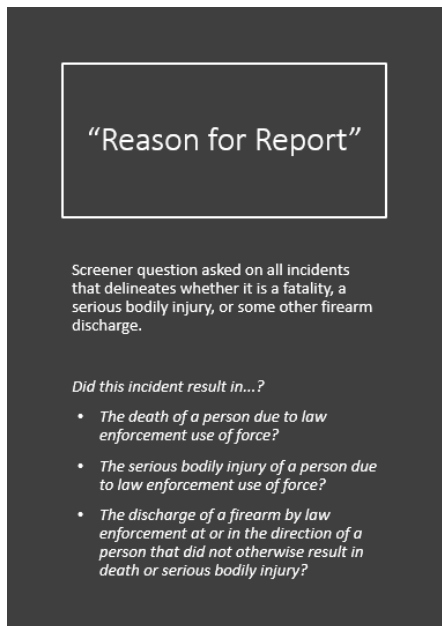
60 percent publication

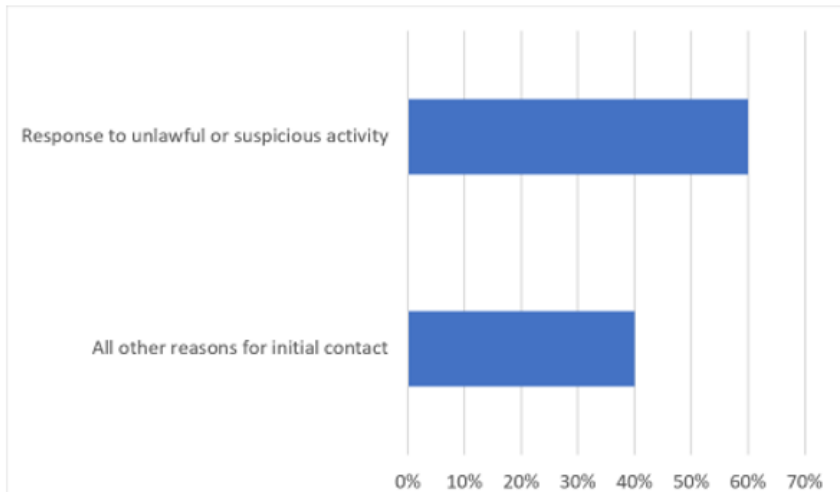
The content on publication pages for 60 percent will be cumulative—including additional data points once an entity has achieved a level of coverage.

- However, coverage is not cumulative. Coverage will be calculated at each publication cycle and content will be determined by the coverage at the time of publication.
- If a state meets the minimum criteria for at least 60-percent coverage, then data elements can be displayed.
- Otherwise, the state/department page will show the participation metrics previously approved by management if it can meet the 40-percent coverage threshold.

The terms of clearance allow for the publication of percentages, proportions, ratios, and lists once the data has reached 60-percent or better coverage. The proposed publication of use-of-force data can incorporate incremental growth based on coverage and completeness of data to avoid situations where data elements are published one year and removed from the CDE the following year. The data elements displayed would be “percent of reported incidents” as allowed once coverage reaches a minimum of 60 percent coverage.

Screenshots of Proposed 60 percent Publication





Reason indicates whether the contact was due to the investigation of possible criminal activity or some other reason.

What was the reason for initial contact between the subject(s) and the officer(s)?

- Response to unlawful or suspicious activity
- Medical, mental health, or welfare assistance
- Routine traffic stop
- Warrant service
- Service of a court order
- Mass demonstration
- Follow up investigation
- Other

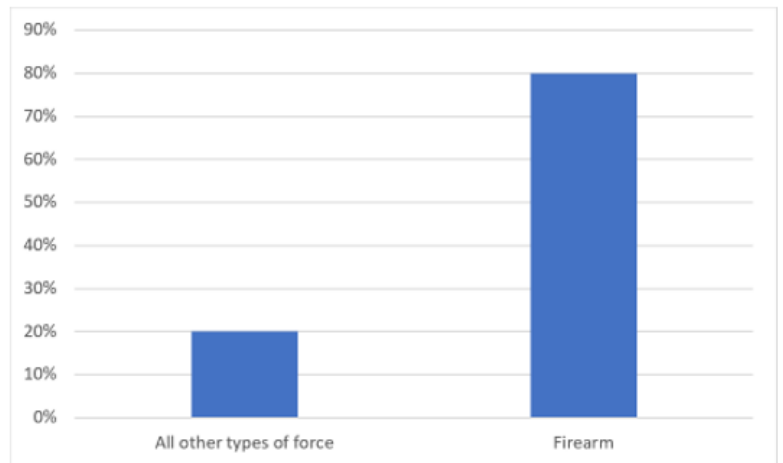
“Reason for initial contact”

“Types of force used”

Force indicates whether it was the use of a firearm by a law enforcement officer or some other type of force.

Types of force used by law enforcement connected to serious bodily injury or death of the subject

- Firearm
- Electronic control weapon
- Explosive device
- Chemical agent/Pepper or OC spray
- Baton
- Impact projectile
- Blunt instrument/flashlight
- Hands-fists-feet
- Canine
- Other



“Resistance Encountered”

Two-part question with an initial "yes/no" screener regarding any resistance encountered.

Top Five Resistance or Weapon Encountered

Failing to comply to verbal commands or other types of passive resistance

Attempted to escape or flee from custody

Display a weapon at an officer or another

Using a firearm against an officer or another

Resisted being handcuffed or arrested

What resistance or weapon was or believed to be involved?

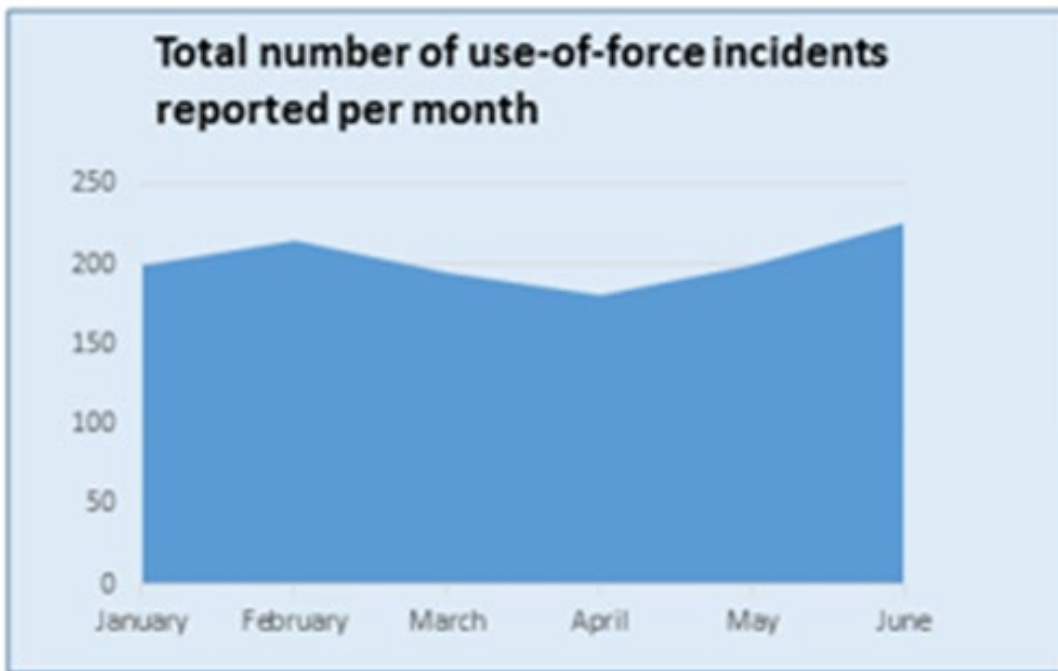
- Attempted to escape or flee from custody*
- Resisted being handcuffed or arrested*
- Barricading self*
- Using a firearm against an officer or another*
- Using another weapon against an officer or another*
- Using hands/fist/feet against an officer or another*
- Displaying a weapon at an officer or another*
- Directing a vehicle at an officer or another*
- Intentional spitting or bleeding on an officer*
- Throwing an article or object at an officer*
- Making verbal threats*
- Failing to comply to verbal commands or other types of passive resistance*

80 Percent Publication

For the 80 percent publication no conditions apply to the data. The FBI may provide both counts and percentages:

- Number of types of incidents reported each month (death, serious bodily injury, or firearm discharges at or in the direction of a person)
- Counts of participating agencies/sworn law enforcement officers at national, federal, regional, and state levels
- Number of incidents at national, federal, regional, and state levels
- Counts of types of resistance encountered
- Counts of types of force used
- Counts of apparent/known impairments
- Counts of location type etc.

Screenshots of proposed 80 percent publication



Engagements

Due to the pandemic, face-to-face meetings did not occur. However, the FBI UCR Program continued to collaborate with law enforcement on participation in the National Use-of-Force Data Collection. Virtual conferences and demonstrations have been utilized to market the data collection.

The Use-of-Force Task Force continues to support the FBI's engagement activities and advocate with fellow law enforcement partners to increase participation. These representatives from the law enforcement community meet quarterly via teleconference and serve as champions, sharing the importance of the data collection to peer groups. Task force members include representatives from the International Association of Chiefs of Police, Major Cities Chiefs Association, Major County Sheriffs of America, National Organization of Black Law Enforcement Executives, National Sheriffs' Association, Association of State Uniform Crime Reporting Programs, Association of State Criminal Investigative Agencies, Police Executive Research Forum, along with representatives from federal, state, local, tribal, and college and university law enforcement agencies.

Direct engagement with the law enforcement community continues to be the primary focus to increase participation in the National Use-of-Force Data Collection. With more than 18,000 law enforcement agencies across the country, engagement activities throughout 2021 continue to focus on federal, state, local, tribal, and college and university law enforcement agencies for increased discussions on the National Use-of-Force Data Collection.

The FBI continues to encourage participation from federal agencies via direct outreach to the 114 known agencies. One of the challenges faced is in determining which federal agencies employ sworn law enforcement. If agencies do not employ sworn law enforcement officers, they do not house relevant use-of-force information. Currently, there are 29 federal agencies participating in this data collection.

The FBI is actively working to gain participation from all tribal entities. Tribal engagement activities have involved the APB Tribal Task Force, the Criminal Justice Information Services Tribal Engagement Program, the Department of Justice's Tribal Access Program and the Department of Interior's Bureau of Indian Affairs. As of October 22, 2020, 41 tribal agencies are participating in the data collection.

Continued work with university law enforcement associations to promote the National Use-of-Force Data Collection is ongoing. Active engagement and discussions are occurring between the FBI and the International Association of Campus Law Enforcement Administrators. Endeavors are ongoing with various university chiefs of police who bring great insight and assistance to the FBI's liaison efforts. As of October 22, 2020, 184 college and university law enforcement agencies are participating.

Conclusion

The FBI continues to liaise with law enforcement agencies, major law enforcement organizations, legislative bodies, advocacy groups, criminologists, criminal justice students, media outlets, and the general public utilizing publications, conferences, training events, and social media to increase participation.

If non-participating law enforcement agencies do not take action and proactively begin releasing data to the FBI, the FBI may fail partners who have specifically requested the creation of the National Use-of-Force Data Collection. If a better than 60 percent coverage rate is not achieved

within the first three years, the OMB recommends revisiting options with separate statistical entities.

The FBI has many resources easily accessible for state program managers and direct contributors. The FBI developed a webpage located at <http://www.fbi.gov/useofforce>. This website allows law enforcement agencies and the public to obtain answers to frequently asked questions, and access resources and support information. In addition, the Use-of-Force Help Desk may be reached by telephone at 304-625-9998 or via e-mail at useofforce@fbi.gov.

SPRING 2021 WORKING GROUP ACTIONS:

All five workings accepted this topic as information only.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Accepted as information only.

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #13

Status of the National Incident-Based Reporting System (NIBRS) Transition

PURPOSE

To provide an update on the nation's NIBRS transition.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

BACKGROUND

As recommended by the CJIS Advisory Policy Board and approved by the FBI Director, *“The FBI UCR Program will transition to a NIBRS-only data collection by January 1, 2021, and will evaluate the probability of achieving that goal on an annual basis. Federal, state, local, and tribal agencies unable to meet the five year transition and who have committed to transitioning to NIBRS will collaborate with the FBI CJIS [Division] to develop a transition plan and timeline for conversion.”*

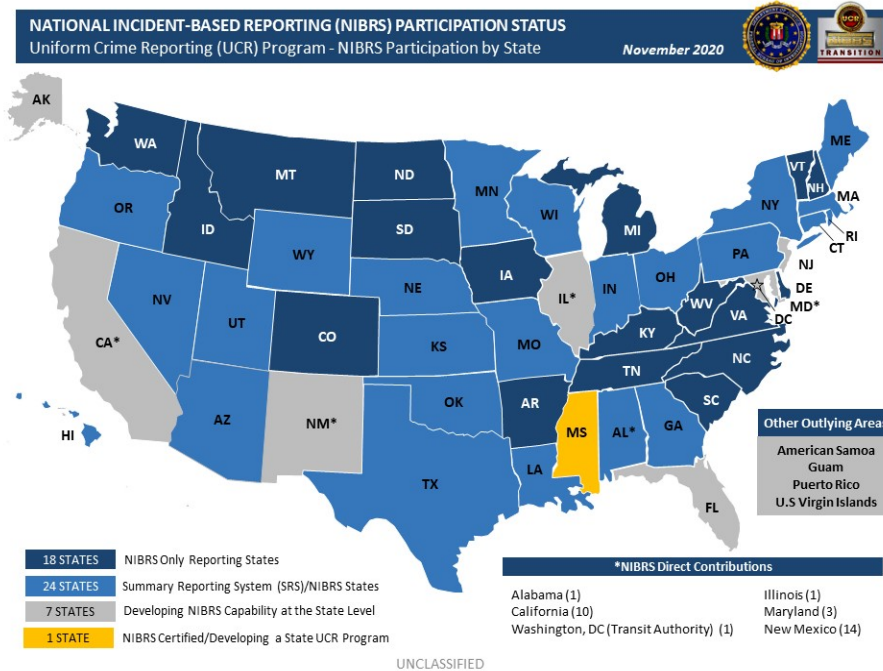
In 2018, the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program intensified marketing and engagement efforts for the nation's transition to NIBRS. Since then, in addition to those agencies reporting NIBRS in 2019, over 3,900 additional agencies have committed to transitioning to NIBRS by January 1, 2021, through their state UCR programs. Some of these committed agencies have already made the transition to NIBRS.

As reported in the 2019 *Crime in the United States (CIUS)* publication, “In 2019, approximately 51 percent of the law enforcement agencies that participated in the FBI UCR Program submitted their data via NIBRS. The populations of these agencies represented approximately 46 percent of the population covered by agencies that submitted data to the FBI UCR Program. Of the 43 states that the FBI has certified to report via NIBRS, 18 states submitted 100 percent of their data via NIBRS; the other NIBRS-certified states submitted data through both NIBRS and the Summary Reporting System. Among states still working toward NIBRS-certification, a few agencies submitted NIBRS data through direct contributions to the FBI.”

As of November 2020, 43 states are FBI NIBRS certified. In addition, agencies from Alabama, California, Illinois, Maryland, and New Mexico are certified and reporting NIBRS data directly

to the FBI UCR Program. As identified in *CIUS* 2019, “While the number of NIBRS participants has increased slightly over the last few years, the FBI anticipates much greater growth in the 2020 and 2021 reporting years as thousands of law enforcement agencies fulfill their current commitments to transition to NIBRS by January 1, 2021.”

NIBRS Participation Map by State

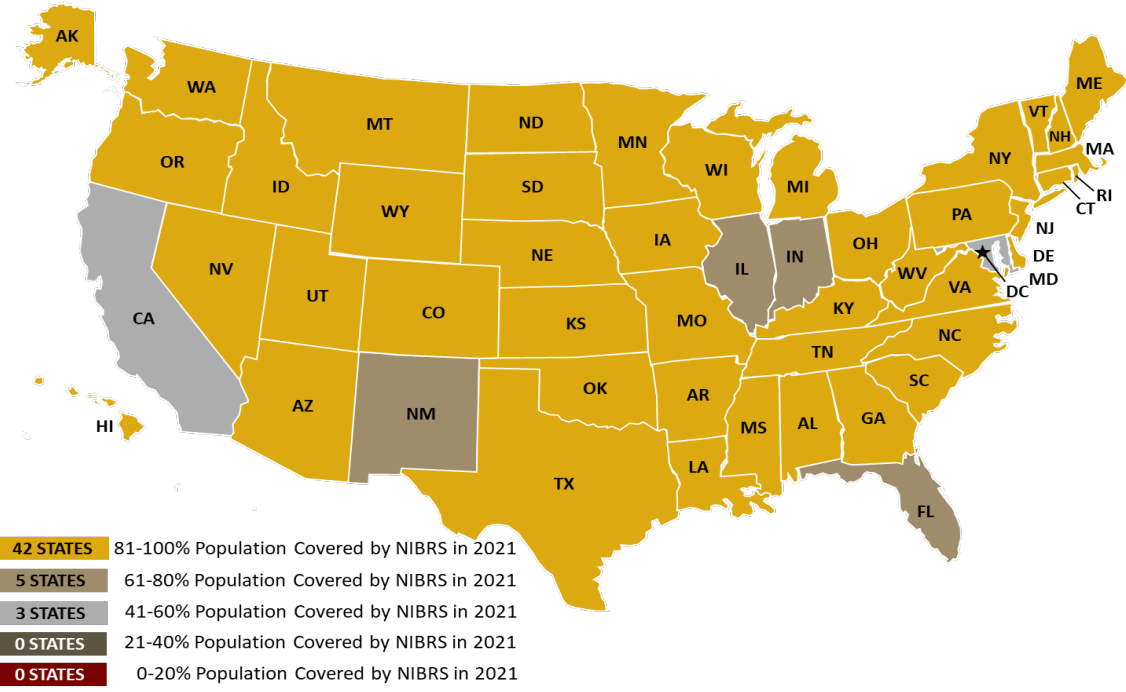


State and Local Law Enforcement Transition Status

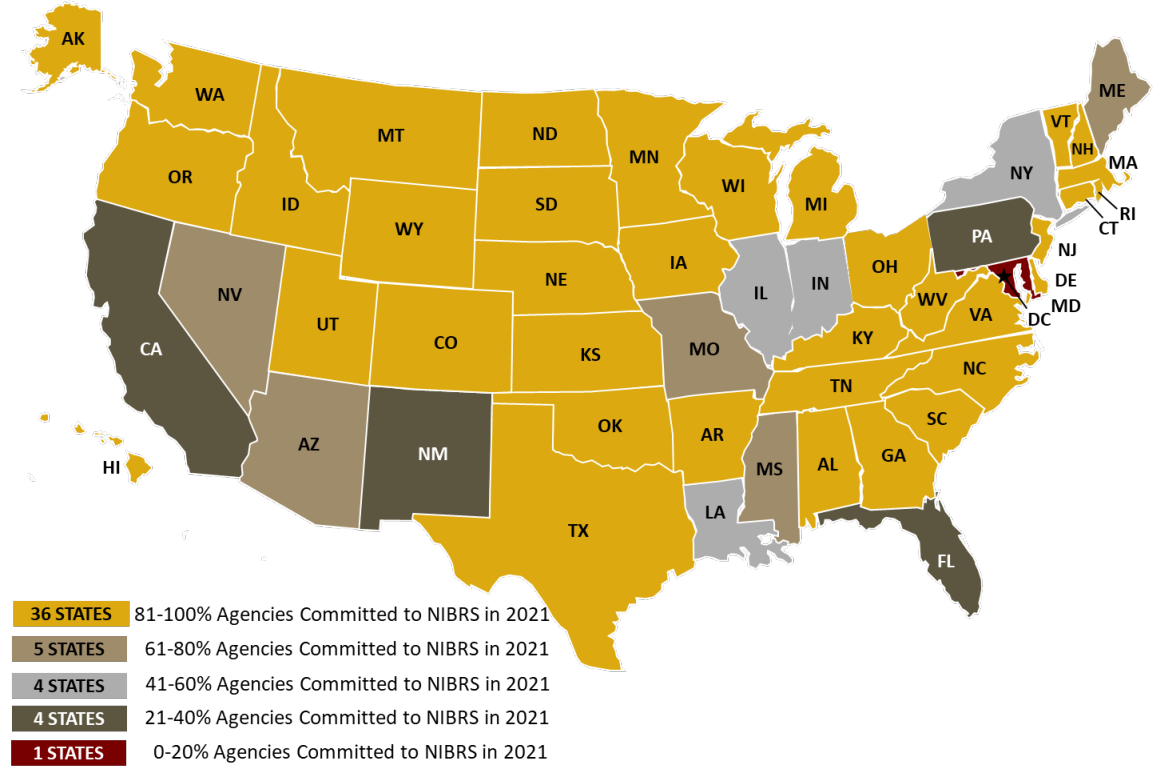
At the state level, seven non-certified states are developing a NIBRS-certified system – Alaska, California, Florida, Illinois, Maryland, New Jersey, and New Mexico. Within calendar year 2021, the FBI UCR Program anticipates every state in the nation will become NIBRS certified. Once certified, the state UCR program can better assist local agencies with the NIBRS transition, and they will be responsible for certifying agencies to submit NIBRS-only data.

Tracking of local agency commitments obtained through state UCR programs continues to help gauge the nation’s transition to NIBRS by 2021. The FBI UCR Program maintains nationwide maps to reflect the NIBRS 2021 projections of agency participation and population coverage within each state.

NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS) 2021 PROJECTED POPULATION COVERED
 BASED ON LAW ENFORCEMENT COMMITMENTS AS OF OCTOBER 2020



NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS) 2021 PROJECTED PARTICIPATION OF AGENCIES
 BASED ON LAW ENFORCEMENT COMMITMENTS AS OF OCTOBER 2020



In 2020, new agency commitments, such as the Chicago Police Department, Pittsburgh Bureau of Police, Atlanta Police Department, St. Louis Metro PD, and the San Diego Police Department resulted in significant increases of state percentage projections. Accordingly, the national projected percentages of agency commitments and population covered also increased. As of November 2020, these percentages were at 75 percent and 81 percent respectively. While these percentages are encouraging, they are only projections based upon commitments provided by the state UCR program managers. Agencies must stay vigilant to meet their transition commitments by the deadline.

Through concentrated engagement and marketing strategies, the FBI UCR Program continues to message to agencies the January 1, 2021, deadline and the benefits of transitioning to NIBRS, the steps for an agency to transition, and training opportunities available to agencies. The FBI UCR Program continues to assist agencies in achieving transition to NIBRS with available resources that include programmatic and technical support, NIBRS training, outreach, and subject matter expertise, at no cost to law enforcement agencies. For more information or assistance, agencies may contact the FBI UCR Program Office as follows:

- NIBRS Website: <https://www.fbi.gov/services/cjis/ucr/nibrs>
- NIBRS E-mail address: UCR-NIBRS@fbi.gov
- NIBRS Contact: 304-625-9999
- NIBRS Training: 888-827-6427

Aside from the information on the NIBRS webpage, the FBI UCR Program continues to publish articles and participate in podcasts encouraging agencies to transition and demonstrating the benefits of NIBRS. Publishing articles and podcasts from different types of law enforcement agencies further promote the NIBRS transition. These articles and podcasts are available in *The Police Chief* and the CJIS Division's blog for law enforcement, the *CJIS Link*, and on www.Police1.com. Recently published articles include:

- "Tennessee's Support for NIBRS" for *The Police Chief* (April 2020)
- "Are You Ready? The Countdown to NIBRS." for *CJIS Link* (August 2020)
- "90 Years of UCR" for *The Police Chief* (October 2020)
- "The FBI's NIBRS deadline is fast approaching. What agencies need to know." for *Police1* (October 2020)

Training events about NIBRS continue to be a priority for the FBI UCR Program. In 2020, the FBI UCR training staff completed approximately 21 NIBRS training sessions with approximately 1,900 attendees from nearly 900 agencies. In calendar year 2020, there were eight in person training sessions, along with 13 virtual training sessions. The FBI UCR training staff has implemented virtual training sessions for the rest of calendar year 2020 and will continue to do so through calendar year 2021.

For more information regarding training, the FBI UCR training staff can be contacted at ucrtrainers@leo.gov.

NIBRS Collection Application

The FBI has developed a solution to provide federal and tribal agencies the opportunity to submit NIBRS data to the FBI UCR Program. Deployed in June of 2020, the NCA provides federal agencies the ability to comply with the UFCRA of 1988 by providing them with a no-cost NIBRS submission solution. In addition, the NCA reduces the amount of resources required to submit and manage UCR data. The NCA is an extension of the UCR system and enables users to directly enter and submit NIBRS crime data to the FBI UCR Program for processing, retention, and publication. The data is submitted via the NCA web application, which is accessible through LEEP. The NCA collects and contains the same NIBRS offenses and data elements currently supported within the UCR system to maintain consistency and data uniformity. As for authorized users of the NCA, submitting agency administrators are able to control user authorization/roles and data access controls. The users, based on assigned permissions, are able to enter, save, view, validate, manage, and submit incidents to the UCR system.

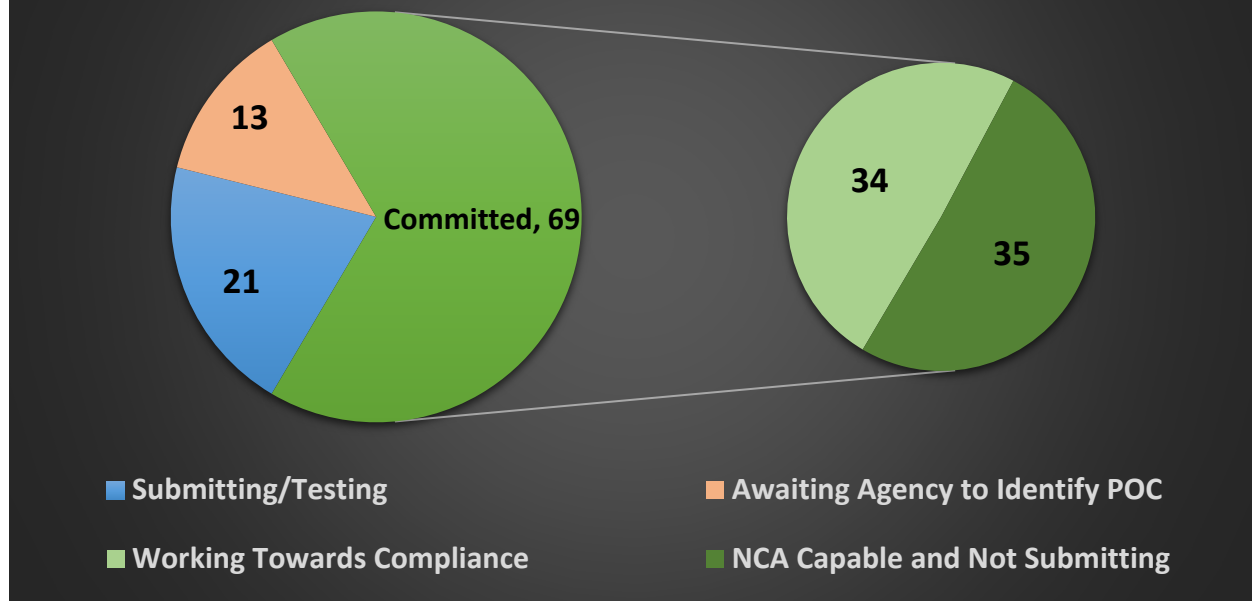
Federal Agency Transition Status

The Uniform Federal Crime Reporting Act (UFCRA) of 1988 was amended on December 21, 2018, when the President of the United States signed into law the Trafficking Victims Protection Act of 2017, Public Law No. 115-393, Title IV, Section 402, 132 Stat. 5265, 5274-75 (2018) (codified as amended at 34 U.S.C. § 41303 (2012)). The amendments direct the FBI to (1) coordinate with federal agencies and departments to implement required reports of crime statistics, and (2) report annually to Congress on the efforts of federal agencies and departments to comply.

The FBI completed further communication efforts in 2019 and 2020, to address added actions of coordination with each department and agency within the federal government that is subject to the mandatory requirement of reporting crime data to the FBI. In January 2020, a memorandum from the FBI Director was provided to the federal agencies with no point of contact, advising them of the requirement, as well as a memorandum from the United States Attorney General to the federal agencies, advising each one of their compliance or lack thereof.

The FBI UCR Program continues outreach to federal agencies to encourage their participation in the NIBRS. The NCA was deployed in June 2020, and is currently being utilized by 19 federal agencies and another 36 have committed to submit NIBRS data to the FBI UCR Program via the NCA.

Federal Agency UFCRA Status (103 Total)



Tribal Agency Transition Status

The FBI's NIBRS transition efforts with tribal law enforcement agencies consists of continued work with tribal law enforcement agencies, the Department of Justice and the Department of Interior. Now that the NCA has been deployed, tribal agencies that were previously unable to submit NIBRS data now have the ability to do so via the NCA. As of November 2020, there is one tribal agency utilizing the NCA. In subsequent months, it is anticipated all tribal agencies will submit data via the NCA, as outlined to the FBI by the Bureau of Indian Affairs.

Looking Ahead

In addition to resource planning, NIBRS can provide a more precise narrative and counter misconceptions about the scope, type, and nature of crime in the United States. Agencies that have yet to transition are encouraged to work with the respective state UCR program to do so. In addition, agencies that have transitioned are encouraged to work with non-transitioned agencies, community leaders, and local media to educate the areas they serve about the benefits of NIBRS data. With accurate, reliable, timely, and accessible reporting, we can all better protect the people we serve.

SPRING 2021 WORKING GROUP ACTIONS:

All five working groups accepted this topic as information only.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Accepted as information only.

**CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 21, 2021**

STAFF PAPER

UCR ISSUE #16

Summary of Recently Conducted UCR Quality Assurance Reviews (QARs)

PURPOSE

To present results of recently conducted UCR QARs.

POINT OF CONTACT

Global Law Enforcement Support Section, Criminal Justice Information Services (CJIS) Audit Unit (CAU)

Questions regarding this topic should be directed to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to review the information provided and authorize Letters of Interest be sent to each CJIS Systems Officer and UCR Program manager as these reviews have been finalized.

BACKGROUND

During the December 2003 CJIS Advisory Policy Board (APB) meeting, the APB adopted a recommendation from the UCR Subcommittee to provide Letters of Interest to UCR Programs once the agency had the opportunity to respond to the CAU's UCR QAR report. It was agreed that this process would be initiated for all QARs.

The QAR, designed to enhance the Federal Bureau of Investigation's (FBI) UCR Program, provides an assessment of a UCR Program in its adherence to the national UCR Program's standards of reporting. For the QAR, the CAU staff determine how each UCR Program and/or local law enforcement agency manages incidents and whether the data submitted to the FBI's UCR Program comply with national standards. There are two standards assessed during a QAR.

1. A UCR Program must conform to the national UCR Program's submission standards, definitions, specifications, and required deadlines.

2. A UCR Program must establish data integrity procedures and have personnel assigned to assist contributing agencies in quality assurance practices and crime reporting procedures.

The FBI’s UCR Program standards under which a UCR Program must operate are published in the *CJIS Division UCR Program National Incident-Based Reporting System User Manual* at fbi.gov.

Listed below are the findings from six QARs, which were finalized from November 2019 to December 2020. Finalized QARs are available upon request.

UCR Programs Participating in a QAR	Number of Local Agency Participants	Number of Incidents Reviewed	Number of Errors	Classification Error Rate Percentage	Findings From the QAR
Kentucky (KY)*	70	300	52	17.33	1
Louisiana (LA)*	12	300	69	23.00	2
Massachusetts (MA)*	103	261	13	4.98	0
South Carolina (SC)*	43	174	16	9.20	1
Arizona (AZ)**	5	201	31	15.42	2
Georgia (GA)**	7	154	30	19.48	3

* For the KY, LA, MA, and SC UCR Programs, the QAR process entailed a review of up to 300 incidents to determine the accuracy of reported offense classifications. Furthermore, for every tenth incident the QAR team also reviewed 21 of the 58 data elements.

** For the AZ and GA UCR Programs, only agencies submitting NIBRS data at the time of the QAR participated in the review. For every incident, the QAR team also reviewed 21 of the 58 data elements. In addition, incidents with Group B offenses were reviewed, but separately.

SPRING 2021 UCR SUBCOMMITTEE ACTION:

Motion: Authorize Letters of Interest be sent to each CJIS Systems Officer and UCR program manager as these reviews have been finalized.

Action: Motion carried.

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FLORIDA**

STAFF PAPER

APB ITEM #6

Report on the National Crime Information Center (NCIC) Subcommittee

NCIC ISSUE #1

Proposal from the National Insurance Crime Bureau (NICB) to Modify the Memorandum of Understanding with the FBI CJIS Division

NCIC ISSUE #2

Modification of the Protected Person Date of Birth (PPB) Field Edits

NCIC ISSUE #3

Creation of an Extreme Risk Protection Order (ERPO) File in the NCIC System

NCIC ISSUE #4

Sunset Date for File Transfer Protocol (FTP)

NCIC ISSUE #5

NCIC Third Generation (N3G) Project

NCIC ISSUE #6*

N3G Task Force Status Update

NCIC ISSUE #7*

NCIC Enterprise File Transfer Service (EFTS) Migration Update

NCIC ISSUE #8*

NIEM XML Presentation and Transformation Style Sheet Update

NCIC ISSUE #9 (*Info O*)**

CJIS Division NCIC Status

NCIC ISSUE #10*

NCIC Validation Extension Discussion

*No staff paper

**Delivered with the information only staff papers

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 19, 2021**

STAFF PAPER

NCIC ISSUE #1

Proposal from the National Insurance Crime Bureau (NICB) to Modify the Memorandum of Understanding (MOU) with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division

PURPOSE

To determine whether the current MOU between the FBI and the NICB should be modified to expand the NICB's "Authorized Use" of the National Crime Information Center (NCIC) data to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations.

POINT OF CONTACT

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information provided in this paper and provide appropriate comments, suggestions or recommendations to the NCIC Subcommittee.

BACKGROUND

The NICB is a private, not-for-profit, organization dedicated to combating insurance-related crime. The NICB receives support from approximately 1,100 property-casualty insurers and self-insured companies. The NICB agents work in partnership with insurers and federal, state, and local law enforcement to identify, investigate, and prosecute organized crime rings, corrupt professions, and repeat offenders.

Before the NCIC was created in 1967, the NICB, known then as the National Automobile Theft Bureau (NATB), had the most complete file of stolen vehicle records in the country. The NATB agreed to provide the NCIC with its stolen vehicle records for entry into the NCIC Vehicle File and, in return, was authorized NCIC Vehicle File entry and inquiry access via state or local law enforcement terminals.

In 1973, the NCIC Advisory Policy Board (APB) voted to continue to allow the NICB limited inquiry access to NCIC, but discontinued the NICB's ability to enter records into the NCIC system. In 1994, the CJIS APB voted to give the NICB the capability to access the NCIC Vehicle File via a "mirror image file" to be updated automatically and simultaneously via a direct CJIS Wide Area Network connection to NCIC. The NICB use of the NCIC Vehicle "mirror image file" is currently regulated by an MOU between the FBI and NICB and outlines the following uses, access, and services made available to the NICB through their NCIC Vehicle "mirror image file." The MOU:

- Permits an electronic telecommunication link between NCIC and the NICB;
- Permits query-only access to the NCIC Vehicle, License Plate, Boat and Vehicle/Boat Part Files;
- Permits the NICB to receive a copy of NCIC transactions that enter, modify, or cancel records in the Vehicle File;
- Provides the authority to disseminate copies of NCIC stolen property records to heavy or farm equipment manufacturers regarding the theft of equipment they manufacture and copies of stolen aircraft records to the Aviation Crime Prevention Institute;
- Provides the authority to disseminate copies of "inactive" NCIC stolen property records, canceled, or purged, to authorized United States law enforcement agencies;
- Provides the authority to match NCIC records with pertinent export, impound, and total loss (salvage) records for appropriate notification to the agency originating the NCIC record when there is a record match; and,
- Provides only a confirmation of the existence of an NCIC stolen property record to the following:
 1. Entities required to participate in the National Motor Vehicle Title Information System;
 2. Special Investigative Units and Claims Investigators of the insurance industry;
 3. Entities legally authorized and substantially engaged in the business of vehicle rentals;
 4. Auto auction companies;
 5. Vehicle finance companies; and,
 6. Heavy equipment fleet owners who are self-insured and heavy equipment rental companies.

DISCUSSION AND ANALYSIS

The NICB is requesting to expand its authorized use of NCIC data to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations. The shipping and logistics companies, i.e., Amazon, FedEx and United States Postal Service, are not promptly notified when one of their vehicles is stolen, recovered, or impounded. This results in entities managing large fleets to be financially and operationally impacted when their vehicles are stolen and not in service. Through current systems and processes that are in place, the NICB would monitor the entities' fleet of vehicles and provide a notification when a vehicle within their fleet is reported stolen and recovered.

The NICB believes the proposal will mutually benefit the NICB and the law enforcement community. First, it will enhance the ability to identify and recover stolen vehicles that are self-insured and part of a large fleet, which will increase the recovery rate. Second, by automatically notifying the self-insured fleet and logistic entities of a recovery, it will reduce storage fees and the need to contact law enforcement to inquire on the status of a vehicle. Lastly, the NICB would include self-insured fleet vehicles in the information provided to law enforcement when searching against NICB data. This would assist law enforcement in identifying the entity that has an interest in the vehicle.

If approved, the "Authorized Use" section of the current MOU will be modified to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations. This is only a change in policy and has no technical impact on the CJIS System Agencies or the CJIS Division.

The FBI's Office of the General Counsel has expressed no legal objections to this proposal.

Subcommittee members are requested to review the proposal and provide appropriate feedback and recommendations.

RECOMMENDATIONS

Option 1: Expand the "Authorized Use" of NCIC data by NICB to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations.

Option 2: No change.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SPRING 2021 NCIC SUBCOMMITTEE ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 19, 2021**

STAFF PAPER

NCIC ISSUE #2

Modification of the Protected Person Date of Birth (PPB) Field Edits

PURPOSE

Proposal to modify the PPB Field Edits to allow for the current date to be entered.

POINT OF CONTACT

Global Law Enforcement Support Section, National Crime Information Center (NCIC)
Operations and Policy Unit

Questions regarding this topic should be directed to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information provided in this paper and provide appropriate comments, suggestions or recommendations to the APB.

BACKGROUND

According to the *NCIC Operating Manual*, the criteria for entry into the Protection Order File (POF) is as follows:

- Any injunction, restraining order, or any other order issued by a civil or criminal court for the purpose of preventing violent or threatening acts or harassment against, sexual violence or contact or communication with, or physical proximity to another person including any temporary and final orders issued by civil or criminal courts, whether obtained by filing an independent action or as a *pendente lite* order in another proceeding, so long as any civil order was issued in response to a complaint, petition, or motion filed by or on behalf of a person seeking protection and;
- Any support, child custody or visitation provisions, orders, remedies, or relief issued as part of a protection order, restraining order, or stay away injunction pursuant to local, state, tribal, or territorial law authorizing the issuance of protection orders, restraining orders, or injunctions for the protection of victims of domestic violence, dating violence, sexual assault, or stalking.

- Additionally, reasonable notice and opportunity to be heard must be given to the person against whom the order is sought; or, in the case of *ex parte* orders, notice and opportunity to be heard must be provided within the time required by state laws, and in any event within reasonable time after the order is issued, sufficient to protect the respondent's due process rights.

When entering a POF record, the entry of Protected Person data is not mandatory. However, if an agency elects to provide Protected Person data, the Protected Person Name must be entered along with either the PPB or Protected Person Social Security Number. The Protected Person Sex and Protected Person Race are optional fields upon entry.

DISCUSSION AND ANALYSIS

During recent analysis of current NCIC system data fields, the Criminal Justice Information Services Division determined the PPB could not be entered using the current date. Currently, the NCIC fields edits for the PPB state that the field must be a valid Gregorian date less than the date of entry, which does not allow for the entry of a newborn child who may qualify for entry as a protected person.

In comparison, the Missing Person File chapter of the *NCIC Operating Manual* states the Date of Birth (DOB) must be a valid Gregorian date if it is the only numeric identifier. The DOB cannot be later than the current date. If the DOB is not the only numeric identifier, 00 may be entered for the month and/or day when the actual date is unknown.

With current system edits in place, a newborn child may be entered into the Missing Person File the same day they are born, but they may not be entered as a Protected Person in the POF until the day after they are born. These edits may preclude entry of some protection orders in a complete, accurate, and timely manner.

The FBI's Office of the General Counsel has expressed no legal objections to this proposal.

Subcommittee members are requested to review the proposal and provide appropriate feedback and recommendations.

OPTIONS

Option 1: Modify the PPB Field edits to allow for the current date. Depending on technical feasibility, this enhancement may be implemented during the development of NCIC 3rd Generation (N3G) or post N3G initial operating capability.

The Criminal Justice Information Services Division staff performed a technical analysis and determined that it is a low to moderate change (2 to 4 weeks) to the NCIC System.

Option 2: No Change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned a priority: _____ (enter 0-5) and categorized as _____ (enter High, Medium, Low).

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 4M.
Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.
Action: Motion carried.

SPRING 2021 NCIC SUBCOMMITTEE ACTION:

Motion: To accept Option 1 as presented in the topic paper. Option 1: Modify the PPB Field edits to allow for the current date. Depending on technical feasibility, this enhancement may be implemented during the development of NCIC 3rd Generation (N3G) or post N3G initial operating capability. Priority of 3H.
Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 19, 2021**

STAFF PAPER

NCIC ISSUE #3

Creation of an Extreme Risk Protection Order (ERPO) File in the National Crime Information Center (NCIC) System

PURPOSE

To present the policy requirements established by the ERPO File policy group for records entered into the new NCIC ERPO File.

POINT OF CONTACT

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review this paper and provide appropriate comments, suggestions, or recommendations to the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

BACKGROUND

In recent years, mass shootings and other types of gun violence have prompted states to enact legislation attempting to prevent gun tragedies. Many states have passed “red flag” laws which permit law enforcement, family members, and other parties to petition state courts to order the temporary removal of firearms from a person based on the belief they may present a danger to themselves or others. Many of these laws have been identified as Extreme Risk Protection Orders, or ERPOs.

As of November 2020, 20 states and the District of Columbia have enacted ERPOs or similar red flag laws (Connecticut, Indiana, California, Washington, Oregon, Florida, Vermont, Maryland, Rhode Island, Delaware, Massachusetts, Illinois, New York, New Jersey, New Mexico, Hawaii, Nevada, Colorado, Maine, and Virginia). Other states have plans to introduce similar legislation in the near future. Although legislation varies from state to state regarding ERPOs, the same general principles apply nationwide. An ERPO (generally):

- makes it illegal for the respondent to purchase or possess firearms

- is filed against a person who poses a significant danger of causing personal injury to self or others by possessing firearms
- may be initiated by law enforcement, a family or household member, mental health professionals, educators, co-workers, etc. (depending on state law)
- may not exceed one year

During the fall round of the 2019 Advisory Process, a topic paper was drafted based on a request to expand the criteria for entry for NCIC Protection Order File (POF) to allow for the entry of ERPOs. At that time, it was determined that most ERPOs did not meet the criteria for entry into the POF since they are for the restriction of firearms and not intended to protect a specific individual from harassment or domestic violence. Further, entry into the NCIC System requires a criminal justice nexus unless there is specific Federal authority. ERPOs are considered civil orders because they affect the private rights of citizens as compared to administering penal justice. This led to an initial determination that unless current entry criteria for an existing NCIC File was met, ERPOs could not be entered in the NCIC System. The Advisory Process stressed the importance of allowing ERPOs into NCIC where they would be accessible to the criminal justice community for officer and public safety.

Due to feedback from the Advisory Process, a more in-depth policy and legal analysis was conducted. The FBI determined that, so long as there is a criminal justice nexus, ERPOs could be entered into the NCIC System. This analysis established that in order for criteria to be met, the petitioner of the order must be a criminal justice agency (or an authorized employee of a criminal justice agency) or the order must have been issued by a criminal court. NCIC Program Office staff delivered this message during the fall 2019 NCIC Subcommittee meeting. At that time, the NCIC Subcommittee made a recommendation to the CJIS APB to “endorse the creation of a new NCIC file specifically for the entry of ERPOs and endorse the entry of all authorized ERPOs into the newly created NCIC file.” During the December 2019 APB meeting in Atlanta, Georgia, the recommendation for the creation of the new file was approved. On June 23, 2020, the FBI Director approved this recommendation to become NCIC policy.

DISCUSSION AND ANALYSIS

Once the creation of an ERPO File was approved, it was apparent that input from the NCIC user community would be necessary to assist in the establishment of policy to govern the new file. As a result, an ERPO File Policy Group was created. The policy group met via teleconference on ten occasions between May and October 2020. Agenda items for meetings included the criteria for entry, the establishment of fields and codes, and validation requirements for the new file. A synopsis of key discussion points, along with policy group recommendations are provided below.

RECOMMENDATION

Issue 1: Criteria for Entry

ERPOs are similar to protection orders in that they are issued by state courts with legal requirements that vary from state to state. However, since they are intended to restrict an

individual from possessing a firearm rather than for protecting individuals from harm, matters such as the petitioner of the order are vastly different. The policy group compared state ERPO laws with the criteria for entry into the POF in order to assist in the establishment of criteria that would encompass guidelines that allowed for the entry of all orders into the national system meeting the criminal justice nexus requirement.

The policy group discussed incorporating a definition of “firearms” as part of the entry criteria. Title 18 United States Code, Chapter 44, § 921, which is the United States Bureau of Alcohol, Tobacco, Firearms, and Explosives definition was considered, in addition to those cited in state laws. The group eventually agreed there was danger in using a definition that strayed from the restriction outlined in the respective state laws. Therefore, the criteria would best be served by deferring to the state law in which the order was issued.

Much time was spent discussing petitioner data, restrictions named in state laws other than firearms, and ensuring that universal language was used when referring to court proceedings. The group ultimately decided to take a broad view when developing the criteria, so as not to unintentionally limit entry due to stringent national guidelines. Based on policy group deliberation, the final draft of the criteria for entry is recommended as follows (in *italics*):

1 Background

1.1 The Extreme Risk Protection Order (ERPO) File contains orders issued by a criminal or civil court for temporarily restricting an individual from purchasing or possessing a firearm, ammunition, or other related items, based on a finding that they may pose a significant danger of personal injury to themselves or others. The types of ERPOs and the information contained in them vary from state to state.

1.2 CRITERIA FOR ENTRY

Each record in the ERPO File must be supported by a court order (electronic or hard copy). ERPOs must meet the following criteria before an entry can be made into the file:

1. The ERPO includes a court finding that the named respondent of the order poses a significant danger of causing personal injury to themselves or others by having a firearm, ammunition, or other related items as set forth in state law, in their custody or control.

2. Reasonable notice and opportunity to be heard must be given to the person against whom the order is sought; or, in the case of ex parte orders, notice and opportunity must be provided within the time required by state laws, and in any event within reasonable time after the order is issued, sufficient to protect the respondent’s due process rights.

Ex parte - without notice to the respondent or the opportunity of the respondent to be heard.

Please note: Ex Parte orders should be entered as temporary ERPO records.

3. The named petitioner in the ERPO is a criminal justice agency or an employee of a criminal justice agency who is statutorily authorized to serve in such capacity and must be doing so within the scope of his or her official duties (e.g., Law Enforcement Officer, States Attorney).

If the named petitioner is not a criminal justice agency or a statutorily authorized employee of a criminal justice agency (e.g., family member), the order must be issued by a court that is acting pursuant to its lawful authority to adjudicate criminal matters.

An ERPO may be entered based on the type of petitioner and/or the type of court proceeding under which the order is issued. The intention of the inclusion of the second half of the third criterion is to ensure agencies have an understanding that the two are not mutually exclusive. In addition, it is intended to clarify that if the petitioner is a family member, educator, co-worker, or other individual who is authorized under state law, but falls outside of the criminal justice community, the order must have been issued by a court that judicially resolves criminal cases. Strictly civil orders with a non-criminal justice petitioner will not meet criteria.

Option 1: Accept the criteria for entry as recommended by the ERPO File policy group.

Option 2: Do not accept the criteria for entry as recommended by the ERPO File policy group and suggest recommendations as appropriate.

RECOMMENDATION

Issue 2: Record Retention

The policy group recommended that like POF records, ERPO File records should remain active until they are canceled or cleared by the record-entering agency or until the expiration date is reached. Agencies will have the ability to modify the expiration date if it is changed by the court. POF records differ from most NCIC person file records in that once a record has expired, it goes into an inactive status but remains available for up to five years as part of an on-line inquiry response if a direct query into the POF is conducted via the Query Protection Order (QPO) message key (MKE). However, since most state ERPO laws indicate that records should be removed from federal systems once the order has been vacated, ERPO File records will not be made available in this manner.

Regarding retention, the policy group stressed the importance of entering the ERPO's exact date of expiration as deemed by the court in the Expiration Date (EXP) Field. The same policies, codes, and system edits in place for the EXP Field in the POF are recommended for use in the ERPO File.

Option 1: Accept the following recommendations from the ERPO File policy group regarding ERPO File record retention:

1. The ERPO File policy group recommends that ERPO File records remain active until the record entering agency takes action to clear or cancel the record, or the expiration date has been reached.

2. The ERPO File policy group recommends that once ERPO File records are removed from active status they are no longer available in the on-line environment.
3. The ERPO File policy group recommends that policy be created to ensure agencies enter the accurate expiration date, as established by the issuing court, into the EXP Field.

Option 2: Do not accept the ERPO File policy group recommendations regarding record retention and suggest recommendations as appropriate.

RECOMMENDATION

Issue 3: Message Key (MKE) Codes

All NCIC files maintain specific MKEs that initiate the entry of base record and supplemental data, as well as the modification and removal of data. Some NCIC person files maintain MKEs that allow agencies to inquire directly into records within specific files. This is true for the Gang, Known or Suspected Terrorist, Identity Theft, Missing, Protection Order, Unidentified, and National Sex Offender Registry (NSOR) Files. In addition to the direct inquiry, records within these files may also be returned as a result of a wanted person inquiry. The remaining files (Immigration Violator, Protective Interest, Supervised Release, and Violent Person) do not contain an MKE for a direct inquiry and records are only returned as a result of a wanted person query.

As mentioned above in Issue 2, once a POF record has reached its expiration date or is cleared by the record-entering agency, it is retained in the NCIC System operational environment and may be accessed via a direct inquiry. Since it has been established that cleared and expired ERPO File records will not be accessible via a direct inquiry, the policy group decided that it would not be necessary to create an inquiry MKE for the ERPO File. Therefore, ERPO File records will be returned as a result of Query Wanted transactions. In addition, in order to remain consistent with files that do not allow for a direct inquiry, Query Vehicle transactions will return records when vehicle information in ERPO File records is hit upon. ERPO records will be returned in test transactions as well.

Caution indicators are added to the MKE when it is known that an individual is armed and dangerous, is a drug addict, or whatever is appropriate to the particular circumstances of the individual. However, the policy group recommended that based on the potential threat to officer and public safety, a caution will be included in all ERPO File record responses. Therefore, caution indicators would not be necessary in the ERPO File as they are in other person files. As a result, the Caution and Medical Conditions (CMC) Field will not become mandatory with the presence of a caution in the ERPO File as it does in other NCIC person files. The following chart provides a representation of the MKEs available in the ERPO File as recommended by the ERPO File policy group:

Message	MKE	Definition	Translation
Entry	ERO	Enter Risk Order	EXTREME RISK PROTECTION ORDER
	ETRO	Enter Temporary Risk Order	TEMPORARY EXTREME RISK PROTECTION ORDER
Modify	MRO	Modify Risk Order	
	MTRO	Modify Temporary Risk Order	
Cancel	XRO	Cancel Risk Order	
	XTRO	Cancel Temporary Risk Order	
Inquiry	QW	Query Wanted	
	QWA	Query Wanted - All	
	QWE	Query Wanted - Extraditable	
	QWF	Query Wanted - Felony	
	QWS	Query Wanted - State	
	ZW	Test/Training	
	QWB	Query Wanted - Batch	
	QWI	NGI/III and NCIC Transaction	
	QV	Query Vehicle	
	ZV	Test/Training	
Clear	CRO	Clear Risk Order	
	CTRO	Clear Temporary Risk Order	
Entry of Supplemental	ENRO	Enter Supplemental Risk Order	
Cancel Supplemental	XNRO	Cancel Supplemental Risk Order	

Option 1: Accept the MKEs for entry, modification, removal, and inquiry of ERPO File records as recommended by the ERPO File Policy Group.

Option 2: Do not accept the MKEs as recommended by the ERPO File Policy Group and suggest recommendations as appropriate.

RECOMMENDATION

Issue 4: Record Integrity

Agencies entering records into NCIC are responsible for the accuracy, timeliness, and completeness of the data. The CJIS Audit Unit (CAU) conducts triennial audits in an attempt to confirm that agencies are following policy guidelines by keeping their records accurate and up-to-date. The ERPO File policy group reviewed each aspect of the NCIC policies for record integrity. Summarizations of policy group discussions and recommendations are provided below.

Validation

The NCIC validation policy is intended to ensure that record-entering agencies confirm that records are complete, accurate, and active. All NCIC person file records, with the exception of the NSOR and the Known or Suspected Terrorist (KST) Files, are validated 60-90 days from entry and yearly thereafter. NSOR Files records are validated based on the Offender Registration Date (ORD) since the subject's information is updated during annual check-ins and the ORD may differ from the date of entry due to incarceration or other factors. KST File records are validated monthly by the Terrorist Screening Center (TSC). The policy group determined that ERPO File records did not present any specific justification for variance from the validation policy. Therefore, it was recommended that ERPO File records be validated in accordance with the standard NCIC validation process.

Accuracy

The accuracy of NCIC records is an integral part of the NCIC System. The accuracy of a record must be double-checked by a second party. The verification of a record should ensure all available cross checks were conducted and that the data in the NCIC record match the data in the investigative report. The ERPO File policy group could not identify any reason for ERPO File record entries to differ from all other NCIC person file records in regards to the policy for record accuracy. As such, it was recommended that ERPO File records be subjected to second party check requirements.

Record Timeliness

The NCIC timeliness policy states that NCIC entries must be entered immediately when the conditions for entry are met, not to exceed 3 days, upon receipt by the entering agency. The only exceptions to immediate entry are when otherwise prescribed by federal law or when documentation exists to support delayed entry. Federal warrants and missing persons under the age of 21 are the only subset of person file records that fall into the category of "exceptions." All other files should be entered as soon as possible once the minimum amount of data required for entry (i.e., all mandatory fields) and the appropriate record documentation are available. Since there is no federal law prescribing ERPO File records to be entered in an expedited manner (as there is with Missing Person File records), the policy group recommended that ERPO File records will be susceptible to the timeliness policy of all other person files.

Record Completeness

Record completeness includes all critical information that was available on the person or property at the time of entry. Critical information is defined as data fields that will:

- 1) Increase the likelihood of a positive hit on the subject or property and aid in the identification of the subject or property; or
- 2) Assist in compliance with applicable laws or requirements.

Validation should include a review of additional information which is missing from the original entry that could be added has become available for inclusion to the record.

The policy group could not determine any justification for ERPO File records to deviate from all other person files regarding record completeness. For this reason, the ERPO File policy group recommended that ERPO File records will be reviewed for record completeness as are all other NCIC records under the existing policy.

Audit

The policy group made a recommendation that the CAU include the ERPO File in their review of records during triennial audit cycles.

Critical Fields for Audit Purposes

Critical fields are those reviewed by the CAU for record completeness and accuracy. The policy group considered the fields identified as critical for the Wanted, Missing, and Protection Order Files. After much deliberation, the policy group recommended that the following fields would be considered critical for audit purposes, and as a result be reviewed during the CJIS audit process: Name (NAM), Date of Expiration (EXP), Sex (SEX), Race (RAC), Date of Birth (DOB), Social Security Number (SOC), FBI Number (FBI), Alias (AKA), Scars, Marks, Tattoos, and Other Characteristics (SMT), Miscellaneous (MIS), Caution and Medical Conditions (CMC), Miscellaneous Number (MNU), Operator's License Number (OLN) (data set), and License Plate Number (LIC) (data set). These fields are consistent with other NCIC person files.

Hit Confirmation

An NCIC hit alone is not probable cause to arrest. NCIC procedure requires that the inquiring agency contact the record-entering agency to confirm that data within the record is accurate and up-to-date. A hit confirmed with the originating agency can be adequate grounds to recover stolen property, return a missing person, arrest a fugitive, or charge a person with violation of a protection order. Some NCIC Files do not require hit confirmation and were designed to provide law enforcement officers with warning regarding individuals who have had involvement with criminal activities or are known to represent potential danger to the public. However, the ERPO File policy group recommended that ERPO File records remain consistent with POF records and require hit confirmation.

Option 1: Accept the following recommendations from the ERPO File policy group regarding the record integrity of ERPO File records:

1. The ERPO File policy group recommends that the validation policy for ERPO File records is 60-90 days from entry and yearly thereafter.
2. The ERPO File policy group recommends that record-entering agencies will be responsible for conducting a second party check and all other requirements as outlined in the existing policy for record accuracy for ERPO File records.
3. The ERPO File policy group recommends ERPO File records must be entered immediately when the conditions for entry are met, not to exceed 3 days, upon receipt by the entering agency (unless documentation exists to support delayed entry). ERPO File records should be entered as soon as possible once the minimum amount of data required for entry (i.e., mandatory fields) and the appropriate record documentation are available.

4. The ERPO File policy group recommends that ERPO File records will be reviewed for record completeness as are all other NCIC records under the existing policy.
5. The ERPO File policy group recommends that the ERPO File be audited by the CJIS Audit Unit.
6. The ERPO File policy group recommends the following fields be critical for audit purposes: NAM, EXP, SEX, RAC, DOB, SOC, FBI, AKA, SMT, MIS, CMC, MNU, OLN (data set), and LIC (data set).
7. The ERPO File policy group recommends that hit confirmation be required for ERPO File records.

Option 2: Do not accept the ERPO File policy group’s recommendations for record integrity and provide recommendations as appropriate.

RECOMMENDATION

Issue 5: ERPO File Fields

The ERPO File policy group referenced numerous NCIC person files in order to create data fields that would apply to the ERPO File. In addition, the National Instant Criminal Background Check System (NICS) Section was contacted to provide their perspective. The group made decisions regarding the creation of fields for base record entry, supplemental data entry, and policy and system edits for applicable fields. Since NCIC is in the process of transitioning from the current system to the NCIC 3rd Generation (N3G), the policy group made recommendations for current and future system field requirements. A brief overview of policy group recommendations for new fields is outlined below.

Fields Available at Entry

The policy group reviewed fields available in several other NCIC person files in order to reach decisions for fields they believed should be available for entry in the ERPO File. Again, due to similarities, fields available in the POF were closely considered. It became evident that several new fields would need to be created in order to capture data unique to the new file. For example, the POF contains the Protected Person data set. Unlike protection orders, the petitioner named in ERPOs is not necessarily facing a similar form of danger. Therefore, petitioner data in ERPO File records is less relevant to those reviewing record responses. For this reason, the group elected to omit the protected person data set in lieu of an optional “Petitioner” field to allow record-entering agencies to enter the agency or individual (depending on state laws and other factors) into the ERPO File record if they so choose.

The POF contains a Protection Order Number (PNO) Field. Both the NICS Section and policy group recognized the importance of capturing the unique number issued by courts in ERPO File records. Since ERPOs are not standard protection orders, the policy group recommended the creation of an “Order Number” field in lieu of the PNO Field. The new field will follow the same system edits as the PNO Field in the POF (conditional for entry based on population of the Originating Agency Case Number [OCA]).

After close review of fields in existing NCIC Files, the policy group recommended the following fields be available at the time of an ERPO File record entry (mandatory fields represented in bold font): **Header (HDR), Message Key (MKE), Originating Agency Identifier (ORI), Name (NAM), Sex (SEX), Race (RAC)**, Place of Birth (POB), **Date of Birth (DOB), Date of Expiration (EXP)**, Height (HGT), Weight (WGT), Eye Color (EYE), Hair Color (HAI), FBI Number (FBI), Skin Tone (SKN), Scars, Marks, Tattoos, and Other Characteristics (SMT), Fingerprint Classification (FPC), Miscellaneous Number (MNU), Social Security Number (SOC), Operator's License Number (OLN), Operator's License State (OLS), Operator's License Year of Expiration (OLY), **Date of Issue (ISD), Originating Agency Case Number (OCA) or Order Number (ORN)**, Miscellaneous (MIS), Notify Originating Agency (NOA), License Plate Number (LIC), License Plate State (LIS), License Plate Year of Expiration (LIY), License Plate Type (LIT), Vehicle Identification Number (VIN), Vehicle Year (VYR), Vehicle Make (VMA), Vehicle Model (VMO), Vehicle Style (VST), Vehicle Color (VCO), Court Identifier (CTI), Petitioner (PET), Caution and Medical Condition (CMC), DNA Profile Indicator (DNA), DNA Location (DLO), Citizenship (CTZ), Ethnicity (ETN), Service Information (SVC), Service Date (SVD), Linking Agency Identifier (LKI), Linking Case Number (LKA), and State Identification Number (SID).

As mentioned, the policy group was cognizant of future enhancements approved as part of the N3G Project throughout ERPO File deliberations. The ERPO File will be implemented in the current system. In regards to fields used to initiate entries, modifications, and record removal, the policy group recommended to remain consistent with those used in the POF. Also, field lengths, system edits, etc., will be the same until such time that full N3G capabilities are made available and N3G-approved enhancements can be applied to ERPO File fields in concurrence with all other NCIC Files.

The policy group also made a recommendation to the N3G Task Force to consider the inclusion of address data in the ERPO File. Since the requirement to incorporate address data in Files other than the Wanted Person and NSOR has not yet been approved, the ERPO File policy group could not make a recommendation to include address data in the current system.

Supplemental Data Fields

Once the policy group finalized recommendations for data fields allowable for the entry of a base record in the new ERPO File, supplemental data fields were reviewed. Once again, existing supplemental data fields in other NCIC person files were used for reference. Supplemental information exists in all other NCIC person files and is used to capture additional identifiers. For consistency purposes, the policy group elected to replicate the fields available for supplemental entry in other person files where applicable. Taking field additions into consideration, the ERPO File policy group recommendations for available supplemental data fields in the ERPO File are as follows: Alias (AKA), DOB, SMT, MNU, SOC, OLN (data set), LIC (data set), VIN (data set), Image NCIC Number (IMN), Image Type (IMT), CMC, CTZ, and SID. All field character limitations and system edits are recommended to remain consistent with other existing NCIC person file supplemental data elements. Once N3G capabilities are fully implemented, ERPO File supplemental field requirements will be updated accordingly.

Option 1: Accept the following recommendations from the ERPO File policy group regarding ERPO File fields:

1. The ERPO File policy group recommends the following fields be available at the time of record entry: **HDR, MKE, ORI, NAM, SEX, RAC, POB, DOB, EXP, HGT, WGT, EYE, HAI, FBI, SKN, SMT, FPC, MNU, SOC, OLN, OLS, OLY, ISD, OCA/ORN, MIS, NOA, LIC, LIS, LIY, LIT, VIN, VYR, VMA, VMO, VST, VCO, CTI, PET, CMC, DNA, DLO, CTZ, ETN, SVC, SVD, LKI, LKA, and SID.**
2. The ERPO File policy group recommends the following supplemental data fields be available in the ERPO File: **AKA, DOB, SMT, MNU, SOC, OLN, OLS, OLY, LIC, LIS, LIY, LIT, VIN, VYR, VMA, VMO, VST, VCO, IMN, IMT, CMC, CTZ, and SID.**
3. The ERPO File policy group recommends that the N3G Task Force consider the inclusion of address data in the NCIC ERPO File. Further, the fields, field character limitations, and conditions for the address data set available in the Wanted Person File should be mirrored in the new File. This would include the following fields: Street Number (SNU), Street Name (SNA), City Name (CTY), County (COU), State (STA), Zip Code (ZIP), Address Type (ADD), and Date of Documented Address (DDA).
4. The ERPO File policy group recommends that the following combination of fields be used to initiate transactions in the ERPO File: NAM and NIC, NIC and OCA, NAM and OCA, and NAM and ORN.
5. The ERPO File policy group recommends the following number of additional identifiers for supplemental entries in the ERPO File in the current and future (as recommended by the N3G Task Force and approved by the APB) NCIC environments:

Field	Current	Future (N3G)
AKA	99	99
DOB	9	25
SMT	9	99
MNU	9	25
SOC	9	25
OLN (data set)	9	25
LIC (data set)	9	25
VIN (data set)	9	25
IMN (data set)	12	25
CMC	10	25
CTZ	9	25
SID	9	25

6. The ERPO File policy group recommends all current field lengths be consistent with other person files when the ERPO File is made available in the current NCIC environment.
7. The ERPO File policy group recommends the acceptance of increased field lengths (as recommended by the N3G Task Force and approved by the APB) for applicable fields in the ERPO File when N3G functionality is made available. The current and future field lengths are provided below:

Field	Current	Future (N3G)
NAM	30	50
MIS	500	1000
MNU	15	30
OCA	20	30
ORN (equivalent to PNO)	15	30

Option 2: Do not accept the ERPO File policy group recommendations for ERPO File fields and provide recommendations as appropriate.

RECOMMENDATION

Issue 6: Codes

Each field available in the NCIC System allows for the entry of either coded data maintained by the FBI or space to enter a range of free-text information. Codes are commonly referred to as Message Field Codes (MFCs). As referenced above in Issue 5 of this topic paper, the PET and ORN were the only fields recommended by the policy group to be created specifically for the ERPO File. They recommended that both new fields would allow agencies to enter information via free-text rather than codes. The ERPO File policy group closely reviewed existing codes associated with fields that would be available in the ERPO File. They elected to accept the current codes for all applicable fields in order to remain consistent with all other NCIC person files. Further, the policy group approved of recommendations made by the N3G Task Force for additional codes and proposed that the new codes are made available in the ERPO File when appropriate.

Option 1: Accept the following recommendations from the ERPO File policy group pertaining to ERPO File MFCs:

1. The ERPO File policy group recommends all codes for fields being implemented in the ERPO File remain consistent with other NCIC person files when applicable.
2. The ERPO File policy group recommends that the PET and ORN Fields allow for a range of free-text data.
3. The ERPO File policy group recommends the addition of the following CMC codes in the ERPO File when N3G functionality is made available (as previously approved by the N3G Task Force and the APB): Blind, Deaf, Prior Law Enforcement Experience, Special Military Training, Behavioral Issues, Speech Impediment, and Universal Medical.
4. The ERPO File policy group recommends to adopt the recommendations of the N3G Task Force and create two separate fields for “cautions” and “medical conditions” in the ERPO File when N3G functionality is made available.

Option 2: Do not accept the ERPO File policy group recommendations for ERPO File MFCs and suggest recommendations as appropriate.

RECOMMENDATION

Issue 7: Indication of Firearm Prohibition

The POF allows agencies to enter specific terms and conditions of a protection order as identified in court proceedings. These conditions are indicated in the Protection Order Conditions (PCO) Field. The PCO Field is mandatory at entry and is populated with codes 01-09. Per NCIC policy, the details of terms and conditions, other than what is captured in available codes, are to be placed in the Miscellaneous (MIS) Field. The ERPO File policy group considered the inclusion of a field to indicate conditions other than firearm restriction in the ERPO File.

Generally, state ERPO laws identify the criteria for issuance of an ERPO as a threat that an individual may endanger themselves or others by possessing a firearm. ERPO File conditions are limited to the restrictions of firearms, ammunition, dangerous weapons, concealed carry permits, and dealer's licenses. Most state ERPO legislation specifically indicates that no other restrictions apply to a court-issued ERPO. Since courts have the ability to issue standard protection orders, if conditions other than firearm restrictions are deemed necessary a standard protection order may be issued in addition to, or in place of, an ERPO.

The policy group debated the inclusion of the PCO Field in the ERPO File, mostly based on PCO Code 07, which states: "THE SUBJECT IS PROHIBITED FROM POSSESSING AND/OR PURCHASING A FIREARM OR OTHER WEAPONS AS IDENTIFIED IN THE MISCELLANEOUS FIELD." Although it will most likely be understood that the presence of an ERPO File record in a hit response is indicative of a firearm prohibition, the policy group stated that officers at roadside, as well as those making firearm background check determinations in the NICS Section would benefit from a specific "flag" that would assist in quickly identifying a prohibited individual. This led to discussion regarding the Brady Indicator (BRD) Field. The BRD is available in the POF to indicate federal firearm prohibition under 18 United States Code (USC) § 922(g) (8). However, since there is currently no federal law recognizing ERPOs, the BRD would not apply.

It was ultimately decided that it was not necessary to create a conditions field for the sole purpose of indicating firearm prohibition and that a caveat would better serve the recipient of ERPO File record responses. The policy group, in consultation with representatives from the NICS Section, drafted the following caveat to precede all ERPO file record responses:

******THE SUBJECT OF THIS RECORD IS PROHIBITED FROM RECEIVING OR POSSESSING A FIREARM AND OTHER RELATED ITEMS BY COURT ORDER******

The policy group believes this encompasses their intention to assist those reviewing NCIC record responses in understanding the subject of record is prohibited from possessing a firearm, and also aligns with the criteria for entry into the ERPO File.

Option 1: Accept the ERPO File policy group recommendation to create the following caveat to precede all ERPO File records responses in order to alert those reviewing record responses that the subject of record is prohibited from possessing a firearm:

******THE SUBJECT OF THIS RECORD IS PROHIBITED FROM RECEIVING OR POSSESSING A FIREARM AND OTHER RELATED ITEMS BY COURT ORDER******

Option 2: Do not accept the ERPO File policy group recommendation to create the caveat as drafted and provide recommendations as appropriate.

RECOMMENDATION

Issue 8: MIS Field Requirements

Each NCIC File contains a Miscellaneous/MIS Field. The MIS Field is a free-text field intended to be the location within the NCIC record in which the record-entering agency may capture any information they believe relevant that is not available in existing NCIC fields. NCIC policy indicates that in the event data cannot be captured within the confines of character limitations, the remaining data should be entered into the MIS Field. Further, each NCIC File has specific data that should be entered into the MIS Field based on the nature of the data within the file. For example, POF policy encourages agencies to enter specific terms and conditions of court-issued orders not able to be captured by one of the available PCO codes in the MIS Field. As mentioned in Issue 7 of this topic paper, the policy group made the recommendation that the ERPO File not contain a field to capture conditions of ERPOs, since at present time state ERPO laws solely restrict an individual for purchasing or possessing firearms, ammunition, etc. Taking future state laws into consideration, the policy group made a recommendation that policy guidance be created to advise agencies to enter conditions of court-issued ERPOs (other than firearm restrictions) into the MIS Field.

The ERPO File policy group reviewed MIS Field requirements for numerous existing NCIC Files. During deliberations for mandatory fields for entry, the policy group considered recommending the CTI Field be mandatory. However, it was determined that not all courts have an ORI. As a result, the policy group agreed that policy should be created to encourage agencies to enter court data into the MIS Field if it cannot be entered into the CTI Field.

Option 1: Accept the following recommendations from the ERPO File policy group pertaining to policy requirements for data to be entered into the MIS Field:

1. The ERPO File policy group recommends the following guidance be included in the appropriate location within the ERPO File section of the NCIC Operating Manual concerning the MIS Field:
 - Any data exceeding character limitations in NCIC fields should be entered into the MIS Field.
 - Specific details regarding cautions and medical conditions when CMC/Other is used should be entered into the MIS Field.

- The edit table in the ERPO File section of the NCIC Operating Manual will indicate that if a non-conforming VIN is present, “SVIN” should be entered as the first four characters in the MIS Field.
- 2. The ERPO File policy group recommends policy be created to advise agencies to enter court information in the MIS Field if the CTI Field cannot be populated.
- 3. The ERPO File policy group recommends policy be created to advise agencies to enter conditions of which the subject of the ERPO File record must adhere (other than firearm restrictions) in the MIS Field.

Option 2: Do not accept the ERPO File policy group recommendations for policy requirements and provide recommendations as appropriate.

RECOMMENDATION

Issue 9: ERPO File Placement in NCIC Hit Responses

The NCIC System returns hit responses based on file type. The order is decided upon by the NCIC user community via the Advisory Process. NCIC person files are returned ahead of property files. The current order of person file records is as follows:

1. Wanted Person
2. Missing Person
3. KST
4. Gang
5. Violent Person
6. Sex Offender
7. Supervised Release
8. Immigration Violator
9. Protection Order
10. Identity Theft
11. Protective Interest
12. NICS Denied Transaction

The ERPO File policy group began deliberations on the topic by considering criteria previously used to place files in the existing hierarchy of hit responses. Although no clear criteria was established, it was determined that officer safety and the likelihood of data being actionable were the main influences. The hierarchy was last revisited in 2012 when the Violent Person File (VPF) was implemented. The VPF was created to alert law enforcement officers that an individual they are encountering may have the propensity for violence against law enforcement. As listed above, VPF records are returned in the fifth position of the hits order hierarchy. However, when placing the VPF, the hierarchy was less of a priority since the following caveat would precede all other hits when a VPF record is present in the response:

WARNING-A SUBJECT IN THIS RESPONSE HAS BEEN IDENTIFIED AS A VIOLENT OFFENDER OR A SERIOUS THREAT TO LAW ENFORCEMENT OFFICERS. REVIEW THIS RESPONSE IN ITS ENTIRETY TO OBTAIN ADDITIONAL INFORMATION ON THIS SUBJECT. USE EXTREME CAUTION IN APPROACHING THIS INDIVIDUAL.

Because the caveat is displayed at the top of all record responses and is not directly associated with returned VPF records, agencies employing an Extensible Markup Language (XML) format must produce technical solutions to ensure a link between the caveat and the record. Since NCIC will be migrating to a native XML communication protocol beginning September 30, 2022, the policy group determined that a caveat should not be created for ERPO File records in the same manner. Rather, as described previously a caveat will be included as part of each individual ERPO record returned in a hit response.

During the fall round of the 2019 Advisory Process, the user community stressed the importance of the creation of the ERPO File due to officer safety. After considering the likelihood of an ERPO File record being actionable, the threat that a subject may be a danger to officer and public safety, the potential volume of records that will be present in the File, as well as similar factors for all other NCIC person files, the policy group ultimately determined that ERPO File records should be placed just below Wanted Person File records in NCIC hit responses.

Option 1: Accept the ERPO File policy group recommendation to modify the NCIC hit response hierarchy to the following:

1. Wanted Person
2. **Extreme Risk Protection Order**
3. Missing Person
4. KST
5. Gang
6. Violent Person
7. Sex Offender
8. Supervised Release
9. Immigration Violator
10. Protection Order
11. Identity Theft
12. Protective Interest
13. NICS Denied Transaction

Option 2: Do not accept the ERPO File policy group recommendation for the placement of ERPO File records in the NCIC hit response hierarchy and provide recommendations as appropriate.

An addendum to this topic paper for comprehensive ERPO File requirements will be forthcoming at a later time.

The FBI's Office of the General Counsel has expressed no legal objections to this proposal.

The CJIS Division staff performed a technical analysis and determined that it is a medium change (12 to 20 weeks) to the NCIC System.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned a priority: _____ (enter 0-5) and categorized as _____ (enter High, Medium, Low).

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Issue 1: Criteria for Entry

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issues 2-9:

Motion: To accept Option 1 on Issues 2-9 as presented in the topic paper.
Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Issue 1: Criteria for Entry

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 2: Record Retention

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 3: Message Key (MKE) Codes

Motion: To accept Option 1 as presented in the topic paper
Action: Motion carried.

Issue 4: Record Integrity

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 5: ERPO File Fields

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 6: Codes

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 7: Indication of Firearm Prohibition

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 8: MIS Field Requirements

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 9: ERPO File Placement in NCIC Hit Responses

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Issue 1: Criteria for Entry

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue 2: Record Retention

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue 3: Message Key (MKE) Codes

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 4: Record Integrity

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue 5: ERPO File Fields

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 6: Codes

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

Issue 7: Indication of Firearm Prohibition

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 8: MIS Field Requirements

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 8: MIS Field Requirements

Motion: To accept Option 1

Action: Motion carried.

Issue 9: ERPO File Placement in NCIC Hit Responses

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Issue 1: Criteria for Entry

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 2: Record Retention

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 3: Message Key (MKE) Codes

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 4: Record Integrity

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 5: ERPO File Fields

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 6: Codes

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 7: Indication of Firearm Prohibition

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 8: MIS Field Requirements

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 9: ERPO File Placement in NCIC Hit Responses

Motion: To accept Option 1 as presented in the topic paper. Priority 3M
Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Issue 1: Criteria for Entry

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 2: Record Retention

Motion: To accept Option 1 as presented in the topic paper.
Action: Motion carried.

Issue 3: Message Key (MKE) Codes

Motion: To accept Option 1 modified: Accept the MKEs for entry, modification, removal, and inquiry of ERPO File records as recommended by the ERPO File Policy Group with the exception of the addition of the automatic caution indicator. Add the caution indicator to the message key as is consistent with all other NCIC person files.

Action: Motion carried.

Issue 4: Record Integrity

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 5: ERPO File Fields

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 6: Codes

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 7: Indication of Firearm Prohibition

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 8: MIS Field Requirements

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 9: ERPO File Placement in NCIC Hit Responses

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

SPRING 2021 SUBCOMMITTEE ACTIONS:

NCIC SUBCOMMITTEE ACTION:

Issue 1: Criteria for Entry

Motion: To accept Option 1 as presented in the topic paper

Action: Motion carried.

Issue 2: Record Retention

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 3: Message Key (MKE) Codes

Motion: To accept a new Option 3 to adopt the Western Working Group's recommendation: Accept the MKEs for entry, modification, removal, and inquiry of ERPO File records as recommended by the ERPO File Policy Group with the

exception of the addition of the automatic caution indicator. Add the caution indicator to the message key as is consistent with all other NCIC Person Files.

Action: Motion carried.

Issue 4: Record Integrity

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 5: ERPO File Fields

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 6: Codes

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 7: Indication of Firearm Prohibition

Motion: To accept **Option 1 as modified:** Accept the ERPO File Policy Group's recommendation to create a caveat to precede all ERPO File records responses in order to alert those reviewing record responses that the subject of record is prohibited from possessing a firearm; however, modify the caveat to the following:

******THE SUBJECT OF THIS RECORD IS PROHIBITED FROM RECEIVING OR POSSESSING A FIREARM. REFER TO THE MIS FIELD FOR ANY OTHER ADDITIONAL COURT ORDERED PROHIBITIONS******

Action: Motion carried.

Issue 8: MIS Field Requirements

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Issue 9: ERPO File Placement in NCIC Hit Responses

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

NICS SUBCOMMITTEE ACTION:

Accepted as information only.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 19, 2021**

STAFF PAPER

NCIC ISSUE #4

Sunset Date for File Transfer Protocol (FTP)

PURPOSE

To establish a community sunset date for the File Transfer Protocol used to transfer large data files from National Crime Information Center (NCIC).

POINT OF CONTACT

Information Technology Management Section, Information Security Officer

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are to review the information included in this paper and provide appropriate comments, suggestions, and recommendations to the Advisory Policy Board to establish the sunset date for the use of file transfer protocol to transfer large data sets between users and the Federal Bureau of Investigation Criminal Justice Information Services Division.

BACKGROUND

The NCIC File Transfer Protocol, or FTP server, exchanges large data files between the NCIC System and authorized users. Examples of the larger files that require FTP are: lists of records to validate (both \$.C. and Fixed Formats) as well as ORI validations, data extracts such as the License Plate Reader (LPR) extract or Pawn Article and Gun extracts, and large offline search results. Smaller record sets do not require FTP and accomplish data transfers via the NCIC file transfer message key; however, complex results, including long lists of records, currently transfer via FTP. During the NCIC Third Generation (N3G) Task Force user canvas, users requested a more secure method for exchanging large files with FBI CJIS; additionally, federal agency information assurance experts within, and external to the FBI, have continually questioned the legitimacy of using this file transfer method when more secure technology exists.

DISCUSSION AND ANALYSIS

As part of a High Value Asset (HVA) review, a federal security assessment team identified some concerns with use of FTP technology. While CJIS took steps to mitigate the concerns raised by the federal security assessment team, CJIS also explored more secure file transfer methods. This exploration addressed the federal security assessment team's recommendations as well as requests from the user community to evaluate alternative outbound communication methodologies. NCIC Third Generation (N3G) Concept 12 (Alternative Outbound Communications) was created out of necessity and request from the N3G user canvas. The users wanted a new, secure method to transfer large files between agencies and the CJIS Division. This user request, along with the federal assessment team's recommendation for an analysis of alternatives, led to the creation of N3G requirement 12.02.TF03 wherein NCIC will explore additional methodologies to facilitate file transfers.

The CJIS Division explored various options for NCIC file transfers and selected the CJIS Enterprise File Transfer Service or EFTS. Transitioning to EFTS accomplishes the goals of both internal and external stakeholders by mitigating the above-mentioned security risks, and individual users may elect to use an established interface on the Law Enforcement Enterprise Portal (LEEP) or connect machine to machine (sFTP) and incorporate EFTS into established user procedures. Another benefit of transitioning to EFTS is the users' desired increased ability to automate file retrieval. Currently many files, such as validations and extracts, are provided to users at set frequencies, whereas, with EFTS, users can access authorized data at user convenience, which enhances efficiency. A recent example of a state needing more frequent extracts, while accomplished, required much coordination within the CJIS Division. With EFTS, the user can obtain authorized information at the frequency the user chooses.

The CJIS Division, NCIC Operations and Policy Unit (NOPU) brought forth a topic paper in March 2020 notifying the users that EFTS has been chosen as the path forward for file transfers. In May and July 2020, CJIS Systems Officers (CSOs) were notified via letter that CJIS is migrating to EFTS (May), and to advise agencies that record validation can be accomplished via EFTS (July). In September 2020, CSOs were notified that license plate reader extracts and ad hoc offline searches are available via EFTS. Other extracts, such as pawn data, missing/unidentified are now also available via EFTS.

A sunset date for discontinuing FTP services has not yet been decided. During an EFTS demonstration to the N3G Task Force, NOPU requested a notional sunset date for FTP. A notional sunset date was suggested as September 30, 2022 to align with the transition to National Information Exchange Model (NIEM) Extensible Markup Language (XML) transition. NOPU presented the notional sunset to the NCIC Subcommittee and the Security Access Subcommittee without objection and no earlier date for sunset was recommended.

OPTIONS

Option 1: Recommend to the APB Subcommittees an FTP sunset date of December 31, 2021.

Option 2: Recommend to the APB Subcommittees an FTP sunset date of <Subcommittee recommendation>.

RECOMMENDATION

If the FTP server continues to operate, the FBI CJIS Division is required to justify the outstanding security risks to the FBI Authorized Official, the FBI Chief Information Security Officer, and external assessment associations. Therefore, the CJIS Information Security Officer recommends a sunset date of December 31, 2021.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Recommend to the APB Subcommittees an FTP sunset date of December 31, 2021.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: Recommend to the APB Subcommittees an FTP sunset date of December 31, 2021.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Recommend to the APB Subcommittees an FTP sunset date of December 31, 2021.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1: Recommend to the APB Subcommittees an FTP sunset date of December 31, 2021.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2: Recommend to the APB Subcommittees an FTP sunset date of June 30, 2022 due to the time required to implement script changes.

Action: Motion carried.

SPRING 2021 SUBCOMMITTEE ACTIONS:

NCIC SUBCOMMITTEE ACTION:

Motion: To accept Option 1 - Recommend to the APB an FTP sunset date of December 31, 2021.

Action: Motion carried.

SECURITY AND ACCESS SUBCOMMITTEE ACTION:

Motion: To accept Option 1 - Recommend to the APB an FTP sunset date of December 31, 2021.

Action: Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 19, 2021**

STAFF PAPER

NCIC ISSUE #5

National Crime Information Center (NCIC) Third Generation (N3G) Project

PURPOSE

To provide a status on recommendations of the N3G Task Force

POINT OF CONTACT

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to agmu@leo.gov.

BACKGROUND

The purpose of the N3G Project is to identify requirements which will improve, modernize, and expand the existing NCIC System to continue providing real-time, accurate, and complete criminal justice information in support of law enforcement and criminal justice communities.

In June 2016, the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) approved, for further exploration, 14 high-level concepts as representation of more than 5,500 user requests. Functional requirements correlating to those high-level concepts were subsequently forwarded for further review and are listed with the status of the approval process.

Concept 1: Flexible Data Format – Director Approved
Concept 2: Tailored Functionality – Director Approved
Concept 3: Access Data Repositories – Director Approved
Concept 4: Name Search Algorithm – Director Approved
Concept 5: Enhanced Data Search – Director Approved
Concept 6: System Search - Director Approved
Concept 7: Enhanced Training Resources – Director Approved
Concept 8: Enhanced Testing Environment – Director Approved
Concept 9: Record Content – Director Approved
Concept 10: Enhanced Multimedia – Director Approved
Concept 11: Improved Data Management – Director Approved
Concept 12: Alternative Outbound Communications – Director Approved
Concept 13: Alternative Access – Director Approved
Concept 14: Improved Outbound Communications – Director Approved

An N3G Task Force was established to assist with the development of the N3G Project. The purpose of the N3G Task Force is to offer continuous subject matter expertise and user experience to the CJIS Division project personnel during the development of N3G. The APB also granted the N3G Task Force the discretion to provide the initial review, acceptance, and disposition or disposal of the concepts and their associated functional requirements before introducing them through the CJIS Advisory Process. The inaugural N3G Task Force meeting was held on 08/18/2015, and meetings have routinely been conducted both in person and telephonically since the initial meeting. As a result of the collaborative efforts of the N3G Project Team and the N3G Task Force, over 1,200 functional requirements associated with the 14 high-level concepts were identified.

The N3G Task Force dispositioned all 1,200 of the initial functional requirements and recommended 376 move forward for further exploration. Those functional requirements were approved by the APB during meetings held in June 2017 through December 2018. None of the initial functional requirements proposed for Concept 13 were approved by the N3G Task Force. This recommendation was subsequently endorsed by the APB at the December 2017 meeting.

N3G Functional Requirement Exploration Strategy

Since the initial Advisory Process review of N3G Task Force approved functional requirements has concluded, the N3G Task Force has moved into its next area of responsibility to further explore APB approved functional requirements in conjunction with the NCIC Program Office. The method to further explore the remaining N3G functional requirements and an agile Advisory Process approval strategy were adopted by the APB in June 2018. The APB recognized that a streamlined approval process was necessary to ensure the successful and timely deployment of N3G functionality using the Agile Development Methodology.

As a reference, the APB approved process, for moving functional requirements forward, allows the N3G Task Force to determine if a functional requirement falls into either the “straight forward” or “needs further research” category. As described in the spring 2018 topic paper, many of the APB-approved “for further exploration” functional requirements are very straight forward and need no further policy-related information for development. For instance, a requirement may read “expand the name field to 50 characters.” This requirement is straight forward, needing no further policy review for development. As such, it can be turned over to developers as currently defined. The N3G Task Force has identified approximately 150 requirements which fall into the straight-forward category. Other functional requirements do need further policy, legal, and technical refinement, such as the ability to enter “multiple warrants for the same subject by the same Originating Agency Identifier (ORI).” Further research, legal review, and technical impact analysis on 260 of those types of requests will be conducted by the N3G Task Force and the CJIS Division NCIC Program Office collectively. Once completed, those identified as adding value and benefit to NCIC stakeholders will move to the development stage.

As a reminder, any requirements needing major modifications or new requirements identified by the N3G Task Force will be forwarded through the Advisory Process for final approval.

Functional requirements no longer supported by the N3G Task Force will not be moved forward for inclusion in N3G Project development. Functional requirements excluded after the N3G Task Force further exploration are identified in an addendum to this paper for traceability purposes. These items will continue to be included with the N3G Project staff paper for the next several rounds of the Advisory Process meetings until all the exclusions are exhausted.

N3G Functionality Approval Strategy

As the N3G Task Force continues exploring the APB approved functional requirements, new system functionality emerges. This includes an emphasis on streamlining processes when possible, coupled with the development of new or modified policy definitions. In accordance with the APB agile approval process, as N3G Task Force approved functionality advances to the development effort and is ready to demonstrate, the N3G Task Force will confirm functionality (virtually or in person) meets the original intent, as approved by the APB. Their decisions will be forwarded to the NCIC Subcommittee for advisement and endorsement. If the NCIC Subcommittee concurs with the Task Force decision, the recommended N3G functionality will advance to the non-operational environment or directly to the APB for final disposition. Conversely, if the N3G Task Force determines the functionality requires further refinement, it will be returned to a development program backlog and then reintroduced into the development process once necessary changes are identified. Although this approach places considerable responsibility on the N3G Task Force up front, it will pave the way for continued user engagement in the N3G development effort.

The N3G Task Force has established and continues to reiterate several “guiding principles” to be taken into consideration as the requirements are further analyzed and developed. One such principle is to ensure current system performance and response times are not degraded with the introduction of new functionality. Another principle established is continued support of legacy functionality. Since CJIS Systems Agencies (CSAs) and many local agency systems will require upgrades and/or additional programming to take advantage of new capabilities, the CJIS Division is committed to support legacy NCIC System functions during a transition period, to be defined by the APB. This will ensure vital services remain available to all users. The intent of the N3G Project is to be forward looking, but backward compatible. Additional guiding principles include the integration of national standards, when applicable, and scalability. The next generation of the NCIC System should provide scalable capacity for additional input, storage, processing, and output functionality. Furthermore, the N3G Task Force determined enhancements to the NCIC System should be established as user friendly and intuitive as possible. Providing a more intuitive system could simplify training new users and allow current users to be more efficient and effective.

N3G User Transition Fundamentals

The N3G Task Force supported two fundamental N3G transition requirements. These are based on the understanding in which NCIC will continue to release newly developed functionality in the operational environment consistent with the annual enhancement build schedule and associated notification process existing today. They are also in keeping with the “guiding

principles” as described previously. During their June 2019 meeting, the APB approved the following two N3G User Transition Fundamentals as recommended by the N3G Task Force:

1. Extensible Markup Language (XML) User Transition Timeframe

- a. All CSAs and direct interface agencies must convert to the National Information Exchange Model (NIEM) data processing format, using web service applications, from the current NCIC socket supported dot delimited and Global Justice Data Model (GJXDM) formats by **September 30, 2022**.
- b. Dot delimited and GJXDM XML formatted messages, along with Transmission Control Protocol/Internet Protocol socket and MQ Series Protocols will no longer be supported effective **September 30, 2022**.

2. Availability of New Functionality

- a. N3G developed functionality, to include improved and streamlined capabilities, along with new files, fields, and codes will only be available for entry and maintenance using the NIEM XML data processing format. However, dot delimited and GJXDM XML users must be able to accept new data in responses.

At the September 2019 N3G Task Force meeting, the User Transition Fundamentals were discussed at length. The focus of the discussion was whether CJIS Systems Officers (CSOs) have a clear understanding of the intent and implications of not only the approved NIEM XML compliance deadline date, but the availability of new N3G functionality being tied to NIEM compliance. NCIC Program Office staff detailed how a new NCIC System header (1X01) would be utilized in all incoming NIEM XML formatted transactions to delineate new files, fields, and codes are included in the messages. After much discussion, the Task Force requested the Program Office staff create a “Transition to NIEM XML” quick reference sheet for all CSOs to be made available upon request. The quick reference sheet is currently in draft and upon Task Force approval, it will be made available via JusticeConnect through the NCIC Community. As a reminder, the NCIC NIEM Information Exchange Package Data and the Web Services Definition Language documents can also be found in the JusticeConnect NCIC Community.

DISCUSSION AND ANALYSIS

N3G Project – Functionality Approved by the N3G Task Force for Development

As the N3G Task Force further explores approximately 260 functional requirements associated with the original 14 high-level N3G concepts, policy subgroups are formed to thoroughly investigate all aspects of the proposed functionality. Thus far, nine policy groups, including Gang, Warrant, Supplemental Data, Message Key, Missing and Unidentified Persons, Image, Offline Search, XML, and Blue Alert, have been established and meet on a regular basis. Each group is represented by members of the N3G Task Force in addition to other law enforcement and criminal justice community subject matter experts. The following policy groups have concluded and have previously provided recommendations through the Advisory Process: Gang, Message Key, Supplemental Data, Offline Search, and Blue Alert. As the groups presented recommendations to the N3G Task Force for further consideration, it became evident that

individual functional requirements have inter-dependencies. As such, holistic functionality has emerged which encompasses some, or even many individual functional requirements. Individual functional requirements will no longer be presented individually through the Advisory Process with the understanding that the functionality approved by the N3G Task Force satisfies all of the associated functional requirements. Conversely, as discussed previously, functional requirements the N3G Task Force excludes will be identified in the addendum at the end of the staff paper for traceability purposes. The N3G Task Force approved functionality, as described below, is being provided for your information and awareness as it will move forward to the agile development process.

Missing and Unidentified Policy Group

During the N3G User Canvass, participants requested simplifying and enhancing the NCIC Missing Person File and the Unidentified Person File as well as the Cross Match process that occurs between the files. The N3G Task Force established a Missing and Unidentified (M&U) Policy Group to review the NCIC's Missing Person and Unidentified Person Files for refinement and clarification.

The N3G Task Force approved the following functionality related to streamlining the Unidentified Person File and enhancing the Cross Match:

- Streamline Message Key (MKE) for Enter Unidentified Person (EU).
- Create a Category Field for Unidentified – Deceased, Living, and Catastrophe.
- Make the Footprint Available (FPA) Field optional at the time of entry.
- Make the Manner and Cause of Death field two separate, optional fields.
 - Manner of Death Field (MDA) – Coded Field
 - Cause of Death Field (CDA) – Free text Field
- Create a Pelvis Body Part Status Code – 16 – Pelvis.
- Expand the length of the Dentist's Remarks Field (DRE) from 50 to 100 characters.
- Create a Dental Images Available Field (DIA) – Y or N Field. New DIA field would combine and replace Dental X-rays Available (DXR) and Dental Models/ Photographs (MPA).
- Create a field to capture the Dental Images Location (DIL). Free text field, 100 characters.
- Remove the \$.N. Administrative Notifications from the Cross Match.
- Add the Estimated Date of Death (EDD) to the Cross Match Notification.
- Add Category Field to the \$.M. notification for dental comparison. Utilize the Match Data column within the \$.M. notification to depict the matching categories from the Missing Person and Unidentified Person records.
- Incorporate a pre-sort of the Sex data field prior to running the dental comparison algorithm in the Cross Match.
- Analyze the results of the Cross Match and determine how the NCIC System can increase the accuracy of hits produced.

Image Policy Group

The Image Policy Group was established to further explore functional requirements relating to Concept 10 – Enhanced Multimedia. The policy group focused on providing images in all files, overhauling the Image Type (IMT) codes available for record entry, establishing procedures for customizable image responses, and exploring image standards.

Document Images

The ability to append supporting documentation to NCIC records was widely requested during the N3G User Canvass. Users believed returning the documentation during an inquiry would improve the officer's situational awareness. The Image Policy Group explored the various types of documentation associated with NCIC records. The policy group determined many of these documents would negatively impact tactical encounters by increasing both the response time and the time required to review the record. The policy group specified only documents demonstrating a benefit in tactical scenarios should be included in the NCIC System. As a result, the policy group recommended document files be allowed in the Wanted Person and Protection Order Files only. The policy group also established a limit of one document image per record which corresponds to the court issued protection order or the most severe warrant associated with the record.

The N3G Task Force recognized the impact of accepting a copy of the warrant in the NCIC System. The Image Policy Group and Warrant Policy Group were requested by the Task Force to collectively discuss the user benefit and address potential issues relating to hit confirmation and record responses. The policy groups ensured the entry of a copy of the warrant would remain optional like all NCIC image entries. Additionally, the policy groups desired the ability for the inquiring agency to specify whether a document image should be returned as a result of the NCIC query. This will be accomplished via the previously recommended changes to select the maximum number and type of images desired by the agency in the Image Indicator (IND) Field and the IMT filter field.

The Warrant Policy Group also explored improvements to the NCIC System hit confirmation policy to coincide with the addition of document images to the Wanted Person File. A comprehensive outline of the hit confirmation policy and other Wanted Person File issues will be provided following the policy group's conclusion.

The N3G Task Force approved the following functionality relating to Images in All Files:

- Allow the Document (D) IMT code in the Wanted Person File and Protection Order File only. The NCIC policy will be updated to include protection orders and warrants as the only acceptable types of documents for inclusion in NCIC at this time.
- Allow a maximum of one image using the Document (D) IMT code per record. The image will correspond to the most severe warrant or the protection order supporting the record.

Again, the N3G Task Force will continue reviewing APB approved N3G functional requirements until all are exhausted. The CJIS Division continues to explore Task Force approved functionality and will provide updates through this process on any new N3G capability to be delivered.

National Crime Information Center (NCIC) Third Generation (N3G) Project Addendum
Functionality excluded after Program Office Research

Concept 5 – Enhanced Data Search

- Provide the ability to perform searches of active and/or inactive records in the operational environment.

The CJIS Division performed additional review on the ability for local agencies to retrieve inactive records in the operational environment. NCIC records may be considered in active, located, inactive, or retired status. Any record considered current would be in an active status. Located status advises entering agencies the subject has been encountered by another agency. Inactive records are National Sex Offender Registry and Protection Order File records which have expired or have been cleared by the entering agency. Retired records refer to any canceled records and cleared records from the remaining files. Currently, records in inactive status can only be retrieved via the Sex Offender Inquiry (QXS) and Protection Order Inquiry (QPO) MKEs. Retired records must be retrieved via an NCIC offline query.

The CJIS Division determined expanded access to inactive or retired records in the NCIC System operational environment could not be supported as the records do not meet the requirement to be timely and accurate. Furthermore, the records are not subject to the record validation process. The CJIS Division supports access to these records through the established offline searches by the CSA or the FBI. Additionally, local agencies will have access at the CSA's discretion to their own inactive or retired NCIC records as part of the N3G offline search functionality.

- Provide the ability to perform customized searches by allowing the user to indicate specifically which files to search in the operational environment.

The N3G Task Force reviewed the ability to indicate files to search in the operational environment. Users currently indicate the files to be searched via the MKE. While some inquiry MKEs such as the Inquiry - All Persons, Vehicle, License Plate (QW) search multiple files, other MKEs only target one specific file. The Task Force determined the functionality already exists through the current transaction structure but could be improved by interfacing agencies. As a result, the Task Force excluded the functional requirement from further consideration.

- Provide the ability to narrow searches in the Article File by additional numeric identifiers in the operational environment.

The N3G Task Force also considered using additional numeric identifiers to filter Article File inquiries. Article File inquiries can include the property's Serial Number (SER) and/or Owner Applied Number (OAN). The SER and OAN search the Article File for matching identifiers independently. The Task Force reviewed available numeric identifiers for Article File inquiries.

The Task Force determined the identifiers were either non-unique or unlikely to be known at inquiry. Furthermore, other N3G requirements will expand the searchable fields in the operational environment. Therefore, the N3G Task Force recommended the functional requirement be excluded.

- Expand the cross match between the Missing Person and Unidentified Person Files to include image to image searches.
- Expand the cross match between the Missing Person and Unidentified Person Files to include all other NCIC Person Files.

There were requests during the user canvass to modify the cross match by including images and other files in the match. The Task Force believed the accuracy could be impacted negatively due to the number of potential cross-searches which would be performed and users would also be inundated with notifications. Therefore, the group elected to exclude these functional requirements.

Concept 9 – Record Content

- Create a Silver Alert Missing Person Circumstance Code.
- Revisit dental codes and provide better descriptions.
- Require enhanced Body Part Status codes D, F, and S.
- Create a field to capture clothing description in the Missing Person File.
- Create a field to capture clothing description in the Unidentified Person File.
- Create a field to indicate that dental image information is available in the National Dental Image Repository (NDIR) in all person file records (already exists in Wanted, Missing, and Unidentified Person Files).
- Create a field to add additional detail to Dental Characteristics Fields to describe type of restoration.
- Create a field to capture the person is a previous runaway.
- Create a field to capture for post-mortem interval.
- Create a field to capture the Universal Control Number [FBI] field in the Unidentified Person File.

The policy group reviewed many recommendations regarding the content of the Missing and Unidentified Person Files including the addition of many fields and codes. Many requests were excluded based on previous recommendations that negate the need for the recommendations. After reviewing current utility and statistics related to the files, the group agreed that the requirements listed above would not significantly enhance the files and elected to exclude those requirements.

Concept 11 – Improved Data Management

- Provide an easier method to enter vehicle parts.

During the N3G Canvass, users requested providing an easier method to enter vehicle parts in NCIC. Although this request was very broad in scope, the N3G Task Force discussed the NCIC definition of vehicle parts as well as the entry criteria and mandatory fields required for entry. It was also discussed that recommendations made by the MKE Policy Group previously would ultimately streamline the entry process for vehicle parts. Considering all previous streamlining efforts, the Task Force agreed that this request was satisfied. As such, the N3G Task Force recommended that the functional requirement be excluded.

- Revisit dental coding rankings in responses.
- Provide access to dental images directly.
- Expand the cross match to the Wanted Person File.

Current capabilities in the NCIC System regarding dental coding and matching were discussed by the policy group. Upon hearing the available resources, the group determined that there were no potential enhancements to the dental codes that would increase the accuracy of identification. It was also determined that current access to dental images does not need modified and access should not be direct through the NCIC System, as it falls beyond the scope of NCIC. Therefore, the group elected to exclude the requirements listed above.

SPRING 2021 WORKING GROUP ACTIONS:

All five working groups accepted this topic as information only.

SPRING 2021 NCIC SUBCOMMITTEE ACTION:

Accepted as information only.

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FLORIDA**

STAFF PAPER

APB ITEM #8

Report on the National Data Exchange (N-DEx) Subcommittee

N-DEx ISSUE #1* (*Info M*)
N-DEx Program Office Update

N-DEx ISSUE #2 (*See APB Item #6, IS Issue #09*)
The N-DEx System to Obtain More Images from the Next Generation Identification System

N-DEx ISSUE #3
Explore the Ability to Query the Search History of the N-DEx System

N-DEx ISSUE #4* (*Info K*)
Fiscal Year 2020 Audit Results Summary

Ad-Hoc Topic**

Using Derived ORIs to Address Law Enforcement Information Sharing Gaps Within the N-DEx System

*Delivered with the information only staff papers

**No staff paper

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL DATA EXCHANGE (N-DEx) SUBCOMMITTEE
VIRTUAL MEETING**

APRIL 23, 2021

STAFF PAPER

N-DEx ISSUE #3

Explore the Ability to Query the Search History of the National Data Exchange (N-DEx) System

PURPOSE

To present a proposal to explore a query of the search history in the N-DEx System. With the increased use of the N-DEx System by the criminal justice community, an opportunity exists to discover contacts with entities of investigative interest that could lead to the apprehension of criminal suspects and resolution of criminal cases. A review of historical queries in the N-DEx System could provide information to users about the location of suspects and connect the user with other criminal justice professionals who have information about their investigation or suspect.

POINT OF CONTACT

Global Law Enforcement Support Section /Data Sharing Services Unit (DSSU)

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the options presented in this paper and recommend one alternative for the Federal Bureau of Investigation (FBI) staff to pursue.

BACKGROUND

The N-DEx System is a national investigative information sharing system, which includes records from criminal justice agencies across the United States. Criminal justice professionals can search for people, vehicles, telephone numbers, keywords, and much more to discover information that will aid them in the administration of criminal justice. The N-DEx System subscription feature provides notifications to a user concerning future queries of an item of investigative interest. The N-DEx System users can set a subscription on anything searched in the system and receive a notification if another user searches for the same information. However, the subscription does not alert users that a query of the same information was performed prior to the subscription. An N-DEx System query of the search history would allow the user to receive information about past queries of an item of investigative interest. The National Crime Information Center (NCIC) offline transaction log search is a similar feature, which provides information to requested users about queries that have occurred in the

past. Two days after the 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City, an NCIC Offline transaction log search for suspect Timothy McVeigh, alerted investigators he was queried through NCIC ninety minutes after the bombing. The information provided to the investigators led to the subsequent arrest of Mr. McVeigh. An N-DEx System query of the search history would offer the same service to the criminal justice community via the N-DEx System.

DISCUSSION AND ANALYSIS

The N-DEx System is a national investigative information sharing system used by federal, state, local, and tribal criminal justice agencies. The N-DEx System houses information about the queries conducted by all users and could be used to connect criminal justice professionals who have an investigative interest in the same entities or information. A search of the N-DEx System search history could reveal connections, which are not available in an NCIC offline search. The N-DEx System allows the user to search keywords and other structured fields within a criminal justice agency record. These searches could include monikers, modus operandi, Internet Protocol addresses, and other types of information.

The capability to search historical search criteria currently exists in the N-DEx System and is referred to as the Search Criteria Report (SCR). However, the capability is only available for users who have the N-DEx Audit administrative feature and is limited to the agencies under the administrative purview of the user. These restrictive parameters inhibit the ability to fully perform an appropriate query of the search history, which negatively affects an investigation. The following information is currently available from the SCR:

- Date/Time of Query
- User ID
- First and Last Name
- Agency
- Search Purpose
- Search Reason
- Search Parameters

The current SCR is limited to searching one year at a time and is a resource intensive search of the historical search criteria in the N-DEx System. For example, a SCR for a person name completes in approximately one and a half hours for a one-year timeframe. The report also impacts system performance because it is completed within the N-DEx System Audit feature. Development would be required to implement a more efficient search that does not impact N-DEx System performance.

Aside from the technical implementation of a query of the search history, the following policy items should be explored:

- How would users submit a request for a query of the search history?
 - Directly to the DSSU or through the CJIS Systems Agency (CSA)?

- What purposes would be acceptable for a query?
 - Acceptable System Use is defined in the *N-DEx Policy and Operating Manual 1.3.4*.
 - There are twelve acceptable uses listed. Which ones would be appropriate?
- Should a query of the search history be limited in timeframe?
- Should users be able to exclude their search history from a query of the search history?
- Should controls be implemented to restrict the N-DEx System response to return only specific results (such as the inquiring agency's searches or searches from a particular locale or region)?

OPTIONS

Option 1: Explore the implementation of a query of the search history by DSSU staff of the N-DEx System and report the results to the working groups.

Option 2: No change

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

SPRING 2021 N-DEx SUBCOMMITTEE ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

Intentionally Left Blank

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FLORIDA**

STAFF PAPER

APB ITEM #9

Report on the Identification Services (IS) Subcommittee

IS ISSUE #01*

Miscellaneous Action Items Update

IS ISSUE #02*

Identification Services Coordination Group Update

IS ISSUE #03

Consideration of Additional Use Cases for the Next Generation Identification (NGI) Iris Service

IS ISSUE #04

NGI Iris Service Search upon Enrollment Enhancement

IS ISSUE #05

Update to 2019 Topic “Driver’s License Numbers (DLN) in the NGI System

IS ISSUE #06

Posting Federal Dispositions to Multiple Dates of Arrest

IS ISSUE #07

Update on the Interstate Identification Index (III) Delete Record Cycle and Modify Record Cycle Message Key Development

IS ISSUE #08

Unknown and Known Deceased Searches of the Department of Homeland Security’s (DHS) Automated Biometric Identification System and the Department of Defense’s (DoD) Automated Biometric Identification System

IS ISSUE #09

The N-DEx System to Obtain More Images from the NGI System

IS ISSUE #10*

Joint Task Force on Rap Sheet Standardization Update

*No staff paper

IS ISSUE #11** (*Info A*)

Rapid Deoxyribonucleic Acid (Rapid DNA) Update

IS ISSUE #12** (*Info B*)

NGI System Purpose Code F Responses vs Purpose Code C Responses

IS ISSUE #13** (*Info E*)

Update on the FBI's Manual Fingerprint and Name Check Services

IS ISSUE #14** (*Info F*)

Criminal History Update

IS ISSUE #15** (*Info G*)

Identification for Firearm Sales

IS ISSUE #16** (*Info H*)

The NGI System Interstate Photo System (IPS) Update and IPS Policy and Implementation Guide Revisions

IS ISSUE #17** (*Info I*)

Biometric Interoperability Update

IS ISSUE #18** (*Info P*)

Programs Research and Standards Unit (PRSU) Update on Contactless Fingerprint Collection Studies

AdHoc Issue*

Data Protection Strategy

*No staff paper

**Delivered with the information only staff papers

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #3

Consideration of Additional Use Cases for the Next Generation Identification Iris Service

PURPOSE

This paper provides background information on the current and future intended uses of the Next Generation Identification Iris Service and a request by the Criminal Justice Information Services (CJIS) Division for feedback/recommendations regarding how it could expand the scope of the Next Generation Identification Iris Service to better serve the needs of the criminal justice community.

POINT OF CONTACT

Biometric Services Section, Biometric Identification and Analysis Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information included in this paper and provide a recommendation on future use cases for the Next Generation Identification (NGI) Iris Service.

BACKGROUND

The NGI Iris Service went operational on 09/29/2020, culminating a multi-year Iris Pilot effort which led to the 05/07/2020 recommendation from the FBI Director to transition from the Iris Pilot to the NGI operational environment. Today, correctional facilities in California and Texas are capturing iris images in their respective booking systems upon intake. Once captured, the images are submitted and enrolled into the NGI Iris Service repository. Multiple correctional facilities in Texas then conduct an Iris Image Identification Search (IIDS) as an identification verification prior to an inmate being released or moved within or to a different facility.

The three main benefits to utilizing the iris biometric for an identification verification are that it is fast, accurate, and contactless. The IIDS processing time is measured in terms of seconds, as demonstrated by the Iris Pilot. In addition, the iris biometric capture process is fast and easy to do. Regarding accuracy, a study of iris algorithms conducted by the National Institute of Science and Technology, titled *IREX IX Part One Performance of Iris Recognition Algorithms*,

demonstrated that the most accurate one-to-many iris matcher yielded a False Negative Identification Rate of (approximately 1 in every 150 searches or a true match rate of 99.33%) and a False Positive Identification Rate of (1 in every 1,000 searches or a false positive rate of .1%) when searching against an enrolled population of 160,000 people. Accuracy was reported for two-eye matching since most iris cameras acquire samples of both irises simultaneously. As for the benefit of the iris biometric being contactless, there is a certain safety benefit realized when not being required to physically handle a subject to collect their biometrics.

DISCUSSION AND ANALYSIS

The NGI Iris Service includes an iris image repository and features an iris search capability. All iris images submitted for enrollment into the repository must be associated with tenprint fingerprints and must be collected pursuant to an arrest or subsequent criminal justice process (e.g., incarceration). The search functionality of the NGI Iris Service consists of a one-to-many, lights-out search and provides the user with an identification validation for the submitted iris image. An iris search will return either an identification or a non-identification response along with other descriptive information as specified by the submitter.

As the use of the NGI Iris Service and iris functionality grows, the CJIS Advisory Process will be asked to consider newly identified use cases and provide guidance. In addition, legal review will be provided by the FBI's Office of the General Counsel.

Examples of current uses and future use case expansions of the NGI Iris Service are outlined below.

Identification Validation Use Cases

Incarceration Facilities

Current Use Case—The primary criminal justice use case for the NGI Iris Service is identity management. Correctional facilities, sheriff's offices, and police departments in both Texas and California currently submit iris images for enrollment into the NGI Iris Service repository. Multiple agencies within only Texas currently submit iris images for searches against the repository. These facilities enroll iris images upon initial booking and conduct subsequent searches of the NGI Iris Service to validate the identity of the inmate. Once an identification is established, a search is cascaded to the National Crime Information Center to determine if there are any wants or warrants on the subject before release

The next step for the NGI Iris Service is to expand this use case to correctional facilities across the country. For this to occur, the FBI's CJIS Division needs to work closely with CJIS Systems Officers (CSO) to convey the benefit of using the iris biometric in this manner and to ensure their systems have the capability to successfully process and submit iris types of transactions to the NGI System. Once the appropriate mechanisms are put into place between the agency and the NGI Iris Service, the CJIS Division will work directly with correctional facilities to convey the benefits previously discussed.

Future Use Case Expansion - As previously stated, the iris biometric is currently being used by incarceration facilities to support inmate release procedures. In addition to this, the iris biometric could be used to enhance the security and accuracy of other prison processes such as prisoner ingress and egress procedures, movement within the facility, reduction of intake and booking times and errors, and curtailing false identity claims. This would effectively place identity management in the care of this fast and accurate iris algorithm, reduce the potential of human error, and improve operator safety by utilizing a contactless biometric.

Supervised Release

Current Use Case Expansion—The United States (U.S.) Probation and Pretrial Services System has contact with pretrial defendants and post-conviction offenders monthly. Early in the Iris Pilot, the U.S. Probation Office for the Northern District of West Virginia utilized the iris biometric to quickly and accurately, verify supervised release individuals and ensure the individuals were in the correct jurisdictional location. Utilization of the NGI Iris Service search capability for identification verification could prove to be extremely beneficial in larger metropolitan jurisdictions.

Future Use Case Expansion—Probation is a supervised release activity administered by more than 2,000 separate agencies, with nearly 4 million adult offenders under supervision.¹ Since a prison sentence may be suspended on the condition that the offender follow certain prescribed rules and commit no further crimes, the identification validation use case of the iris biometric could be of great benefit for supervising offenders for curfew checks or visits to home, work, or school.

Future Use Case Expansion—Parole enables post-release supervision for a population that is approaching 1 million people.² The criminal justice system could greatly benefit from a fast, accurate and contactless biometric used for the management and validation of these identities.

Use in the Court System

Future Use Case Expansion—With the iris biometric being fast, accurate, and contactless, the court system could benefit from using the NGI Iris Service to validate the identity of individuals as they traverse the courts' processes. For example, as an individual enters the pretrial and trial phases of the criminal justice process, the Iris Service would provide a safe and accurate identity validation mechanism to confirm that the individual who was previously arrested and processed for the offense is the same individual presenting for any pretrial and trial proceedings.

Identification Use Cases

Law Enforcement

Future Use Case Expansion—The iris biometric modality may offer an important application as

¹ Referenced article: *Corrections: An Introduction, 4th Edition*, 2014, Richard P. Seiter

² Reference: *U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics; Title: Probation and Parole in the United States, 2017-2018*

mobile iris recognition could be used by law enforcement in the field. Today, mobile fingerprint identification technology is widely used by law enforcement agencies across the nation. The NGI Iris Service repository volume needs to increase substantially to parallel mobile fingerprint identification. The CJIS Division would work with all CSOs and state agencies to navigate the programming requirements necessary to participate in the NGI Iris Service for enrollments to grow the repository, for searches to capitalize on the service, and to develop mobile iris capabilities for the law enforcement community.

Homeland Security

Current Use Case—The Department of Homeland Security (DHS), United States Visitor and Immigrant Status Indicator Technology (US VISIT) program, and Customs and Border Protection (CBP) officials have implemented the iris biometric into their operational environments. The US VISIT program was established in accordance with several Congressional mandates that required the DHS to create an integrated automated entry and exit data system. Due to iris images boasting exceptional performance as a law enforcement biometric, requiring a much smaller storage capacity than traditional fingerprint files, and being more difficult to alter than fingerprints, the CBP conducted its own iris pilot and now have nine locations across the nation submitting images for enrollment into the NGI Iris Service.

Future Use - The CJIS Division intends to pursue the integration of DHS agencies for authorized IIDS uses of the NGI Iris Service.

OPTIONS

The CJIS Division is requesting Subcommittee members review the two options below.

Option 1:

Endorse the expansion of the NGI Iris Service for the following use cases:

1. Identification Validation
 - a. Incarceration - to enhance the security and accuracy of other prison processes such as prisoner ingress and egress procedures and movement within the facility
 - b. Supervised Release – to aid in the management and verification of identities in the Probation and Parole Systems.
 - c. Court System - to validate the identity of individuals as they traverse the courts' processes.
2. Identification
 - a. Law Enforcement - to work with all CSOs and state agencies to navigate the programming requirements necessary to participate in the NGI Iris Service for enrollments to grow the iris repository, for searches to capitalize on the service, and to develop mobile iris capabilities for the law enforcement community.
 - b. Homeland Security - to pursue the integration of DHS agencies for authorized IIDS uses of the NGI Iris Service.

Option 2:

Make no change at this time to the current NGI Iris System use cases.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: (enter 0-5) and categorized as: ___(enter High, Medium, or Low).

RECOMMENDATION

The FBI does not have a recommendation.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SPRING 2021 IS SUBCOMMITTEE ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3H.

Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #4

Next Generation Identification Iris Service Search upon Enrollment Enhancement

PURPOSE

This paper is to obtain Criminal Justice Information Services Division Advisory Policy Board endorsement for searching iris images during the iris image enrollment process.

POINT OF CONTACT

Biometric Services Section, Biometric Identification and Analysis Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information included in this paper and provide input on the proposal to search iris images upon enrollment.

BACKGROUND

The FBI's Criminal Justice Information Services Division (CJIS) Division, with the endorsement of the Advisory Policy Board and approval of the FBI Director, implemented and deployed the Next Generation Identification (NGI) Iris Service on 09/29/2020. The NGI Iris Service continues the capabilities of the FBI Iris Pilot that successfully operated for seven years. The new service includes an iris image repository, and an iris search capability. All iris images submitted for enrollment in the repository and available for searching must be associated with tenprint fingerprints and must be collected pursuant to an arrest, subsequent criminal proceeding, incarceration, or post-trial release. The NGI Iris Service is housed within the FBI's NGI System, which serves as the national repository for biometric-based identity history and criminal history record information.

DISCUSSION AND ANALYSIS

Currently, iris images are enrolled into the NGI Iris Service repository with a criminal tenprint submission. Iris images may also be enrolled with a Biometric Image Submission transaction for an existing criminal identity, (e.g., iris images and the Universal Control Number (UCN)). At present, iris images that are being submitted for enrollment without the criminal tenprint are not searched against the existing iris images maintained in the NGI System.

If a search of iris images occurred upon enrollment, it could identify biographic and biometric discrepancies in records associated with matching iris image sets. For example, if newly enrolled iris images matched against iris images already in the repository but the associated UCN or fingerprints were different, this would alert the user to potential errors in the identity record.

Both of the following scenarios assumes the tenprint submission is successfully enrolled or that the UCN is valid and that the iris submission meets entry level validation requirements to successfully enroll the iris images:

Current process flow:

- Iris images are submitted to the NGI System for enrollment with a UCN or a tenprint submission.
- Iris images are enrolled.

Proposed iris search upon enrollment process flow:

- Iris images are submitted to the NGI System for enrollment with a UCN or a tenprint submission.
- Iris images are then searched against iris images already enrolled in the repository.
 - The search returns a different UCN or biographic.
 - Additional research is required by the CJIS Division prior to the iris enrollment.
 - The anomaly is corrected, and the irises are enrolled; or
 - The anomaly cannot be corrected, and the irises are not enrolled.

The submitting agency would be automatically notified with a new NGI Iris Service message returned in the Submission Results Electronic Status/Error Field, 2.060. This message indicates further review is required by the CJIS Division and the iris images were not enrolled. The message is as follows:

Manual Review - Enrollment

A search of the submitted iris enrollment requires CJIS to adjudicate the results. The iris images were not enrolled.

It is important to note, this new validation process would not affect current tenprint processing. The CJIS Division would review the tenprint records and make a recommendation to the

submitting/owning agency regarding a resolution, which in this case, may include merging of the tenprint records to reflect a single identity. Users may need to make technical changes to receive a new iris Status/Error Field message from the NGI System.

If adopted, the validation process of searching iris images upon enrollment will help ensure the NGI System and federal/state repositories contain appropriately consolidated biometrics and follows the CJIS Division's existing business practice for fingerprint enrollments. This enhancement would also be applied to the iris bulk enrollment process.

If the search on enrollment feature would be approved for implementation, the CJIS Division will provide the users with a one year's notice prior to implementation.

OPTIONS

The CJIS Division is requesting Subcommittee members review the two options below:

Option 1

Endorse the enrollment validation process, as proposed. Iris images submitted for enrollment will be searched against iris images already enrolled in the repository. If the iris images do not pass validation, return the new Status/Error Field notification message of:

Manual Review - Enrollment

A search of the submitted iris enrollment requires CJIS to adjudicate the results. The iris images were not enrolled.

This validation process will have an analysis component if an anomaly is discovered through the NGI search. In this instance, collaboration with the submitting agency of the iris and the current tenprint record (or records) hit upon will be necessary.

Option 2

Make no change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: ____ (enter 0-5) and categorized as: ____ (enter High, Medium, or Low).

RECOMMENDATION

The FBI does not have a recommendation.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

SPRING 2021 IS SUBCOMMITTEE ACTION:

Motion: To accept Option 1 as presented in the topic paper. Priority 3M.

Action: Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #5

Update to 2019 topic “*Driver’s License Numbers (DLN) in the Next Generation Identification (NGI) System*”

PURPOSE

The purpose of this paper is to discuss methods for capturing Driver’s License Numbers in the Next Generation Identification System. The information should also be available on the criminal history record shared via the Interstate Identification Index.

POINT OF CONTACT

Biometric Services Section, Criminal History Information and Policy Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

The Biometric Services Section (BSS) Criminal History Information and Policy Unit (CHIPU) requests that the Subcommittee members review and provide appropriate comments, suggestions, and recommendations for capturing DLNs in the NGI System.

BACKGROUND

In June 2005, the APB considered adding DLNs to the Interstate Identification Index (III) Miscellaneous Identification Number (MNU) field. The APB motioned to make no change to the MNU field but established an action item for the FBI’s CJIS Division to “look into expanding the fields and study if a new field is needed” to capture the DLN information for display on the criminal history record.¹ The APB further recommended the CJIS Division “include in the study an assessment of the value and importance of National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System compatibility.”²

Before the 2005 request, the DLN field was available on the criminal history record but was not included in the Electronic Biometric Transmission Specification (EBTS). The NGI System does not have a field to capture reported DLNs and does not disseminate DLN information as a

¹ CJIS Division Electronic Communication to the Director’s Office, 08/18/2005.

² Ibid.

specific data field. While state-issued identification card information is collected in the MNU field, system edits prevent entry of DLNs in this field. The DLN is therefore not searchable via the III. If reported and provided on the criminal history record, the DLN could be valuable information when law enforcement conducts criminal investigations.

In spring 2019, the topic “*Driver’s License Numbers (DLNs) in the Next Generation Identification (NGI) System*” was presented to the WGs to gauge the interest in capturing DLNs in the NGI System. The APB moved to “continue to pursue the addition of a DLN field to the NGI System for the fall 2019 CJIS APB.”³ A Technical Impact Assessment (TIA) was requested to provide a technical requirements analysis to support the addition of the DLN field.

DISCUSSION AND ANALYSIS

The DLN is a useful piece of information when conducting authorized name-based checks such as criminal justice searches and firearms-related background checks. Without positive identification, numerical identifiers associated with an individual including the DLN, social security number (SOC), alien registration number (ARN), and military identification numbers become important markers to verify identity. Driver’s licenses are routinely accepted as a primary form of photo identification⁴ and the presentation and review of the driver’s license is recorded by documenting the DLN on many government forms.

The uniqueness of the DLN varies from state to state. Individuals may be assigned a DLN, and if it expires, may be issued another one. Several states issue different types of driver’s licenses to an individual, including personal vehicle driver’s license, motorcycle driver’s license, commercial driver’s license (and different classes of commercial licenses), chauffeur’s licenses, etc. People frequently move from one state to another and may be issued an additional DLN for the new state. States may change the algorithm used to assign DLN, and the DLN will change over time, accommodating old and new numbers, or changing all the numbers to adjust with advancements in technology. Because the driver’s license incorporates a photograph with the numerical identifier, the DLN, while not necessarily unique, is frequently used for identity verification.

The FBI explored options to capture and provide DLNs in the NGI System. One option is to create an optional DLN field in the NGI System to capture the information when included in fingerprint-based types of transactions (TOTs), but not scored in the search algorithm. This option would require programming changes by the FBI and federal, state, and tribal contributors. The creation of a DLN field in the NGI System allows for the DLN to be captured when submitted and appear on FBI-supported criminal history records. However, the creation of a single DLN field in the NGI System differs from the NCIC’s use of three fields: An Operator’s License Number (OLN) field in combination with the Operator’s License State (OLS) and the Operator’s License Year of Expiration (OLY) fields to capture DLN information.

³ CJIS Division Memorandum for the FBI Director, 09/20/2019.

⁴ <https://www.fbi.gov/file-repository/compact-council-identity-verification-program-guide-booklet.pdf/view>.

A second option is to incorporate the use of the OLN, OLS, and OLY fields in the NGI System to capture the information on the criminal history record. Although the FBI and federal, state, and tribal contributors would need to program to use these fields, this would be consistent with the NCIC's use of three fields. However, this would be inconsistent with how the National Instant Criminal Background Check System (NICS) uses the MNU field to capture this information today. The NICS captures the DLN in the MNU field using up to 17 alphanumeric characters beginning with DL-. In contrast to the NCIC and the NICS, the National Data Exchange (N-DEx) Information Exchange Package Documentation (IEPD) Version 4.0 captures DLN information using three National Information Exchange Model-compliant fields. The N-DEx IEPD uses the Driver's License Expiration Date field to collect either year, year/month, year/month/day, or year/month/day/time. The N-DEx IEPD uses either the Driver's License Issuing Authority Code (DLIAC) field or the Driver's License Issuing Authority Text (DLIAT) to collect information regarding the issuance of the DLN. If using the DLIAC, the code must be selected from American Association of Motor Vehicle Administrators jurisdiction authority code list. The DLIAT accepts free text with no length or character restrictions. The N-DEx IEPD also uses a DLN field with no field length restriction and should not include any special characters.

A third option is to modify the NGI System's MNU field to accept DLNs. This will require programming changes by the FBI and federal, state, and tribal contributors. Current edits to the MNU field restrict the entry of DLNs. The MNU field format consists of a two-letter identifying code followed by a hyphen (-), followed by the number itself. The size of the MNU field is limited to 15 characters, and as many as four MNUs may be included in this field, separated from the next by the {} record separator character. The MNU field length will need expanded to at least 22 alphanumeric and special characters to capture the prefix DL- and accommodate the varying state DLN formats, which may contain from 8-19 alphanumeric characters.⁵ The MNU field in the NGI System uses different codes and options than the MNU field in the NCIC and is currently the same length.

As with other identifiers, the DLN, regardless of how it is submitted (using a new DLN field, the OLN, OLS, and OLY fields, or using the MNU field), will be submitted with a biometric to the NGI System. Regardless of the uniqueness of the DLN, this information should be included on the subject's criminal history record in a similar manner as the SOC, ARN, and other identifying data because it will be associated to the criminal history record using a biometric match. The NGI System should be able to accommodate up to 999 DLN in a similar manner as the MNU field accommodates multiple SOC and ARN today.

The DLN will be a searchable identifier in III if entered in the proposed DLN field, or using the proposed OLN, OLS, or OLY fields, but will require additional programming changes affecting the query index QH (Query Index) and QR (Query Record) record request messages. The DLN, if entered in the MNU field, would be searchable using the QH name-based inquiry message without additional programming; the MNU is already a searchable field in III when name, sex, race, date of birth, and the MNU are provided.

⁵ Per the National Traffic Safety Institute. Data for territories was not available <https://ntsi.com/drivers-license-format/>.

The CJIS Division's Information Technology Management Section completed a TIA. The TIA recommended modifying and using the existing MNU field. The NGI System, the NCIC, and the NICS already contain the MNU field but will require system changes for federal, state, and tribal partners as well as the NGI System changes to be able to search the DL- prefix within the MNU field. The NICS captures the DLN in the MNU field using the prefix DL-, and modifications must be made to pass the information to the NGI System and the NCIC. Contributors may use the III Entering Supplemental Identifiers Message Key (MKE) and the III Cancel Supplemental Identifiers MKE to add, modify, and delete alphanumeric identifiers in the MNU field in the NGI System. Up to 999 MNUs, regardless of type, can be included on an individual's criminal history record. When returned, the DLN will appear at the event and identity levels on criminal history record information, like the MNU. The TIA recommended no additional modifications to the NGI System to validate the DLN's expiration or value; however, requirements for validation, expiration, and removal could be managed by policy. Updates will be needed to the *III/NFF Operational and Technical Manual* and the *NCIC Code Manual*.

OPTIONS

Option One: Create a new DLN field in the NGI System to submit the DLN. An additional EBTS field must be created to capture the DLN for EBTS TOTs.

Option Two: Create an OLN, OLS, and OLY field in the NGI System to collect DLN in a manner consistent with the NCIC. Additional EBTS fields must be created to capture the DLN in the OLN, OLS, and OLY fields for EBTS TOTs.

Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-.

Option Four: Make no change.

If Option One, Two, or Three is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _____ (enter 0-5) and categorized as: _____ (enter High, Medium, or Low).

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option Two: Create an OLN, OLS, and OLY field in the NGI System to collect DLN in a manner consistent with the NCIC. Additional EBTS fields must be created to capture the DLN in the OLN, OLS, and OLY fields for EBTS TOTs. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option Two: Create an OLN, OLS, and OLY field in the NGI System to collect DLN in a manner consistent with the NCIC. Additional EBTS fields must be created to capture the DLN in the OLN, OLS, and OLY fields for EBTS

Action: TOTs. Priority 3M.
Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option Two: Create an OLN, OLS, and OLY field in the NGI System to collect DLN in a manner consistent with the NCIC. Additional EBTS fields must be created to capture the DLN in the OLN, OLS, and OLY fields for EBTS TOTs. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-. Priority 4H.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-. Priority 3M.

Action: Motion carried.

SPRING 2021 IS SUBCOMMITTEE ACTION:

Motion: To accept Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-. Priority: 3M.

Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETINGS
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #6

Posting Federal Dispositions to Multiple Dates of Arrest

PURPOSE

In December 2013, the FBI's Advisory Policy Board recommended a procedure to cross-reference federal disposition data to multiple related dates of arrest in the Next Generation Identification System. An update is provided and a request for guidance to determine if this procedure should be continued.

POINT OF CONTACT

Biometric Services Section, Criminal History Information and Policy Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review a previous recommendation and provide guidance if this procedure should be continued or discontinued.

BACKGROUND

In the fall of 2013, the FBI's Criminal Justice Information Services (CJIS) Division sought to update federal arrest cycles with corresponding court dispositions. Procedural guidance was requested from the Advisory Policy Board (APB) for a process to eliminate related federal arrests without dispositional data by using a cross-reference to a related arrest with a disposition. The Fall 2013 Federal Working Group recommended the following and the APB concurred:

“The APB moved that when court data/disposition information is received from a federal contributing agency and the IAFIS ¹ lists multiple dates of arrest by multiple agencies related to the court disposition provided, the CJIS Division will indicate the court data

¹ The Integrated Automated Fingerprint Identification System (IAFIS) has been replaced by the Next Generation Identification (NGI) System.

supplied on the first federal arrest and indicate ‘see court/data/disposition on 00/00/0000’ on all others regardless of the contributing federal agency.”

In mid-2014, the FBI Director approved this recommendation and the CJIS Division implemented this procedure.

DISCUSSION AND ANALYSIS

The NGI System currently has over 13 million federal arrests with dispositions. Of those, 416,807 (3.2 percent) have the cross-reference phrase ‘see court data’ in the disposition. This procedure has not been as beneficial as expected and obstacles have been identified and will be discussed.

In the last six years, there has been an increase in electronic data submission methods with programming being developed for additional electronic disposition submission methods, record modifications, and record deletions.

The NGI System programming prevents automation of the cross-referencing procedure due to numerous variables in determining ‘related’ arrests, therefore, the cross-reference procedure remains a manual review. More federal agencies continue to explore the best way for their agency to submit electronic disposition transactions. Currently, nine federal agencies are actively pursuing electronic disposition submission programming. One of the nine has started submitting small samples in the NGI System’s live environment and is integrating programming into their production environment. As the volume of electronic disposition submissions continue to increase, fewer transactions will be routed for the manual review and cross-referencing.

Since the cross-referencing procedure cannot be duplicated in the electronic environment, the posting of a disposition will be inconsistent and dependent solely upon the method of submission. This will result in potential issues as manual processing provides more flexibility for review and updating the criminal history records than the automated process for posting of federal dispositions.

The Interstate Identification Index (III) Seal Record Cycle (SRC) message key (MKE) was deployed during fiscal year 2020. This MKE provides an electronic means for authorized federal contributors to seal and unseal criminal history record information (CHRI) at the arrest level. Federally sealed arrests are available for four purpose codes. However, the use of all other purpose codes will not allow sealed CHRI to be disseminated. This will be problematic if the sealed arrest is the arrest cycle with the disposition data anchoring all the cross-referenced arrests. CHRI users will not be able to use the ‘see court data’ cross-reference as designed. A potential legal consequence would be the dissemination of an incomplete or inaccurate CHRI.

Two more III MKE tools are being developed and will give federal agencies the capability to remove a complete arrest cycle, and to process multiple record modifications. This will add to the possible removal of the federal arrest cycles with the anchoring disposition data. Currently,

these functionalities require manual processing. Procedures are in place to ensure when a federal arrest with anchoring disposition data is being removed, the next related arrest cycle has the ‘see court data’ cross-reference removed, and the disposition data is manually moved to that arrest cycle. This control will not be available as future electronic sealing/expungement/deletion requests will remove the arrest cycle as requested.

Title 28, United States Code (U.S.C.) , Section 534, and the Attorney General tasked the FBI with the acquisition, preservation, and exchange of identification records and information. This ensures the FBI functions as the sole repository for federal identification and criminal arrest records. Pursuant to Title 28, Code of Federal Regulations Section 20.37, every criminal justice agency submitting disposition information to the FBI is responsible for assuring the accuracy, completeness, and currency of the records and must, to the extent possible, ensure that dispositions are made available for all arrest data included on the individual’s record. In addition, pursuant to the Privacy Act of 1974, 5 U.S.C. 552a (e)(6), the FBI must make reasonable efforts to assure that records disseminated from NGI are accurate, complete, timely, and relevant. The Fix NICS Act of 2018 requires federal departments and agencies to submit a semi-annual certification of record submission requirements of the NICS Improvement Amendments Act (NIAA) of 2007 to the United States Attorney General, establish an implementation plan to make available the records required by the NIAA and improve the accuracy of those records. One of the goals of the Fix NICS Act is to “ensure complete and accurate reporting of relevant records, including efforts to monitor compliance and correct any reporting failures or inaccuracies.”

The Fix NICS Act and Title 28 both place the responsibility on federal agencies to submit complete and accurate data to the FBI for retention. The FBI has the responsibility of being the sole repository of all federal arrest records.

Subcommittee members are asked to review the current procedure considering all the above factors and determine its use moving forward.

OPTIONS:

1. Continue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.
2. Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

RECOMMENDATION

The FBI recommends discontinuing the procedure to ensure the accuracy and integrity of the CHRI.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: Continue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Continue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

Action: Motion carried.

SPRING 2021 SUBCOMMITTEE ACTIONS:

IS SUBCOMMITTEE ACTION:

Motion: To accept Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

Action: Motion carried. 1 Abstain

NICS SUBCOMMITTEE ACTION:

Accepted as information only.

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #7

Update on the Interstate Identification Index Delete Record Cycle and Modify Record Cycle Message Key Development

PURPOSE

The purpose of this paper is to provide an update on the development of the Interstate Identification Index Delete Record Cycle and Modify Record Cycle Message Key as it enhances the Criminal Justice Information Services Advisory Policy Board recommendation from 2006.

POINT OF CONTACT

Biometric Services Section, Criminal History Information and Policy Unit

Direct any questions regarding this topic to agmu@leo.gov

BACKGROUND

In 2006, the Criminal Justice Information Services (CJIS) Advisory Process Board (APB) approved the creation of the Interstate Identification Index (III) Delete Record Cycle (DRC) and Modify Record Cycle (MRC) Message Keys (MKEs). The III DRC MKE was approved as a tool for removing a complete arrest cycle. The III MRC MKE was approved as a tool to reactivate arrest cycles removed in error and to add or modify charge information within the arrest cycle. During development, the CJIS Division divided the CJIS APB-approved functionality into two pieces: one to reactivate arrest cycles that were erroneously removed, and one to modify information within the record. The development effort now includes the III Activate Record Cycle (ARC) MKE to reactivate records removed in error. The III MRC MKE will enable record modifications, including charge modifications that cannot be accomplished using other III MKE.

The III DRC MKE provides a tool for federal, National Fingerprint File (NFF), and non-NFF state contributors to delete arrest cycles. NFF states may use the III DRC MKE to delete an

arrest cycle in a FBI-maintained (pseudo-pointer) record¹ with multiple arrest cycles from that state. Non-NFF states may use the III DRC MKE to delete a complete arrest cycle in state-maintained (contains a State Identification [SID] Number) and pseudo-pointer records that contain multiple arrest cycles from that state. The III DRC MKE will incorporate a 60-minute window to be consistent with the III Delete Record SID (DRS) MKE. If a federal or state contributor submits a III DRC MKE message erroneously, it must submit the new III ARC MKE within 60 minutes to electronically reactivate the cycle. Otherwise, to re-establish the cycle, the federal or state contributor will have to re-submit the arrest fingerprint submission. Federal and state contributors cannot use the III DRC MKE to remove the last arrest cycle. However, states may use the III DRS MKE to completely remove a state-maintained record. Federal and state contributors may also submit the *FBI Expungement Form* FD-1114 to completely remove federal, non-NFF state-maintained, or NFF and non-NFF pseudo-pointer records.

The III MRC MKE will be used by federal contributors, NFF states, and non-NFF states to update information at the identity and event levels within the criminal history record, including modifying charges or information that cannot be accomplished using other III MKEs. NFF states may submit the III MRC MKE for identity level data for state-maintained records and identity and event level data for pseudo-pointer records. Non-NFF state contributors may submit updated information at the identity and event levels for state-maintained and pseudo-pointer records. The CJIS Division is collecting requirements for the III MRC MKE to incorporate many of the record modification requests that are currently processed manually. The III MRC MKE will immediately update records in the Next Generation Identification (NGI) System.

Federal and state contributors will need to program to use the new MKEs.

SPRING 2021 WORKING GROUP ACTIONS:

Accepted as information only.

SPRING 2021 IS SUBCOMMITTEE ACTION:

Accepted as information only.

¹ NFF states must manage state-maintained records because the NGI System has no criminal history record information for these records.

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #8

Unknown and Known Deceased Searches of the Department of Homeland Security's Automated Biometric Identification System and the Department of Defense's Automated Biometric Identification System

PURPOSE

To provide the fingerprint images from Unknown Deceased and Known Deceased (deceased) tenprint transactions to the Department of Homeland Security's Automated Biometric Identification System and the Department of Defense's Automated Biometric Identification System to discover identity information for this important population.

POINT OF CONTACT

Biometric Services Section Investigative Support Services Unit

Questions regarding this topic should be directed to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to provide comments, suggestions, and impacts the proposal will have on state systems, as well as the advantages and disadvantages of having the opportunity to search the Unknown Deceased (DEU) and Known Deceased (DEK) transactions against the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) and the Department of Defense's (DoD) Automated Biometric Identification System (ABIS). Subcommittee members are also requested to review the options presented and provide their recommendation to the APB.

BACKGROUND

The FBI's Criminal Justice Information Services (CJIS) Division and the DHS Office of Biometric Identity Management have been working together to achieve interoperability between the FBI's Next Generation Identification (NGI) System and the DHS's IDENT. The FBI's CJIS

Division and the DoD's Defense Forensics Science Center have been working together to achieve interoperability between the FBI's NGI System and the DoD's ABIS.

The CJIS Division's Special Processing Center (SPC) has conducted limited manual tenprint searches of the DHS IDENT since February 2017 to determine the identity of DEU individuals. As of 10/01/2020, the SPC has submitted 953 requests to the DHS IDENT resulting in 84 matches. In addition, the SPC has conducted limited manual tenprint searches of the DoD's ABIS since September 2017 to determine the identity of DEU individuals. As of 10/01/2020, the SPC has submitted 718 requests to the DoD's ABIS resulting in no matches.

On 09/17/2020, the Office of the Chief Medical Examiner in Washington, DC submitted fingerprints from a cold case to the SPC for processing. The unidentified male was discovered deceased on 07/29/2005, in Washington, DC. After an unsuccessful search of the NGI System, the SPC was able to make an identification through a DHS IDENT search.

DISCUSSION AND ANALYSIS

To take advantage of current NGI/IDENT and/or NGI/ABIS interoperability, NGI System contributors could submit tenprint images associated with a deceased individual to identify the person or obtain additional identity information from the DHS IDENT and/or DoD ABIS. By notifying the DHS of a deceased person's identity, agencies such as the DHS United States Citizenship and Immigration Services would know to discontinue immigration benefits for the deceased individual.

Two possible options to provide the deceased transactions to the DHS IDENT and the DoD ABIS have been identified and are detailed below:

- 1) Full deployment – All deceased tenprint transactions that are submitted to the NGI System would be automatically forwarded to be searched through the DHS IDENT and the DoD ABIS.

Currently, only 16 states receive a subsequent response from the DHS IDENT when they submit tenprint transactions utilizing NGI/IDENT interoperability. NGI contributors, not currently receiving the IDENT response, would need to contact the CJIS Division to coordinate receiving the IDENT response. To begin to receive the DoD ABIS response, NGI contributors would need to contact the CJIS Division.

- 2) Name of Designated Repository (NDR) – The NGI System contributor could utilize the NDR field to request the deceased transaction be forwarded for a search of the DHS IDENT and/or the DoD ABIS. Use of the NDR field would require coordination with the CJIS Division.

Regardless of the option chosen, the DEK and DEU transactions would be retained in the DHS IDENT System if there is an independent DHS or Department of State encounter. The DEU and DEK transactions would not be retained in the DoD ABIS.

OPTIONS

Considering the advantages and disadvantages discussed for providing deceased transactions to the DHS IDENT and the DoD ABIS, the CJIS Division is requesting Subcommittee members review the three options below and make a recommendation to the APB regarding which option should be approved:

- Option 1: No change. Deceased tenprint transactions will not be provided to the DHS IDENT or the DoD ABIS unless an agency makes a specific request of the SPC.
- Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.
- Option 3: Utilize the NDR field to allow contributors to choose when to search the DHS IDENT and/or the DoD ABIS with deceased tenprint transactions. The requesting agency will need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response. Priority 3M.

Action: Motion carried. 1 Nay.

SPRING 2021 IS SUBCOMMITTEE ACTION

Motion: To accept Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response. Priority: 3H.

Action: Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 20, 2021**

STAFF PAPER

IS ISSUE #9

The National Data Exchange (N-DEx) System to obtain more images from the Next Generation Identification (NGI) System

PURPOSE

To present a proposal to enable criminal justice (CJ) and law enforcement (LE) users to obtain additional NGI images via the N-DEx System.

POINT OF CONTACT

Global Law Enforcement Support Section / Data Sharing Services Unit (DSSU)

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

The DSSU is requesting input from Subcommittee members on enhancing the NGI System to accept a request for the Biometric Image List (BIL), enhancing the N-DEx System to accept and display the BIL, and enhancing the N-DEx System to display more images from the NGI System.

EXECUTIVE SUMMARY

The N-DEx System is a role-based, web-based Criminal Justice Information Services (CJIS) System, available nationwide over the Internet for the LE and CJ communities. The N-DEx System offers users a single portal to access multiple data sources, houses information of strategic investigative value, and assists investigators in connecting the dots between seemingly unrelated information.

In 2013, the N-DEx Program Office (PO) completed a Phase 1 project integrating the NGI Interstate Photo System (IPS) as a federated data source in the N-DEx System. This capability allows investigators to query the NGI System by FBI Number (FNU)/Universal Control Number (UCN) and to obtain the most recent frontal facial booking photo of the subject. Phase 2 of this partnership would be ongoing in calendar years (CY) 2021 and 2022 and would involve obtaining a BIL for all events of the UCN, followed by obtaining facial, scars, marks, and tattoo images from the BIL, as requested by the user. Increasing the availability of images via different

methods will significantly enhance the investigative power of the N-DEx System and facilitate cross-program partnerships within the CJIS Division.

BACKGROUND

N-DEx System: The N-DEx System is a national strategic investigative information-sharing system, available to federal, state, local, and tribal criminal justice agencies. The N-DEx System is an unclassified system, developed and managed by the FBI's CJIS Division in Clarksburg, West Virginia. Records in the N-DEx System span the criminal justice lifecycle and include information related to incident and case reports, arrests, missing persons reports, service calls, booking reports, pre-trial, probation and parole reports, warrants, citations and tickets, and field contacts and interviews. This information enhances the administration of criminal justice, from the initial patrol stop, to the supervision of an individual reintegrated into the community.

NGI System: The NGI System provides biometric identification services and criminal history information to NGI System users. The NGI System improves the efficiency and accuracy of biometric services to address evolving federal, state, local, and tribal, national, and international CJ requirements. New capabilities include a national Rap Back service; the Interstate Photo System; fingerprint verification services; more complete and accurate identity records; and, enhancements to the biometric identification repository.

N-DEx System / NGI Project: By leveraging the NGI System, the N-DEx PO can continue progressing toward the goal of providing strategic investigative leads to CJ and LE users and connecting investigations from federal, state, local, and tribal agencies across the United States.

Phase 1 (Complete): Connection to the NGI IPS

Establishing a federated data source **connection to the NGI IPS** was a major milestone in integrating the NGI System services into the N-DEx System. N-DEx System users can check the NGI IPS box, conduct a UCN search of the N-DEx System, and receive the most recent frontal facial image from NGI. This capability allows users to obtain more information (an image) in less time, making their access to CJIS services more streamlined and a force multiplier.

Phase 2 (CY21-22): Obtain more images from the NGI System

Retrieving full event image sets of Type 10 images from the NGI System is the next logical progression of the investigative capability the N-DEx System provides its users. With each UCN search of the NGI IPS, the N-DEx System would receive the BIL, including dates of the enrollment events and Biometric Set Identifiers (BSIs), which are unique identifying numbers. These dates and image counts would be displayed as hyperlinks by date in the N-DEx System, in proximity to the most recent frontal facial image from the NGI System, where the user can click on an event date of interest. The N-DEx System would then send a standard Electronic Biometric Transmission Specification (EBTS) Image Request (IRQ) transaction to the NGI System and receive an Image Request Response (IRR) containing the full set of Type 10 images from the event (booking/arrest/other) represented by the BSIs in the BIL. The N-DEx System would display the facial images, scars, marks, and tattoo (SMT) thumbnail images, and provide the user the ability to click on a thumbnail image and obtain an enlarged image. The user could choose to click on the next/other event dates and obtain the additional images associated with

those Event Identifiers (EVIs). Being able to retrieve NGI System biometric image sets would substantially increase the investigative power of the N-DEx System as users conduct casework and follow up on investigative leads.

DISCUSSION AND ANALYSIS:

Justification

In the annual N-DEx System user survey, N-DEx System users have consistently requested more images in the N-DEx System. For example, when asked in the 2020 User Assessment about desired future data sources or general data enhancements, nearly one-third of all users' comments involved the need for more images or photos in the system. The "Obtain More NGI Images" topic presented in this paper allows the CJIS Division to enhance the value of the N-DEx System using the images already available within its NGI System, providing more investigative power to CJIS System users, with only one feature-level system enhancement needed for each system.

Use Cases:

Use cases demonstrate the needed capability in a narrative fashion, showing how a user would use the capability:

Phase 1: Federated Data Source (Complete)

- An authorized N-DEx System user logs on to obtain images of a subject.
- The user conducts an N-DEx System search, and the results reveal a candidate's FNU.
- The user selects the NGI System federated data source and re-queries the N-DEx System based on the FNU.
- The response includes an NGI tab with the most recent frontal facial image from the NGI System.
- The investigator evaluates the image and determines it is of value in the case.
- The user complies with N-DEx and NGI Systems policies in using the image.

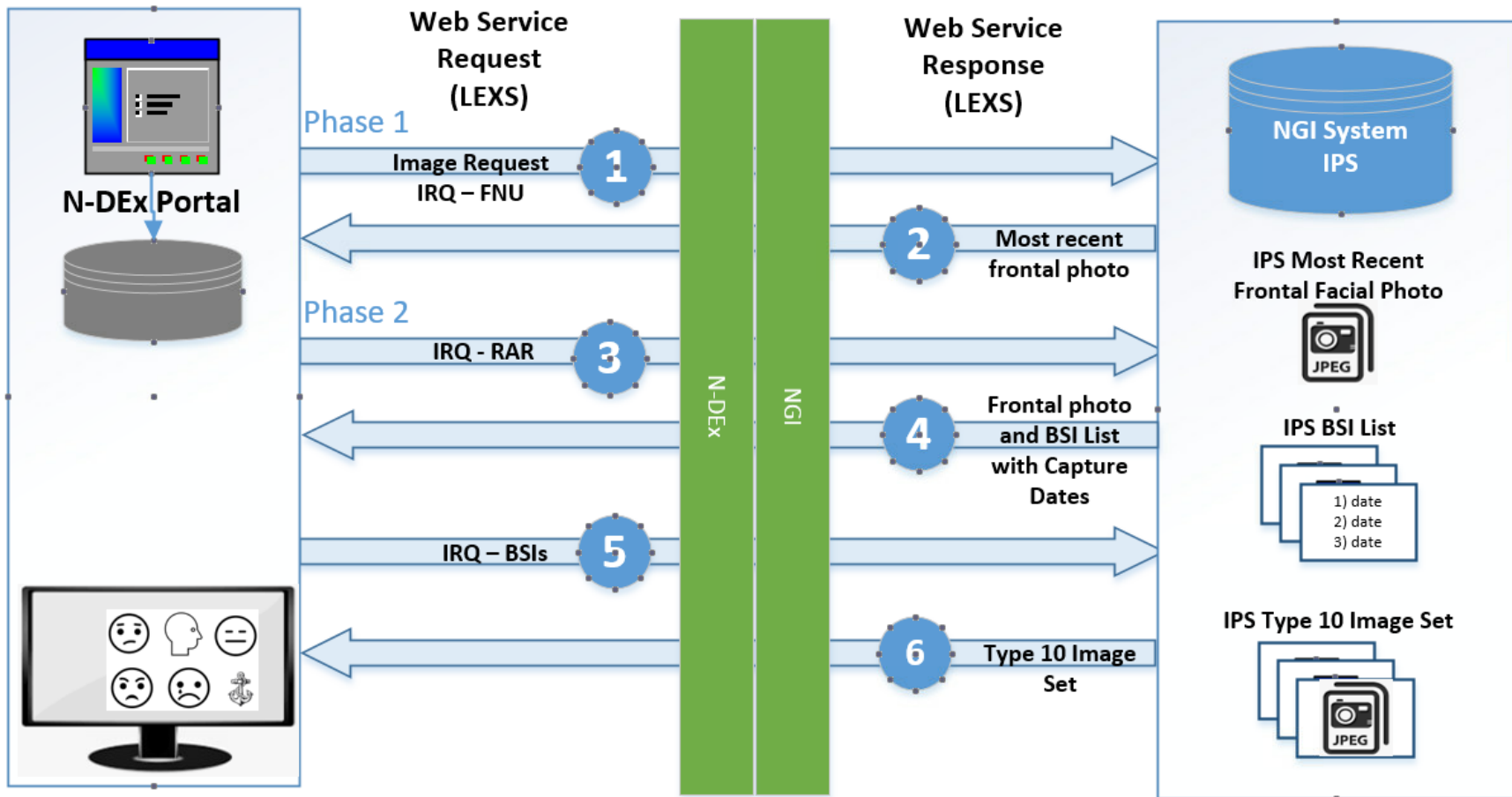
Phase 2: Increase NGI System Images (CY21-CY22)

- An authorized N-DEx System user selects NGI as a federated data source and searches a UCN.
- The user obtains a subject's complete BIL, including dates and counts of image types.
- The user clicks on an event or capture date displayed below the single NGI System image.
- The N-DEx System queries the NGI System for the complete set of Type 10 images from the event of interest, based on their BSIs.
- The N-DEx System displays the additional subject facial and SMT thumbnail images.
- The user clicks on a thumbnail(s) to obtain a larger image(s).
- The user clicks on a second and additional event date(s) and image(s), as desired.
- The user complies with N-DEx and NGI Systems policies in using the images.

SOLUTION

The following diagram demonstrates the message flow between the N-DEx System and the NGI IPS System once the enhancements have been conducted.

N-DEx / NGI Message Flow Diagram



*Logical Entity eXchange Specifications (LEXS)
**Return All Records (RAR)

Diagram Steps by Project Phase

Phase 1 (Complete): A user conducts a search using a UCN when the NGI IPS federated data source box is checked. The N-DEx System sends an IRQ with the UCN (*Step 1*) to the NGI System. The NGI System responds with an IRR containing the most recent frontal facial photo (*Step 2*).

Phase 2a (CY21): A user conducts a search using a UCN when the NGI IPS federated data source box is checked. The N-DEx System sends a transaction including a new Return All Images (RAR) field set to “Y.” (*Step 3; and will be combined with Step 1 in the final implementation to the NGI System*). The NGI System responds with a BIL with capture (event) dates for the UCN (*Step 4; and will be combined with Step 2 in the final implementation*). This is new functionality in NGI that will need a system change.

Change Details:

- The NGI System would be programmed to recognize the Return All Records (RAR) 2.2047 field in the IRQ (Biometric Image Retrieval Request).
- The partial format for the Biometric Image Description (BID 2.2028) is:
 - SI (Subject Identifier/UCN) of the identity.
 - Image Type (IMT) (2.2028B) of the image to be retrieved (“FACE” and “SMT”).
 - RAR (2.2047) set to “Y.”
- When the RAR is set to “Y,” the BIL field 2.2073 would be added to the Image Summary Response (ISR) from the NGI System.
- The ISR would return the BIL with all the BSIs associated with that UCN (0-1000), and the Biometric Capture Dates (BCDs).
- The format for the BIL is:
 - SI (Subject Identifier) of the candidate
 - BSI of the available image
 - BCD of the available image
 - IMT of the available image. (FACE, SMT)
- The N-DEx System will provide the list to their users as follows:
 - Event 3/4/2019, facial images (4) and SMT images (14)
 - Event 5/5/2018, facial images (1) and SMT images (0)
 - Event 7/4/2017, facial images (6) and SMT images (34)
- NGI Level of Effort (LOE) is one feature, within one Program Increment (PI).

Phase 2b (CY22): A user selects an event date from Step 4, and the N-DEx System sends a second (or subsequent) IRQ with the associated SI (UCN) and each BSI, RAR field set to “N” since all the images were returned in the first IRQ. (*Step 5*) A separate IRR will be returned for each image requested in this second (or subsequent) IRQ. The NGI System responds with those images (*Step 6*) in a response transaction to the N-DEx System. This functionality currently exists, with no changes needed to NGI for Phase 2b. The N-DEx System would be programmed to send the request(s) and receive and display the images to the user.

Audit Logging

- All Phase 1 and Phase 2 activities will be logged and audited per existing policy and procedure. Phase 2 activity will be documented in the audit logs in the same fashion as Phase 1 activity is currently logged. Copies of the images will not be retained in the N-DEX System.

OPTIONS

Option 1: Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number.

Option 2: No change.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number. Priority 3M.

Action: Motion carried.

SPRING 2021 SUBCOMMITTEE ACTIONS:

IS SUBCOMMITTEE ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEx System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number. Priority: 3M.

Action: Motion carried.

N-DEx SUBCOMMITTEE ACTION:

Motion: To accept Option 1: Expand sharing from NGI to provide access for the N-DEx System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number. Priority 3M.

Action: Motion carried.

Intentionally Left Blank

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FLORIDA**

STAFF PAPER

APB ITEM #11

Report on the Security and Access (SA) Subcommittee

SA ISSUE #1* (*Info K*)

Fiscal Year 2020 Audit Results Summary

SA ISSUE #2**

CJIS Security Policy Modernization Task Force Update

SA ISSUE #3**

Criminal Justice Data Categorization

SA ISSUE #4**

Interpretive Guidance Task Force Update

SA ISSUE #5 (*See APB Item #3, NCIC Issue #4*)

Sunset Date for File Transfer Protocol (FTP)

* Delivered with the information only staff papers

** No staff paper

Intentionally Left Blank

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FLORIDA**

STAFF PAPER

APB ITEM #13

Report on the National Instant Criminal Background Check System (NICS) Subcommittee

NICS ISSUE #1*

Old Action Items

NICS ISSUE #2 (*Info R*)**

NICS Operational Update

NICS ISSUE #3 (*Info S*)**

NICS Enhancements Status

NICS ISSUE #4 (*Info B*)**

Next Generation Identification (NGI) System Purpose Code F Responses vs Purpose Code C Responses

NICS ISSUE #5 (*Info G*)**

Identification for Firearm Sales

NICS ISSUE #6 (*Info K*)**

Fiscal Year 2020 Audit Results Summary

NICS ISSUE #7

Additional Date of Birth (DOB) Requirements for NICS Indices Entry

NICS ISSUE #8 (*See APB Item #3, NCIC Issue #3*)

Creation of an Extreme Risk Protection Order (ERPO) File in the National Crime Information Center (NCIC) System

NICS ISSUE #9 (*See APB Item #6, IS Issue #6*)

Posting Federal Dispositions to Multiple Dates of Arrest

NICS ISSUE #10*

NICS/The Bureau of Alcohol, Tobacco, Firearms and Explosives Denials

NICS ISSUE #11*

Ad Hoc Topics

* No staff paper

** Delivered with the information only staff papers

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
NATIONAL INSTANT CRIMINAL
BACKGROUND CHECK SYSTEM (NICS) SUBCOMMITTEE
VIRTUAL MEETING
APRIL 22, 2021**

STAFF PAPER

NICS ISSUE #7

Additional Date of Birth (DOB) Requirements for NICS Indices Entry

PURPOSE

Currently, the National Instant Criminal Background Check System (NICS) will accept a partial DOB in a NICS Indices entry. A NICS Indices hit with a partial DOB may make it difficult for a NICS User receiving the hit to determine if the individual with the NICS Indices hit is a match with their subject. The purpose of this paper is to provide options for additional DOB requirements for a NICS Indices entry when a partial DOB is present.

POINT OF CONTACT

NICS Section, NICS Business Unit.

Please send all questions or comments concerning this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the options in this paper and provide appropriate comments, suggestions, and recommendations to the APB; and, if appropriate, provide what priority should be assigned to the enhancement.

BACKGROUND

The Brady Handgun Violence Prevention Act of 1993 required the U.S. Attorney General to establish the NICS for Federal Firearms Licensees to contact for immediate information on whether the transfer of a firearm is in violation of federal or state law. When a NICS background check is conducted, a prospective firearm transferee's name and biographical information is searched against the name and biographical information of the records maintained in the following three national databases: (1) the Interstate Identification Index; (2) the National Crime Information Center; and (3) the NICS Indices. In addition, an Immigration Alien Query is submitted to the Department of Homeland Security's U.S. Immigration and Customs Enforcement on all persons who claim non-U.S. citizenship when completing the required Bureau of Alcohol, Tobacco, Firearms and Explosives Form 4473.

The NICS Indices contain the descriptive information of individuals identified as being prohibited from receiving firearms or a firearm-related permit based on federal or state firearm prohibitions. The information available in the NICS Indices is contributed by federal, state, local, and tribal agencies.

DISCUSSION AND ANALYSIS

As part of a NICS background check, based on biographical descriptors, possible matches to biographical information in the NICS Indices to the prospective firearm transferee or firearm permit applicant are returned to the user, who then makes the determination if a descriptive match exists. A matching NICS Indices hit to a prospective firearms transferee or firearm permit applicant allows the user to render an immediate denial determination, as all NICS Indices information is validated by the contributor as prohibiting prior to submission. This pre-validation, in turn, provides greater efficiency by eliminating the user’s need to conduct additional research to determine if the information is prohibiting for the firearm transfer or the receipt of a firearm permit. In order to search for potential matches to the NICS Indices, an algorithm is used for searching subjects and subject attributes. For the NICS, the search algorithm is used to facilitate the NICS background check process using the biographical information stored within the NICS Indices.

As outlined in the NICS Interface Control Document (ICD),¹ the data currently required for a NICS Indices submission is listed in Table 1.

Table 1

Mandatory Data Fields for NICS Indices Entry
First Name
Last Name
Gender
DOB ² , SOC, MNU ³ (DOB may be replaced by either the SOC or the MNU)
Agency Record Identifier
Originating Agency Identifier
Prohibited Category Code

In addition to the mandatory data required, a contributor can provide additional data that is optional.⁴ Although the majority of the optional data is not part of the search algorithm during the search for viable matches, the inclusion of additional data within the NICS Indices submission enhances the user’s ability to more accurately determine if a descriptive match exists, which, in turn, reduces the propensity of an invalid match which could prompt an inaccurate denial decision. The optional data fields currently available are listed in Table 2.

¹ The ICD is available via the NICS Community on the Justice Connect in the Law Enforcement Enterprise Portal.
² As of October 1, 2019, the DOB is a required field if the information is contained within the source documentation maintained by the contributor.
³ The allowable MNU categories are outlined in the NICS ICD.
⁴ The allowable values for optional data are outlined in the NICS ICD.

Table 2

Optional Data Fields for NICS Indices Entry	
Middle Name ⁵	Expiration Date
Cadence	Originating Agency Case Number
Place of Birth	Universal Control Number/FBI Number
Height	SOC
Weight	MNU
Hair	Race
Eye	Scars/Marks/Tattoos
Also Known As	Miscellaneous (MIS) Comments

Over the years these data fields, whether mandatory or optional, have proven to play an integral part in the process of determining a descriptive match between a firearms transferee or firearm permit applicant and a NICS Indices hit and has aided in identity issues during the challenge process. When submitting information to the NICS Indices, each contributor has the capability (and is encouraged) to “pack the record” with as much relevant information as is available by populating the appropriate data field. The contributor can also provide additional information specific to the individual by noting it in the MIS field. Since the NICS background check searches by biographical descriptors, it is imperative contributors provide as much information as possible to allow the best search for viable matches and to better assist the NICS User when determining whether a descriptive match to a prospective firearm transferee or firearm permit applicant occurs.

As recommended by the APB and approved by the FBI Director, beginning October 1, 2019, populating the DOB and Middle Name fields became required if the source documentation maintained by the contributor contained this information. For the DOB, the contributor must include the DOB listed in the source documentation or one that can be linked to the individual. A contributor should not be creating a DOB that is not listed in the source documentation in order to meet the requirements for a NICS Indices entry since the NICS will accept a partial DOB if entered. For example, if a contributor has a qualified individual for entry into the NICS Indices, but only has a partial DOB, such as 04/00/1944, the entry can be completed with this DOB, even without an additional descriptor, such as the SOC or MNU. However, if no DOB is contained within the source documentation and no additional descriptors exist, the contributor should not create an arbitrary partial DOB in order to complete the entry process.

Of the nearly 22 million records in the NICS Indices, over 2,500 contain a partial DOB. Although a small percentage of entries, when a hit occurs in the NICS Indices with a partial DOB, it may be difficult to determine if the individual is a descriptive match with the hit, especially if the name provided is an exact match with the hit. If there is a hit in the NICS Indices, the lack of DOB information may lead to an inaccurate denial decision, which may cause extensive work on the part of the individual who is denied to disprove the information. On

⁵ As of October 1, 2019, the Middle Name is required if the middle name or middle initial is contained within the source documentation maintained by the contributor.

several occasions, state partners have expressed concern and frustration over the lack of or incomplete biographical descriptors in the NICS Indices. Therefore, it is imperative that a complete DOB be provided with each NICS Indices entry.

OPTIONS

In order to promote complete DOB information in the NICS Indices going forward, the following options are being presented:

Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. That is to say a complete month, day, and year must be entered for individuals who are 120 years of age old or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message.

Option 2: With this option, the NICS will be programmed to accept a partial DOB for a NICS Indices entry, only if an additional descriptor is included, e.g., SOC or MNU. If a contributor attempts to enter a partial DOB without an additional descriptor, they will receive a reject message.

Option 3: No change, partial DOBs will continue to be accepted by the NICS.

If Options 1 or 2 are approved, the NICS Section will complete the system enhancement. There should be no impact to the system for the states, only awareness of the additional requirement. The system enhancement necessary to implement the change should be assigned a priority and categorized.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age old or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. That is to say a complete month, day, and year must be entered for individuals who are 120 years of age old or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message. Priority 3M.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age old or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message. Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 2: With this option, the NICS will be programmed to accept a partial DOB for a NICS Indices entry, only if an additional descriptor is included, e.g., SOC or MNU. If a contributor attempts to enter a partial DOB without an additional descriptor, they will receive a reject message. | Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age old or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message. Priority 3M.

Action: Motion carried.

SPRING 2021 NICS SUBCOMMITTEE ACTION:

Motion: To accept Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age old or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message. Priority 3M.

Action: Motion carried.

Intentionally Left Blank

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
JUNE 9, 2021
ORLANDO, FLORIDA**

STAFF PAPER

APB ITEM #14

Report on the Public Safety Strategy (PSS) Subcommittee

PSS ISSUE #1*

Welcome of New Members
Objectives of the PSS Subcommittee

PSS ISSUE #2*

Follow-up of CJIS Programs and One-pagers

PSS ISSUE #3*

Strategy Discussion

PSS ISSUE #4

F2020 Recommendation for Changes to Sex Codes within Uniform Crime Reporting (UCR)

PSS ISSUE #5 *(See APB Item #10, UCR Issue #3)*

Beyond 2021 Update – Addition of Geolocation to the National Incident-Based Reporting System (NIBRS)

PSS ISSUE #6*

Suicide Data Collection Update

PSS ISSUE #7

S2021 Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program

*No staff paper

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
PUBLIC SAFETY STRATEGY SUBCOMMITTEE
VIRTUAL MEETING
APRIL 26, 2021**

STAFF PAPER

PSS ISSUE #4

Recommendation for Changes to Sex Codes within UCR

PURPOSE

To propose changes to sex codes in the UCR Program.

POINT OF CONTACT

Global Law Enforcement Support Section (GLESS), Crime Statistics Management Unit (CSMU)

Questions regarding this topic should be directed to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the following proposal to provide a recommendation.

BACKGROUND

The Association of State Uniform Crime Reporting Programs requested the Federal Bureau of Investigation (FBI) address non-binary gender classification within the FBI UCR Program. In addition, state program managers have requested an FBI recommendation concerning how to report non-binary identifications, as a result of the inability to report a non-binary sex code for the arrestee segment of a National Incident-Based Reporting System (NIBRS) submission. Although sex code reporting within NIBRS is a known issue requiring resolution, the UCR Program is researching a solution that can be applied across the UCR Program and all its collections in their entirety. This would include NIBRS, the National Use-of-Force Data Collection, the Law Enforcement Officers Killed and Assaulted (LEOKA) Collection, the Hate Crime Statistics Collection, the Police-Public Contact Collection, and Police Employee data.

Historically, most data segments within the FBI UCR Program allow a selection of M for male, F for female, or U for unknown to be chosen and submitted. However, the NIBRS arrestee sex code segment is an outlier that only allows the selection of M for male or F for Female. Any additional code attempted, is rejected as an error and not accepted. Thus, law enforcement agencies that encounter an individual who does not identify as male or female, are underreporting criminal data due to the FBI's rejection.

The FBI UCR Program determined FBI Criminal Justice Information Services (CJIS) systems are primarily using three sex codes, F for female, M for male, and U for unknown. The FBI Director signed and approved the spring 2019 CJIS APB recommendation to change existing sex codes of G, N, X, Y, and Z to U within the Next Generation Identification (NGI) System and the Electronic Biometric Transmission Specification in September 2019. In addition, under this approved recommendation, the definition of U includes non-binary as well as unknown/unspecified.

Although the solution to use U for unknown and define it to include non-binary as well as unknown/unspecified provides benefits for operational systems within CJIS by minimizing impact on identity algorithms, reducing the risk of misidentification when performing cross-system searches, and aligns CJIS system compatibility and usability for shared information and services, this recommendation may not provide a clear solution for the FBI UCR Program, which has historically defined and used U for unknown differently. Therefore, if the FBI UCR Program chooses to adopt this policy, it would ensure historical increases in statistical trends in the unknown sex code category that would be inaccurate. Due to this fact, the FBI UCR Program is working with stakeholders to propose recommendations regarding how to resolve the sex code reporting issue across the program, and all collections in their entirety, while aligning CJIS systems as well as maintaining uniformity.

DISCUSSION AND ANALYSIS

As a statistical program, the FBI UCR Program needs to collect specific non-binary sex code data to better align with, and aid law enforcement in identifying trends within the United States, which result from UCR data submissions. Sex and gender are different. According to the American Psychological Association (APA), sex refers to a person's biological status, typically characterized as male, female, or intersex. There are a number of indicators of biological sex, such as physical and biological traits including sex chromosomes, gonads, internal reproductive organs, and external genitalia (APA, 2012). In addition, gender implies the psychological, behavioral, social, and cultural aspects of being male or female (APA, 2012).

Gender can be decomposed into gender expression and gender identity. The APA defines gender expression as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008). Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006). Based on these definitions, the UCR Program is most interested in capturing gender expression and/or gender identity in place of traditional sex.

The UCR Program collaborated with 22 state UCR program managers whose states have pending or established legislation to allow for non-binary gender to be captured on drivers' licenses with a sex code of X in 2020. The goal was to determine how often law enforcement

agencies are interacting with individuals who identify as non-binary, in which the data would be provided to the UCR Program.

The following metrics were captured based on a preliminary data request to Arkansas, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Indiana, Maine, Maryland, Massachusetts, Minnesota, Nevada, New Hampshire, New York, Oregon, Pennsylvania, Rhode Island, Utah, Vermont, Washington, and Washington D.C.:

Question	Response
Do not currently allow non-binary arrestee sex code submissions <i>*However, one state UCR program does allow for non-binary arrestee gender code submissions at the state level, and one state UCR program expressed the importance in distinguishing sex and gender</i>	14
Will have the ability to collect non-binary sex code submissions at the state level in 2020	1
No response	7

The majority of state UCR program managers engaged for feedback did not indicate there is a widespread issue warranting an immediate action. In addition, only four states, Arkansas, Colorado, Vermont, and Washington, provided metrics from collectively 10 local agencies. Four out of the 10 local agencies are currently acknowledging non-binary gender during the arrest process. Although the non-binary arrestee sex code issue does need to be addressed based on feedback received, it does not appear to be encountered often at this time, or is not being tracked at the local level due to agencies waiting for FBI guidance. However, since 22 states have pending or established legislation to allow for non-binary gender to be captured on drivers' licenses, there is a growing need for this data to be properly categorized and captured accurately.

The UCR Program collaborated with the Bureau Equality (BE) Committee to better understand the relationship between sex assigned at birth and gender identity. BE is one of nine FBI Diversity Advisory Committees that report to the Office of Diversity and Inclusion, Human Resources Department. BE's purpose is to bring attention to, as well as propose recommendations on how to address issues surrounding the FBI Lesbian, Gay, Bisexual, and Transgender workforce.

In order to be consistent with the 22 states that have pending or established legislation to allow an X for non-binary on drivers' licenses as an option, BE advocates for uniformity, and supports the creation of an exclusive, non-binary sex code option. BE does not recommend including non-binary in the unknown/unspecified field that was previously approved for NGI, as a non-binary person's gender identity is both known and specified.

The FBI also engaged the Office of Management and Budget (OMB) Office of Information and Regulatory Affairs, as well as the OMB Sexual Orientation and Gender Identity (SOGI) Working Group to inquire about future plans for sex and gender designations. OMB does not currently have a standard in mind for recommendation, and is not sure when this task will be complete. However, OMB recommended the FBI proceed with determining the most logical solution for

capturing this data within the UCR Program as a whole. The FBI collaborated with the SOGI Working Group to gain an additional understanding between the relationship of sex, gender expression, and gender identity and applied this feedback to the proposed recommendations below.

In summary, the impact of modifying the existing sex code structure within the UCR program to states and contributing agencies include modification to current systems and reports that are used to provide data within UCR submissions. The benefit to the law enforcement community and general public is better and more accurate contextual data that can be used to facilitate the proper interpretation of data collected by the UCR Program.

OPTIONS

Option 1 – The UCR Program should allow sex code selections of M for male, F for female, X for non-binary, or U for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008).

Option 2 – The UCR Program should resolve sex and gender in two phases.

Phase 1: The UCR Program should allow sex code selection of M for male, F for female, X for non-binary, or U for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008). Phase 1 may be immediately implemented.

Phase 2: The UCR Program should implement a new data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined) or U for unknown/unspecified are allowed. Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts to the law enforcement community at one time due to the nations ongoing transition to NIBRS.

Option 3 – The UCR Program should allow sex code selection of M for male, F for female, X for non-binary, man (code to be determined), woman (code to be determined), transgender male (code to be determined), transgender female (code to be determined), or U for unknown/unspecified. These code selections capture gender expression and gender identity together.

Option 4 – The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy.

If one of the above options is approved, the system enhancements necessary to implement the proposal should be assigned a priority: _____ (enter 0-5) and categorized as _____ (enter High, Medium, or Low).

Option 5 – No change.

RECOMMENDATIONS

The recommendations are proposed for consideration for subcommittee members in an attempt to collect more accurate data within the UCR Program as a whole, while aligning CJIS systems and maintaining uniformity. This would include NIBRS, the National Use-of-Force Data Collection, the LEOKA Collection, the Hate Crime Statistics Collection, the Police-Public Contact Collection, and Police Employee data. The UCR Program’s recommendation is we move forward to address both gender expression and gender identity as separate data categories.

For awareness, a separate staff paper regarding sex/gender data collected on the Police Employee form is proposing recommendations during the fall 2020 APB Working Group meetings as well.

FALL 2020 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 3: The UCR Program should allow sex code selection of M for male, F for female, X for non-binary, man (code to be determined), woman (code to be determined), transgender male (code to be determined), transgender female (code to be determined), or U for unknown/unspecified. These code selections capture gender expression and gender identity together. Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 5: No change.

Action: Motion carried.

Motion: To recommend the UCR Subcommittee consider the addition of a new gender field to capture gender identity.

Action: Motion carried.

Motion: To recommend the UCR Subcommittee forward this to a task force to further research on how to proceed. The North Central Working Group recommends the new gender field be an optional field

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 4: The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy, Priority 3M.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 2: The UCR Program should resolve sex and gender in two phases.

Phase 1: The UCR Program should allow sex code selection of M for male, F for female, X for non-binary, or U for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008). Phase 1 may be immediately implemented.

Phase 2: The UCR Program should implement a new data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined) or U for unknown/unspecified are allowed. Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts to the law enforcement community at one time due to the nations ongoing transition to NIBRS.

Action: Motion passed. One opposed.

Motion: To accept a priority level 4M.

Action: Motion passed.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: The UCR Program should allow sex code selections of M for male, F for female, X for non-binary, or U for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008). Priority 3M.

Action: Motion carried.

FALL 2020 SUBCOMMITTEE ACTIONS:

UCR SUBCOMMITTEE ACTION:

Motion: To accept Option 4 – The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy. Priority 3M.

Action: Motion carried.

Action Item – CJIS Division explore best practices for collecting gender identity and gender expression in crime data by law enforcement agencies.

NICS SUBCOMMITTEE ACTION:

Accepted as information only.

PSS SUBCOMMITTEE ACTION:

Motion: To accept Option 4 – The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy. Priority 3M.

Action: Motion carried.

FALL 2020 APB ACTION:

Motion: The CJIS APB moved to refer the topic to the PSS Subcommittee for further review.

Action: Motion carried.

SPRING 2021 PSS SUBCOMMITTEE ACTION:

Motion: To accept New Option 6: The UCR Program should resolve sex and gender in two phases. Priority 3M.

Phase 1: The UCR Program should implement a third sex code category of for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy.

Phase 2: The UCR Program should implement a new optional data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined) or U for unknown/unspecified are allowed. Gender identity is defined as one’s sense of oneself as male, female, or transgender. Since gender identity is internal, a person’s gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts to the law enforcement community at one time due to the nations ongoing transition to NIBRS.

Action: Motion carried.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
PUBLIC SAFETY STRATEGY SUBCOMMITTEE
VIRTUAL MEETING
APRIL 26, 2021**

STAFF PAPER

PSS ISSUE #7

Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program

PURPOSE

To present a proposal for changes to the race code data element within FBI UCR Program data collections to allow for multiple race code choices within race code data elements.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Direct any questions regarding this topic to agmu@leo.gov.

REQUEST OF THE SUBCOMMITTEE

Subcommittee members are requested to review the information in this paper outlining the changing of race code elements to allow for multi-choice race code selection within FBI UCR Program data collections.

BACKGROUND

The FBI UCR Program received a request from a law enforcement agency detailing the need for the National Incident-Based Reporting System (NIBRS) to allow for the selection of multiple race codes within the offender, arrestee, and victim segments. The Office of Management and Budget (OMB) requires the FBI UCR Program to collect a minimum of five race codes (White, Black or African American, American Indian or Alaska Native, Asian, and Native Hawaiian or Other Pacific Islander). Race information provided by participating agencies must meet these requirements for the purpose on standardizing the collection of race across OMB authorized data collections. Agencies are allowed to collect additional codes within their collections, but must make sure any additional categories can be aggregated into the five required race codes at higher levels of aggregation.

DISCUSSION AND ANALYSIS

In many cases, an individual involved in an incident may identify as bi-racial or multi-race. In these cases, Law Enforcement Agencies (LEA) must select a single race code for which the

individual best fits based on the law enforcement officer's observation. This may lead to inaccurate coding for the arrestee, offender, and victim segments, as well as an increase in racial trends that would lead to the improper interpretation of data. NIBRS allows for increased granularity in data collection and provides a system of tracking the racial breakdown of individual within the arrestee, offender, and victim segments.

This issue could be mitigated by allowing for the race category in NIBRS to be multi-choice. By allowing LEAs to select multiple race codes for an individual, NIBRS can accurately collect the racial breakdown of bi-racial or multi-race individuals.

IMPACT

State UCR Programs would have to implement the NIBRS Technical Specifications change to their repositories, as well as provide technical guidance and a planned implantation date to all local law enforcement partners and associated vendors.

OPTIONS

Option 1 – Change the NIBRS race category to allow for multiple selections for the arrestee, offender, and victim segments.

Option 2 – No Change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: _ (enter 0-5) and categorized as: ___ (enter High, Medium, or Low).

RECOMMENDATION

The FBI UCR Program recommends option 1.

SPRING 2021 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Change the NIBRS race category to allow for multiple selections for the arrestee, offender, and victim segments.

Priority 3M.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 2: No change.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To accept Option 2: No change.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To accept Option 1: Change the NIBRS race category to allow for multiple selections for the arrestee, offender, and victim segments. Priority 3M.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept a New Option: Refer to the PSS Subcommittee for further exploration. No change until that is completed.

Action: Motion carried.

SPRING 2021 SUBCOMMITTEE ACTIONS:

UCR SUBCOMMITTEE ACTION:

Motion: To accept a New Option: No change. Refer to the PSS Subcommittee for further exploration.

Action: Motion carried. 1 Nay, 2 Abstained.


PSS SUBCOMMITTEE ACTION:

Motion: To accept Option 2: No change.

Action: Motion carried. 1 Nay.

Action Item: CJIS to develop a strategic plan on how to reconcile race, sex, and gender codes across CJIS Systems with other relevant fields as practical and establish goals in harmonizing CJIS services when it comes to specific data elements.

Intentionally Left Blank




The FBI's CJIS Division

Michael A. Christman
Assistant Director
Federal Bureau of Investigation
Criminal Justice Information Services Division

June 2021

1




Pandemic effect:

**National Crime Information Center
daily volumes:**

- **April 30, 2019: 11,659,721**
- **April 30, 2020: 4,906,951**
- **April 30, 2021: 7,518,361**

2




Pandemic effect:

Tenprint monthly processing:

	<u>Criminal</u>	<u>Civil</u>
April 2019:	1,049,626	3,313,335
April 2020:	296,508	948,709
April 2021:	544,621	2,340,817

3




Pandemic effect:

National Instant Criminal Background Check System monthly transactions:

- **April 2019: 2,334,249**
- **April 2020: 2,911,128**
- **April 2021: 3,514,070**

4




Pandemic effect:

National Threat Operations Section

FY daily average (calls and E-Tips) through:

- **April 2019: 3,376**
- **April 2020: 3,275**
- **April 2021: 5,883**

5



Pandemic effect:

National Data Exchange

monthly searches:

- **April 2019: 1,422,903**
- **April 2020: 1,386,806**
- **April 2021: 1,386,746**


6



CJIS Division initiatives

- **Law Enforcement Enterprise Portal-
FirstNet partnership**
- **NCIC Extreme Risk Protection Orders/
Red flag laws**
- **Next Generation Identification
Iris Service**

7



CJIS Division initiatives

- **Uniform Crime Reporting Hate Crime
Review, more timely data releases**
- **National Threat Operations Center
dual-routing initiative**

8



Law enforcement outreach

Law Enforcement Engagement Unit

Marking one year of service to partners

Need to connect with CJIS Services?

Contact LEEU@fbi.gov
or 304-625-7768



9

Intentionally Left Blank



Uniform Crime Reporting (UCR) Subcommittee Report

Mr. Derek Veitenheimer - Chair
Criminal Justice Information Services (CJIS)
Advisory Policy Board (APB) Meeting
June 2021

UNCLASSIFIED

1



UCR Issue #2

Beyond 2021 Initiative Update – National Incident-Based
Reporting System (NIBRS) Data Elements

Purpose:

Recommend an option on proposed modifications to the NIBRS
data collection recommended by the Beyond 2021 Task Force.

UNCLASSIFIED

2

2



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue A: Creation of a New Data Element – Firearm Discharge on the NIBRS Offense Segment

Option A1: Add the ability to capture discharge of a firearm on the NIBRS Offense Segment.

Option A2: No change.

UNCLASSIFIED

3

3



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Working Group Actions:

- Northeastern, Southern, and Federal Working Groups motioned for Option A1: Add the ability to capture discharge of a firearm on the NIBRS Offense Segment. Priority 3M.
- North Central and Western Working Group motioned for Option A2: No Change.

UNCLASSIFIED

4

4



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: New Option** – Add a new code to an existing data element such as Type of Weapon or Force Used. **Priority of 3M.**

UNCLASSIFIED

5

5



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue B: Creation of a New Data Element – Firearm Stolen on the NIBRS Offense Segment

Option B1: Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment.

Option B2: No change.

UNCLASSIFIED

6

6



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Working Group Actions:

- North Central, Southern, and Federal Working Groups motioned for Option B1: Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment. Priority 3M.
- Western Working Group motioned for Option B2: No Change.
- Northeastern Working Group motioned for New Option: Create a new Data Element to collect stolen firearm information on the NIBRS Offense Segment. With a caveat of not mandatory. Priority 3M.

UNCLASSIFIED

7

7



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: New Option** – Add a new code to an existing data element such as Type of Criminal Activity. **Priority of 3M.**

UNCLASSIFIED

8

8



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue C: Creation of a New Injury Code – Gunshot Wound to be Recorded on the NIBRS Victim Segment

Option C1: Create a new NIBRS injury code of Gunshot Wound to be added on the NIBRS Victim Segment. If approved, the new injury codes will be as follows:

- N = None
- B = Apparent Broken Bones
- **G = Gunshot Wound**
- I = Possible Internal Injury
- L = Severe Laceration
- M = Apparent Minor Injury
- O = Other Major Injury
- T = Loss of Teeth
- U = Unconsciousness

Option C2: No change.

UNCLASSIFIED

9

9



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option C1** – Create a new NIBRS injury code of Gunshot Wound to be added on the NIBRS Victim Segment. If approved, the new injury codes will be as follows:

- N = None
- B = Apparent Broken Bones
- **G = Gunshot Wound**
- I = Possible Internal Injury
- L = Severe Laceration
- M = Apparent Minor Injury
- O = Other Major Injury
- T = Loss of Teeth
- U = Unconsciousness

Priority of 3M.

UNCLASSIFIED

10

10



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue D: *Expansion of Data – Collection of Injury Information on Homicide Victims*

Option D1: Add the ability to capture injury information for homicide victims within NIBRS.

Option D2: No change.

UNCLASSIFIED

11

11



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Working Group Actions:

- Federal Working Group motioned for Option D1: Add the ability to capture injury information for homicide victims within NIBRS. Priority 3M.
- North Central and Western Working Groups motioned for Option D2: No Change.
- Northeastern Working Group motioned for a New Option: Add the ability to capture injury information for homicide victims within NIBRS and add a new data value of “Unknown” as an option.
- Southern Working Group motioned for a New Option: Add the ability to capture injury information for deceased victims within NIBRS.

UNCLASSIFIED

12

12



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option D1** – Add the ability to capture injury information for homicide victims within NIBRS. **Priority of 3M.**

UNCLASSIFIED

13

13



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue E: Creation of a New NIBRS Offense – Criminal Negligence

Option E1: Create a new NIBRS Offense of *Criminal Negligence* to capture offenses not specified within current NIBRS offense definitions.

Option E2: No change.

UNCLASSIFIED

14

14



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Working Group Actions:

- Northeastern, Southern, and Federal Working Group motioned for Option E1: Create a new NIBRS Offense of *Criminal Negligence* to capture offenses not specified within current NIBRS offense definitions. Priority 3M.
- North Central and Western Working Groups motioned for Option E2: No Change.

UNCLASSIFIED

15

15



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option E2 – No change.**

UNCLASSIFIED

16

16



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue F: *Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to all NIBRS Offenses*

Option F1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to expand the collection of NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS offenses.

Option F2: No change.

UNCLASSIFIED

17

17



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Working Group Actions:

- North Central, Southern, Western, Federal Working Groups motioned for Option F1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to expand the collection of NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS offenses. Priority 3M.
- Northeastern Working Group motioned for Option F2: No Change.

UNCLASSIFIED

18

18



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option F1** – Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to expand the collection of NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to all NIBRS offenses. **Priority of 3M.**

UNCLASSIFIED

19

19



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue G: Modification of Data Element – Type Criminal Activity/Gang Information (Data Element 12) to Include Additional Values

Option G1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include the additional values recommend by the Beyond 2021 Task Force. If approved values will be as follows:

O = Operating/Promoting/Assisting/**Abetting**

W = Conspiracy

Option G2: No change.

UNCLASSIFIED

20

20



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Working Group Actions:

- North Central, Southern, Western, Federal Working Groups motioned for Option G1: Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include *abetting and conspiracy*.
 - North Central, Western, and Federal: Priority 3M.
 - Southern: Priority 4L.
- Northeastern Working Group motioned for Option G2: No Change.

UNCLASSIFIED

21

21



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option G1** – Modify NIBRS Data Element 12 (Type Criminal Activity/Gang Information) to include the additional values recommended by the Beyond 2021 Task Force. If approved, the additional values will be as follows:
 - O = Operating/Promoting/Assisting/**Abetting**
 - W = **Conspiracy**

Priority of 3M.

UNCLASSIFIED

22

22



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue H: Modification of Data Element – Suspected Drug Type (Data Element 20)

Option H1: Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force and create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.

Option H2: Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force. Do not create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.

Option H3: Do not modify NIBRS Data Element 20 (Suspected Drug Type) but create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.

Option H4: No change.

UNCLASSIFIED

23

23



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option H1** – Modify NIBRS Data Element 20 (Suspected Drug Type) to reflect the recommended updates made by the Beyond 2021 Task Force and create a process for assessing Data Element 20 (Suspected Drug Type) for future modifications.
Priority of 3M.

UNCLASSIFIED

24

24



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue I: Modification of Data Element – Type Drug Measurement (Data Element 22)

Option I1: Modify NIBRS Data Element 22 (Type Drug Measurement) to reflect the changes recommended by the Beyond 2021 Task Force.

Option I2: No change.

UNCLASSIFIED

25

25



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option I1** – Modify NIBRS Data Element 22 (Type Drug Measurement) to reflect the changes recommended by the Beyond 2021 Task Force. **Priority of 3M.**

UNCLASSIFIED

26

26



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue J: Modification to FBI UCR Policy – Specifying Conversion of Drug Quantities to Common Units

Option J1: Modify FBI UCR Program policy to allow for the conversion of NIBRS drug quantities to common units proposed by the Beyond 2021 Task Force.

Option J2: No change.

UNCLASSIFIED

27

27



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option J1** – Modify FBI UCR Program policy to allow for the conversion of NIBRS drug quantities to common units proposed by the Beyond 2021 Task Force. **Priority 3M.**

UNCLASSIFIED

28

28



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

Subcommittee Options:

Issue K: Additional Property Values of Utilities and Services and Intellectual Property

Option K1: Add the data values of *Intellectual Property* and *Utilities and Services* to NIBRS Data Element 15 (Property Description).

Option K2: No change.

UNCLASSIFIED

29

29



UCR Issue #2 continued

Beyond 2021 Initiative Update – NIBRS Data Elements

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option K1** – Add the data values of *Intellectual Property* and *Utilities and Services* to NIBRS Data Element 15 (Property Description). **Priority of 3M.**

UNCLASSIFIED

30

30



UCR Issue #3

Beyond 2021 Update – Addition of Geolocation to NIBRS

Purpose:

Provide the recommendations of the Beyond 2021 Task Force for the implementation of geolocation as a data point within the NIBRS.

UNCLASSIFIED

31

31



UCR Issue #3

Beyond 2021 Update – Addition of Geolocation to NIBRS

Subcommittee Options:

Option 1: Pursue the addition of x/y/z (i.e., latitude/longitude) coordinates of the incident, but not address, to the NIBRS data collection. In order to implement this approach, the FBI UCR Program and the FBI Office of the General Counsel will need to detail a method to collect incident to a geographic point while also providing a dissemination strategy that addresses the risks to privacy.

Option 2: Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract.

Option 3: No change.

UNCLASSIFIED

32

32



UCR Issue #3 continued

Beyond 2021 Update – Addition of Geolocation to NIBRS

Working Group Actions:

- North Central Working Group motioned for Option 1. Priority 3M.
- Northeastern and Western Working Groups motioned for Option 2.
 - Northeastern: Priority 3M.
- Southern and Federal Working Groups motioned for Option 3.

UNCLASSIFIED

33

33



UCR Issue #3 continued

Beyond 2021 Update – Addition of Geolocation to NIBRS

Public Safety Strategy Subcommittee Actions:

- **Motion: Option 2** – Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract.

UNCLASSIFIED

34

34



UCR Issue #3 continued

Beyond 2021 Update – Addition of Geolocation to NIBRS

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option 2** – Pursue the collection of geographic location of the incident through the indication of a small aggregate area, such as Census tract. **Priority 3M.**

UNCLASSIFIED

35

35



UCR Issue #4

Expansion of Location Data Values within NIBRS Data Element 9

Purpose:

Provide a proposal to implement changes and expansion to the Valid Data Values for NIBRS Data Element 9 (Location Type).

UNCLASSIFIED

36

36



UCR Issue #4

Expansion of Location Data Values within NIBRS Data Element 9

Subcommittee Options:

Option 1: Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the chart. The provided changes include a modification of existing Location Code 09=Drug Store/Doctor's Office/Hospital code to be separated into three individual Location Types: 09=Drug Store/Pharmacy, 62=Doctor's Office, and 66=Hospital. These changes will be effective immediately upon approval.

Option 2: Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the chart. The provided changes include a modification of existing Location Code 09=Drug Store/Doctor's Office/Hospital code to be separated into three individual Location Types: 09=Drug Store/Pharmacy, 62=Doctor's Office, and 66=Hospital. The implementation will be included as part of the Beyond 2021 effort. All changes will be incorporated into the Beyond 2021 schedule accordingly.

Option 3: No change.

Note: the chart referenced in the motions is available on slide 38.

UNCLASSIFIED

37

37



UCR Issue #4

Expansion of Location Data Values within NIBRS Data Element 9

The options include proposed amendments to the existing NIBRS Data Element 9 (Location Type):

CODE	VALID DATA VALUE	DESCRIPTOR	COMMENTS
9	Drug Store/Pharmacy	Store where the Food and Drug Administration approved medicinal drugs are dispensed and sold.	Exists in NIBRS Technical Specification with other V/DVs under same code.
59	Auto Salvage/Junkyard	Location where unusable vehicles or vehicle parts can be bought, sold, or stored, a place where scrap is collected before being recycled or discarded.	
60	Carpport/Garage/Driveway	An area around residential space not constituting a residential structure.	
61	Cemetery	An area set apart which contain graves, tombs or funeral urns.	
62	Doctor's Office	A medical facility in which one or more medical doctors, usually general practitioners, receive and treat patients.	
63	Gym/Fitness Club	Indoor club, building, or large room where people exercise or participate in indoor sporting activities to enhance physical fitness.	
64	Golf Course	Outdoor areas of land where golf is played.	
65	Hospital	An institution providing medical and surgical treatment and nursing care for sick or injured people.	Routine, preventative, and scheduled care would be included in Doctor's Office. This would include urgent care facilities and inpatient behavioral health centers.
66	Library	Room or building containing collections of books, periodicals, software programs, films, or recorded music for people to read, borrow, or utilize as reference.	
67	Loan/Cash Advance/Check Cashing Facility	Commercial business where individuals obtain financial services over the counter for a clear fee.	Specialty Store denotes "retail" element. These stores are not considered retail stores and are becoming more prevalent.
68	Marijuana Dispensary	Establishment primarily used for selling medical or recreational marijuana.	Specialty Store denotes "retail" element. These stores are not considered retail stores and are becoming more prevalent.
69	Marijuana Facility	Indoor or outdoor site used for the commercial production and harvesting of cannabis for recreational or medical use.	This is a facility for the manufacture of the product – not a sales facility.
70	Movie Theater	Venue where movies are shown for public entertainment.	
71	Museum	Building in which objects of historical, scientific, artistic, or cultural interest are stored and exhibited.	
72	Pawnshop	Commercial establishment for lending money in exchange for personal property which can be sold if the loan is not repaid by a predetermined time.	
73	Public Transportation	Busse, trains, subways, and other forms of transit which charge set fares, run on fixed rates, and are available to the public.	Incidents which happen on public modes of transportation cannot be considered a static location – need an option to distinguish this.
74	Tattoo Parlor	Place in which the primary function is professional tattooing.	
75	Zoo	Indoor or outdoor establishment, which maintains a collection of wild animals for study, conservation, or display to the public.	

UNCLASSIFIED

38

38



UCR Issue #4 continued

Expansion of Location Data Values within NIBRS Data Element 9

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option 2** – Implement the requested modifications and additions to the NIBRS Offense Segment, Data Element 09 (Location Type) as provided in the *Data Element 09 Recommendations* chart. The provided changes include a modification of existing Location Code 09=Drug Store/Doctor's Office/Hospital code to be separated into three individual Location Types: 09=Drug Store/Pharmacy, 62=Doctor's Office, and 66=Hospital. The implementation will be included as part of the Beyond 2021 effort. All changes will be incorporated into the Beyond 2021 schedule accordingly. **Priority 3M.**

Note: the chart referenced in the motion is available on slide 38.

UNCLASSIFIED

39

39



UCR Issue #5

Addition of Data Elements to the NIBRS for the Collection of Lawful Access Data

Purpose:

Present options for adding Lawful Access data elements to the NIBRS data collection.

UNCLASSIFIED

40

40



UCR Issue #5

Addition of Data Elements to the NIBRS for the Collection of Lawful Access Data

Subcommittee Options:

Option 1: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection.

Option 2: No change.

UNCLASSIFIED

41

41



UCR Issue #5 continued

Addition of Data Elements to the NIBRS for the Collection of Lawful Access Data

Working Group Actions:

- Southern, Western, and Federal Working Groups motioned for Option 1: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Priority 3M.
- North Central Working Group motioned for Option 2: No change.
- Northeastern Working Group motioned for a New Option: Add three data elements to both the Victim and Offender Segments of the NIBRS data collection. Caveat to create process to update the data values within data elements.

UNCLASSIFIED

42

42



UCR Issue #5 continued

Addition of Data Elements to the NIBRS for the Collection of Lawful Access Data

The UCR Subcommittee recommends the following APB motion:

- **Motion: New Option** – To have the UCR Program identify a collection mechanism outside of the NIBRS data file that leverages the UCR Program data collection infrastructure.
Priority 3H.

UNCLASSIFIED

43

43



UCR Issue #6

Expansion of Victim to Offender Relationship in NIBRS Data Element 35

Purpose:

Present a proposal for additions to the acceptable codes within NIBRS Data Element 35 to allow for new victim values with NIBRS.

UNCLASSIFIED

44

44



UCR Issue #6 continued

Expansion of Victim to Offender Relationship in NIBRS Data
Element 35

Subcommittee Options:

Issue A: Addition of “FP=Victim was Foster Parent” and “FC=Victim was Foster Child”

Option A1: Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35.

Option A2: No change.

UNCLASSIFIED

45

45



UCR Issue #6 continued

Expansion of Victim to Offender Relationship in NIBRS Data
Element 35

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option A1** – Create values “FP=Victim was Foster Parent” and “FC=Victim was Foster Child” and make allowable for NIBRS Data Element 35. **Priority of 3M.**

UNCLASSIFIED

46

46



UCR Issue #6 continued

Expansion of Victim to Offender Relationship in NIBRS Data
Element 35

Subcommittee Options:

Issue B: Addition of "CO=Cohabitant (non-intimate relationship)"

Option B1: Create value "CO=Cohabitant (non-intimate relationship)" and make allowable for NIBRS Data Element 35.

Option B2: No change.

UNCLASSIFIED

47

47



UCR Issue #6 continued

Expansion of Victim to Offender Relationship in NIBRS Data
Element 35

Working Group Actions:

- All Working Groups motioned for Option B1: Create value "CO=Cohabitant (non-intimate relationship)" and make allowable for NIBRS Data Element 35.
 - North Central, Western, and Federal Working Groups: Priority 3M.
 - Northeastern Working Group: Priority 3H.
 - Southern Working Group: Priority 4L.

UNCLASSIFIED

48

48



UCR Issue #6 continued

Expansion of Victim to Offender Relationship in NIBRS Data
Element 35

The UCR Subcommittee recommends the following APB motion:

- **Motion: New Option** – Create value “CO=Cohabitant (non-intimate/non-family relationship)” and make allowable for NIBRS Data Element 35. **Priority of 3M.**

UNCLASSIFIED

49

49



UCR Issue #7

Addition of a New Criminal Offense in Progress Data Element in
the NIBRS

Purpose:

Present a proposal to create a new data element to track criminal offenses in progress when a justifiable homicide takes place.

UNCLASSIFIED

50

50



UCR Issue #7 continued

Addition of a New Criminal Offense in Progress Data Element in the NIBRS

Subcommittee Options:

Option 1: Change the name of Data Element 32 to “Data Element 32A” and create a new data element of 32B (Criminal Offense in Progress) with acceptable values for all crimes against persons and crimes against property offenses. This new data element would be mandated only when a justifiable homicide has taken place.

Option 2: Create a new data element for “Criminal Offense in Progress” with acceptable values for all crimes against persons and crimes against property offenses. This would include no changes to Data Element 32. This new data element would be mandated only when a justifiable homicide has taken place.

Option 3: No change.

UNCLASSIFIED

51

51



UCR Issue #7 continued

Addition of a New Criminal Offense in Progress Data Element in the NIBRS

Working Group Actions:

- Northeastern, Southern, Western, and Federal Working Groups motioned for Option 1: Change the name of Data Element 32 to “Data Element 32A” and create a new data element of 32B (Criminal Offense in Progress) with acceptable values for all crimes against persons and crimes against property offenses. This new data element would be mandated only when a justifiable homicide has taken place. Priority 3M.
- North Central Working Group motioned for Option 3: No change.

UNCLASSIFIED

52

52



UCR Issue #7 continued

Addition of a New Criminal Offense in Progress Data Element in the NIBRS

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option 3 – No change.**

UNCLASSIFIED

53

53



UCR Issue #8

Changes to Race Codes within the FBI UCR Program

Purpose:

Present a proposal for changes to the race code data element within FBI UCR Program data collections to allow for multiple race code choices within race code data elements.

UNCLASSIFIED

54

54



UCR Issue #8 continued

Changes to Race Codes within the FBI UCR Program

Subcommittee Options:

Option 1: Change the NIBRS race category to allow for multiple selections for the arrestee, offender, and victim segments.

Option 2: No change.

UNCLASSIFIED

55

55



UCR Issue #8 continued

Changes to Race Codes within the FBI UCR Program

The UCR Subcommittee recommended:

- **Motion: New Option** – No change. Refer to Public Safety Strategy Subcommittee for further exploration.

The Public Safety Strategy Subcommittee will cover Issue 8.

UNCLASSIFIED

56

56



UCR Issue #9

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Purpose:

Present the proposed modifications to the NIBRS data collection recommended by the Beyond 2021 Task Force.

UNCLASSIFIED

57

57



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Subcommittee Options:

Issue A: Replacing the NIBRS offense – “Fondling”

Option A1: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

“Criminal Sexual Contact includes the following:

- *The intentional touching of the clothed or unclothed genitalia, anus, groin, breast or buttocks of any person by the actor’s clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*
- *The forced touching by the victim of the actor’s clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

Option A2: No change.

UNCLASSIFIED

58

58



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Working Group Actions:

- Northeastern Working Group motioned for Option A1: As presented. Priority 3M.
- Western Working Group motioned for a New Option: No change to the current definition of “*fondling*”. Replace the term “*fondling*” with “*criminal sexual contact*”. Priority 3M.

UNCLASSIFIED

59

59



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Working Group Actions:

- North Central Working Group motioned for a New Option: Modify the NIBRS offense “*fondling*” to “*criminal sexual contact*” with the below definition:
“Criminal Sexual Contact includes the following:
 - *The intentional touching of the clothed or unclothed genitalia, anus, groin, breast or buttocks of any person, without the consent of the victim.*
 - *The forced touching by the victim of the actor’s clothed or unclothed genitalia, anus, groin, breast or buttocks, without the consent of the victim.**This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”*
Priority 3M.

UNCLASSIFIED

60

60



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Working Group Actions:

- Southern Working Group motioned for a New Option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:
“Criminal Sexual Contact includes the following:
 - *The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*
 - *The forced touching by the victim of the actor’s clothed or unclothed body parts, without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.**This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”*

Priority 3M.

UNCLASSIFIED

61

61



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Working Group Actions:

- Federal Working Group motioned for a New Option: Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:
“Criminal Sexual Contact includes the following:
 - *The intentional touching of the clothed or unclothed body parts without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*
 - *The forced touching by the victim of the actor’s clothed or unclothed body parts, without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.**This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”*

Priority 3M.

UNCLASSIFIED

62

62



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

The UCR Subcommittee recommends the following APB motion:

- **Motion: New Option** – Modify the NIBRS offense “fondling” to “criminal sexual contact” with the below definition:

“Criminal Sexual Contact

- *The intentional touching of the clothed or unclothed body parts without the consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*
- *The forced touching by the victim of the actor’s clothed or unclothed body parts, without consent of the victim for the purpose of sexual degradation, sexual gratification, or sexual humiliation.*

This includes instances where the victim is incapable of giving consent because of age or incapacity due to temporary or permanent mental or physical impairment or intoxication for the purpose of sexual degradation, sexual gratification, or sexual humiliation.”

Priority of 3M.

UNCLASSIFIED

63

63



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Subcommittee Options:

Issue B: Updating the NIBRS offense – “Incest”

Option B1: Modify the NIBRS offense “incest” definition to state:

“Consensual intercourse between individuals related by blood within the degree that the individuals are prohibited based on state provision.”

Option B2: Modify *incest* to be captured as a NIBRS Group B Offense with data captured as part of 90Z-All Other Offenses.

Option B3: Discontinue collection of *incest* for national reporting.

Option B4: No change.

UNCLASSIFIED

64

64



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

Working Group Actions:

- North Central, Southern, and Federal Working Groups motioned for Option B1: Modify the NIBRS offense “incest” definition to state:
“Consensual intercourse between individuals related by blood within the degree that the individuals are prohibited based on state provision.”
 - North Central and Federal Working Groups: Priority 3M.
 - Southern Working Group: Priority 4M.
- Northeastern and Western Working Groups motioned for Option B4: No change.

UNCLASSIFIED

65

65



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense Nomenclature

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option B4 – No change.**

UNCLASSIFIED

66

66



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense
Nomenclature

Subcommittee Options:

Issue C: *Modification of NIBRS offense – “Statutory Rape”*

Option C1: Modify the NIBRS offense “*statutory rape*” definition to state:

“Consensual sexual intercourse with an individual who is under the age of majority but meets the state provisions for the age of consent.”

Option C2: No change.

UNCLASSIFIED

67

67



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense
Nomenclature

Working Group Actions:

- Northeastern, North Central, and Federal Working Groups motioned for Option C1: Modify the NIBRS offense “*statutory rape*” definition to state:

“Consensual sexual intercourse with an individual who is under the age of majority but meets the state provisions for the age of consent.”

Priority: 3M.

- Southern and Western Working Groups motioned for Option C2: No change.

UNCLASSIFIED

68

68



UCR Issue #9 continued

Beyond 2021 Initiative Update - Revision to NIBRS Sex Offense
Nomenclature

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option C2 – No change.**

UNCLASSIFIED

69

69



UCR Issue #10

Creation of a NIBRS Offense Code Mapping Crosswalk Repository

Purpose:

Present a proposal for the creation of a NIBRS offense code
mapping crosswalk displaying state-level statute mapping to
NIBRS offense definitions.

UNCLASSIFIED

70

70



UCR Issue #10 continued

Creation of a NIBRS Offense Code Mapping Crosswalk Repository

Subcommittee Options:

Option 1: Create a NIBRS offense crosswalk repository hosted by the FBI UCR Program and maintained by state UCR programs containing state-level statute information crosswalked/mapped to NIBRS offense codes.

Option 2: No change.

UNCLASSIFIED

71

71



UCR Issue #10 continued

Creation of a NIBRS Offense Code Mapping Crosswalk Repository

Working Group Actions:

- Northeastern, North Central, Southern, and Federal Working Groups motioned for Option 1: Create a NIBRS offense crosswalk repository hosted by the FBI UCR Program and maintained by state UCR programs containing state-level statute information crosswalked/mapped to NIBRS offense codes. Priority 3M.
- Western Working Group motioned for Option 2: No change.

UNCLASSIFIED

72

72



UCR Issue #10 continued

Creation of a NIBRS Offense Code Mapping Crosswalk Repository

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option 1** – Create a NIBRS offense crosswalk repository hosted by the FBI UCR Program and maintained by state UCR programs containing state-level statute information crosswalked/mapped to NIBRS offense codes. **Priority 3M.**

UNCLASSIFIED

73

73



UCR Issue #16

Summary of Recently Conducted Quality Assurance Reviews

Purpose:

Present results of recently conducted UCR Quality Assurance Reviews.

UNCLASSIFIED

74

74



UCR Issue #16 continued

Summary of Recently Conducted Quality Assurance Reviews

The UCR Subcommittee recommends the following APB motion:

- **Motion:** Authorize Letters of Interest be sent to each CJIS Systems Officer and UCR program manager as these reviews have been finalized.

UNCLASSIFIED

75

75



Informational Topics

The UCR Subcommittee accepted the following topics for Information Only:

- UCR Issue #1** – UCR Status Report
- UCR Issue #11** – Law Enforcement Suicide Data Collection Update
- UCR Issue #12** – National Use-of-Force Data Collection
- UCR Issue #13** – Status of the NIBRS Transition
- UCR Issue #14** – Beyond 2021 Task Force Update
- UCR Issue #15** – Fiscal Year 2020 Audit Results Summary

UNCLASSIFIED

76

76



National Use-of-Force Data Collection Update

1



Current Metrics (As of May 10, 2021)

- 2021 Participation
 - Total of 6,092 agencies participating
 - Accounting for 43.6 percent of sworn law enforcement
 - Tribal Agencies: 47
 - Colleges/University Agencies: 265
 - Federal Agencies Reported: 36
 - Territories: 1

2

UNCLASSIFIED

2



Current Metrics (As of May 10, 2021)

- 2020 Participation
 - Total of 6,247 agencies participating
 - Accounting for 53.3 percent of sworn law enforcement
 - Tribal Agencies: 47
 - Colleges/University Agencies: 252
 - Federal Agencies Reported: 34

UNCLASSIFIED

3

3



40 Percent Publication, for 2020



- Released on November 9, 2020
- Displayed on the Crime Data Explorer
<https://crime-data-explorer.fr.cloud.gov/pages/le/uof>

United States

National use-of-force data is voluntarily submitted to the FBI for participating law enforcement agencies. Only agencies that submitted use-of-force incident reports or area reports for January through August 2020 are included in this report.

Resources

- National Use of Force Data Collection website
- National Use of Force Data Collection FAQ

Participation

In 2020, 6,039 out of 18,344 federal, state, local, and tribal law enforcement agencies throughout the nation participated and provided use-of-force data. The officers employed by these agencies represent 40% federal, state, local, and tribal sworn officers in the nation.

UNCLASSIFIED

4

4



Upcoming Data Release

A July 2021, data release is scheduled and will include:

- 2019 data refreshed
- 2020 data representing 50 percent of all federal, state, local, college/university, and tribal sworn law enforcement officers
- Calendar year 2021 first quarter data

5

5



60 Percent Coverage Threshold

- Ratios, percentages, and lists would include data such as:
 - Percentage of type of use-of-force incident
 - Percentage of reason of initial contact
 - Highest types of resistance encountered
 - Most frequent types of force used

6

6



States Managing the National Use-of-Force Data Collection

- | | | |
|-------------|---------------|----------------|
| Alabama | Maine | Oklahoma |
| Alaska | Michigan | Oregon |
| Arizona | Minnesota | South Carolina |
| Colorado | Montana | South Dakota |
| Connecticut | Nebraska | Tennessee |
| Delaware | New Hampshire | Texas |
| Florida | New Jersey | Utah |
| Georgia | New Mexico | Virginia |
| Idaho | New York | Washington |
| Kansas | North Dakota | Wisconsin |
| Kentucky | Ohio | |

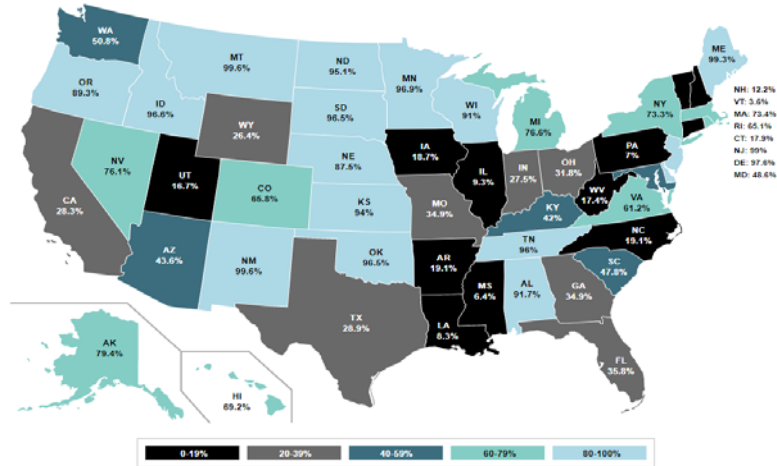
UNCLASSIFIED

7

7



National Use-of-Force Data Collection Participation Percentage by State (Police Employment Count)



Percentages calculated by totaling the PE counts of all agencies within the state. Agencies that have not submitted PE counts to UCR will affect the percentage.

*as of May 17, 2021

UNCLASSIFIED

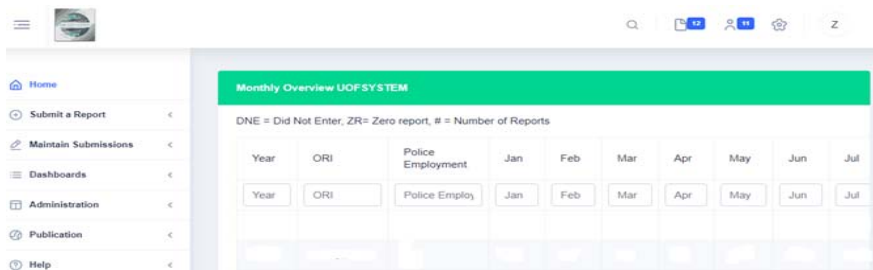
8

8



Use-of-Force Angular 9 Upgrades

- The Use-of-Force Portal is being upgraded to enhance the user experience.
- All UCR applications/systems will have the same look and feel which will decrease the learning curve for users.



UNCLASSIFIED

9

9



Law Enforcement Public Contact

- The Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program piloted a collection of recorded law enforcement public contacts.
 - The pilot ran from September 1 – October 30, 2020.
 - 52 agencies were scheduled to participate with 36 submitting data.
 - Participating agencies represented federal, state, local, tribal and college/university law enforcement agencies of varying populations.
- Results of the collection are awaiting final approval from the OMB.
- January 1, 2022, collection start date with data releases beginning in 2023.

UNCLASSIFIED

10

10



Points of Contact

For information or assistance with the National
Use-of-Force Data Collection



National Use-of-Force Data Collection Support

Email: useofforce@fbi.gov

Phone: 304-625-9998

UNCLASSIFIED

11

11



National Incident-Based Reporting System (NIBRS) Update

UNCLASSIFIED

1



Current Metrics (As of 05/12/2021)

- 10,109 - Agencies Reporting NIBRS Data
– 44 States NIBRS Certified
- 61.1 percent – Represents Percentage of Total Reporting Agencies
- 56.4 percent – Represents Percentage of Population Covered by NIBRS Reporting

UNCLASSIFIED

2

2



Areas of Primary Focus

- Continue messaging the transition to all stakeholders
- Continue to assist agencies in and/or wanting to transition
 - Resources
 - Training
 - Virtual
 - Upcoming locations
- Continue to track agency commitments to the transition
 - What are the projected national percentages now (based on state feedback)?
 - Population covered
 - Agency participation

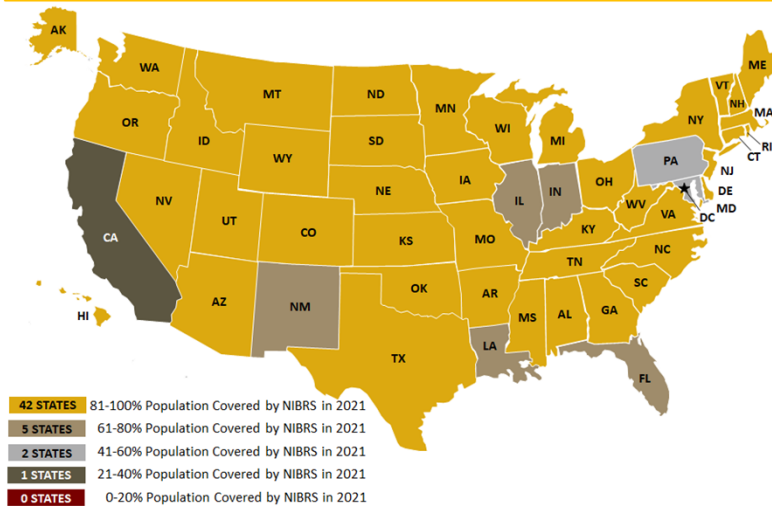
UNCLASSIFIED

3

3



NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS) 2021 PROJECTED POPULATION COVERED BASED ON LAW ENFORCEMENT COMMITMENTS AS OF MARCH 2021



UNCLASSIFIED

4

4



State UCR Program Certification

- **18** states in full NIBRS compliance.
- **26** states are partial NIBRS contributors.
 - In May 2021, Mississippi attained State UCR Program certification
- **6** states and all the territories are not yet NIBRS certified. These states and territories are working toward NIBRS certification.

UNCLASSIFIED

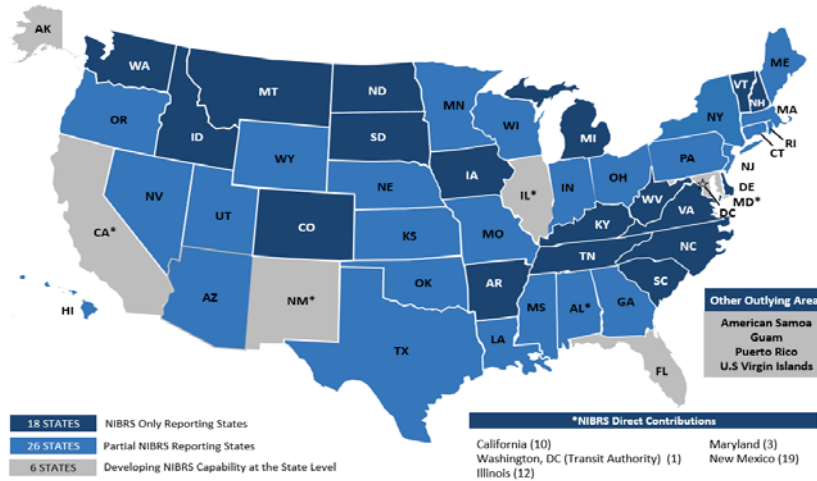
5

5



NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS) PARTICIPATION STATUS Uniform Crime Reporting (UCR) Program - NIBRS Participation by State

May 2021



UNCLASSIFIED

6

6



“Effects of NIBRS on Crime Statistics 2019”

- A 2019 study finds minimal impact from the NIBRS transition to reported crime levels.
- This study can be found on the Explorer page of the Crime Data Explorer under the Resources section.

<https://crime-data-explorer.fr.cloud.gov/>

7

7



NIBRS Collection Application (NCA)

- The NCA enables users to directly enter and submit NIBRS data to the UCR system for processing, retention, and publication.
 - Submit via the Law Enforcement Enterprise Portal.
 - Collects and contains the same NIBRS offenses and data elements currently supported within the UCR system.
 - Uses the established business rules to ensure valid submissions.

UNCLASSIFIED

8

8



NIBRS Collection Application (NCA)

- June 2020, the NCA was deployed for federal and tribal agencies.
- As of May 12, 2021, 30 federal agencies and 118 tribal agencies are submitting NIBRS data via the NCA.
- The Federal Bureau of Investigation made the NCA available to non-transitioned state and local agencies. States and territories were notified and the following actions were conducted to assist with NCA participation:
 - Email solicitations
 - Workflow
 - Help desk
 - Training

UNCLASSIFIED

9

9



Points of Contact

For information or assistance with NIBRS



NIBRS Support

Email: UCR-NIBRS@fbi.gov
NIBRS Website: www.fbi.gov/nibrs
NIBRS contact: 304-625-9999

UNCLASSIFIED

10

10

Intentionally Left Blank



APB Item #6
**Chairman's Report on the National Crime
Information Center (NCIC) Subcommittee**

Brian Wallace, Chairman
June 2021 CJIS APB Meeting

1



Accepted as Information Only

- **NCIC Issue #5 – N3G Project Status**
- **NCIC Issue #6 – N3G Task Force Status Update**
- **NCIC Issue #7 – NCIC EFTS Migration Update**
- **NCIC Issue #8 – NIEM XML Presentation and Transformation Style Sheet Update**
- **NCIC Issue #9 – CJIS Division NCIC Status**

2



NCIC Issue #1

Proposal from the National Insurance Crime Bureau (NICB) to
Modify the Memorandum of Understanding (MOU) with the FBI CJIS
Division

Purpose:

To determine whether the current MOU between the FBI and the NICB should be modified to expand the NICB's "Authorized Use" of the NCIC data to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations.

3



NCIC Issue #1 - continued

Proposal from the National Insurance Crime Bureau (NICB) to
Modify the Memorandum of Understanding (MOU) with the FBI CJIS
Division

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to endorse Option 1:

Expand the "Authorized Use" of NCIC data by NICB to include self-insured entities that operate and manage a large fleet of vehicles in furtherance of shipping and logistic operations.

4



NCIC Issue #1 - continued

Proposal from the National Insurance Crime Bureau (NICB) to
Modify the Memorandum of Understanding (MOU) with the FBI CJIS
Division

Recommended APB Motion:

Expand the “Authorized Use” of NCIC data by
NICB to include self-insured entities that operate
and manage a large fleet of vehicles in
furtherance of shipping and logistic operations.

5



NCIC Issue #2

Modification of the Protected Person Date of Birth (PPB) Field Edits

Purpose:

To present a proposal to modify the PPB Field
edits to allow for the current date to be entered

6



NCIC Issue #2 - continued

Modification of the Protected Person Date of Birth (PPB) Field Edits

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to endorse Option 1:

Modify the PPB Field edits to allow for the current date. Depending on technical feasibility, this enhancement may be implemented during the development of NCIC 3rd Generation (N3G) or post N3G initial operating capability.

Priority of 3H.

7



NCIC Issue #2 - continued

Modification of the Protected Person Date of Birth (PPB) Field Edits

Recommended APB Motion:

Modify the PPB Field edits to allow for the current date. Depending on technical feasibility, this enhancement may be implemented during the development of NCIC 3rd Generation (N3G) or post N3G initial operating capability. Priority of 3H.

8



NCIC Issue #3

Creation of an Extreme Risk Protection Order (ERPO) File in the NCIC System

Purpose:

To present the policy requirements established by the ERPO File Policy Group for records entered in the new NCIC ERPO File and introduce the ERPO File chapter of the *NCIC Operating Manual*.

9



NCIC Issue #3 - continued

Creation of an Extreme Risk Protection Order (ERPO) File in the NCIC System

Issue 1 – Criteria for Entry

Option 1: Accept the criteria for entry as recommended by the ERPO File Policy Group.

Issue 2 – Record Retention

Option 1: Accept the recommendations from the ERPO File Policy Group regarding ERPO File record retention.

Issue 3 – MKE Codes

Option 3: Accept the MKEs for entry, modification, removal, and inquiry of ERPO File records as recommended by the ERPO File Policy Group **with the exception of the addition of the automatic caution indicator. Add the caution indicator to the message key as is consistent with all other NCIC Person Files.**

10



NCIC Issue #3 - continued

Creation of an Extreme Risk Protection Order (ERPO) Fil in the NCIC System

Issue 4 – Record Integrity

Option 1: Accept the recommendations from the ERPO File Policy Group regarding the record integrity of ERPO File records.

Issue 5 – ERPO File Fields

Option 1: Accept the recommendations from the ERPO File Policy Group regarding ERPO File fields.

Issue 6 – Codes

Option 1: Accept the recommendations from the ERPO File Policy Group pertaining to ERPO File Message Field Codes.

11



NCIC Issue #3 - continued

Creation of an Extreme Risk Protection Order (ERPO) Fil in the NCIC System

Issue 7 – Indication of Firearm Prohibition

Option 1 as modified: Accept the ERPO File Policy Groups recommendation to create a caveat to precede all ERPO File record responses in order to alert those reviewing record responses that the subject of record is prohibited from possessing a firearm; however, modify the caveat to the following:

******THE SUBJECT OF THIS RECORD IS PROHIBITED FROM RECEIVING OR POSSESSING A FIREARM. REFER TO THE MIS FIELD FOR ANY OTHER ADDITIONAL COURT ORDERED PROHIBITIONS.******

12



NCIC Issue #3 - continued

Creation of an Extreme Risk Protection Order (ERPO) File in the NCIC System

NCIC Subcommittee Motion:

Issue 8 – MIS Field Requirements

Option 1: Accept the recommendations from the ERPO File Policy Group pertaining to policy requirements for data to be entered into the MIS Field.

Issue 9 – ERPO File Placement in NCIC Hit Responses

Option 1: Accept the ERPO File Policy Group recommendation to modify the NCIC hit response hierarchy as shown.

13



NCIC Issue #3 - continued

Creation of an Extreme Risk Protection Order (ERPO) File in the NCIC System

Recommended APB Motion:

Accept Issues 1-9 as recommended by the NCIC Subcommittee.

14



NCIC Issue #4

Sunset Date for File Transfer Protocol (FTP)

Purpose:

To establish a community sunset date for the File Transfer Protocol used to transfer large data files from NCIC.

15



NCIC Issue #4 - continued

Sunset Date for File Transfer Protocol (FTP)

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to endorse Option 1:

Recommend to the APB an FTP sunset date of December 31, 2021.

Security and Access (S&A) Subcommittee Motion:

The S&A Subcommittee moved to endorse Option 1:

Recommend to the APB an FTP sunset date of December 31, 2021.

16



NCIC Issue #4 - continued

Sunset Date for File Transfer Protocol (FTP)

Recommended APB Motion:

Recommend to the APB an FTP sunset date of December 31, 2021.

17



NCIC Issue #10

COVID-19 Guidance

Purpose:

To obtain feedback on the NCIC guidance provided at the beginning of the pandemic and determine path moving forward.

18



NCIC Issue #10- continued

COVID-19 Guidance

NCIC Subcommittee Concurrence:

Guidance for Terminal Operator and User Training, Testing, and Recertification during the National Emergency – COVID-19

The NCIC Subcommittee recommended discontinuing terminal operator and user training, testing, and recertification COVID-19 guidance limitations, and relayed the importance of providing advanced notice to the states so they are prepared.

Guidance for NCIC Wanted Person records entered during COVID-19

The NCIC Subcommittee recommended continuing with NCIC Wanted Person record entry guidance until further notice.

Guidance for Hit Confirmation and Locate Procedures during COVID-19

The NCIC Subcommittee recommended continuing with hit confirmation and locate procedure guidance until further notice.

Guidance for Validation Procedures during COVID-19

The NCIC Subcommittee recommended continuing with validation guidance until further notice.

N3G Task Force Update

Jeff Wallin, Chairman
June 2021 CJIS APB Meeting

1

N3G Task Force Update

2021 Virtual Meetings Continue

- White Papers
- Policy Group Recommendations

2

N3G Task Force Update

Policy Groups

- **Active** – Warrant, Response/Notification and Record Integrity
- **Completed** – Blue Alert, MKE, Supplemental, Offline Search, Gang, and Missing/Unidentified
- **Identified** – Training, Advanced Search and Codes

3

Conclusion

Questions or Comments?

4



APB Item #8

Chairman's Report on the National Data Exchange (N-DEX) Subcommittee

Ms. Carol Gibbs, Chair
Illinois State Police

1

1



N-DEX Issue #01

N-DEX Program Status

Purpose:

The Data Sharing Services Unit (DSSU) presented an update on program activities.

- N-DEX System Participation
- N-DEX System Technical Updates and Enhancements
- Distance Learning Opportunities
- Success Story Program

Subcommittee Action:

This issue was accepted for information only.

2

2



N-DEX Issue #02

The N-DEX System to Obtain More Images from the Next Generation Identification (NGI) System

Purpose:

The DSSU proposed initiating Phase 2 of the partnership with NGI.

- Phase 1 complete.
- Users currently search and obtain most recently submitted image.
- Phase 2 would expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and Federal Bureau of Investigation (FBI) number.

3

3



N-DEX Subcommittee Recommendation

To accept Option 1:

Expand sharing from NGI to provide access for the N-DEX System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number.

4

4



N-DEx Issue #03

Explore the Ability to Query the Search History of the N-DEx System

Purpose:

To present a proposal to explore a query of the N-DEx System search history.

- Creates a service in the N-DEx System similar to the National Crime Information Center (NCIC) Offline Transaction Log Search.
- Nearly 20 million searches of the N-DEx System in the last fiscal year (FY) creates an opportunity to learn about past queries for criminal justice purposes.
- Extends what is already available in the system for Subscription (future only queries).

5

5



Spring 2021 Working Group Actions:

- **Option 1:** Explore the implementation of a query of the search history by DSSU staff of the N-DEx System and report the results to the working groups.

Option 2: No Change.

All five working groups accepted Option 1, as written.

6

6



Subcommittee Recommendation to APB

- **Option 1:** Explore the implementation of a query of the search history by DSSU staff of the N-DEx System and report the results to the working groups.

7

7



N-DEx Issue #04 FY 2019/2020 Audit Results Summary

Purpose:

To summarize the audit results from both FY19 and FY20 audits.

- 28 CJIS Systems Agencies (CSAs) were audited (6 federal and 22 state level).
- 143 agencies were audited (19 federal and 124 state level).

8

8



FY 2019/2020 Audit Findings

The findings were as follows:

- Acceptable Use: 9/28
- Incorrect Use Code: 4/28
- N-DEx Agency Coordinator: 2/28
- Triennial Audits: 2/28
- Employer Originating Agency Identifier: 2/28
- Private Contractors: 1/28
- System Access: 1/28
- User Management: 1/28

Subcommittee Action:

This issue was accepted for information only.

9

9



Ad Hoc Topic

Addressing Law Enforcement (LE)-to-LE Data Sharing Gaps Within the National Data Exchange (N-DEx) System.

Purpose:

The topic outlined stakeholder concerns with the application of N-DEx System data sharing rules to LE users operating in criminal justice agencies (non-LE).

Subcommittee Action:

An action item was created to initiate a task force to address this topic and report a recommendation to the subcommittee.

10

10

Intentionally Left Blank



Chairman's Report on the Identification Services (IS) Subcommittee Meeting

Mr. Charles Schaeffer, Chairman
CJIS Advisory Policy Board Meeting
June 9, 2021

1



Informational Topics

IS Issue #1	Miscellaneous Action Items Update
IS Issue #2	Identification Services Coordination Group (ISCG) Update
IS Issue #7	Update on the III Delete Record Cycle and Modify Record Cycle Message Key Development
IS Issue #10	Joint Task Force (JTF) on Rap Sheet Standardization Update
IS Issue #11	Rapid DNA Update
IS Issue #12	NGI System Purpose Code F Responses
IS Issue #13	Update on the FBI's Manual Fingerprint and Name Check Services
IS Issue #14	Criminal History Update
IS Issue #15	Identification for Firearms Sales (IFFS)
IS Issue #16	NGI Interstate Photo System (IPS) Update and <i>IPS Policy and Implementation Guide</i> Revisions
IS Issue #17	Biometric Interoperability Update
IS Issue #18	PRSU Update on Contactless Fingerprint Collection Studies
Ad hoc Issue	Data Strategy

2



IS Issue #1

Miscellaneous Action Items Update

Purpose: To provide updates on the action items.

3



IS Issue #2

ISCG Update

Purpose: To provide an update on ISCG-related items.

4



IS Issue #7

Update on the III Delete Record Cycle (DRC) and Modify Record Cycle (MRC) Message Key Development

Purpose: To provide an update on the development of the III Delete Record Cycle (DRC) and Modify Record Cycle (MRC) Message Key.

5



IS Issue #10

JTF on Rap Sheet Standardization Update

Purpose: To provide an update on JTF Rap Sheet Standardization activities.

6



IS Issue #11

Rapid DNA Update

Purpose: To provide an update on Rapid DNA activities.

7



Rapid DNA Implementation



8



IS Issue #12

NGI System Purpose Code F Responses

Purpose: To alleviate confusion with the type of record information returned with Purpose Code F responses versus Purpose Code C responses.

9



IS Issue #13

Update on the FBI's Manual Fingerprint and Name Check Services

Purpose: To provide an update on the FBI's manual fingerprint and name check services.

10



IS Issue #14

Criminal History Update

Purpose: To provide a criminal history update.

11



The following states do not respond to Purpose Code I:

California, Illinois, Massachusetts, Nebraska, North Dakota, Pennsylvania, Texas, and Washington.

The following state does not respond to Purpose Code S:

California.

The following states do not respond to Purpose Code X:

Alabama, California, Illinois, Massachusetts, Nebraska, North Dakota, and Pennsylvania.

12



IS Issue #15
Identification for Firearms Sales
(IFFS)

Purpose: To provide an update on the IFFS Program.

13



IS Issue #16
NGI Interstate Photo System (IPS)
Update and *IPS Policy and*
***Implementation Guide* Revisions**

Purpose: To provide an update on the IPS and *IPS Policy and Implementation Guide* revisions.

14



IS Issue #17

Biometric Interoperability Update

Purpose: To provide an update on the FBI's NGI System interoperability with the DHS's IDENT and DoD's ABIS.

15



IS Issue #18

PRSU Update on Contactless Fingerprint Collection Studies

Purpose: To provide an update on the FBI's contactless fingerprint studies.

16



Contactless Fingerprint Technology

True Positive Identification Rate (TPIR) False Positive Identification Rate (FPIR) at threshold 4100 (%) NISTIR 8307 Published 5/19/2020

Device	Single Finger		Fingers 02, 03		Fingers 02, 07		Fingers 02,03,07,08		Fingers 02,03,04,05		Fingers 07,08,09,10		Eight Fingers	
	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR
D1	96.00	0.26	98.97	1.55	98.97	1.55	99.48	1.55	98.97	1.55	98.97	1.55	99.81	1.55
D2	91.49	0.19	97.95	1.54	98.97	1.54	99.49	1.53	98.47	1.53	98.98	1.53	99.49	1.53
D3	83.73	0.19	94.97	1.51	96.48	1.51	98.99	1.51	90.98	1.51	96.48	1.51	98.49	1.51
D4	68.83	0.25	86.80	1.52	84.34	1.52	89.39	1.52	92.89	1.52	88.78	1.53	91.92	1.52
D5	45.51	0.19	75.88	1.51	77.00	1.50	86.00	1.50	81.91	1.51	74.37	1.51	88.00	1.50
D6	45.84	0.19	76.80	1.55	77.84	1.55	78.87	1.55	76.80	1.55	78.35	1.55	78.35	1.55
D7	20.42	0.19	48.73	1.52	55.05	1.52	59.00	1.52	51.78	1.52	52.55	1.52	63.13	1.52
D8	33.28	0.19	86.87	1.52	90.91	1.52	92.42	1.52	87.88	1.52	85.35	1.52	89.39	1.52

Unclassified

5

17



Ad hoc Issue Data Strategy

Purpose: To provide information on the FBI's data protection strategies.

18



Action Topics

- IS Issue #3 Consideration of Additional Use Cases for the NGI Iris Service
- IS Issue #4 NGI Iris Service Upon Enrollment Enhancement
- IS Issue #5 Update to 2019 Driver's License Numbers (DLN) in the NGI System
- IS Issue #6 Posting Federal Dispositions to Multiple Dates of Arrest
- IS Issue #8 Unknown and Known Deceased Searches of the DHS's IDENT and the DoD's ABIS
- IS Issue #9 The NDEx System to Obtain More Images from the NGI System

19



IS Issue #3

Consideration of Additional Use Cases for the NGI Iris Service

Purpose: To provide information on the intended NGI Iris Service use cases and consideration of additional uses cases for endorsement.

20



Options:

Option One: Endorse the expansion of the NGI Iris Service for the following cases:

Identification Validation:

Incarceration facilities: to enhance the security and accuracy of other prison processes such as prisoner ingress and egress procedures and movement within the facility.

Supervised release: to aid in the management and validation of identities in the probation and parole systems.

Court system: to validate the identity of individuals as they traverse the courts' processes.

Identification:

Law enforcement: to work with all CSOs and state agencies to navigate programming requirements necessary to participate in the NGI Iris Service for enrollments to grow the iris repository, for searches to capitalize on the service, and to develop mobile iris capabilities for the law enforcement community.

Homeland Security: to pursue the integration of DHS agencies for authorized Iris Image Identification Search uses of the NGI Iris Service.

Option Two: No change.

21



IS Recommended Motion for APB:

Option One: Endorse the expansion of the NGI Iris Service for the following cases:

Identification Validation:

Incarceration facilities: to enhance the security and accuracy of other prison processes such as prisoner ingress and egress procedures and movement within the facility.

Supervised release: to aid in the management and validation of identities in the probation and parole systems.

Court system: to validate the identity of individuals as they traverse the courts' processes.

Identification:

Law enforcement: to work with all CSOs and state agencies to navigate programming requirements necessary to participate in the NGI Iris Service for enrollments to grow the iris repository, for searches to capitalize on the service, and to develop mobile iris capabilities for the law enforcement community.

Homeland Security: to pursue the integration of DHS agencies for authorized Iris Image Identification Search uses of the NGI Iris Service.

Priority 3H.

22



IS Issue #4

NGI Iris Service Search Upon Enrollment Enhancement

Purpose: To propose endorsement of the searching of iris images during the iris image enrollment process.

23



Options:

Option 1: Endorse the enrollment validation process, as proposed. Iris images submitted for enrollment will be searched against iris images already enrolled in the repository. If the iris images do not pass validation, return the new Status/Error Field notification message of:

Manual Review - Enrollment

A search of the submitted iris enrollment requires CJIS to adjudicate the results. The iris images were not enrolled.

This validation process will have an analysis component if an anomaly is discovered through the NGI search. In this instance, collaboration with the submitting agency of the iris and the current tenprint record (or records) hit upon will be necessary.

Option 2: No change.

24



IS Recommended Motion for APB:

Option 1: Endorse the enrollment validation process, as proposed. Iris images submitted for enrollment will be searched against iris images already enrolled in the repository. If the iris images do not pass validation, return the new Status/Error Field notification message of:

Manual Review - Enrollment

A search of the submitted iris enrollment requires CJIS to adjudicate the results. The iris images were not enrolled.

This validation process will have an analysis component if an anomaly is discovered through the NGI search. In this instance, collaboration with the submitting agency of the iris and the current tenprint record (or records) hit upon will be necessary.

Priority 3M.

25



IS Issue #5

Update to 2019 Topic “DLNs in the NGI System”

Purpose: To provide an update on DLNs and proposed options for capturing DLNs in the NGI System.

26



Options:

Option One: Create a new DLN field in the NGI System to submit the DLN. An additional EBTS field must be created to capture the DLN for EBTS TOTs.

Option Two: Create an Operator's License Number (OLN), Operator's License State (OLS), and Operator's License Year of Expiration (OLY) field in the NGI System to collect the DLN in a manner consistent with the NCIC. Additional EBTS fields must be created to capture the DLN in the OLN, OLS, and OLY fields for EBTS TOTs.

Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-.

Option Four: Make no change.

27



IS Recommended Motion for APB:

Option Three: Use the MNU field to submit the DLN and provide guidance to fingerprint contributors to use the prefix DL-.

Priority 3M.

28



IS Issue #6

Posting Federal Dispositions to Multiple Dates of Arrest

Purpose: To present information on the cross-referencing procedure associated with posting Federal dispositions to multiple dates of arrest and determine whether it should be discontinued.

29



Options:

Option 1: Continue the current procedure of cross-referencing federal dispositions data to multiple related dates of arrest.

Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

30



IS Recommended Motion for APB:

Option 2: Discontinue the current procedure of cross-referencing federal disposition data to multiple related dates of arrest.

31



IS Issue #8

Unknown and Known Deceased Searches of the DHS's IDENT and the DoD's ABIS

Purpose: To propose the ability to search prints from deceased individuals against IDENT and ABIS to identify unknown deceased individuals who may not be identified in the NGI System and to also obtain additional identity information on known deceased individuals.

32



Options:

Option 1: No change. Deceased tenprint transactions will not be provided to the DHS IDENT or the DoD ABIS unless an agency makes a specific request of the SPC.

Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.

Option 3: Utilize the Name of Designated Repository (NDR) field to allow contributors to choose when to search the DHS IDENT and/or the DoD ABIS with deceased tenprint transactions. The requesting agency will need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.

33



States that currently receive the IDENT response:

1. Texas
2. Washington
3. Alaska
4. Utah
5. California
6. Michigan
7. Colorado
8. North Carolina
9. South Carolina
10. Georgia
11. Florida
12. Massachusetts
13. Virginia
14. Delaware
15. Wyoming
16. Idaho

34



IS Recommended Motion for APB:

Option 2: Full deployment of all deceased tenprint transactions searching the DHS IDENT and the DoD ABIS. The requesting agency may need to coordinate with the CJIS Division to ensure receipt of the DHS IDENT and/or DoD ABIS response.

Priority 3H.

35



IS Issue #9

The NDEx System to Obtain More Images from the NGI System

Purpose: To propose that criminal justice and law enforcement users would be allowed to obtain more NGI System images via the NDEx System.

36



Options:

Option 1: Expand sharing from NGI to provide access for the NDEx System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number.

Option 2: No change.

37



IS Recommended Motion for APB:

Option 1: Expand sharing from NGI to provide access for the NDEx System to retrieve facial, scars, marks, and tattoo images based on date of arrest and FBI number.

Priority 3M.

38



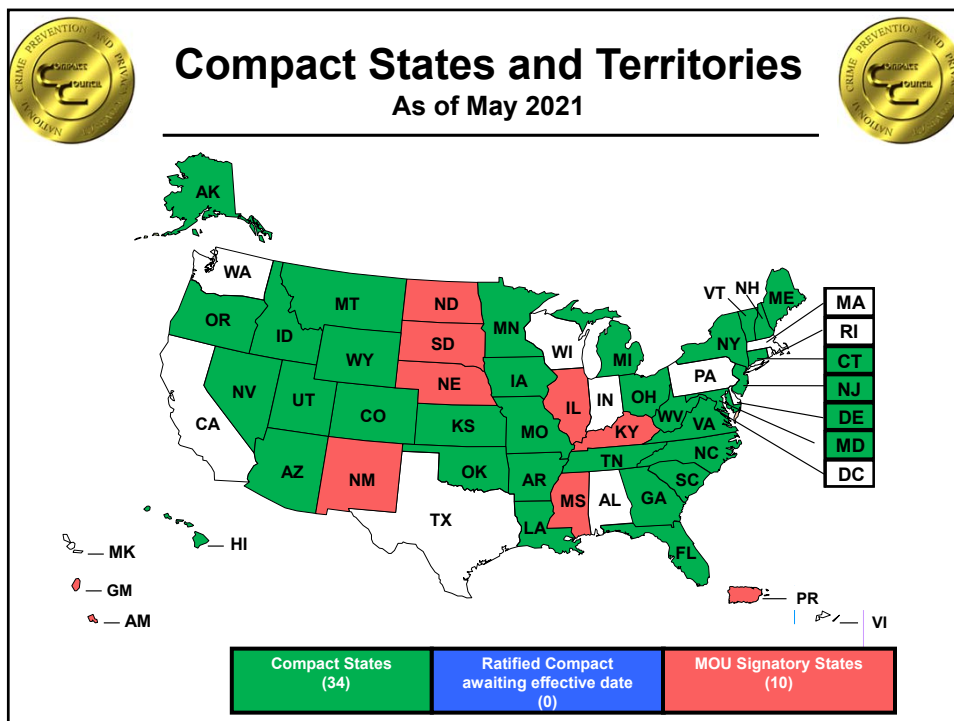
Questions?

National Crime Prevention and Privacy Compact Council Update

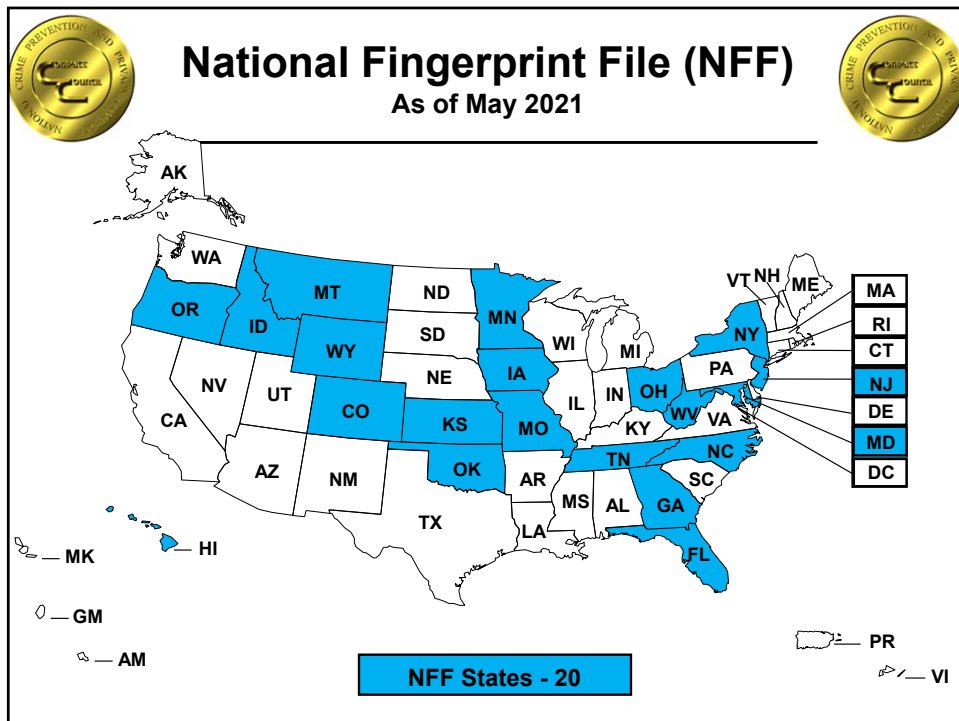


Ms. Leslie Moore
Council Chair

1



2



3

Council Initiatives

- Separation and Clarification of the Message Literals Associated with the NGI System's L0008 Reject Code
- Draft *Federal Register* Notices for the Colorado and Oklahoma Proposals for Delayed Submission of Fingerprints during the COVID-19 Pandemic
- Review of the NFF Implementation Plans

4



Message Literals Associated with L0008 Reject Code



- Transportation Security Administration topic suggestion to automate and streamline processes and remove ambiguity regarding whether a name check should be requested after two fingerprint quality reject submissions.
- Council moved for no change.

Current Message Literal	Proposed Message Literal
The quality of the characteristics is too low to be used. Candidate(s) were found. Please resubmit a new set of fingerprints for comparison to the candidate(s).	The quality of the characteristics is too low to be used. Biographic candidate(s) were found. Please resubmit a new set of fingerprints for comparison to the biographic candidate(s) and to potentially identify biometric candidate(s).
The quality of the characteristics is too low to be used.	The quality of the characteristics is too low to be used. No biographic candidate(s) were found based on the descriptive information provided. Please resubmit a new set of fingerprints to potentially identify biometric candidate(s).

5



Federal Register Notice for Delayed Submission of Fingerprints



- Council's Fingerprint Submission Requirements Rule, often referred to as "Purpose Code X."
- Coronavirus (COVID-19) pandemic:
 - Unavailability or limited availability of noncriminal justice fingerprinting services due to physical distancing measures
 - ✓Oklahoma Proposal
 - ✓Colorado Proposal

6



Review of the NFF Program Implementation Plans



- Plans required to be submitted by the 14 Non-NFF Compact States.
- States reviewed and updated the 2019 Plans to include changes that occurred in 2020, including any impact the COVID-19 pandemic had on progress towards NFF participation.
- Council approved the recommendation to have NFF mentors conduct outreach to states needing assistance, as well as an NFF Information Sharing Symposium.

7



Collaborative Efforts with the APB



- Driver's License Numbers in the NGI System Update
- Update on Posting Federal Dispositions to Multiple Dates of Arrests in the NGI System



8



Council Membership

(Effective 10/01/2021)



State Compact Officers

<u>Council Chair</u>	Ms. Leslie Moore	Kansas Bureau of Investigation
<u>Vice Chair</u>	Mr. Jason Bright	Montana Department of Justice
	Maj. Charles "Monty" Coats	South Carolina Law Enforcement Division
	Ms. Julie Lackner	Minnesota Department of Public Safety
	Ms. Leila McNeill	Idaho State Police
	Mr. Matthew Ruel	Maine State Police
	Mr. Charles Schaeffer	Florida Department of Law Enforcement
	Ms. Melanie Veilleux	Arizona Department of Public Safety
	Mr. Christopher Young	Hawaii Criminal Justice Data Center

9



Council Membership

(continued)



At-Large Representatives

Federal Bureau of Investigation	Michael Christman	Federal Bureau of Investigation
FBI Advisory Policy Board	Jennifer Reich	California Department of Justice
Federal Criminal Justice Agency	Jason Henry	Department of Homeland Security
Federal Noncriminal Justice Agency	Vacant	
State/Local Criminal Justice Agency	Carol Gibbs	Illinois State Police
State/Local Noncriminal Justice Agency	Denise Matthews	Georgia Department of Community Health

10



Upcoming Meetings

Via teleconference, Clarksburg, West Virginia



Regional Committee Meetings

August 3-5, 2021

Standards and Policy Committee Planning and Outreach Committee

September 21-23, 2021

Sanction Committee

November 2, 2021

Compact Council

November 3-4, 2021



11



Contact Information



Council Chairman

Ms. Leslie Moore

(785) 296-8265

E-mail: leslie.moore@kbi.ks.gov

FBI Compact Officer

Ms. Chasity S. Anderson

(304) 625-2803

E-mail: csanderson@fbi.gov

Council Website: <http://www.fbi.gov/compactcouncil>

12



Security and Access (SA) Subcommittee Report

Joe Dominic, Chairman
June 9, 2021 CJIS APB Meeting
Orlando, FL

1



Accepted as Information Only

SA Issue #1 – Fiscal Year 2020 Audit Results Summary

SA Issue #2 – *CJIS Security Policy* Modernization Task Force (MTF)
Update

SA Issue #4 – Interpretive Guidance Task Force (IGTF) Update

2



SA Issue #3 Criminal Justice Data Categorization

Purpose:

To provide the Criminal Justice Data Categorization Task Force’s methodology and recommendation on the appropriate security categorization for criminal justice information, as defined in the *CJIS Security Policy*.

3




Data Categorization Task Force

Mr. Bill Phillips
DCTF, Chair

4


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division



The What



5

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division



Task

- Identify the appropriate security categorization for Criminal Justice Information





6

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Criminal Justice Information -
CJI

- The current version of the CJIS Security Policy provides the following definition of CJI:
 - Criminal Justice Information is the abstract term used to refer to all of the **FBI CJIS provided data** necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to:
 - biometric,
 - identity history,
 - person,
 - organization,
 - property (when accompanied by any personally identifiable information), and
 - case/incident history data.

In addition, CJI refers to the **FBI CJIS-provided data** necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

7


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

The Who

<p><u>Subject Matter Experts</u></p> <p>ACIC – Tiffany Ward SLED – Bruce Smalley DOJ - Michael Roosa TXDPS- Doc Petty MSP - Mitzi Goldstein CMPD – Crystal Cody</p>	<p><u>Support</u></p> <p>CJIS – Melissa Abel CJIS – Chris Weatherly</p>
---	---



8

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division




Task

- Identify the appropriate security categorization for Criminal Justice Information

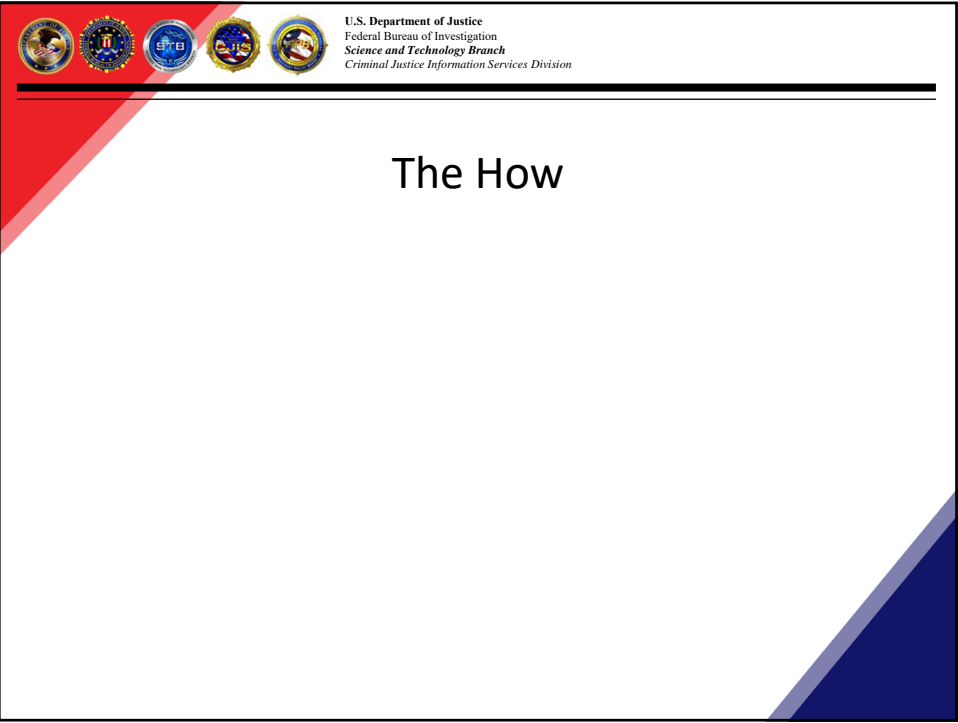


9

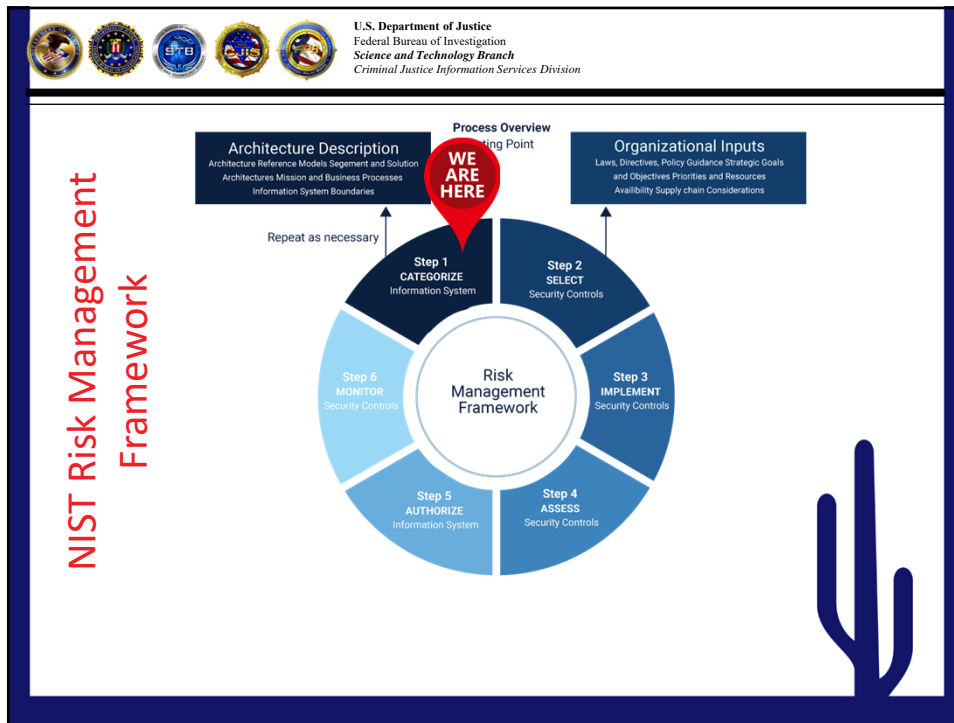
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division



The How



10



11

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Federal Information Security Management Act (FISMA)

National Institute of Standards and Technology (NIST) tasked with the development of:

- Standards to be used by all Federal agencies to *categorize all information and information systems* based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guidelines recommending the types of information and information systems to be included in each such category;

12



Special Publication 800-60

800-60 developed with the objective:
facilitate provision of appropriate levels of
information security according to a range of
levels of impact or consequences that might
result from the unauthorized disclosure,
modification, or loss of availability of the
information or information system.



13



Special Publication 800-60

Recommended security categorization process

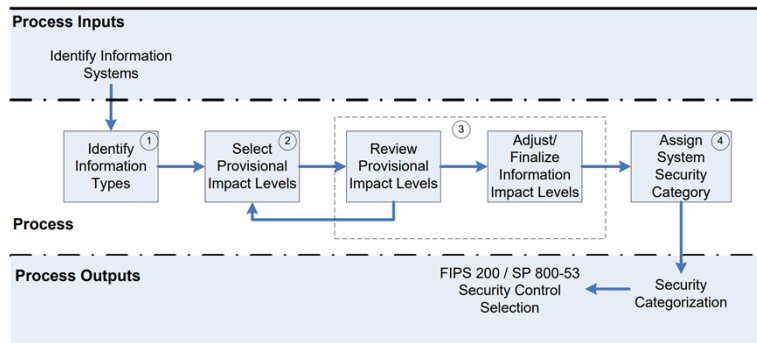


Figure 2: SP 800-60 Security Categorization Process Execution



14



Identify Information Types ¹

Step 1 - Identify Information Types

- Document the agency's business and mission areas
- Identify all of the information types that are input, stored, processed, and/or output from each system within the scope of a CJIS assessment
 - Identify Mission-based Information Type categories [Section 4.1.1]
 - As applicable, identify Management and Support Information Type categories [Section 4.1.2]
 - Specify applicable sub-functions for the identified Mission-based and Management and Support categories [Volume II, Appendices C and D]
 - As necessary, identify other required information types [Sections 4.1.3, 4.1.4]
- Document applicable information types for the identified information system along with the basis for the information type selection



15



Select Provisional Impact Levels ²

Step 2- Select Provisional Impact Level

- Establish provisional impact levels based on the identified information types in Step 1
- Document the initial security categorization for the information type
- Leverage applicable appendices from Volume II
- Identify and determine security categorization for information types processed by an information system not categorized by 800-60 (V.I Section 4.2.2)



16



Special Publication 800-60

Step 3 - Review and Finalize Provisional Impact Levels

- Review and adjust the provisional security impact levels for the security objectives of each information type
 - i. review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing;
 - ii. adjust the security objective impact levels as necessary using the special factors guidance found in Volume II, Appendices C and D; and
- Finalize the impact levels as necessary based on the following considerations:
 - Confidentiality, integrity, and availability factors [Section 4.2.2]
 - Situational and operational drivers (timing, lifecycle, etc.) [Section 4.3]
 - Legal or statutory reasons
- Document all adjustments to the impact levels and provide the rationale or justification for the adjustments.

Review Provisional Impact Levels

Adjust/ Finalize Information Impact Levels



17



Special Publication 800-60

Step 4 - Assign System Security Category

- Assign a system security category based on the aggregate of information types.
 - i. review identified security categorizations for the aggregate of information types;
 - ii. determine the system security categorization by identifying the high water mark for each of the security objectives (confidentiality, integrity, availability) based on the aggregate of the information types;
 - iii. adjust the high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2;
 - iv. assign the overall information system impact level based on the highest impact level for the system security objectives; and
 - v. document all security categorization determinations and decisions.

Assign System Security Category 4



18



Special Publication 800-60

Step 4 - Assign System Security Category

Assign 4
System
Security
Category

- Determine the system security categorization by identifying the security impact level high water mark for each of the security objectives (confidentiality, integrity, availability):

SC System X = {(confidentiality, impact), (integrity, impact), (availability, impact)}

- Adjust the security impact level high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2.
- Assign the overall information system impact level based on the highest impact level for the system security objectives (confidentiality, integrity, availability)



19



Security Objectives

- Confidentiality

Prevent the unauthorized disclosure of information

"A loss of *confidentiality* is the unauthorized disclosure of information."

- Integrity

Assure that information cannot be modified in an unauthorized way

"A loss of *integrity* is the unauthorized modification or destruction of information."

- Availability

Ensure that information is available to authorized users

"A loss of *availability* is the disruption of access to or use of information or an information system."



20



FIPS 199 Impact Level

LOW

- The potential impact is low if:
 - The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
- A **limited** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
 - i. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
 - ii. result in minor damage to organizational assets;
 - iii. result in minor financial loss; or
 - iv. result in minor harm to individuals.



21




FIPS 199 Impact Level

MODERATE

- The potential impact is moderate if:
 - The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals..
- A **serious** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
 - i. cause a significant degradation in mission capability to an extent and duration that the organization *is able to perform its primary functions*, but the effectiveness of the functions is *significantly reduced*;
 - ii. result in *significant damage* to organizational assets;
 - iii. result in *significant financial loss*; or
 - iv. result in significant harm to individuals that *does not involve loss of life or serious life-threatening injuries*

22



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

FIPS 199 Impact Level

HIGH

- The potential impact is High if:
 - The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
- A **severe or catastrophic** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
 - i. cause a degradation in mission capability to an extent and duration that the organization is *not able to perform one or more of its primary functions*;
 - ii. result in *major damage* to organizational assets;
 - iii. result in *major financial loss*; or
 - iv. result in severe or catastrophic harm to individuals involving *loss of life or serious life-threatening injuries*.

23




U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Table 7: Categorization of Federal Information and Information Systems


	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
<div style="display: flex; align-items: center;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); font-weight: bold; color: red; margin-right: 10px;">Special Publication 800-60</div> <div> <p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]</p> </div> </div>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<div style="display: flex; align-items: center;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); font-weight: bold; color: red; margin-right: 10px;">Special Publication 800-60</div> <div> <p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]</p> </div> </div>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<div style="display: flex; align-items: center;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); font-weight: bold; color: red; margin-right: 10px;">Special Publication 800-60</div> <div> <p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]</p> </div> </div>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

24

 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Results


25

 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division


Security Categorization

- 24 Information Types from 800-60
 - No new Information types were created to accommodate CJI
- 16 information types identified as CJI
 - 7 Departures from the provisional impact levels
- 8 information types identified as NON-CJI

26


 U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

Moderate



N/A Item C.2.1.1 Corrective Action Information Type

MMM Item C.2.8.9 Personal Identity and Authentication Information

LML Item C.3.5.1 System Development

MML Item C.3.5.2 Lifecycle/Change Management

MMM Item C.3.5.3 System Maintenance

MMM Item C.3.5.4 IT Infrastructure Maintenance

LML Item C.3.5.5 Information Security

MML Item C.3.5.6 Record Retention

MML Item C.3.5.7 Information Management

MMM Item C.3.5.8 System and Network Monitoring

N/A Item C.3.5.9 Information Sharing

N/A Item D.4.2 Disaster Preparedness and Planning Data

N/A Item D.4.4 Emergency Response Data

LLM Item D.16.1 Criminal Apprehension

MMM Item D.16.2 Criminal Investigation and Surveillance

MMM Item D.16.3 Citizen Protection

MMM Item D.16.4 Leadership Protection

N/A Item D.16.5 Property Protection

MMM Item D.16.6 Substance Control

LLL Item D.16.7 Crime Prevention


MMM Item D.16.8 Trade Law Enforcement

N/A Item D.17.1 Judicial Hearings


N/A Item D.17.3 Legal Investigation

N/A Item D.22.4 Information Infrastructure Management

27


 U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

Questions



28



**SA Issue #3, cont.
Criminal Justice Data Categorization
SA Subcommittee Motion**

Options Considered:

- **Option 1:** Motion to accept the Data Categorization Task Force's recommendation for criminal justice information to be categorized as MODERATE for confidentiality, integrity, and availability.
- **Option 2:** Motion for criminal justice information to be categorized as a _____ impact for confidentiality, integrity, and availability.

The SA Subcommittee and all five Regional Working Groups chose Option 1.

29



**SA Issue #3, cont.
Criminal Justice Data Categorization
APB Recommendation**

Option 1:

Motion to accept the Data Categorization Task Force's recommendation for criminal justice information to be categorized as MODERATE for confidentiality, integrity, and availability.

30



SA Issue #5
Sunset Date for File Transfer Protocol (FTP)

This topic was addressed in the NCIC Subcommittee Report.



NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) SUBCOMMITTEE

Lynn Rolin
Chair

1



NICS ISSUE #1-3 INFORMATIONAL

Action Item Review

NICS Operational Update

NICS Enhancements Update

2



NICS ISSUE #4-6 INFORMATIONAL

Next Generation Identification System Purpose Code F Responses vs Purpose Code C Responses

Identification for Firearm Sales

Fiscal Year 2020 Audit Results Summary

UNCLASSIFIED

3

3



NICS ISSUE #7 VOTING

Additional Date of Birth (DOB) Requirements for NICS Indices Entry

Background

Current Requirements

Voting Recommendations

UNCLASSIFIED

4

4



Option 1: With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message.

Option 2: With this option, the NICS will be programmed to accept a partial DOB for a NICS Indices entry, only if an additional descriptor is included, e.g., SOC or MNU. If a contributor attempts to enter a partial DOB without an additional descriptor, they will receive a reject message.

UNCLASSIFIED

5

5



Option 3: No change, partial DOBs will continue to be accepted by the NICS.

Note: If Options 1 or 2 are approved, the NICS Section will complete the system enhancement. There should be no impact for the states, only awareness of the additional requirement. The system enhancement necessary to implement the change will be assigned a priority and categorized.

UNCLASSIFIED

6

6



Working Group recommendations:

Southern Working Group endorsed Option 2:

With this option, the NICS will be programmed to accept a partial DOB for a NICS Indices entry, only if an additional descriptor is included, e.g., SOC or MNU. If a contributor attempts to enter a partial DOB without an additional descriptor, they will receive a reject message. Priority 3M

UNCLASSIFIED

7

7



Working Group recommendations:

All other Working Groups endorsed Option 1:

With this option, the NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message.

UNCLASSIFIED

8

8



Additional DOB Requirements for NICS Indices Entry

Motion: To endorse option 1—The NICS will be programmed to no longer accept a partial DOB for a NICS Indices entry in any circumstance. A complete month, day, and year must be entered for individuals who are 120 years of age or younger. If a contributor attempts to enter a partial DOB, they will receive a reject message. The priority was set at 3M.

UNCLASSIFIED

9

9



NICS ISSUE #8-10 INFORMATIONAL

Creation of an Extreme Risk Protection Order (ERPO) File in the National Crime Information Center System

Posting Federal Dispositions to Multiple Dates of Arrest

NICS/The Bureau of Alcohol, Tobacco, Firearms and Explosives Denials

UNCLASSIFIED

10

10



NICS ISSUE #11 AD HOC

United States Postal Service Project Update

The NICS Section Biometric Initiative

NICS User Conference Update

UNCLASSIFIED

11

11




CONTACT INFORMATION

Lynn Rolin
Chair, NICS Subcommittee
South Carolina Law Enforcement Division
lrolin@sled.sc.gov
803-896-7162

UNCLASSIFIED

12

12

 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB Item #14

Chairperson's Report on the Public Safety Strategy (PSS) Subcommittee

Mr. Charles I. Schaeffer, Chairperson
June 9, 2021, CJIS APB Meeting
Orlando, Florida

1






Public Safety Strategy (PSS) Subcommittee

The objectives of the PSS Subcommittee are to:

- Provide guidance to the CJIS APB on topics which span across multiple systems and/or potentially influence the CJIS enterprise
- Proactively research, identify, and present findings on items for consideration to the CJIS APB using a future-oriented strategic approach
- Develop efforts to strengthen the CJIS APB's relationship, communication, and interaction with major law enforcement associations and organizations

PSS Subcommittee established 10/20/2020

2

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

PSS Issue #3

Strategy Discussion

To answer the questions,

- “Where do we want to take our information and data (CJIS Systems) in the next 2-5 years?”
- “How do we ensure our multifunction stakeholders know about all the varied systems and services available?”

3


3

- Provide guidance to the CJIS APB on topics which span across multiple systems and/or potentially influence the CJIS enterprise
- Proactively research, identify, and present findings on items for consideration to the CJIS APB using a future-oriented strategic approach
- Develop efforts to strengthen the CJIS APB's relationship, communication, and interaction with major law enforcement associations and organizations

Moving Forward . . .

- **CJIS Division Enterprise of Services**
 - 5-year plan for the advisory process
 - Capitalize on the agile process
- **User Community Education**
 - Market to the sheriff's office/police department level
 - Market to state level offices
 - CJIS Systems Officer education
 - Education opportunities and methods
- **Strategic vs. Reactive**

4


 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

PSS Issue #5 – Beyond 2021 Update –Addition of Geolocation to the National Incident-Based Reporting System (NIBRS)

Addressed in the UCR presentation

5

5






 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

PSS Issue #6 – Law Enforcement Suicide Data Collection Update

Accepted as Information Only

6

6

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #4






Recommendations for Changes to Sex Codes within UCR (fall 2020)

Purpose:

The purpose is to propose changes to sex codes in the UCR Program.

7

7

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #4


Recommendations for Changes to Sex Codes within UCR (fall 2020)

Available Options Considered:

Option 1: The FBI UCR Program should allow sex code selections of “M” for male, “F” for female, “X” for non-binary, or “U” for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual's presentation, including physical appearance, clothing choice, accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person's gender identity (APA 2008) (Western)

8

8



U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #4


Recommendations for Changes to Sex Codes within UCR (fall 2020)

Available Options Considered:

- **Option 2:** The FBI UCR Program should resolve sex and gender in two phases.
 - Phase 1: The FBI UCR Program should allow sex code selection of “M” for male, “F” for female, “X” for non-binary, or “U” for unknown/unspecified. These code selections are capturing gender expression. Gender expression is defined as an individual’s presentation, including physical appearance, clothing choice and accessories, and behavior that communicates aspects of gender or gender role. Gender expression may or may not conform to a person’s gender identity (APA 2008). Phase 1 may be immediately implemented.
 - Phase 2: The FBI UCR Program should implement a new data element for gender identity, in which man (code to be determined), woman (code to be determined), “X” for non-binary, transgender male (code to be determined), transgender female (code to be determined) or “U” for unknown/unspecified are allowed. Gender identity is defined as one’s sense of oneself as male, female, or transgender. Since gender identity is internal, a person’s gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts to the law enforcement community at one time due to the nation’s ongoing transition to NIBRS. (Southern)

9

9



U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #4


Recommendations for Changes to Sex Codes within UCR (fall 2020)

Available Options Considered:

- **Option 3:** The FBI UCR Program should allow sex code selection of “M” for male, “F” for female, “X” for non-binary, man (code to be determined), woman (code to be determined), transgender male (code to be determined), transgender female (code to be determined), or “U” for unknown/unspecified. These code selections capture gender expression and gender identity together. (Federal)
- **Option 4:** The FBI UCR Program should implement a third sex code category of “U” for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current Next Generation Identification (NGI) policy. (Northeastern, PSS, UCR)

10

10

 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

PSS Issue #4


Recommendations for Changes to Sex Codes within UCR (fall 2020)

Available Options Considered:

- **Option 5:** No change.
 - Recommended the UCR Subcommittee consider the addition of a new gender field to capture gender identity.
 - Recommended the UCR Subcommittee forward this to a task force to further research this topic; also recommended making the new gender field an optional field. (North Central)

11

11

 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

PSS Issue #4






Recommendations for Changes to Sex Codes within UCR (fall 2020)

Available Options Considered:

- **Option New:** Refer the topic to the PSS Subcommittee for further review.

12

12

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #4

Recommendations for Changes to Sex Codes within UCR (spring 2021)

PSS Subcommittee Motion:

New Option 6

The PSS Subcommittee moved to endorse New Option 6: The UCR Program should resolve sex and gender in two phases.






Phase 1: The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy.

Phase 2: The UCR Program should implement a new optional data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined), or U for unknown/unspecified are allowed. Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006).

Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts tot the law enforcement community at one time due to the nations ongoing transition to NIBRS. Priority 3M

13

13

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #4

Recommendations for Changes to Sex Codes within UCR (spring 2021)

Recommended APB Motion:






Endorse the PSS Subcommittee recommendation to endorse New Option 6: The UCR Program should resolve sex and gender in two phases.

Phase 1: The UCR Program should implement a third sex code category of U for unknown/unspecified, to be defined to include non-binary gender, for sex codes in order to be consistent with other CJIS systems. This solution aligns with the current NGI policy.

Phase 2: The UCR Program should implement a new optional data element for gender identity, in which man (code to be determined), woman (code to be determined), X for non-binary, transgender male (code to be determined), transgender female (code to be determined), or U for unknown/unspecified are allowed. Gender identity is defined as one's sense of oneself as male, female, or transgender. Since gender identity is internal, a person's gender identity is not necessarily visible to others (APA 2006). Phase 2 may be implemented after a given amount of time determined by the CJIS APB in an effort to avoid multiple system impacts tot the law enforcement community at one time due to the nations ongoing transition to NIBRS. Priority 3M

14

14

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #7






Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program (spring 2021)

Purpose:

The purpose is to propose for changes to the race code data element within the FBI UCR Program data collections to allow for multiple race code choices within race code data elements.

15

15

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #7





Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program (spring 2021)

Available Options Considered:

- **Option 1:** Change the NIBRS race category to allow for multiple selections for the arrestee, offender, and victim segments. (Federal, Southern)
- **Option 2:** No change. (North Central, Northeastern)
- **Option New:** Refer to the PSS Subcommittee for further exploration. No change until that is completed. (Western)

16

16

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #7

Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program (spring 2021)





UCR Subcommittee Motion:

New Option

The UCR Subcommittee moved to endorse New Option: No Change. Refer to the PSS Subcommittee for further exploration.

17

17

U.S. Department of Justice
 Federal Bureau of Investigation
 Science and Technology Branch
 Criminal Justice Information Services Division

PSS Issue #7

Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program (spring 2021)

PSS Subcommittee Motion:


Option 2

The PSS Subcommittee moved to endorse Option 2: No Change.

Action Item: CJIS to develop a strategic plan on how to reconcile race, sex, and gender codes across CJIS Systems with other relevant fields as practical and establish goals in harmonizing CJIS services when it comes to specific data elements.

18

18

 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

PSS Issue #7
Changes to Race Codes within the Federal Bureau of Investigation (FBI) Uniform Crime Reporting Program (UCR) Program (spring 2021)


Recommended APB Motion:

Endorse the PSS Subcommittee recommendation to endorse Option 2: No Change.

Action Item: CJIS to develop a strategic plan on how to reconcile race, sex, and gender codes across CJIS Systems with other relevant fields as practical and establish goals in harmonizing CJIS services when it comes to specific data elements.

19

19


 U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Thank you

Questions or Comments?

20

20




U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Tribal Task Force Update

William J. Denke, Task Force Chairperson

1



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division






Tribal Task Force

- William J. Denke, Chief of Police, Sycuan Tribal Police Department; Tribal Task Force Chair
- Scott Desjadon, Director, Yavapai Prescott Tribal Police Department
- Chris Sutter, Chief of Police, Tulalip Tribal Police Department
- Ronnie Gilmore, Chief of Police, Miami Nation Police Department

- Kathryn M. Monfreda, Chief, Alaska Department of Public Safety
- Brian Wallace, Chief Civil Deputy, Marion County Sheriffs Office (OR)
- Timothy L. Chung, Lieutenant Colonel, Arizona Department of Public Safety
- Vacancy (*Gene Thaxton retirement*)

- Jason O'Neal, Director, Bureau of Indian Affairs (BIA) Office of Justice Services
- Christopher B. Chaney, Senior Counsel, Department of Justice (DOJ) Office of Tribal Justice
- Jerry W. Grambow, Supervisory Special Agent, FBI Indian Country Special Jurisdiction Unit
- Trudy Lou Ford, Section Chief, FBI Global Law Enforcement Support Section (GLESS)

2












U.S. Department of Justice
 Federal Bureau of Investigation
Science and Technology Branch
 Criminal Justice Information Services Division

Fiscal Year (FY) 2020 Accomplishments

- National Incident-Based Reporting System reporting by tribal agencies
- DOJ Tribal Access Program
- 'Dear Tribal Leader' letter focused on Latent cascade of tribal submissions
- Criminal Justice Information Services (CJIS) Division tribal video


3


U.S. Department of Justice
 Federal Bureau of Investigation
Science and Technology Branch
 Criminal Justice Information Services Division

CJIS Division Advisory Process Tribal Representatives

<p><u>Advisory Policy Board</u> William J. Denke Sycuan Tribal Police Department El Cajon, CA</p>	<p><u>Southern Working Group</u> Ronnie Gilmore Miami Nation Police Department Miami, OK</p>
<p><u>Northeastern Working Group</u> Robert Bryant Penobscot Indian Nation Police Indian Nation, ME</p>	<p><u>Western Working Group</u> Scott Desjaddon Yavapai Prescott Tribal Police Department Prescott, AZ</p>
<p><u>North Central Working Group</u> Gary Gaikowski Sisseton Wahpeton Law Enforcement Agency Village, SD</p>	<p><u>Federal Working Group</u> Jason O'Neal BIA Washington, D.C.</p>



4




U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

FY 21 Focus

- Study of Tribal Access to CJIS Division Services
- Missing and murdered indigenous people issue
- CJIS tribal video release
- Virtual outreach to tribal partners

5



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Tribal Task Force Chair
William J. Denke
bdenke@sycuan-nsn.gov

CJIS Division Executive Management Tribal Liaison
GLESS
Trudy Lou Ford
tlford@fbi.gov

CJIS Division Tribal Liaison
Kristi A. Naternicola
kanaternicola@fbi.gov
cjistribaloutreach@fbi.gov

6

Intentionally Left Blank

CJIS APB Minutes - Acronyms Listing

AD	Assistant Director
ADD	Address Type
AKA	Alias
AOL	Arrest Offense Literal
APA	American Psychological Association
APB	Advisory Policy Board
ASAC	Assistant Special Agent in Charge
ASCLD	American Society of Crime Laboratory Directors
ASUCRP	Association of State Uniform Crime Reporting Programs
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BE	Bureau of Equality
BIA	Bureau of Indian Affairs
BRT	Business Relations Team
CDE	Crime Data Explorer
CE	Compliance Evaluation
CHRI	Criminal History Record Information
CIO	Chief Information Officer
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CMC	Caudtion and Medical Condition
CODIS	Combined DNA Index System
COL	Court Offense Literal
COU	County
COVID-19	Coronavirus
CPIC	Canadian Police Information Center
CSA	CJIS Systems Agency
CSO	CJIS Systems Officer
<i>CSP</i>	<i>CJIS Security Policy</i>
CTI	Court Identifier
CTY	City
CTZ	Citizen
DAD	Deputy Assistant Director
DBF	Date Body Found
DDA	Date of Documented Address
DENI	ATF's Denial Enforcement and NICS Intelligence
DFO	Designated Federal Officer
DHS	Department of Homeland Security
DLN	Driver's License Number
DNA	Deoxyribonucleic Acid
DNO	DNA Location
DOB	Date of Birth
DOD	Department of Defense

DOJ	Department of Justice
DRC	Delete Record Cycle
DSSU	Data Sharing Services Unit
DTE	Date of Entry
EAD	Executive Assistant Director
EBTS	Electronic Biometric Transmission Specifications
EDD	Estimated Date of Death
EFTS	Enterprise File Transfer
ENFSI	European Network on Forensic Science Institutes
ERPO	Extreme Risk Protection Order
ETN	Ethnicity
EYE	Eye Color
EXL	Extradition
EXP	Expiration
FACE	Facial Analysis, Comparison, and Evaluation
FBI	Federal Bureau of Investigation
FDLE	Florida Department of Law Enforcement
FO	Field Office
FPC	Fingerprint Classification
FTP	File Transfer Protocol
FY	Fiscal Year
GLESS	Global Law Enforcement Support Section
HDR	Header
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
ICAM	Identity Credential and Access Management
ICE	Immigration and Customs Enforcement
IdHS	Identity History Summary
IdHSR	Identity History Summary Request
IdHSRR	Identity History Summary Request Response
IEPD	Identification Exchange Package Documentation
IFFS	Identification for Firearm Sales
IFS	Interstate Photo System
IGG	Investigative Genetic Genealogy
IGTF	Interpretive Guidance Task Force
III	Interstate Identification Index
IRQ	Image/Feature Retrieval Request
IS	Identification Services
ISCG	Identification Services Coordination Group
ISD	Date of Issue
ISO	Information Security Officer
IT	Information Technology
ITMS	Information Technology Management Section
JTF	Joint Task Force on Rapsheet Standardization

JWIN	DOJ's Justice Criminal Interface to NCIC
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LEEU	Law Enforcement Engagement Unit
LEOKA	Law Enforcement Officers Killed or Assaulted
LESDC	Law Enforcement Suicide Data Collection
LGBTQ+	Lesbian, Gay, Bisexual, and Transgender Plus
LIC	License Plate Number
LinX	Law Enforcement Information Exchange
LIT	License Plate Type
LIY	License Plate Year of Expiration
LKA	Linking Case Number
LKI	Linking Agency Identifier
LMR	Land Mobile Radio
MATCH	Metro Atlanta Child Exploitation Task Force
MCC	Major Cities Chiefs
MCDV	Misdemeanor Crime of Domestic Violence
MOU	Memorandum of Understanding
MRC	Modify Record Cycle
MSG	Message
MTF	Modernization Task Force
NAM	Name
N3G	NCIC Third Generation
NCA	NIBRS Collection Application
NCIC	National Crime Information Center
N-DEx	National Data Exchange
NFF	National Fingerprint File
NGI	Next Generation Identification
NIBRS	National Incident-Based Reporting System
NICB	National Insurance Crime Bureau
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
Nlets	International Justice and Public Safety Network
NMVTIS	National Motor Vehicle Title Information System
NOA	Notify Originating Agency
NOEXL	No Extradition
NOPU	NCIC Operations and Policy Unit
NSA	National Sheriffs' Association
NSO	Non-serious Offense
NSOR	National Sex Offender Registry
NTOC	National Threat Operations Center
NTOS	National Threat Operation Section
NVS	National Vehicle Service
OCA	Originating Agency Case Number

OGC	Office of General Counsel
OLN	Operator's License Number
OLS	Operator's License State
OLY	Operator's License Year of Expiration
OMB	Office of Management and Budget
OPB	Operational Programs Branch
ORI	Originating Agency Identifier
ORN	Order Number
PCA	Prohibiting Code
PET	Petitioner
PLAN	Predictable Learning Automation of the NICS
PO	Planning and Outreach
POB	Place of Birth
POC	Point of Contact
PPB	Protected Person Date of Birth
PRSU	Programs Research and Standards Unit
PSS	Public Safety Strategy
RAC	Race
RCMP	Royal Canadian Mounted Police
R-DNA	Rapid Deoxyribonucleic Acid
RTV	Relationship to Victim
SA	Security and Access and/or Special Agent
SAC	Special Agent in Charge
SC	Section Chief
SEX	Sex
SID	State Identification Number
SKN	Skin Tone
SMT	Scars, Marks, Tattoos, and Other Characteristics
SOC	Social Security Number
SNA	Street Name
SNU	Street Number
SPC	Special Processing Code
SRS	Summary Reporting System
SSA	Supervisory Special Agent
STA	State Identification Number
STB	Science and Technology Branch
SVC	Service Information
SVD	Service Date
SWGDM	Scientific Working Group on DNA Analysis Methods
TEDAC	Terrorist Explosive Devise Analytic Center
THC	Tetrahydrocannabinol
TSA	Transportation Security Administration
TXDPS	Texas Department of Public Safety
UCN	Universal Control Number

UCR	Uniform Crime Reporting
VIN	Vehicle Identification Number
VCO	Vehicle Color
VMA	Vehicle Make
VMO	Vehicle Model
VST	Vehicle Style
VYR	Vehicle Year
WGT	Weight
XML	Extensible Markup Language
ZIP	Zip Code

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS**

INFORMATION ONLY AGENDA

Informational Topic A

Rapid Deoxyribonucleic Acid (Rapid-DNA) Update

Informational Topic B

Next Generation Identification (NGI) System Purpose Code F Responses vs Purpose Code C Responses

Informational Topic C

National Palm Print System (NPPS) Status

Informational Topic D

NGI Iris Service Update

Informational Topic E

Update on the FBI's Manual Fingerprint and Name Check Services

Informational Topic F

Criminal History Update

Informational Topic G

Identification for Firearm Sales

Informational Topic H

The NGI System Interstate Photo System (IPS) Update and IPS Policy and Implementation Guide Revisions

Informational Topic I

Biometric Interoperability Update

Informational Topic J

Summary of the Results from the December 2020 CJIS APB Meeting

Informational Topic K

Fiscal Year 2020 Audit Results Summary

Informational Topic L

Beyond 2021 Initiative Update

Informational Topic M

National Data Exchange (N-DEx) Program Update

Informational Topic N

National Crime Information Center (NCIC) Enterprise File Transfer Service (EFTS) Migration Update

Informational Topic O

CJIS Division NCIC Status

Informational Topic P

Programs Research and Standards Unit (PRSU) Update on Contactless Fingerprint Collection Studies

Informational Topic Q

FBI PRSU Update

Informational Topic R

National Instant Criminal Background Check System (NICS) Operational Update

Informational Topic S

NICS Enhancements Status

Informational Topic T

Uniform Crime Reporting (UCR) Program Status Update

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC A

Rapid Deoxyribonucleic Acid (Rapid DNA) Update

PURPOSE

To provide an update on the FBI Booking Station Rapid DNA Initiative

AUTHOR

FBI Laboratory (Lab) Division
FBI Criminal Justice Information Services (CJIS) Division

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

With the completion of Rapid DNA Pilots on February 29, 2020, the FBI incorporated lessons learned during the pilots into final drafts of the Booking Standards and Booking Procedures as required by the Rapid DNA Act of 2017.

Rapid DNA Pilots

A complete summary of the Rapid DNA Pilots is available in the fall 2020 topic paper. Tests of the Rapid DNA Hit Notification process between CODIS and the CJIS Message Manager (CMM) were completed in July and August 2020 with the Washington Field Office. These checks tested the automated mechanism (to trigger the notification to law enforcement agencies) when there is a DNA match with Rapid DNA arrestee hits in CODIS. The follow-on messaging from the CMM via the International Justice and Public Safety Network known as “Nlets” is necessary to generate an Unsolicited DNA Notification message that is immediately sent to the investigating agency, the booking agency, and the arresting agency (if different from the booking

agency). Additional state/local tests will be conducted as a state applies for the Authority to Operate Rapid DNA in the booking environment within their state.

National Booking Standards and Booking Procedures:

The Scientific Working Group on DNA Analysis Methods (SWGDM), the FBI Director's advisory body for recommending DNA quality standards, approved the *Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies* during their July 2020 meeting. This major accomplishment was only possible due to the collaboration with state and local law enforcement partners during the Rapid DNA Booking Station Pilot in January and February 2020. The successful Pilot activities in Arizona, Florida, Louisiana, Texas and the FBI provided key insight by incorporating important lessons learned into the proposed Standards.

The National DNA Index System (NDIS) Procedures Board approved the *National Rapid DNA Booking Operational Procedures Manual* during their July 2020 meeting. The Rapid DNA Act of 2017 requires the FBI to issue Standards and Procedures to allow Rapid DNA technology outside of the accredited forensic DNA laboratory. These two approvals are significant milestones toward the implementation Rapid DNA in the booking environment, allowing near real-time identification of perpetrators of unsolved crimes during the arrestee booking process.

The FBI Laboratory Director approved the Booking Standards and Booking Procedures on August 18, 2020 and both documents were posted on FBI.gov (see links below) on August 20, 2020 with effective dates of September 1, 2020.

<https://www.fbi.gov/file-repository/standards-for-operation-of-rapid-dna-booking-systems-by-law-enforcement-booking-agencies-eff-090120.pdf/view>

<https://www.fbi.gov/file-repository/national-rapid-dna-booking-operational-procedures-manual-eff-090120.pdf/view>

Rapid DNA Use for Crime Scene Investigations

There are many challenges that must be overcome before the FBI can consider the use of Rapid DNA systems for crime scene sample analysis. The Bureau continues to assess how these challenges can be addressed to include monitoring enhancements to Rapid DNA technology. Among the major challenges is the requirement to determine the amount of DNA present in a sample (necessary to maximize the resulting quality of the DNA profile, assess for contamination, etc.) and the development of expert systems for crime scene sample data analysis. Crime scene DNA samples are frequently degraded, contain mixtures and result in incomplete (partial) DNA profiles that require experienced DNA Casework Examiner data interpretation.

The FBI DNA Crime Scene Task Group, created in 2018, and coordinated by the FBI Laboratory, is investigating the potential use of Rapid DNA technology for the analysis of crime scene evidence samples. This Task Group was separated into two sub-groups: the Non-CODIS

Rapid DNA Best Practices/Outreach and Courtroom Considerations Sub-Group (Non-CODIS Best Practices Group); and, the Rapid DNA Crime Scene Technology Advancement Sub-Group (Technology Advancement Group). Both groups are comprised of individuals from law enforcement, District Attorney's Association, Major Cities Chiefs Association, DNA experts from NDIS participating laboratories, and DNA experts from non-NDIS participating operations.

The primary objective of the Non-CODIS Best Practices Sub-Group is to provide a recognized and singular voice to proactively share best practices for non-CODIS Rapid DNA use with the law enforcement community; as well as to identify, address, and mitigate obstacles to admitting Rapid DNA into a courtroom. This will allow for law enforcement agencies to strategically implement Rapid DNA at crime scenes in an informed and responsible manner, while preventing issues that would damage Rapid DNA reputation. The Non-CODIS Best Practices Group meets monthly and has published 2 guidance documents on FBI.gov, "Non-CODIS Rapid DNA Considerations and Best Practices for Law Enforcement Use" published in September 2019 and "Rapid DNA Testing for Non-CODIS Uses: Considerations for Court" published in August 2020 (see links below).

<https://www.fbi.gov/file-repository/non-codis-rapid-dna-best-practices-092419.pdf/view>

<https://www.fbi.gov/file-repository/rapid-dna-testing-for-non-codis-uses-considerations-for-court-073120.pdf/view>

The primary objective of the Technology Advancement Group is to drive and continuously monitor the maturity of Rapid DNA technology in order to ensure its reliable, responsible and expeditious appropriate implementation for crime scene DNA analyses. The Technology Advancement Group meets monthly to discuss the current state of Rapid DNA through member's own research experiences and the literature. The Technology Advancement Group published a joint position statement with the Scientific Working Group on DNA Analysis Methods (SWGDM) and the European Network of Forensic Science Institutes DNA Working Group (ENFSI) regarding the use of Rapid DNA Technology on forensic evidence for State and National DNA databases in July 2020. The article was published in the reputable scientific journal, *Forensic Science International – Genetics*, entitled *Rapid DNA for crime scene use: Enhancements and data needed to consider use on forensic evidence for State and National DNA Databasing - An agreed position statement by ENFSI, SWGDAM and the Rapid DNA Crime Scene Technology Advancement Task Group*. The Article identified 5 major areas that must be addressed before Rapid DNA instruments can be tested and considered for the analysis of forensic evidence for State and National databasing purposes.

Due to the possible use of Rapid DNA technology for crime scene analysis in the future, the FBI plans to reconstitute the current CJIS APB Rapid DNA Task Force in Fiscal Year (FY) 2021, to include individuals involved in non-CODIS Rapid DNA applications as well as additional accredited laboratory personnel. The goal for an initial web-based meeting is targeted for spring/summer 2021.

Federal DNA Capabilities for Rapid DNA Participation

The FBI's DNA Indicator (Offender DNA Profile in CODIS) capability is available via the Next Generation Identification (NGI) system and is maintained by the Lab Division's Federal DNA Database Unit (FDDU) for limited Federal law enforcement agencies submitting biometric-based booking transactions through the DOJ's Joint Agency Booking System (JABS) and through the Department of Homeland Security's Automated Biometric Identification System (IDENT). Future plans to include all remaining Federal law enforcement will be coordinated with the appropriate Federal SDIS Labs.

Beyond the indicator, the FDDU has continued to work with JABS and the CJIS Division to identify improvements and make system enhancements to the Federal DNA Collection workflow. These enhancements are being implemented in two phases and aim to reduce the number of redundant DNA samples collected and to eliminate the manual collection of biographical data and inked fingerprints at the time of booking. The first phase was deployed to all FBI Field Offices in October 2017 and provided a ".pdf" file of the arrestee's booking record that could be printed directly onto the FD-936 (Request for National DNA Database Entry) form.

The second phase of enhancements includes the new 'Capture DNA Device' page in the Universal Automated Booking System (UABS). The new printable, FD-936 is auto-populated using information from both the booking record and the NGI response, and it is returned to the booking agency only when a DNA profile does not already exist in the NDIS for the subject. The capture of the DNA device barcode and its inclusion as part of the booking package, now tightly links the DNA sample and the NGI fingerprint transaction, allowing for the elimination of the inked fingerprints on the FD-936 form. These enhancements to streamline the Federal DNA collection process are expected to significantly reduce the time and effort spent by law enforcement on DNA collection during the booking process. Pilots for the second phase enhancements concluded in FY2020. All FBI Field Offices are currently able to access the latest version of UABS and distribution to ATF and DEA is expected to occur in FY2021.

Finally, the FBI Lab has also identified resources to develop a Rapid DNA module within the JABS-based workflow that will assist in generating the Arrestee Enrollment Format message and provide a seamless user interface during booking. The development with JABS started at the end of FY2020 and is expected to continue well into FY 2021.

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC B

Next Generation Identification System Purpose Code F Responses vs Purpose Code C Responses

PURPOSE

To provide an explanation of Purpose Codes F and C and how responses could differ with the use of each.

AUTHOR

Biometric Services Section, Criminal History Information and Policy Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. The FBI's Criminal Justice Information Services (CJIS) Division will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

The Interstate Identification Index (III) facilitates the cooperative federal-state exchange of criminal history records (CHRs) and functions as an integral part of the FBI's Next Generation Identification (NGI) System. The III provides a means for authorized criminal or noncriminal justice agencies to conduct national record searches for criminal justice and other purposes as specified by existing federal and/or state laws. A name-based search of the III will reveal if a matching record is contained in the index and will return the FBI Universal Control number (UCN) and/or State Identification (SID) number in the response, if applicable. A copy of a subject's record can be obtained through an additional search utilizing the FBI UCN or SID. As each state joins the III, they must agree to provide their CHRs for, at minimum, firearms-related purposes using the Purpose Code F and criminal justice purposes using the Purpose Code C. There is an additional requirement for states participating in the National Fingerprint File Program to provide records for all purpose codes.

Purpose Codes

A Purpose Code is a required data element used to create an audit trail of each CHR disclosure. There are eleven different purpose codes used to access the III, each with their own requirements and authorities. For the scope of this paper, the focus is solely on the Purpose Codes F and C.

The Purpose Code F is used by criminal justice agencies when issuing firearm-related permits and explosive permits pursuant to state law, regulation, or local ordinance; to return firearms to lawful owners; and to determine if prospective transferees are prohibited from possessing or receiving firearms. pursuant to federal or state laws.

The Purpose Code C is used by criminal justice agencies for official duties in connection with the administration of criminal justice, which is defined in Title 28, *Code of Federal Regulations*, Section 20.3(b). The Purpose Code C is also authorized for use in limited situations by criminal justice agencies when criminal history record checks are necessary to accomplish an agency's mission (e.g., site security).

Although all III participating states are required to provide their criminal history in response to Purpose Code F and C inquiries, responses may differ between the two. State contributors may seal an arrest cycle or the entire state CHR for firearms-related background checks in accordance with state law. If a state's law prohibits sharing sealed records for non-criminal justice inquiries, the sealed information would not be shared in response to the Purpose Code F inquiry. In contrast, a query for the same individual, using a Purpose Code C, would return the sealed arrest details within the record. It is important to remember that Purpose Codes F and C cannot be used interchangeably, and usage is subject to audit. Additional information, such as Identification for Firearms Sales (IFFS) flags, can be available for Purpose Code F requests while not for C.

Impact of Sealing on Record Requests

Sealing functionality is available to federal contributors and III participating states with statutory authority or requirement to seal CHRs for various purposes in accordance with the law. Dissemination of sealed record information is designated by specific purpose codes. As states elect to use the sealing functionality, they must first establish their sealing rules, or the purpose codes for which they will share sealed records. All records, regardless of sealing, are shared for Purpose Code C. Although not a requirement, states are highly encouraged to provide their sealed information for Purpose Code F requests as well.

Currently federal contributors and ten states participate in sealing functionality. Of the participating states, four seal their CHRs for firearms-related background checks. For more information on sealing functionality, please contact the CJIS Division via e-mail at fbi-iii@fbi.gov. The following examples illustrate how different sealing preferences can affect responses to inquiries of the III and NGI System:

An authorized III user requests a record using Purpose Code F as part of a firearms-related background check. The user supplies an FBI UCN in the request but receives a notification that no active record exists for that subject. The record contains sealed criminal history record information (CHRI) for a single state which has agreed to share their sealed information for Purpose Codes A,C,J, and S. This particular state does not share sealed CHRI for Purpose Code F requests.

In contrast, an authorized III user requests a record using Purpose Code F as part of a firearms-related background check. The user supplies an FBI UCN and receives the CHR, including sealed information. In this situation, the record contains sealed information from a state that has agreed to share their sealed CHRI for Purpose Codes C, F, J, and S.

In a third example, an authorized III user requests a record using Purpose Code C as part of an investigation. The user supplies an active SID and receives the CHR, including sealed information. In this situation, the user receives a complete record as all sealing participating states are obligated to respond for Purpose Code C inquiries.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC C

National Palm Print System Status

PURPOSE

To provide an update on the status of the National Palm Print System.

AUTHOR

Biometric Services Section, Biometric Identification and Analysis Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via email at agmu@leo.gov. Submit feedback via the feedback form provided. The Criminal Justice Information Services Division will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

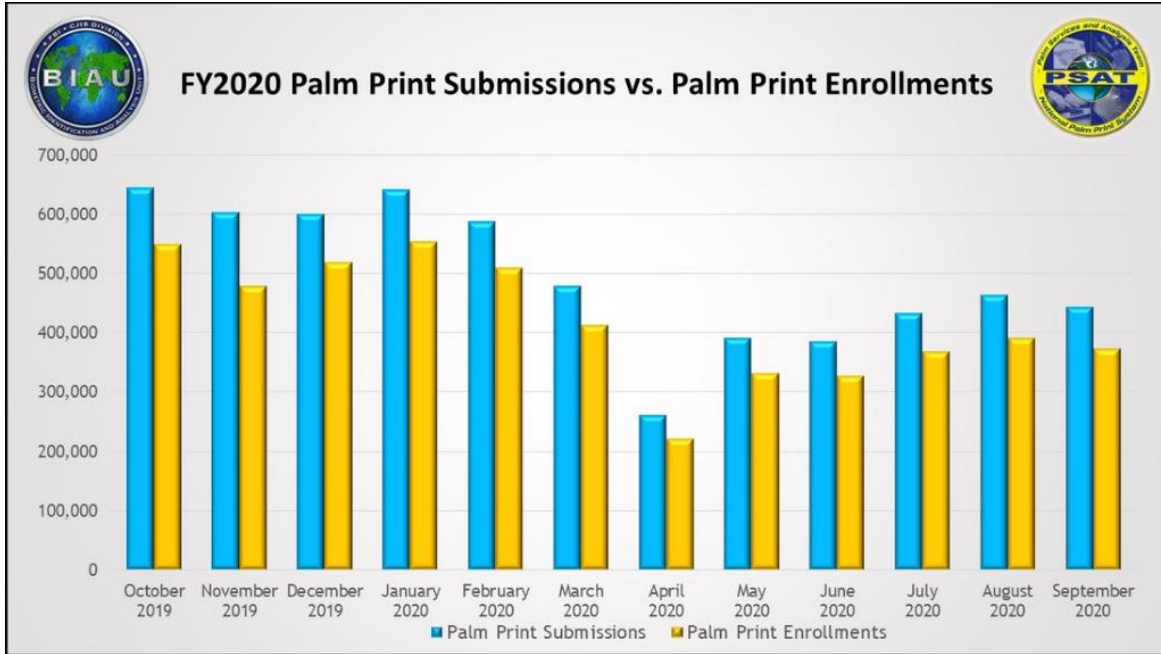
Implemented on 05/05/2013, the Next Generation Identification (NGI) System's National Palm Print System (NPPS) provides an investigative biometric service that has dramatically improved law enforcement's access to palm prints. Previously, palm prints were stored in the databases of federal, state, local, and tribal law enforcement agencies. The NPPS is now a central repository responsible for maintaining known palm prints derived from criminal arrests, civil applications, and national security submissions from a variety of authorized sources nationwide.

Agencies in 48 states, Washington, D.C., and the territories of Guam and Puerto Rico contribute palm prints to the NPPS. Identifications from these submissions have provided numerous successes to our law enforcement partners.

Palm Print Enrollments

In May 2020, the NPPS celebrated its seven-year anniversary and achieved a milestone of 20 million unique palm prints collected. As of the end of fiscal year (FY) 2020, the NPPS contained 20.6 million unique subjects derived from more than 44.1 million events that are available for nationwide investigative leads.

The following chart represents palm print submissions and enrollments for FY2020.

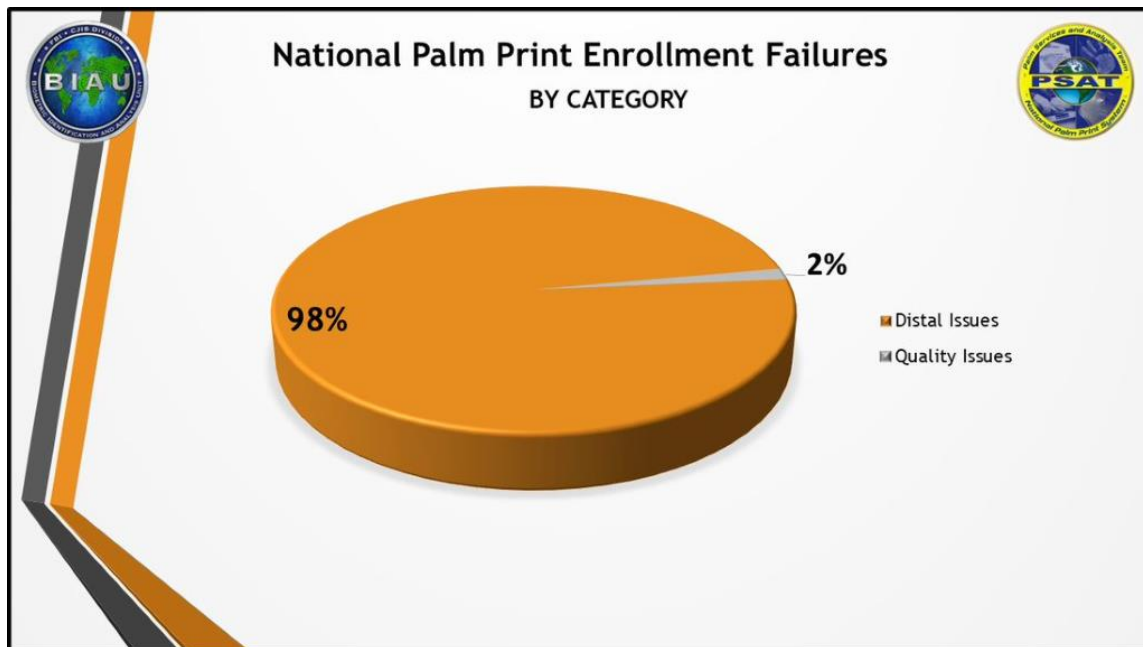


National Enrollment Review

As depicted in the chart above, the NPPS receives numerous palm print submissions that fail to enroll into the system. To assess the issues contributing to these non-enrollments, the FBI's Criminal Justice Information Services (CJIS) Division Palm Services and Analysis Team (PSAT) staff recently conducted an extensive review and analysis of nationwide palm print submissions from all partner agencies submitting to the NGI System. A sample of 7,016 palm print submissions that failed enrollment into the NPPS was selected from the first month of FY2021 and manually reviewed by the PSAT staff. The manual review was based upon the standards defined in the *Electronic Biometric Transmission Specification (EBTS)* and best practices outlined in a document entitled *A Practical Guide for Palm Print Capture*.

The results of this review revealed 100 percent of the analyzed palm prints failed to meet these guidelines/practices for submitting palm prints for various reasons, which can be grouped into two main categories: Distal Issues and Quality Issues.

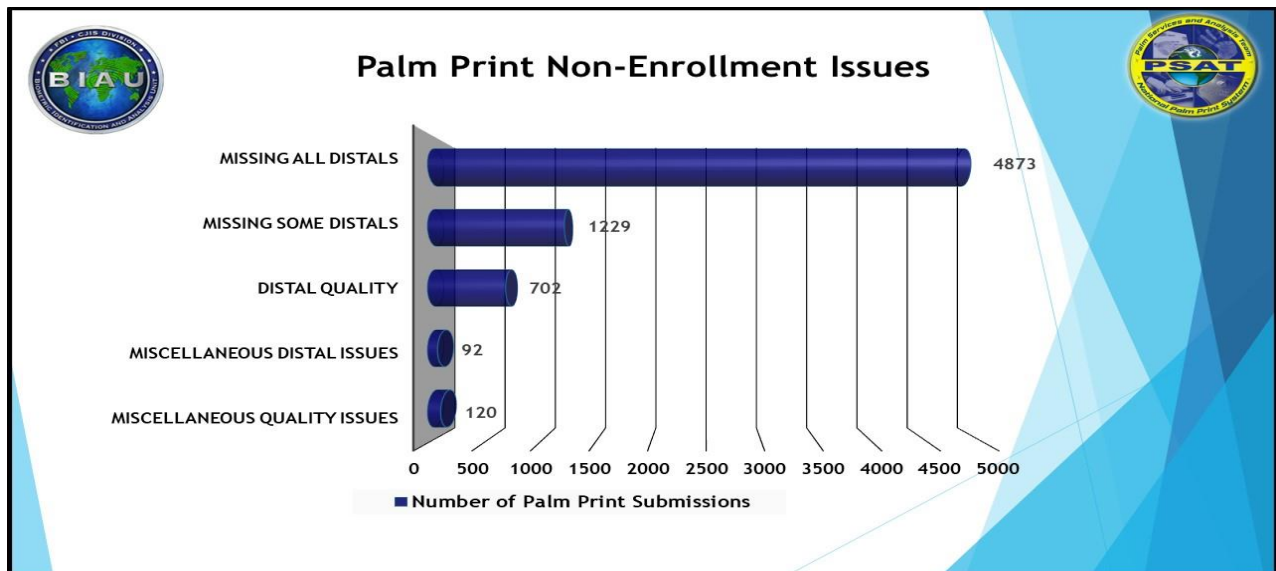
The following graph represents palm print submission issues by category identified as a result of the review.



The overwhelming issue for enrollment failures was attributed to distal issues as depicted in the chart above. Palm print submissions lacking some or all distals (i.e. top joint to include the fingerprint area) in the upper palm print or full palm print area do not meet EBTS guidelines for a palm print submission and frequently cannot be validated. The NGI System’s segmentation software used by the NPPS requires one print from each hand to perform system validation. If fingerprints are missing or lack the quality to determine the segmentation point, the software may use various portions of the palm print (e.g., medial, proximal point) for segmentation. Therefore, a seemingly good print that contains several distal images may not pass system segmentation/validation and will not enroll.

The remaining one percent of issues identified during the review were related to overall quality of palm print submissions. These issues consisted primarily of submissions containing dark spots on fingers, images submitted with obvious residue on the capture platen, and images cut off during capture. Poor quality submissions routinely reveal a need for training at the location of capture.

The following chart represents a detailed breakdown of palm print non-enrollment issues identified as a result of the review.



The most significant palm print non-enrollment issue identified during the review was records “Missing All Distals.” A common reason for this issue is lack of training for those who capture palm prints during the booking process. In addition, in some cases, agencies do not possess the appropriate equipment to capture palm prints correctly.

State Enrollment Reviews

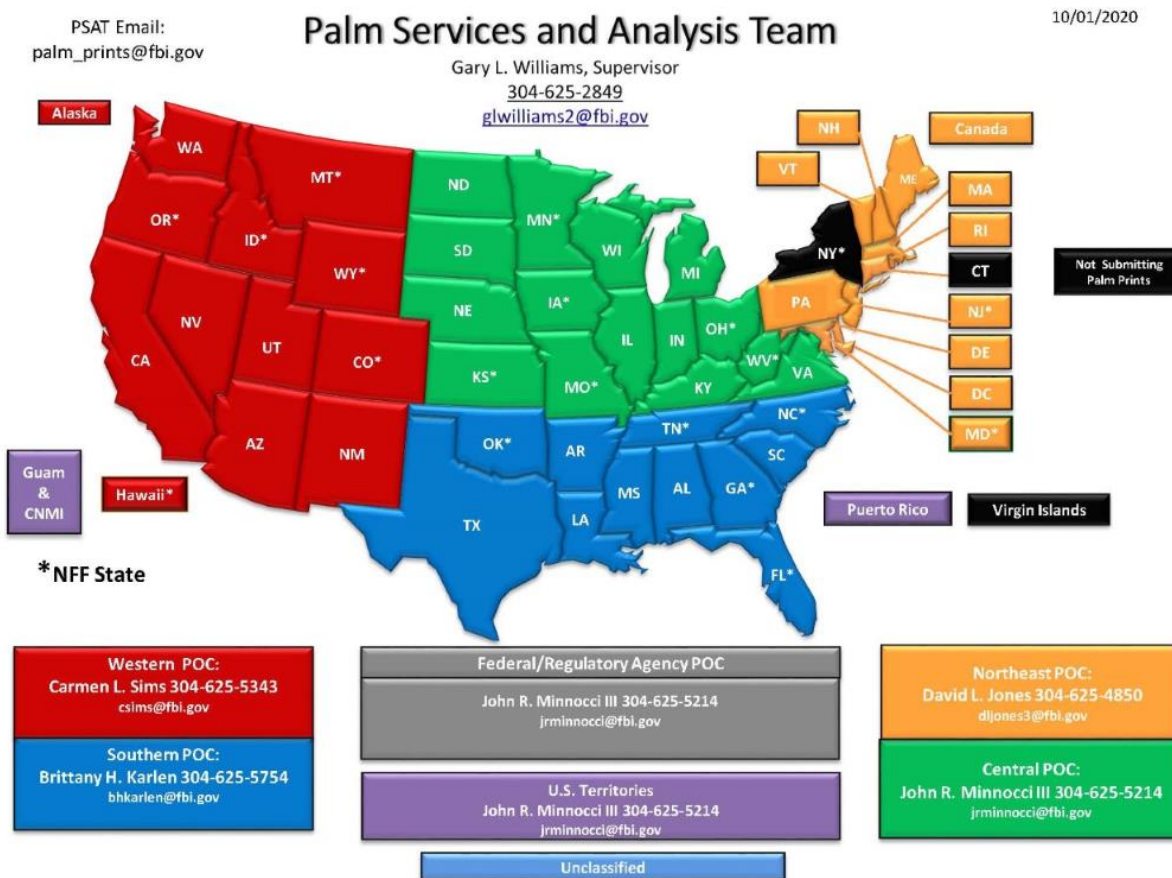
To support the integrity of the NPPS, the PSAT extensively reviews palm prints submitted by authorized agencies within each state. Analysis of daily enrollments and non-enrollments has allowed agencies to take corrective measures within their vendor systems, capture equipment, and trained personnel. This initiative enhances the quality of the national repository and provides a reliable investigative resource for law enforcement agencies. During FY2020, the PSAT conducted reviews on 14 state agencies, manually examining more than 5,600 palm print non-enrollments. These efforts help to identify data quality issues and increase the palm print enrollment rate into the NPPS from 54 percent in 2013 to 84 percent in 2020. The PSAT continues to conduct structured reviews of palm print enrollments and provides feedback to submitting agencies as needed. CJIS Systems Agencies or Federal Service Coordinators can request a review to be conducted of their specific palm print enrollments by submitting an email to palm_prints@fbi.gov.

Outreach

The PSAT staff manage the research, analysis, enhancement, and development of the NPPS. To build the repository, the PSAT staff collaborate with law enforcement agencies to collect data maintained at the state level. Intensive palm print reviews and feedback support the integrity of the repository, enhance the quality, and increase the enrollment rate of customer submissions. In addition, the PSAT staff receive requests daily from various partner law enforcement agencies

across the nation to provide palm print images to support criminal investigations. The PSAT staff provided responses to more than 1,194 such palm print requests in FY2020.

To enhance outreach by using current resources, the PSAT restructured the assignment of regional representatives. The image below depicts the six assigned regions with contact information for each PSAT point of contact (POC).



To support partner agencies and ensure the NPPS has a gallery of high-quality known palm prints, the PSAT has posted documentation to enhance user understanding of the palm anatomy and to provide a practical look at best practices for their capture at www.fbibiospecs.cjis.gov and www.fbi.gov/services/cjis/fingerprints-and-other-biometrics. These tools will help agencies increase accuracy in capturing palm print images. In addition, a link to an eLearning module is available on the fbi.gov webpage.

The NPPS continues to expand and serve as a reliable investigative resource for our law enforcement partner agencies. As the NPPS repository continues to grow, the utility of this system to the criminal justice community will also increase. For more information relating to the NPPS, please email palm_prints@fbi.gov.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC D

Next Generation Identification Iris Service Update

PURPOSE

The information outlined in this paper provides an update of the Next Generation Identification Iris Service.

AUTHOR

Biometric Services Section, Biometric Identification and Analysis Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. The Criminal Justice Information Services Division will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

The Next Generation Identification (NGI) Iris Service has proven, in a limited setting, to have the potential to become a powerful identification tool for federal, state, local and tribal law enforcement and criminal justice partners. The NGI Iris Service includes a national iris image repository and an Iris Image Identification Search (IIDS) capability. The iris biometric offers a highly accurate, contactless, and rapid identification option for criminal justice agencies. The iris contains a unique pattern of ridges and folds that are specific to an individual. Standard iris cameras use a near-infrared light to capture a more useful iris image across a broad range of actual iris colors. Typical iris image collection locations tether an iris camera to a booking station with fingerprint, palm print, and face photo image collection capabilities.

Active participants in the NGI Iris Service include:

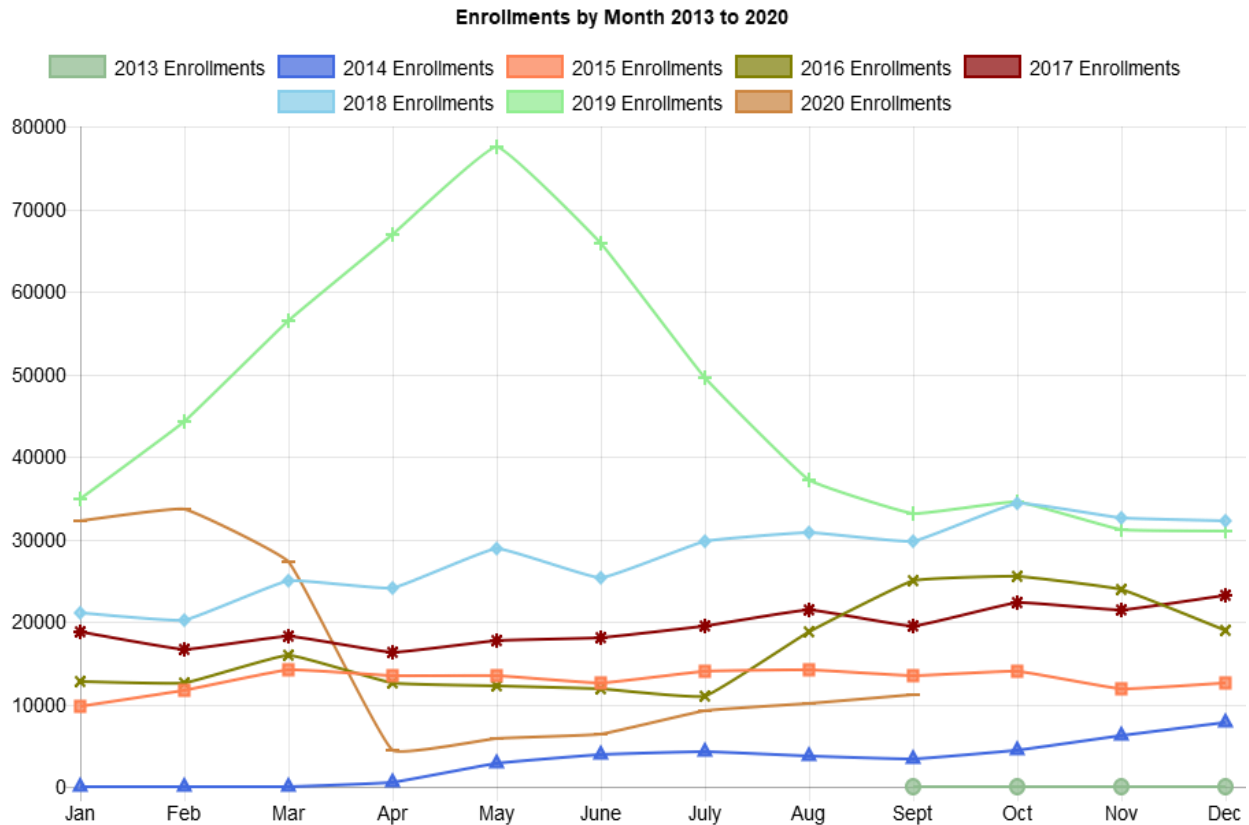
- Department of Homeland Security (DHS), Office of Biometric Identity Management
- DHS Customs and Border Protection
- DHS Immigration and Customs Enforcement
- Department of Justice Joint Automated Booking System

- California Department of Justice
- Long Beach Police Department, California
- Los Angeles County Sheriff's Department, California
- Riverside County Sheriff's Department, California
- San Bernardino County Sheriff's Department, California
- Texas Department of Public Safety
- Texas Department of Criminal Justice

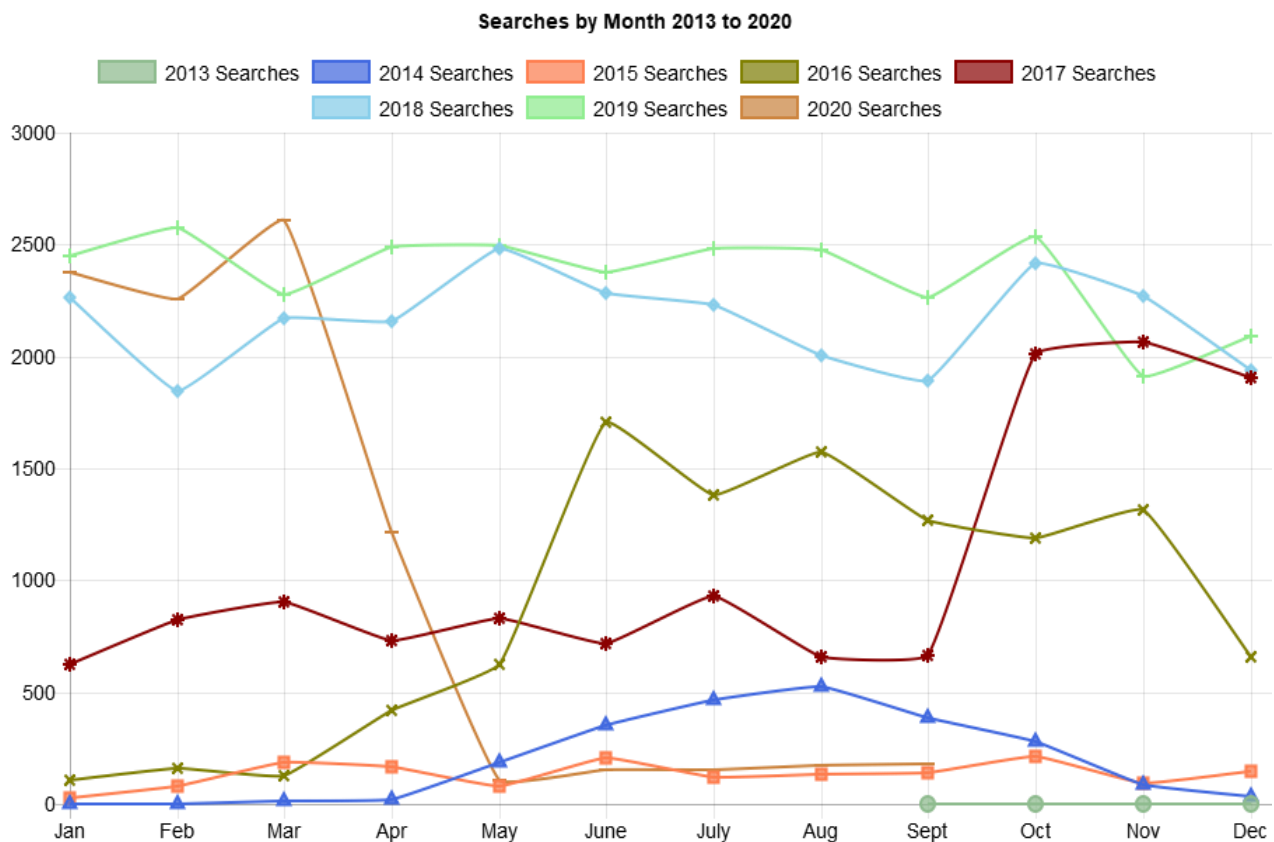
The NGI Iris Service became fully operational on 09/29/2020, following a multi-year Iris Pilot.

The NGI Iris Service repository contains [NUMBER] enrollments, which represents [NUMBER] unique identities, as of [xx/xx/xxxx]. All iris images submitted for enrollment in the repository must be associated with tenprint fingerprints and must be collected pursuant to an arrest, subsequent criminal proceeding, incarceration, or post-trial release. The iris images, obtained during criminal bookings, incarceration, or other criminal justice proceedings, are submitted from federal, state, and local partners.

The chart, on the following page, depicts monthly enrollment comparisons across the Iris Pilot years, 2013-2020. Numbers do not include bulk enrollments or expunged records.



The NGI Iris Service also features an IIDS capability, to provide identification validation. The iris biometric is particularly useful in high-volume environments where identification validation is critical in maintaining the safety and security for the agency professional by using a contactless biometric method. Today, the Texas Department of Criminal Justice is the sole user of the IIDS. The following scenario provides an example of the use case: Staff at a correctional facility use the NGI Iris Service to enroll inmates during the intake process. Upon movement or release, staff conducts an IIDS to ensure the inmate is the same individual. The IIDS provides a method of identifying a subject via a one-to-many, “lights-out” (without human intervention) search. The optimal submitted search transaction includes two iris probe images (right iris/left iris) captured by a near-infrared iris camera in a controlled setting. The submitted probe images are then searched against all iris images in the NGI Iris Service repository. Searching every iris image in the repository is very timely with a return response, either an identification or non-identification. The NGI System requirement for the IIDS response is fifteen minutes, however, the average response times are much shorter. An identification response returns the biographic data, the unique identifier associated with the individual, limited National Crime Information Center (NCIC) data, and an optional mug shot. The chart on the follow page depicts monthly search comparisons across the Iris Pilot years 2013–2020.



The following tables provide a snapshot of the Iris Pilot enrollments and searches from 2013-2020.

Type	Success	Error	Total	Average Time*
Enrollments	1,852,489	84,923	1,937,412	0.9 seconds
Searches	90,895	226	91,121	2.0 seconds

*Response times are measured from the time the Iris Pilot receives a submission to the time that a response leaves the Iris Pilot.

During the NGI Iris Pilot, when an iris search transaction resulted in an identification response, the NGI System initiated an automated query of the NCIC repository. The query utilized the FBI Universal Control Number (UCN) to obtain additional biographic and law enforcement information related to the subject. Results included a list of identifiers and case numbers for several NCIC Persons Files: Supervised Release, Protection Order, Identity Theft, Missing Person, Violent Person, Gang and Known or Suspected Terrorist, Wanted Person, National Sex Offender Registry, and Immigration Violators, that contained the identity. In conjunction with the NCIC Hit based on the iris search transaction, an unsolicited message was sent to the NCIC record owner.

Iris Search Transaction Matches to UCN

Searches	Count	Percent
Match	85,819	94.2%
Nonmatch	5,076	5.6%

Iris Search Transaction Matches (hits) to NCIC records

Matches	Count	Percent
w/NCIC Hit(s)	14,320	16.7%
w/NCIC Want(s)	4,329	5.0%

This process remains in place today; however, an NCIC Number (NIC Number) is utilized instead of the FBI UCN and only the NCIC Wanted Person, National Sex Offender Registry, and Immigration Violators Files are queried.

NGI Iris Service Policy and Implementation Guide

. An electronic copy of the *NGI Iris Service P&I Guide* is available by contacting the Iris Service Business Line at 304-625-IRIS (4747) or via e-mail iris@fbi.gov. The Guide describes policy and technical requirements for authorized law enforcement criminal justice agency users. It also defines the types of NGI Iris Service enrollments and search transactions that are accepted, the responses returned, and references to additional technical resources.

A key component of the *NGI Iris Service P&I Guide* is Appendix C: *Guide to Capturing Iris Images* (included as an attachment to this paper.) The poster, developed by the National Institute

of Standards and Technology, provides guidance on best practices for capturing iris images and educates the operator on how to navigate improper or incorrect scenarios that could result in submission errors.

NGI Iris Service Outreach Efforts

The FBI plans to concentrate on efforts to educate and encourage federal, state, local, and tribal partners to enroll iris images to expand the national repository. There are three methods to submit iris images to the FBI:

- A regular tenprint criminal identification booking transaction
Criminal Answer Required, Criminal No Answer, Criminal Print Direct Route, or, Criminal Fingerprint Card Process Non-Urgent
- Add to an existing identity by providing the FBI UCN and Date Printed in a Biometric Image Submission transaction
- Submit existing iris records in bulk offline

Federal, state, local, and tribal agencies interested in accessing the NGI Iris Service or seeking additional information may call the NGI Iris Service business line at (304) 625-IRIS (4747). Questions may also be submitted via e-mail to iris@fbi.gov.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC E

Update on the FBI's Manual Fingerprint and Name Check Services

PURPOSE

This informational topic paper will provide an update on the FBI's manual fingerprint and name check services.

AUTHOR

Biometric Services Section, Biometric Identification and Analysis Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

The FBI's Criminal Justice Information Services Division Next Generation Identification (NGI) System is the world's largest and most efficient electronic repository of biometric and criminal history information. As the manager of the FBI's fingerprint services, the Biometric Services Section's Biometric Identification and Analysis Unit (BIAU) interfaces with its federal, state, local, tribal, and international partners, providing NGI System support to help ensure complete and accurate criminal history responses.

The BIAU's most critical function is to perform biometric comparisons and other biometric processes in cases where submissions are unable to process in a fully automated fashion through the NGI System. This paper outlines the various fingerprint services offered by the BIAU and details the volume of work performed in each service in fiscal year (FY) 2020.

Manual Fingerprint Processing

Approximately 93 percent of all fingerprint submissions process fully automated through the NGI System. The remaining 7 percent of submissions require manual intervention by an examiner to facilitate the search of a fingerprint submission and, ultimately, a complete and accurate criminal history response. Routine manual fingerprint processing is comprised of

Fingerprint Image Compare (FIC), Fingerprint Sequence Check (FSC), and FIC Evaluation functions.

Function	Percentage of Total NGI Receipts in FY2020	FY2020 Totals
FIC	2.46%	800,578
FSC	6.50%	1,853,304
FIC Evaluation	0.14%	46,031

The FIC function requires an examiner to utilize the Analysis, Comparison, Evaluation, and Verification process to analyze the incoming fingerprint submission and the fingerprint composite in the NGI System to determine whether the images were collected from one individual. The examiner may apply stamps (e.g., in cases of missing or duplicate images), review and adjust segmentation (i.e., the contributor’s or the NGI System’s software isolated an improper or incomplete pattern area for search), and perform necessary image swaps (e.g., where a fingerprint image appearing in a fingerprint box should appear in a different box, and vice versa). These processes help to ensure accurate search and match results.

In the FSC function, an examiner must analyze the sequence of incoming fingerprint submissions to ensure that the rolled images match the plain images. The examiner may apply missing stamps, review and adjust segmentation, and perform necessary swaps before releasing the submission to the NGI System for search.

FIC Evaluation is the process through which fingerprint transactions falling into one of the following categories are reviewed by a second examiner:

- **Conflicting Decisions**—Occurs when two different decisions are made while processing a transaction.
- **Verify Consolidation**—Occurs when the NGI System determines that the submitted fingerprint images may identify to multiple criminal history records.
- **Verify Subject Search**—Occurs when the name, social security number, and date of birth on a submission matches the fingerprint composite in the NGI System and a non-identification decision is made.
- **Verify Non-Identification**—Occurs when a non-identification decision is made with a candidate that has scored above the established threshold within the NGI System.

Criminal Inquiries

The BIAU’s Special Processing Center (SPC) handles the most urgent high-priority fingerprint submissions 24 hours per day, seven days per week. These fingerprint submissions are submitted via e-mail (preferred), facsimile, or Federal Express mail from the FBI Field Offices; federal, state, local, tribal, and international law enforcement agencies; and medical examiners across the country and internationally. The SPC handles criminal inquiries and special processing requests.

Request Type	FY2020 Totals
Fingerprint ID Requests	17,184
Other Fingerprint Requests	41,809
Name Check Queries (via the Interstate Identification Index)	5,054
Telephone Requests	9,762

Fingerprint ID Requests are fingerprint submissions by contributors in open investigations, criminal inquiries, or for deceased individuals for potential identification by the NGI System.

Other Fingerprint Requests are queries from contributors for specific dates of arrest, master fingerprint card copies, photos, identity history information, or other information associated with fingerprints enrolled in the NGI System.

Name Check Queries are special requests from contributors seeking a Universal Control Number for an individual. Most of these requests are from the Strategic Information and Operations Center.

Telephone Requests are calls to the SPC from contributors following up on submitted requests.

Special Requests

Request Type	FY2020 Totals
Unknown Deceased Requests*	402
Unknown Deceased Identifications*	297
Cold Case Requests	40
Cold Case Identifications	4

*The SPC did not begin tracking Unknown Deceased statistics until June 2020.

Unknown Deceased Requests are fingerprints of unknown deceased subjects submitted by criminal justice agencies and medical examiners' offices to help establish an identity. Submissions are received from federal, state, local, tribal, and international contributors. All fingerprints are submitted through the NGI System for a complete search and may be searched through the Civil Name Index (CNI) file and biometric databases maintained by the United States (U.S.) Department of Defense and the U.S. Department of Homeland Security. All responses are returned to the contributor.

Cold Case Identifications are generated as a result of fingerprints submitted by federal, state, local, tribal, and international contributors of individuals involved in current or legacy criminal cases where identity remains unknown. All fingerprints are submitted through the NGI System for a complete search and may be searched through the CNI file and forwarded to the FBI Laboratory Division for processing. Submissions may also be forwarded for search of biometric databases maintained by the U.S. Department of Defense and the U.S. Department of Homeland Security. All responses are returned to the contributor. The SPC encourages the law enforcement community to review any cases where the identity of individuals remains unknown and submit unidentified fingerprints to the SPC for reprocessing.

Noncriminal Hard Copy Card Processing

The BIAU processes hard copy fingerprint cards for federal, state, and regulatory agencies for noncriminal justice purposes. Civil hard copy card processing is limited to those transactions that, by nature or time frame, cannot be processed electronically. A complete criminal history report is provided if the submitted fingerprints identify to fingerprints associated with criminal information in the NGI System.

Request Type	FY2020 Totals
External Requests	19,606
Internal Requests	2,128
National Instant Criminal Background Check System (NICS) Voluntary Appeal File (VAF)	4,063

External Requests are those in which states submit a large batch of noncriminal justice fingerprint cards for ingestion into the NGI System.

Internal Requests are those in which contributors work through the Biometric Services Section’s Customer Service Group to process noncriminal justice requests.

The NICS VAF process allows applicants to request that the NICS maintain their information in the VAF to prevent future erroneous denials or extended delays of a firearm transfer by submitting fingerprints for a biometric-based criminal history check.

Name Check

The Name Check Service enables authorized noncriminal justice agencies to obtain criminal history information for individuals whose fingerprints have been rejected twice for image quality or are double amputees. Name Checks are limited to federal, state, tribal, and regulatory agencies that have the legal authority to submit fingerprints.

Function	FY2020 Totals
Name Check Service Requests	51,076

Name-based checks differ from fingerprint-based checks in that no biometric data is used to conduct the initial search of the Next Generation Identification (NGI) System. Instead, the subject’s biographic data is searched for potential candidates to which the submitted fingerprints can be compared. It is important to note that criminal history record information is not released unless a positive identification is made.

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC F

Criminal History Update

PURPOSE

To provide an update on criminal history record information initiatives, including dispositions, missing arrests, pseudo-pointer records, and functional record support.

AUTHOR

Biometric Services Section, Criminal History Information and Policy Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

Pursuant to Title 28 United States Code (U.S.C.), Section (§) 534, the Attorney General is authorized to exchange criminal history record information (CHRI) for criminal and noncriminal justice purposes. That authority has been delegated to the FBI pursuant to Title 28, Code of Federal Regulations (C.F.R.) § 0.85. The FBI's Biometric Services Section (BSS) Criminal History Information and Policy Unit (CHIPU) supports the criminal justice and the noncriminal justice communities, intelligence agencies, and the public by improving the processes and standards for the collection, storage, maintenance, and dissemination of identity history summary information. The following is an update on criminal history information projects to include dispositions, pseudo-pointer records, and tribal outreach.

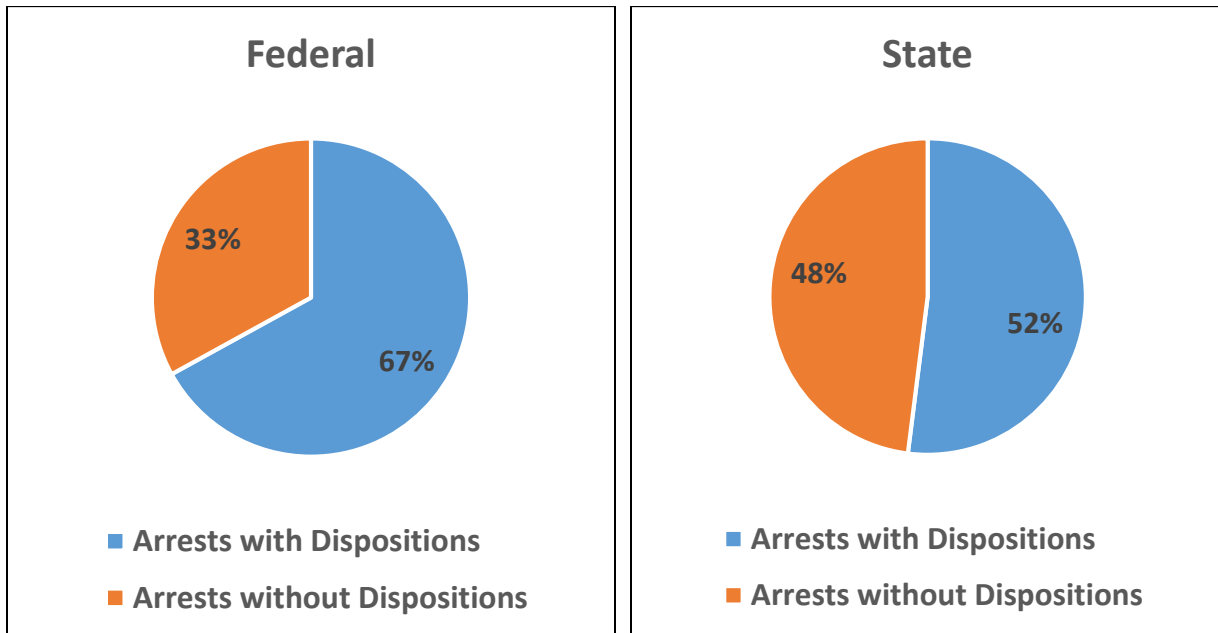
Dispositions

The CHIPU outreach efforts focus on providing support to federal, state, and tribal agencies to obtain missing CHRI, including both arrests and dispositions; emphasizing the importance of collecting and sharing full criminal history information.

The combined totals of dispositions for federal, state and tribal agencies posted to the Next Generation Identification (NGI) System for fiscal year (FY) 2019 and FY2020 is illustrated below:

Type of Disposition	Dispositions Posted FY2019	Dispositions Posted FY2020
Electronic (Posted “Lights Out”)	12,534,874	7,630,089
Manual	611,327	381,675
Total Dispositions Posted	13,146,201	8,011,764

The charts below show the status of arrests with and without dispositions within the NGI System as of 09/30/2020:



Automated Disposition Reporting

Contributors may transmit dispositions via the FBI's Criminal Justice Information Services (CJIS) Division Wide Area Network in an automated process using the Electronic Biometric

Transmission Specification (EBTS) Disposition File Maintenance Request (DSPE) or the Electronic Fingerprint Disposition Submission (FDSP) type of transactions.

The DSPE provides contributors the ability to send an EBTS transaction, similar to a fingerprint submission, with only biographic and disposition information. Agencies may use the DSPE to add, replace, append, or delete court data on an existing criminal event or cycle for a known NGI System identity.

The FDSP transaction contains biographic and disposition information in addition to fingerprints. If the date of arrest is not present on an existing NGI System record, an event cycle will be created to capture only the dispositional data. If no candidate is identified by the fingerprint comparison, a new NGI System record will be created and the disposition retained.

The Interstate Identification Index (III) Disposition (DSP) Message Key (MKE) provides the capability to update the NGI System record with disposition data using III messaging rather than an EBTS transaction. The III DSP MKE may be used to add, replace, append, or delete disposition data on an existing arrest cycle.

Bulk File Processing allows contributors to upload bulk dispositions using the Law Enforcement Enterprise Portal (LEEP). LEEP is an electronic gateway that provides law enforcement agencies, intelligence partners, and criminal justice entities with centralized access to many different resources. This service enables agencies to upload dispositions in a secure and centralized location, eliminating the need for contributors to mail compact discs to the CJIS Division. Submitting dispositions in the Machine-Readable Data (MRD) format results in the addition of disposition data or a complete replacement of any data previously posted for disposition court data. Within minutes of an authorized user uploading the MRD formatted file via the LEEP, the NGI System will retrieve the file and begin processing.

Electronic Submission Method	Number of Agencies Programmed	Transactions Submitted FY2020
DSPE	3	288,946
FDSP	0	0
III DSP MKE	22	5,115,886
Bulk File Processing	18	3,026,454

Current Process Improvement and Automation Efforts

III Seal Record Cycle (SRC) MKE - The development of the III SRC MKE provides an electronic means for III and National Fingerprint File (NFF) states, as well as authorized federal contributors, to seal and unseal CHRI at the arrest level. Previously, sealing states were limited to sealing and unsealing an entire criminal history record via the III entering supplemental identifiers MKE, and only criminal history records containing a state identification number (SID) indexed in the NGI System. Authorized federal contributors relied on the CJIS Division's document processing to seal and unseal arrest cycles because the III MKE was unavailable to them. A National Crime Information Center (NCIC) Technical and Operational Update to provide changes to the III and NFF Operational and Technical Manual was delivered in July 2020. Implementing the single cycle sealing functionality will require programming changes. Once programmed, authorized federal contributors and states will use the SRC to submit single cycle sealing requests to seal and unseal CHRI.

III Delete Record Cycle (DRC) MKE - Currently in development, the III DRC MKE provides a tool for federal, NFF, and non-NFF state contributors to delete arrest cycles. Contributors cannot use the III DRC MKE to remove the last arrest cycle but may submit the FBI Expungement Form FD-1114 to completely remove federal, non-NFF state-maintained, or NFF and non-NFF pseudo-pointer records.

III Modify Record Cycle (MRC) MKE - Also in the development stages, the III MRC MKE provides a tool for federal contributors, NFF states, and non-NFF states to update information at the identity and event levels within the criminal history record, including modifying charges or information that cannot be accomplished using other III MKEs. The CJIS Division is collecting requirements for the III MRC MKE to incorporate many of the record modification requests that are currently processed manually. The III MRC MKE will immediately update records in the NGI System.

Synchronization of Wanted Notifications between NGI and NCIC - As part of the NGI/NCIC Interface Redesign, the effort to remove the majority of want and sexual offender data from the NGI System is almost complete. The NGI System will only store the NCIC number (NIC) and the Originating Agency Identifier (ORI) which link to the data in NCIC. If a response is generated for a Universal Control Number (UCN) where that UCN has also been entered into the NCIC Want or the National Sex Offender Registry (NSOR), the NGI System will send a query to obtain the NCIC Want and/or the Sexual Offender Registry (SOR) data to be included within the NGI response. If NCIC provides a hit response the NGI determines, based on the information provided, whether the Want/SOR status in NCIC is inactive or active. If either a no-hit response is received from NCIC or the response indicates inactive NIC then the NIC is dropped from NGI processing, thus the WANT or SOR will not be provided in the Identity History Summary (IdHS), nor will on-line hit notifications be returned. If NCIC returns a hit response and the status is determined to be active, then NGI will continue processing and include the Want or SOR data cycle within the IdHS, or an on-line hit notification containing the information NCIC provided. If NCIC is down during NGI processing, then an IdHS will still be generated

containing the NIC and ORI stored in NGI along with a caveat of “NCIC IS CURRENTLY OUT OF SERVICE - ADDITIONAL INFORMATION UNAVAILABLE AT THIS TIME.” If NCIC is down during processing of an on-line hit notification, then the notification is held in NGI until NCIC can be contacted. The BSS will no longer be responsible for the maintenance of the want.

Digital Disposition Report (R-84) – The National Instant Criminal Background Check System (NICS) Section is currently developing and assessing the digital R-84. When a NICS examiner is requesting disposition information from an external agency, an R-84 will be provided electronically. When the agency electronically returns the R-84 the NICS examiner will electronically forward the R-84 either to the NGI System or the State Identification Bureau for record update, or to the Disposition Document File. When the examiner selects to forward to the NGI System, the system will format the fields from the R-84 into an electronic message that will update the NGI System in a “lights out” method. The NGI System will return rejects to the NICS and the NICS Assessment Unit will review the rejects and take the appropriate actions.

Pseudo Pointers

A pseudo-pointer record is a state record with no SID, and is not maintained by the state, but by the FBI. States are encouraged to take ownership of pseudo-pointer records to deliver the most accurate and complete CHRI. Before taking ownership, states must ensure their state records contain as much or more CHRI than the records stored in the NGI System. To do so, states are encouraged to complete a self-audit of their CHRI and compare it to the NGI System record to resolve any discrepancies.

The CJIS Division encourages states currently receiving their III synchronization media via the File Transfer Protocol to migrate to the web-based Electronic File Transfer Service (EFTS). The EFTS is available through the LEEP, providing a web interface to securely share and transmit files.

Purpose Code Support

As of 09/30/2020, all states support Purpose Codes C1 and F2, seven states do not support Purpose Code I3, one state does not support Purpose Code S4, and eight states do not support Purpose Code X5. Emphasis is placed on the importance of supporting all Purpose Codes and encouragement of all states to do so. A topic paper detailing the differences between Purpose Codes C and F will be presented to the Advisory Policy Board (APB).

¹ Purpose Code C is used by criminal justice and law enforcement agencies for official duties in connection with the administration of criminal justice as defined in 28 C.F.R. § 20.3(b).

² Purpose Code F is used by criminal justice agencies for weapons-related background checks.

³ Purpose Code I is for interstate-approved, noncriminal justice purposes that involve noncriminal justice employment and/or licensing background checks authorized by federal law, Federal Executive Order, or a state statute approved by the U.S. AG.

⁴ Purpose Code S is for agencies authorized by the Security Clearance Information Act, 5 U.S.C. § 9101.

⁵ Purpose Code X is for authorized agencies to conduct name checks and record requests during exigent circumstances, such as emergency child placements or existing/impending emergencies or disasters. Follow-up fingerprints are required.

Tribal Outreach

Approximately 47 percent of all tribal arrests have dispositions. The remaining 53 percent are without dispositions but include arrests that have not been adjudicated. The CHIPU provided the CJIS Tribal Engagement Program with a document for tribal agencies to outline the criminal history reporting procedures. The document, *Criminal History Reporting Guide for Tribal Agencies*, was created to specifically answer tribal agencies' questions from prior discussions with the APB Tribal Task Force and as a reference for future questions. The guide is available at www.fbi.gov. A one-page reference sheet summarizing how arrest and disposition information may be sent to the CJIS Division for processing was presented at the September 2019 meeting of the APB Tribal Task Force.

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC G

Identification for Firearms Sales Update

PURPOSE

To provide an overview and update of the Identification for Firearms Sale Program.

AUTHOR

Biometric Services Section, Criminal History Information and Policy Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. The FBI's Criminal Justice Information Services will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

The Anti-Drug Abuse Act of 1988 (Public Law 100-690), mandated the United States Attorney General to establish a system for the immediate and accurate identification of felons attempting to purchase firearms. The Gun Control Act of 1968 identifies ten prohibitions that disqualify a person from purchasing a firearm as prescribed under Title 18 United States Code (U.S.C) Section 922 (g) or (n). Title 18 U.S.C. §§ 921 and 922(y) and Title 27 CFR § 478, further defines these prohibitions. The Identification for Firearms Sale (IFFS) Program evolved from this mandate.

The IFFS Program uses flags to quickly identify whether an individual is disqualified from receiving a firearm pursuant to the Brady Handgun Violence and Prevention Act of 1993 (Brady Act). The Brady Act led to the development of the National Instant Criminal Background Check System (NICS).

The program uses two flags for the Interstate Identification Index (III), Purpose Code F name checks, and record requests. The "D" flag is set on records that contain one or more federal firearms disqualifiers. The "X" flag is set for III records when the status of the record is

Information Only Topic G, Page 1

unknown and when additional research is required to identify whether the record contains disqualifying information. When a III record is established for the first time, the record is set to an “X” flag until the IFFS participating state modifies the flag.

Participation is voluntary and open to all III participating states and federal agencies. Participating states and federal agencies must agree to update and maintain the accuracy of the flags. Participants must have the ability to modify the IFFS flags.

Biannually, participating states are required to engage in the III Audit Synchronization process. The states identify discrepancies with records that are indexed in the III. This is a good opportunity to correct the IFFS flags that are set in error. The states use the III Enter Supplemental Identifiers (EHN) Message Key to modify the IFFS flag. If there are numerous flags that are set incorrectly, the CJIS Division can assist with a mass correction of the flags. IFFS Program participants must ensure an exact match for the flag value at the state and national level. If a discrepancy exists, the state must update the flag value correctly.

BENEFITS

The IFFS Program provides significant value to the FBI’s NICS Section, the NICS user community, state and federal law enforcement agencies, and the general public. The immediate notification of disqualification is invaluable for quick decision making in matters of public safety.

When the IFFS flag is set as “D” on a criminal history record, it provides the ability to readily identify individuals who are federally prohibited from possessing a firearm. The NICS users make immediate decisions to determine fitness for firearms sales, firearm related permits or explosives permits. The clear indication of a firearm prohibition on the record also decreases the number of inquiries received by state and federal agencies requesting additional record information. This saves valuable time and resources for state Point-of-Contact agencies and the NICS Section. In addition, Federal Firearms Licensees can provide purchasers with a much quicker response. The ability to immediately deny the transfer of a firearm to a prohibited individual is invaluable to the public and for the safety of law enforcement.

UPDATE

The IFFS Program is managed by the BSS’s Criminal History Information and Policy Unit (CHIPU) under the purview of the III Program. Currently, there are 23 states and 3 federal agencies participating in the Program.

The CHIPU Management and Program Analysts collected information from participating and non-participating states regarding Program challenges or obstacles which may have prevented them from participating. The two primary limiting factors they cited were:

1. The lack of fully developed internal business processes, and
2. A lack of personnel resources.

Other factors include the following: lack of automation to set flags, system technical and programming issues, lack of education and training regarding the federal prohibitors, differences in programming and logic preventing a single solution for all, and the cost of technical maintenance solutions. As a result, the CJIS Division conducted an internal review of the IFFS Program and identified strategies to improve the effectiveness. The state of Virginia made system enhancements and, during this upgrade to their system, they opted out of IFFS Program participation citing obstacles such as a lack of personnel to verify and maintain the IFFS flags.

IFFS Program participants may be unaware that they can leverage the III Synchronization process to resolve discrepancies. In addition, all participants have the necessary tools to set and maintain the IFFS flags, either through III Message Keys, the Machine-Readable Data disposition submission process, or the Electronic Biometric Transmission Specification disposition type of transactions. This information is provided to potential participants to help them decide which method will work best for them to maintain IFFS flags.

The III business line, with the collaboration of the NICS Section, will create an IFFS Program Taskforce to help mitigate these obstacles. The taskforce will assist with educating current and potential participants on the ease of participation and the methods available to maintain flags.

Any IFFS-related questions should be addressed to the CHIPU Criminal History Record Information Policy and Development Team at fbi-iii@fbi.gov.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC H

The Next Generation Identification System Interstate Photo System Update and Interstate Photo System Policy and Implementation Guide Revisions

PURPOSE

The purpose of this paper is to provide information regarding the importance of enrolling type 10 (photos and scars, marks, and tattoos) records into the Next Generation Identification Interstate Photo System; the impact of face coverings on face recognition searches and the guidelines for conducting face recognition searches of the Next Generation Identification Interstate Photo System. In addition, the topic paper will provide a status on the progress of updating the Next Generation Identification *Interstate Photo System Policy and Implementation Guide*.

AUTHOR

Biometric Services Section, Investigative Services Support Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. CJIS will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

Since the fourth increment of the Next Generation Identification (NGI) System, the NGI Interstate Photo System (IPS) has maintained all face photos associated with an existing tenprint fingerprint record. The NGI IPS also assists law enforcement by providing enhanced photo enrollment, retrieval, search, and maintenance capabilities. The NGI IPS continues to serve law enforcement by allowing:

- More photo sets per FBI record for criminal subjects (up to 25 per transaction)
- Bulk submission of face photos maintained at the federal or state level repositories
- Submission of photos other than face photos (scars, marks, tattoos)
- Investigative face recognition (FR) search capabilities

DISCUSSION AND ANALYSIS

The FBI's Criminal Justice Information Services (CJIS) Division encourages federal, state, local, and tribal agencies to voluntarily enroll face photos in the NGI IPS. Face photos not only enhance the accuracy and completeness of criminal history records, they also ensure the availability of the photos for investigations at a national level. It is imperative that agencies capture images properly to ensure maximum system performance.

Authorized law enforcement agencies may submit investigative face photos (probe photos) for an automated face recognition search (FRS) of the NGI IPS which will return a ranked gallery of candidates (2-50) for review as possible investigative leads. Face photos returned in the ranked gallery include the associated FBI Universal Control Number (UCN). In some cases, an FRS does not result in a returned candidate list due to a transaction error, system error, or a probe photo of poor quality. Although the emerging technology of FR has made great strides over the years, FR does not provide positive identification and submitters are prohibited from relying solely on the gallery of candidates returned from the NGI IPS for law enforcement action. The law enforcement agency must conduct additional investigation prior to making an identification.

NGI IPS Volume

The volume of photos in the repository continues to grow steadily. The NGI IPS has grown by approximately 10 million face photos in the past year. As of 09/30/2020, the overall enrollment photo count was more than 103.8 million which includes all face photos received with a tenprint fingerprint submission and 50.1 million are currently available for FR searches. These 50.1 million face photos, representing 22.5 million individuals, do not include photos taken and submitted to the NGI System for noncriminal justice purposes. Face images associated with these transactions are logically separated and are excluded prior to the biometric search and are not disseminated as a result of a face recognition search.

Today, all but nine states enroll criminal face photos in the NGI IPS. States that do not participate cite lack of technology and resources as the reason and some states plan to submit photos once their systems are updated.

Biometric Image Submission Request (FIS)

The FIS supports the enrollment of additional biometric imagery (to include face photos) for an existing identity, when a search is not necessary or in order to enroll face photos that have not previously been submitted to the NGI System. This functionality is used to support the National Fingerprint File states' submission of fingerprints and additional biometric imagery for all subsequent criminal criterion offenses but can be used by all submitters for either individual or bulk submissions.

The submitted face photos will be stored in the NGI IPS to ensure availability of the photos for investigations at a national level and will be associated with the provided UCN. When possible, users should include the Event Identifier (2.2035 EVI) from the associated original response (SRE), so that the additional biometric images may be associated with the existing EVI.

Face Coverings in the NGI IPS

Recently, the CJIS Division has seen an increase in face photo submissions containing face coverings due to the ongoing pandemic. Consequently, if a photo of a face with a covering meets the quality threshold, the photo may be included in a candidate gallery in the future. The FBI recommends that submitting agencies consider the impact of face coverings on FR searches when capturing and submitting photos to the NGI IPS. Agencies should also consider the best practices outlined in the Facial Identification Scientific Working Group *Capture and Equipment Assessment for Face Recognition Systems* document. In that document, it indicates that the camera should be positioned approximately two meters (6.5 feet) from the subject. The guidance also aligns with safety standards allowing agencies to safely take photos of individuals without face coverings.

A CJIS Information Letter (September 2020) and an International Justice and Public Safety Network (NLETS) Administrative Message with the above information has been disseminated to all CJIS System Agencies (CSAs), State Identification Bureaus (SIBs) and Compact Council members. CSAs should consider forwarding the message to all agencies within their states to ensure awareness. Agencies with questions should contact the IPS staff by e-mail at FR_IPS@leo.gov.

Search Connectivity

The CJIS Division's Investigative Services Support Unit (ISSU) continues efforts to assist authorized federal, state, local, and tribal law enforcement in deploying access to the FR functionality of the NGI IPS. States and agencies with existing FR systems will work with their current service providers to program their systems to handle the types of transactions specified in Version 10.0 of the *Electronic Biometric Transmission Specification* (www.fbibiospecs.org).

States who want to conduct an FRS of the IPS must have connectivity to the system and meet the following guidelines:

- **Authorized User**
 - Must be law enforcement agency (principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws);
 - Must have law enforcement Originating Agency Identifier (ORI) for accessing CJIS systems or must be a criminal justice agency conducting the search on behalf of a law enforcement agency; and,
 - Must have approval by the state CJIS Systems Officer (CSO)

- **Usage Policies**
 - User agency is responsible for developing appropriate usage policies (in accordance with applicable laws/policies of governmental jurisdiction to which user agency is subject)
 - Must comply with the CJIS Security Policy and CJIS User Agreement
 - Must protect constitutional rights of all persons, including the express prohibition against the collection of photos in violation of individual's First and Fourth Amendment rights

- **Probe Photos**
 - Searches must be in support of an active/open investigation
 - Must be lawfully obtained pursuant to an authorized criminal investigation (reasonable suspicion, probable cause)

- **Required Training**
 - Must complete FR training prior to conducting an FRS of the IPS
 - Training must be approved by the CSA/SIB for individuals of agencies/states
 - CSA/SIB may opt to use vendors to conduct the training
 - Training must be consistent with the “Guidelines and Recommendations for Facial Comparison Training to Competency,” as outlined by the Facial Identification Scientific Working Group (FISWG) at www.FISWG.org
 - The CJIS Division’s Biometric Training Team offers face comparison and identification training at no cost to external law enforcement
 - If interested, please contact the training staff at FACE-TRNG@leo.gov

NGI Policy and Implementation Guide

The *Interstate Photo System Policy and Implementation Guide* serves as a resource guide for policy, operational, and technical requirements for authorized law enforcement and noncriminal justice agency users who utilize the services of the NGI IPS. The document is modified as the NGI IPS services develop and new services are delivered.

The CJIS Division is updating the *Interstate Photo System Policy and Implementation Guide* to ensure that NGI IPS users are provided with a current, up-to-date document. The CJIS Division will be requesting the Identification Services Subcommittee’s FR Subject Matter Expert Group to review and provide input on the revised document in the future.

NGI IPS Outreach Efforts

The ISSU continues its outreach efforts to additional federal and state CSOs to gauge interest in the NGI IPS and to determine agency readiness and connectivity to conduct FRS of the NGI IPS.

Federal and state agencies interested in accessing the NGI IPS or seeking additional information may call the ISSU at 304-625-FACE (3223), Option #2. In addition, law enforcement agencies may submit questions and share experiences regarding the FR functionality of the NGI IPS to fr_ips@leo.gov.

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC I

Biometric Interoperability Update

PURPOSE

The purpose of this paper is to provide the Next Generation Identification System users with information regarding the expanded implementation of interoperability between the Department of Justice, Federal Bureau of Investigation's Criminal Justice Information Services Division, the Department of Homeland Security's Automated Biometric Identification System (IDENT), and the Department of Defense's Automated Biometric Identification System (ABIS).

AUTHOR

Biometric Services Section, Investigative Services Support Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. CJIS will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

Interoperability fosters the exchange of biometric data among the FBI's Next Generation Identification (NGI) System, Department of Homeland Security's Automated Biometric Identification System (IDENT), and Department of Defense's (DoD)'s Automated Biometric Identification System (ABIS) to facilitate the sharing of biometric and relevant biographic data including criminal history, immigration information and military operations in support of authorized criminal justice purposes, immigration, border enforcement, national security, intelligence, background investigations for national security positions and certain positions of public trust, and other authorized homeland security functions.

Interoperability provides the NGI System contributors:

- Access to external biometric repositories through a single query
- Limited ability to search latent prints against the full repositories of external agencies
- Enhanced federal, state, local, tribal and territorial information sharing

DISCUSSION AND ANALYSIS

The requirement and need for interoperability between the three United States Government biometric systems is supported by existing laws, Executive Orders, and Congressional guidance. These legislative measures include, among others, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (Public Law 107-56 Section 403), requiring a “fully integrated means to share law enforcement and intelligence information,” Section 302 of the *Enhanced Border Security and Visa Entry Reform Act of 2002* (Public Law 107-173). In addition, Title 8, United States Code (U.S.C.), Section 1722, requires the FBI to share fingerprint data in the NGI System with the DHS as that data is relevant to admissibility or deportability determinations.

Interoperability efforts allow for the exchange of relevant data in a secure and timely manner controlled in accordance with sharing agreements. The following outlines information currently exchanged by the NGI System with the IDENT:

- Wants and Warrants

The CJIS Division began providing wants and warrants to the DHS in 2006 to enhance border security. The CJIS Division continues to provide wants and warrants associated with fingerprints in the NGI System to the DHS to be used on the IDENT Watchlist by DHS entities. A great benefit of interoperability and the sharing of the want and warrant information is the potential identification of additional wanted persons. If DHS identifies a Wanted Person, the wanting agency must be advised of the encounter.

Today, wants and warrants are shared in a near-real time basis. The CJIS Division sends DHS the fingerprints associated with the wants and warrants every four hours for inclusion in the IDENT Watchlist.

- Criminal Submissions to the NGI System

As noted above, 8 U.S.C. §1722 requires the FBI to share fingerprint data in the NGI System with the DHS as that data is relevant to admissibility or deportability determinations. Therefore, all criminal submissions received from federal, state, local, tribal and territorial agencies including the Criminal Answer Required (CAR), Ten Print Rap Sheet Search (TPRS), Criminal No Answer (CNA), and Criminal Print Non-Urgent (CPNU) types of transactions are automatically forwarded as a search to the IDENT via interoperability. In addition, when the FBI is notified of subsequent arrests using the Criminal Print Ident message from National Fingerprint File states, the NGI System retrieves the master fingerprints from the initial arrest and then creates a submission to search the IDENT.

Criminal searches of the IDENT include the fingerprints and limited biographic information contained in the NGI System submission but do not include criminal history information. Fingerprints and limited biographic information are not retained within the IDENT unless there has been an independent DHS or Department of State (DOS) encounter.

The IDENT System responds with either a match or no-match IDENT Data Response (IDR). If a matching record is found in the IDENT, the NGI System generates an Immigration Alien Query (IAQ) to the DHS Immigration and Customs Enforcement (ICE) Law Enforcement Support Center (LESC) based on the information returned within the match IDR. The LESC processes the IAQ on a transactional basis and conducts a more extensive search of immigration records to determine the immigration status of the individual and responds to the NGI System with an Immigration Alien Response (IAR). The NGI System then returns a combined IDR/IAR to the State Identification Bureau (SIB) as a subsequent response to the NGI Identity History Summary for states programmed to receive a second response. If a no-match is returned, the NGI System forwards the IDR to the SIB stating there was no-match in the IDENT System.

Currently, there are 16 states capable of receiving the DHS response. This subsequent response provides agencies the ability to develop comprehensive histories for investigations. Participating states receive immigration identity information such as name, date of birth, place of birth, gender, and photographs (if available) provided during the last five DHS and DOS encounters. Some of these states have the capability to provide this information to their local law enforcement agencies either directly or by using web services.

Multiple subsequent responses provide benefits to agencies such as:

- Determining the use of aliases for the establishment and/or verification of identity
- Enhanced ability to develop threat profiles
- Notifications to the appropriate parties on the activities of terrorists and other dangerous criminals
- Enhanced ability to coordinate responses to an encounter
- Improved officers' knowledge related to the safety of their environment and the ability of officers to control that environment
- Enhanced threat assessment as a result of the improvements in identification
- Improved data quality across the federal enterprise, enabling a reduction in data errors and the consolidation of multiple records pertaining to a single subject
- Improved ability to conduct trend analysis
- Improved ability to obtain intelligence
- Improved ability to develop investigative leads with respect to crime, immigration, and terrorism

Special programming within the NGI System is required to ensure states are receiving the DHS response. Therefore, if your state has the capability to receive a subsequent response but you are not receiving the DHS response, please contact the CJIS Division for assistance to acquire this interoperability functionality.

- Identification for Firearm Sales (IFFS) and Sex Offender Registrants (SOR)

The CJIS Division began sharing the IFFS records flagged by the states with a

disqualifier for acquiring or possessing firearms and SOR records with the IDENT in 2011 to support DHS’ ability to enforce immigration laws. These records were identified to align closely with information relevant in making admissibility or deportability determinations and provided the DHS Customs and Border Protection (CBP) a positive indication of criminal history to quickly make determinations at CBP Primary Points of Entry until a rapid search of the full Criminal Master File could be achieved.

The sharing of this information is conducted using the existing shared services functionality. Specifically, when a state flags a record as an IFFS or a SOR, the NGI System pulls the master print and sends a search to the IDENT System. Retention of this data remains consistent with the IDENT/NGI Interoperability Memorandum of Understanding (MOU), thereby the DHS will only link an IFFS or SOR record when it matches to an independent DHS or DOS encounter.

- IDENT No Match (INM)

The Advisory Policy Board authorized the CJIS Division to provide IAQs through NGI/IDENT Interoperability to the ICE LESC for NGI System tenprint criminal submissions lacking indicia of United States citizenship in the fall 2008. If no fingerprint match is found in the IDENT, but the subject lacks indicia of United States citizenship (as indicated on the submission or on the master print on file within the NGI System), the IAQ is identified and processed by ICE as a “No Match”.

The DHS ICE vets the INM IAQs in bulk to identify all potentially removable criminal aliens who are in local law enforcement custody or who have been subsequently encountered through immigration and law enforcement processes. The INM process results in customized leads, by ICE field offices, of aliens who may be amenable to removal from the United States. It should be noted that this process excludes United States Citizen (USC) data and no USC data is retained beyond the INM IAQ, which constitutes the record of the information shared with ICE.

The INM process is a cooperative effort between the ICE and the National Criminal Analysis and Targeting Center, both located in Williston, VT and within ICE Enforcement and Removal Operations.

STATISTICS

The following chart outlines the cumulative number of interoperability searches conducted between the NGI and IDENT Systems as of the end of fiscal year 2020:

Category	Searches	Identifications	Hit Rate
NGI to IDENT	125,182,637	9,253,099	7.39%
IDENT to NGI*	285,333,517	10,262,452	3.6%

*Numbers do not include the TPRS submissions from the CBP

RECENT BIOMETRIC INTEROPERABILITY MILESTONES

Although Interoperability was achieved between the NGI System, IDENT and ABIS in 2008, the CJIS Division, DHS Office of Biometric Identity Management (OBIM), and DoD Defense Forensic Science Center (DFSC) continue to coordinate on a regular basis to enhance and expand interoperability functionality to ensure the exchange of information is accurate, timely and complete.

- **Want and Warrant Synchronization Process**

The CJIS Division and the DHS OBIM implemented a synchronization (sync) process on 06/04/2020 to ensure all want and warrant records shared by the CJIS Division with the IDENT are being properly maintained and stored. The sync process initially identified 76,078 records to be deleted and 902 records which needed to be added. Due to the discrepancies acknowledged during the June sync, it was determined the process would occur on a monthly basis.

The want and warrant sync process has proven to ensure the data shared with the IDENT remains accurate. In July, the sync determined only 237 records needed to be deleted. Since then, the synchronization results have shown no discrepancies.

The Investigative Services Support Unit Interoperability Team continues to work with the OBIM to monitor all NGI System data shared with the IDENT is properly maintained.

- **Face Recognition Interoperability**

The DHS OBIM programmed the IDENT System to conduct face recognition searches (FRS) of the NGI Interstate Photo System (IPS). The CJIS Division and the OBIM deployed the capability via interoperability in October 2019.

Currently, only the CBP National Targeting Center (NTC) has the capability to access the NGI IPS via face recognition interoperability. The NTC's use is limited to its screening rules to identify the small percentage of travelers whose photos will be sent on an individualized basis to the NGI IPS for a face recognition search when there is a law enforcement purpose. The NTC screening rules are used to determine which travelers are reasonably suspected to pose a risk to border security or public safety, who may be a terrorist or suspected terrorist, who may be inadmissible to the United States, or who may otherwise be engaged in activity in violation of United States criminal law. As with all users, the candidate photos returned to the NTC are for investigative lead purposes only, cannot be used for positive identification, and the NTC must perform additional research to resolve the identities of the subjects before taking any action.

- **IDENT/ABIS Interoperability**

The NGI System has been the conduit between the ABIS and the IDENT Systems for biometric interoperability transactions since 2011. This has been a highly effective method to ensuring all three federal biometric systems are searched and has closed gaps

in biometric information sharing. The DoD and DHS have now established a direct connection between the ABIS and IDENT. Therefore, to alleviate duplicate DoD transactions in the IDENT, the CJIS Division worked with the DHS OBIM and DoD DFSC and discontinued submitting all ABIS transactions, except the United States Coast Guard, to the IDENT on 09/02/2020. The discontinuation will not have an impact on the identity sharing currently in place between the NGI and ABIS Systems.

INTEROPERABILITY LOOK AHEAD

Interoperability MOUs: The CJIS Division, OBIM, and DOS Consular Affairs have been coordinating efforts to revise the current MOU between the agencies. The updated MOU will authorize the exchange of approved biometrics to include expansion of latent interoperability.

In addition, the CJIS Division and DFSC have been collaborating to draft an agreement between the agencies to cover the interoperability between the NGI System and the ABIS. The agreement will be an Annex to the larger FBI and DoD MOU currently in place.

Future Interoperability: The CJIS Division is expanding its biometric interoperability focus by continuously improving information sharing with other federal agencies. The long-term vision of biometric interoperability is to make the NGI System fully interoperable with additional biometric systems. These continued interoperability efforts ensure federal, state, local, tribal, and territorial agencies have access to relevant and up-to-date information.

The CJIS Division will continue to work with the DHS and DoD to manage current and emerging Department of Justice/DHS/DOD biometric interoperability in support of agency and national goals.

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC J

Summary of the Results from the December 2020 CJIS APB Meeting

PURPOSE

To inform Advisory Process members of the actions taken by the APB on topics discussed at the December 2020 virtual meeting.

AUTHOR

Global Law Enforcement Support Section, Advisory Process Management Office

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. CJIS will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

The following are recommendations and actions taken at the December 2020 APB meeting. The topic papers addressed by the APB can be found on the LEEP SIG service under the CJIS SIG.

To retrieve the topic papers, select:

- *Advisory Process Information
- *Advisory Policy Board

Then scroll down to "APB Topic Papers" and select [December 2-3, 2020 Action Topic Papers - Virtual Meeting](#)"

The APB meeting minutes will be distributed and posted to the CJIS SIG in the future.

DECEMBER 2020 APB - ALL MOTIONS AND ACTION ITEMS

APB Item #2 Chairman's Report on the NCIC Subcommittee, NCIC Issue #S01 Interstate Compact Offenders in the NCIC

Issue 1 Interstate Compact Offender Indicator Field

APB ACTION: The CJIS APB moved to add an Interstate Compact Offender Indicator Field to the NCIC Wanted Person, Missing Person, and Supervised Release Files as an optional, one alpha-character field (Y/N). If the compact information is unknown, the field may be left blank. Depending on technical feasibility, this enhancement may be implemented during the development of NCIC Next Generation (N3G) or post N3G initial operating capability. Missing person entries where a juvenile is entered into the NCIC with a populated Compact Field indicator shall receive a message when the juvenile reaches date of emancipation age for purposes of determining if the record should be modified or if a wanted person entry should be made. The priority should be 3M and designated as non-critical for audit purposes. The motion passed.

Issue 2 Bond Amount Field Data Type

APB ACTION: The CJIS APB moved to recommend Option 1: Support the use of alpha and numeric characters in the Bond Amount Field as it is considered in the N3G implementation. The priority should be 3M. The motion passed.

APB Item #2 Chairman's Report on the NCIC Subcommittee, NCIC Issue #S02 Reciprocal Sharing of NCIC Records with Canada

APB ACTION: The CJIS APB moved to recommend Option 1: Approve the reciprocal sharing of Missing Person records with Canada through a pointer system. Depending on technical feasibility, this enhancement may be implemented during the development of N3G or post N3G initial operating capability. The priority should be 3M. The motion passed.

APB Item #2 Chairman's Report on the NCIC Subcommittee, NCIC Issue #S03 Proposal to Allow the Entry of Unidentified Person File Records with an Estimated Date of Death (EDD) Greater than 50 Years from the Date of Entry (DTE)

APB ACTION: The CJIS APB moved to recommend Option 1: Allow the entry and maintenance of Unidentified Person file records with an EDD greater than 50 years from the DTE. Depending on technical feasibility, this enhancement may be implemented during the development of N3G or post N3G initial operating capability. The priority should be 3M. The motion passed.

APB Item #2 Chairman's Report on the NCIC Subcommittee, NCIC Issue #S04 The National Vehicle Service (NVS) Parking Violation Stolen Vehicle Project

Information Only Topic J, Page 2

APB ACTION: The CJIS APB moved to approve the NVS's expanded authorization to conduct comparisons of NCIC Vehicle File data with parking citations, to include a recommendation that NVS use the license plate and state of registration for comparison. Also approving for the National Insurance Crime Bureau and the National Motor Vehicle Title Information System if a similar request is received. The priority should be 3M. The motion passed.

APB ACTION: The CJIS APB moved to recommend the FBI modify the current Memorandum of Understanding regarding the Parking Violation Stolen Vehicle Project to require the NVS, and similarly situated entities, to make prompt notification to the recovering and entering agency. The priority should be 3M. The motion passed.

**APB Item #4 Chairman's Report on the N-DEx Subcommittee, N-DEx Issue #S02
Modifying the N-DEx System Advanced Permission and Verification (AP&V) Policies**

Issue A

APB ACTION: The CJIS APB moved to recommend Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing policies 1.3.9, 1.3.10, and 1.3.11 and replacing with the following new policy.

Authorized Use and Verification Requirement: N-DEx System information may be used and shared, without restrictions imposed by the record-owning agency, provided both of the following conditions are met:

- The recipient(s) of shared information resides within the record-requesting agency or within another authorized agency, with which a primary information exchange agreement exists; and
- The information will not be used for the following actions: inclusion of the information in an official case file; use in the preparation of judicial processes such as affidavits, warrants, or subpoenas; use in an adverse eligibility or suitability determination when retrieving information under Use Codes J, F, B, or S; or dissemination to another authorized entity not part of the releasing agency's primary information exchange agreement (otherwise known as secondary dissemination).

Any sharing or use of N-DEx System data not meeting the above conditions requires the N-DEx System user to verify the information with the record-owning agency for completeness, timeliness, accuracy, relevancy, and any use restrictions on the data prior to actionable use or secondary dissemination of the data. The motion passed.

Issue B

APB ACTION: The CJIS APB moved to recommend Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the “immediacy” policy (1.3.13), specifically by modifying the policy as follows:

*Policy 1.3.13 – Immediate use of N-DEx System information can be made without ~~the advanced permission of verification from~~ the record-owning agency if there is an **exigent circumstance— an emergency situation- actual or potential threat of criminal activity or terrorism** requiring swift action to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect, or destruction of evidence. The record-owning agency shall be immediately notified of any use made as a result of **exigent above** circumstances.*
The motion passed.

Issue C

APB ACTION: The CJIS APB moved to recommend Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to include expectations language in the current policy dealing with use authorization requests and concurrences (1.3.14) as follows:

*Policy 1.3.14 – Participating **record-owning** agencies are encouraged to consider how they may wish to account for ~~use authorization requests and concurrences verification requests in a complete and timely manner, including the maintenance of accurate POC information on agency records.~~ While the N-DEx System does not systematically support nor require a log to be maintained, agencies are encouraged to consider how ~~the advanced permission, verification, and data provision verification requests~~ may be documented within their own organization.*
The motion passed.

APB Item #4 Chairman’s Report on the N-DEx, N-DEx Issue #S03 N-DEx Data Sharing Task Force Policy and System Recommendations

Issue A - N-DEx Policy 1.4.3

APB ACTION: The CJIS APB moved to recommend Option 1: Update the *N-DEx Policy and Operating Manual*, policy 1.4.3 to read:

Agency-Configurable Data Sharing Controls: **All data is presumed sharable. The record-owning agency may restrict data access** ~~The N-DEx System is designed to allow record-owning agencies to protect their data~~ in accordance with the laws, **regulations, and or** policies which govern dissemination and privacy for their jurisdictions. ~~All data is presumed sharable unless the record-owning agency restricts data access, in accordance with their sharing policy.~~ **Restricted data access requires the submission of relevant authorizing laws, regulations, or policies to the N-DEx Program Office.** The N-DEx System enables data sharing

at the following data item (i.e., reports) dissemination criteria values:
The motion passed.

Issue B – N-DEx Policy 1.4.3.4

APB ACTION: The CJIS APB moved to recommend Option 1: Update the *N-DEx Policy and Operating Manual*, policy 1.4.3.4 to read:

Record-owning agencies shall have the ability to configure sharing policy based on agency, agency type, ~~individual users~~, or *select* data characteristics to create exception groups for their data. ~~Therefore, an N-DEx System record may be red to one user, yellow to a second, and green to a third. Record-owning agencies are encouraged to submit records using the green value; however, if an agency must submit records using the red or yellow values, they are encouraged to make their records green for their own agency to realize the full benefit of automatic entity integration, data correlation, and other tools within the N-DEx System, including the creation of subscriptions.~~

The motion passed.

Issue C – System Enhancement for Juvenile Rule

APB ACTION: The CJIS APB moved to recommend Option 1: Simplify the juvenile rule available within the N-DEx System to allow juvenile restrictions with three age options (<18, <17, or <16) in three report types (Incident, Booking, Arrest Reports) and dissemination values (red or yellow). The priority should be 3M. The motion passed.

APB Item #4 Chairman’s Report on the N-DEx Subcommittee, N-DEx Issue #05 Next Generation Identification (NGI) Interstate Identification Index (III) Derived Criminal Biometrically Confirmed Death Notice Extracts ingested as Records into the N-DEx System

APB ACTION: The CJIS APB moved to recommend Option 1: Implement the system changes necessary in the NGI and N-DEx System to extract new NGI deceased identities daily, submit them as records to the N-DEx System, and display the "**DECEASED**" notice to the N-DEx System users in their search results. The priority should be 3M. The motion passed.

APB Item #6 Chairman’s Report on the N-DEx Subcommittee, N-DEx Issue #6 Increase the Timeout Session for Inactivity in the N-DEx System

APB ACTION: The CJIS APB moved to recommend Option 1: In accordance with the *CJIS Security Policy*, Section 5.5.5 Session Lock, increase the inactivity session timeout period in the N-DEx System to 30 minutes. The priority should be 3M. The motion passed.

APB Item #7 Chairman’s Report on the Compliance Evaluation (CE) Subcommittee

APB ACTION: The CJIS APB moved to accept the recommendations of the CE as presented below:

Administrative Office of the United States Courts – 2018
NCIC – Follow-up to CJIS Systems Office (CSO)

Alabama – 2016
Information Technology (IT) – Follow-up to Governor

Alabama – 2019
NCIC, IT, NGI – Follow-up to CSO
National Sex Offender Registry (NSOR), NICS, N-DEX – Closure to CSO

Alaska – 2017
IT – Follow-up to CJIS Systems Agency (CSA) Head

Arkansas – 2016
NSOR – Closure to Governor

Arkansas – 2019
NSOR – Closure to CSO

Arkansas State Identification Bureau (SIB) – 2019
NGI – Closure to POC

California – 2017
NSOR – Closure to CSO

Colorado – 2018
IT – Follow-up to CSO
NCIC, NSOR – Closure to CSO

Connecticut – 2017
IT – Follow-up to CSO
NGI – Follow-up to Repository POC

Delaware – 2019
IT, NICS – Follow-up to CSO
N-DEX, NGI – Commendation to CSO
NCIC, NSOR – Closure to CSO

Florida – 2015
IT – Call/Close or Follow-up to Governor

Florida – 2018
NSOR, IT – Follow-up to CSO

Guam – 2018
NSOR – Follow-up to CSO
IT – Closure to CSO

Hawaii – 2018
NCIC – Call/Close or Follow-up to CSO

Idaho – 2017
IT – Follow-up to CSA Head

Illinois – 2015
NCIC, NSOR – Email Follow-up to CSO

Illinois – 2018
IT, NGI – Follow-up to CSO
NCIC, NSOR – Email Follow-up to CSO

Indiana – 2018
IT – Closure to CSA Head

Iowa – 2018
NSOR – Follow-up to CSO
IT – Follow-up to CSA Head (elevation)

Kansas – 2018
IT – Email Follow-up to CSO

Kentucky – 2019
NSOR – Follow-up to CSO
NICS, N-DEx, NGI – Commendation to CSO
NCIC, IT – Closure to CSO

Louisiana – 2017
NSOR – Call/Close or Follow-up to CSA Head

Maine – 2010, 2013, 2016
NCIC – Email Follow-up to CSO

Maine – 2019

NSOR, NGI – Follow-up to CSO

NICS, N-DEx – Commendation to CSO

IT – Closure to CSO

NCIC – Email Follow-up to CSO

Maryland – 2017

IT – Call/Close or Follow-up to CSA Head

Massachusetts – 2017

NCIC, NSOR, IT, NICS – Follow-up to CSA Head

Massachusetts SIB – 2017

IT, NGI – Follow-up to Repository POC

Michigan – 2019

NSOR, IT, NGI – Follow-up to CSO

N-DEx – Commendation

NCIC, NICS – Closure

Minnesota – 2015

IT – Follow-up to Governor

Minnesota – 2018

IT – Follow-up to CSA Head

Mississippi

NSOR, NGI – Follow-up to CSO

NICS, N-DEx – Commendation to CSO

NCIC, IT – Closure to CSO

Missouri – 2018

NCIC, NSOR – Follow-up to CSA Head

IT – Closure to CSA Head

Montana – 2014

IT – Follow-up to Attorney General

Montana – 2017

NSOR, IT – Follow-up to CSA Head

Nlets

IT – Commendation to POC

Nebraska – 2019
IT, NICS – Follow-up to CSO
N-DEx – Commendations to CSO
NCIC, NSOR, NGI – Closure to CSO

Nevada – 2017
IT – Email Follow-up to CSO with notification to Governor via letter

New Hampshire – 2018
NCIC, IT, N-DEx, NGI – Follow-up to CSO

New Jersey – 2019
NCIC, NSOR, IT – Follow-up to CSO
NICS, N-DEx – Commendation to CSO

New Mexico – 2016
IT – Follow-up to Governor

New Mexico – 2019
NCIC, IT, NICS, NGI – Follow-up to CSO
NSOR, N-DEx – Closure to CSO

New York – 2014
NCIC, NSOR, IT – Follow-up to Governor

New York – 2018
NCIC, NSOR, IT – Follow-up to CSO

New York SIB – 2018
IT – Follow-up to POC

North Carolina – 2016
IT – Follow-up to Governor

North Carolina – 2019
IT – Follow-up to CSO
NICS – Closure to CSO

North Dakota – 2019
NGI – Follow-up to CSO
N-DEx – Commendation to CSO
NCIC, NSOR, IT, NICS – Closure to CSO

Office of Biometric Identity Management – 2019
IT – Follow-up to POC
NGI – Closure to POC

Ohio Bureau of Criminal Investigation – 2017
IT, NICS – Follow-up to Superintendent
NSOR – Closure to Superintendent

Oklahoma – 2019
NSOR, IT – Follow-up to CSO
NICS, N-DEx – Commendation to CSO
NCIC – Closure to CSO

Oklahoma SIB– 2019
IT – Commendation to CSO

Oregon – 2015
NSOR – Email Follow-up to CSO with notification to Governor via letter

Oregon – 2018
IT – Follow-up to CSO
NSOR – Email Follow-up to CSO

Pennsylvania – 2017
IT – Closure to CSO

Puerto Rico – 2013, 2015
NCIC – Follow-up to Governor

Puerto Rico – 2019
NCIC, IT – Follow-up to CSO
NSOR, NICS – Closure to CSO

Rhode Island – 2017
IT – Closure to CSA Head

Rhode Island Repository – 2017
IT – Follow-up to Attorney General

South Carolina – 2013
IT – Email Follow-up to CSO with notification to Governor via letter

South Carolina – 2017
NSOR, IT – Follow-up to CSA Head

South Dakota – 2016
NSOR – Closure to Governor

South Dakota – 2019
NSOR, IT, NICS – Follow-up to CSO
N-DEx – Commendation to CSO
NCIC – Closure to CSO

South Dakota SIB – 2019
NGI – Follow-up to POC
IT – Commendation to POC

Tennessee – 2019
IT – Follow-up to CSO
N-DEx – Commendation to CSO
NCIC, NSOR, NICS – Closure to CSO

Texas – 2019
NSOR – Follow-up to CSO
NICS, NGI – Commendation to CSO
NCIC, IT, N-DEx – Closure to CSO

Transportation Security Administration – 2019
IT – Follow-up to CSO
NCIC, N-DEx – Commendation to CSO

United States Air Force Office of Special Investigation – 2018
NCIC, IT – Follow-up to CSO

United States Coast Guard – 2019
NCIC – Commendation to CSO
IT, NICS – Closure to CSO

United States Customs and Border Protection – 2019
IT – Follow-up to CSO
NCIC, N-DEx – Closure to CSO

United States Immigration and Customs Enforcement – 2019
NCIC, IT, NICS, N-DEx – Commendation to CSO

United States Postal Inspection Service – 2019
IT – Closure to CSO

United States Secret Service – 2019
NCIC, IT, NICS, N-DEx – Commendation to CSO

United States Virgin Islands – 2019
NSOR, IT – Follow-up to CSO
NCIC – Closure to CSO

Vermont – 2019
NSOR, IT, NGI – Follow-up to CSO
NCIC, NICS, N-DEx – Commendation to CSO

Virginia – 2015
NSOR – Email Follow-up to CSO with notification to Governor via letter

Virginia – 2018
NSOR – Email Follow-up to CSO

Washington – 2018
IT – Follow-up to CSO

West Virginia – 2018
NCIC – Follow-up to CSO
IT – Closure to CSO

Western Identification Network – 2020
IT – Commendation to POC

Wisconsin – 2018
IT – Follow-up to CSO
NSOR – Closure to CSO

The motion passed.

**APB Item #8 Chairman’s Report on the NICS Subcommittee, NICS Issue #S05
Enhancement to the NICS Indices to Include the Special Processing Code (SPC)
Functionality to All Files of the NICS Indices. Modification of the Description of the NICS
Indices Prohibiting Category Code J File**

Expand the SPC Functionality to ALL NICS Indices Files

APB ACTION: The CJIS APB moved to recommend Option 1a: Enhance the functionality of the NICS Indices federal files by allowing the SPC functionality to be an optional field when applicable. The motion passed.

Modification of the Description of the NICS Indices J File

APB ACTION: The CJIS APB moved to recommend Option 2a: Amend the description of the NICS Indices J File from “State Prohibitor” to “State Prohibitor or Court-Ordered Firearm Restriction”. The priority should be 3M. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S03 Expand L0008 Reject Response for Clarity by Creating Two Separate and Distinct Error Messages

Action Item: The topic will be referred back to the CJIS Division for additional work. The topic should be brought back to the APB if the technical issues will impact the criminal justice community.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S04 Creation of a Specific Message to Indicate When an Identity History Summary (IdHS) is Incomplete

APB ACTION: The CJIS APB moved to recommend Option 1: Pursue creating a new message to be returned in the NGI 2.060 Message (MSG) field when the IdHS is requested and a “timeout” response is received from a National Fingerprint File (NFF) participant. The motion passed.

APB ACTION: The CJIS APB moved to recommend Option 2: Pursue creating a new message to be returned in the NGI 2.060 MSG field when the IdHS is requested and a “timeout” message is received for a III participant and the FBI-held data is provided. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S05 Creation of Identity History Summary Response (IDHSR) Type of Transaction (TOT) and Identity History Summary Request Response (IDHSRR)

APB ACTION: The CJIS APB moved to recommend Option 1: Pursue the creation of the IDHSR and IDHSRR TOTs for noncriminal justice agency purposes. The priority should be 3M. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S07 Request to Remove the Want Notice Modification and National Sexual Offender Registry (SOR) Modification from Rap Back Trigger Notification Options and to Update the *NGI Criminal Justice (CJ) Rap Back Policy and Implementation (P&I) Guide* Accordingly

APB ACTION: The CJIS APB moved to recommendation Option 1: Endorse the removal of the WANT and SOR Modification from the Rap Back Trigger Notification Options and update the *NGI Criminal Justice Rap Back Policy and Implementation Guide* to show the removal of these trigger notifications and the additional of “Not currently used” in trigger numbers 7 ad 10 as reflected below:

1. Criminal Retain Submission (Default)
2. Dispositions
3. Civil Retain Submission (Security Clearance Information Act Only)
4. Expungement/Partial Expungement (No longer an NGI Noncriminal Justice Rap Back Service Trigger Option)
5. Want Addition with FBI/UCN included
6. Want Deletion
7. ~~Want Modification~~ Not currently used
8. Sexual Offender Registration Addition
9. Sexual Offender Registration Deletion
10. ~~Sexual Offender Registration Modification~~ Not currently used
11. External (intentionally skipped as this number is not operational)
12. Death Notice with Fingerprints
13. Death Notice without Fingerprints

The proposed updates are found in the *NGI CJ P&I Guide* on pages 14-15. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S09 Charge Severity Indicator to Reflect the Conviction Level in the NGI System

APB ACTION: The CJIS APB moved to recommend Option 1: Explore the creation of a new method to capture the severity of a charge/conviction level of crimes in the NGI System as a felony, misdemeanor, or other. The priority should be a 4M. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S10 Relationship to Victim (RTV) Field in the NGI System

APB ACTION: The CJIS APB moved to explore the creation and policy implications of a new NGI field to capture the RTV for person-to-person crimes, domestic violence crimes, or crimes that could contain elements of force. The priority should be 3H. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #S11 Notifications for a Consolidated Identity Involving Retained Civil Events

APB ACTION: The CJIS APB moved to recommend Option 1: The FBI CJIS Division develop interim technical modifications to the NGI System, while developing a proactive notification capability to address when the FBI Universal Control Number (UCN) returned to the agency on

a retained noncriminal justice tenprint submission response has been changed to a different FBI UCN. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #13 Proposed Modification to the NGI Systems’ State Outreach Mechanism

APB ACTION: The CJIS APB moved to recommend the FBI’s CJIS Division staff explore a technical solution to create a Criminal History Record Information (CHRI) dissemination date that would modify the NGI System state outreach mechanism to allow both the FBI and the state to respond with CHRI on behalf of a single state. The priority should be 3M. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #14 Update on the Proposal to Expand the NGI System’s Biometric Image/Feature Retrieval Request (IRQ) TOT Functionality

APB ACTION: The CJIS APB moved to recommend Option 4: Endorse Options 2 and 3: Create two new TOTs: one to return certification files only and one to return composite fingerprints. The priority should be 3M. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #16 NGI Iris Service Update and Policy and Implementation Guide Concurrence

APB ACTION: The CJIS APB moved to endorse the *NGI Iris Service Policy and Implementation Guide* as presented to the APB by the IS Subcommittee. The motion passed. (See Attachment #1.)

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #17 Identifying Non-serious Offenses (NSOs) for Removal from the NGI System

APB ACTION: The CJIS APB moved to recommend Option 1: Remove the NSOs with the charges listed below from records within the NGI System when unaccompanied by a serious offense. Additionally, future submission of these NSOs will not be retained by the NGI System.

- A. Theft under \$5
- B. Sleeper
- C. Minor
- D. Unregistered auto and/or vehicle

The priority should be 3M. The motion passed.

APB Item #9 Chairman’s Report on the IS Subcommittee, IS Issue #18 FBI Electronic Biometric Transmission Specification (EBTS) Updates

APB ACTION: The CJIS APB moved to endorse the attached EBTS 11 redlines as outlined in the topic paper. The motion passed. (*See Attachment #2.*)

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #2 Modification of the National Incident-Based Reporting System (NIBRS) Arson Victims

APB ACTION: The CJIS APB moved to recommend Option 2: No change. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #S03 Modification of the NIBRS Rape Definition

Issue A – Modifications to the Rape Definition/Discontinuation of the categories “Sodomy” and “Sexual Assault with an Object”

APB ACTION: The CJIS APB moved to accept Option 1: Modify the NIBRS rape definition to reflect the Summary Reporting System (SRS) rape definition approved in 2012 which states: “Penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another person, without consent of the victim.” If the recommendation to modify the NIBRS rape definition is approved, continuation of the categories of “sodomy” and “sexual assault with an object” is no longer required. The priority should be 3M. The motion passed.

Issue B – Replacing “Fondling” with “Unwanted Sexual Contact”

APB ACTION: The CJIS APB moved to replace the term “fondling” with the term “criminal sexual contact” with a priority of 3M. The motion was defeated 25 against to 8 in favor.

Issue C – Replacing “Incest” and “Statutory Rape”

APB ACTION: The CJIS APB moved to recommend Option 2: No change. The motion passed.

Issue D – Creation of an “Other Sex Crimes” Category

APB ACTION: The CJIS APB moved to recommend Option 2: No change. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #S04 FBI’s UCR Program to Include Additional Case Disposition Information to the NIBRS Data Collection

APB ACTION: The CJIS APB moved to add the Beyond 2021 recommendation to combine Administratively Closed/Suspended and Transferred with the new definition with a priority of 4L. The motion was defeated 30 against to 3 in favor.

APB ACTION: The CJIS APB moved to add additional case status information after the National Program’s 2021 transition to a NIBRS only data collection embedded in the

recommendations provided by the Beyond 2021 Task Force. In addition, the Beyond 2021 Task Force should provide definitions that are clear and succinct and represents the activity and needs of local law enforcement agencies. The motion was defeated 20 against to 13 in favor.

APB ACTION: The CJIS APB moved for the UCR Subcommittee and Beyond 2021 Task Force to revisit this issue to determine case dispositions and their definitions. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #S05 FBI’s UCR Program Adding Unfounded to the NIBRS Data Collection

APB ACTION: The CJIS APB moved to recommend Option 3: Collect Unfounded in the Offense Segment in Data Element 7 – Offense Attempted/Completed Data Element. The priority should be 3L. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #S06 Expansion of the Exceptional Clearance Category

APB ACTION: The CJIS APB moved to recommend Option 3: No change. The motion passed with 1 opposed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #S07 FBI’s UCR Program’s Hate Crime Anti-Mormon Bias Type

APB ACTION: The CJIS APB moved to recommend Option 1: Modify the Hate Crime bias type designations of Anti-Mormon to Anti-Church of Jesus Christ. This would involve modifying the following documents:

- *2019.1 NIBRS Technical Specifications*
- *2019.1 NIBRS XML Developer’s Guide*
- *2019.1 NIBRS XML IEPD*
- *2019.1 NIBRS User Manual and Hate Crime Data Collection Guidelines and Training Manual*

The priority should be 3M. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #08 FBI’s UCR Law Enforcement Officers Killed and Assaulted (LEOKA) Suicide Data Collection

APB ACTION: The CJIS APB moved to recommend Option 1: Implement the data collection as a 1-year pilot using the proposed questionnaire in Appendix B of the topic paper. The motion passed. (*See Attachment #3.*)

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #09 Recommendation for Changes to Sex Codes with UCR

APB ACTION: The CJIS APB moved to refer the topic to the Public Safety Strategy (PSS) Subcommittee for further review. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #10 Revision to the UCR Program’s Police Employee Collection

APB ACTION: The CJIS APB moved to recommend Option 1: As presented in Appendix B. (See Attachment #4.) Add the “Unknown/unreported” category to the list of races/ethnicities and **gender expressions** that allow for the recording of police employee counts when individuals opt out of providing either information. In addition, the category of “non-binary” will be added to the list of gender expressions available for reporting police employee counts. The priority should be 3L. The motion passed with 1 opposed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #16 Translation of the Frequency of Release Date

APB ACTION: The CJIS APB moved to recommend the UCR Program release quarterly data by the third Monday of June, September, December, and March. The motion passed.

APB Item #11 Chairman’s Report on the UCR Subcommittee, UCR Issue #18 Summary of Recently Conducted Quality Assurance Reviews

APB ACTION: The CJIS APB moved to authorize Letters of Interest be sent by e-mail to the state UCR Program Managers and CSOs of the states included in the presentation, as these reviews have been finalized. The motion passed.

APB Item #14 Chairman’s Report on the PSS Subcommittee, PSS Issue #4 Height, Weight, and Hair Codes Standardization across CJIS Division Systems

Issue 1- Hair

APB ACTION: The CJIS APB moved to recommend Option 1a: Standardize the Hair Codes across CJIS Division Systems to include the addition of Hair Code XXX for Unspecified or Unknown, Hair Code BAL for Bald, and Hair Code STR for Streaked as referred to in the ANSI/NIST-ITL 1-2011 Update: 2015 specification. The priority should be 3M. The motion passed.

Issue 2 – Height

APB ACTION: The CJIS APB moved to recommend to standardize the Height Codes across CJIS Division Systems to include UNK for Unknown, a minimum value of 001, and a maximum value of 911. The priority should be 3M. The motion passed.

Issue 3 - Weight

APB ACTION: The CJIS APB moved to recommend to standardize the Weight Codes across CJIS Division Systems to include UNK for Unknown, a minimum value of 001 and a maximum value of 999. The priority should be 3H. The motion passed.

Intentionally Left Blank



Next Generation Identification

Iris Service

Policy and Implementation Guide

Version 3.7

07/13/2020

Prepared by:

Biometric Identification and Analysis Unit (BIAU)

Biometric Services Section (BSS)

Federal Bureau of Investigation (FBI)

Criminal Justice Information Services (CJIS) Division

1000 Custer Hollow Road

Clarksburg, WV 26306

SIGNATURE PAGE

Signatures/Approvals		
 Michael D. DeLeon Assistant Director CJIS Division		<u>07/14/2020</u> Date
 Kimberly J. Del Greco Deputy Assistant Director Information Services Branch CJIS Division		<u>07/13/2020</u> Date
 Scott A. Rago Section Chief BSS		<u>07/10/2020</u> Date
 Joseph W. Sensibaugh Assistant Section Chief BSS		<u>7/10/20</u> Date
 Krista L. Koch Unit Chief BIAU		<u>7/10/20</u> Date
 Debra L. Tennant Project Manager BIAU Iris Program and Scars, Marks, Tattoos, and Symbols Team		<u>7-10-2020</u> Date

TABLE OF CONTENTS

<u>1</u>	IRIS SERVICE	2
1.1	Introduction.....	2
1.2	Purpose.....	2
1.3	Overview.....	2
<u>2</u>	APPROPRIATE USE OF THE NGI IRIS SERVICE.....	3
2.1	Enrollment.....	4
2.2	Search.....	5
<u>3</u>	ADDITIONAL TYPES OF TRANSACTIONS	6
3.1	Biometric Image/Feature Retrieval Request (IRQ)	6
3.2	Biometric Delete Request (BDEL)	6
3.3	Biometric Delete Response (BDEL)	7
<u>4</u>	PARTICIPATION REQUIREMENTS	7
<u>5</u>	PROPER IMAGE CAPTURE	7
5.1	Iris Cameras	7
5.2	Technical Resources	9
<u>6</u>	INFRASTRUCTURE	9
<u>7</u>	CONTACT INFORMATION.....	10
<u>8</u>	APPENDIX A: ACRONYMS	11
<u>9</u>	APPENDIX B: REFERENCES.....	13
<u>10</u>	APPENDIX C: GUIDE TO CAPTURING IRIS IMAGES	15
<u>11</u>	APPENDIX D: FREQUENTLY ASKED QUESTIONS	16

1 IRIS SERVICE

1.1 Introduction

The Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division, with the endorsement of the CJIS Advisory Policy Board (APB) and approval of the FBI Director, implemented the Iris Service within the Next Generation Identification (NGI) System to further advance biometric identification services.

The NGI Iris Service contains an iris image repository and features an iris search capability. All iris images submitted for enrollment in the repository and available for searching must be associated with tenprint fingerprints and must be collected pursuant to an arrest, subsequent criminal proceeding, incarceration, or post-trial release. The Iris Service is housed within the FBI's NGI System, which serves as the national repository for biometric-based identity history and criminal history record information.

1.2 Purpose

This document describes policy and technical requirements for authorized criminal justice agency users to utilize the NGI Iris Service. It defines the types of NGI Iris Service enrollments and search transactions that are accepted, the responses returned, and references to additional technical resources. The NGI Iris Service Policy and Implementation Guide is a living document and will be modified as needed as the NGI Iris Service develops. All substantive modifications will be appropriately reviewed and approved by advisory entities, such as the APB, as appropriate.

1.3 Overview

An iris offers a highly accurate, contactless, and rapid biometric identification option for criminal justice agencies. The iris contains a unique pattern of ridges and folds that are specific to an individual. This biometric is particularly useful in high-volume environments where identification is critical and to maintain the safety and security for the agency professionals by using a contactless biometric method. The capture of a subject's irises, using a near-infrared camera, can be achieved in seconds and can easily be integrated into an existing biometric capture process. The NGI Iris Service contains iris images from federal, state, local, and tribal agencies that are obtained during arrest, booking, and incarceration proceedings. These iris images are associated with tenprint fingerprints and the Universal Control Number (UCN). This

enables the agency to enroll the record in the NGI Iris Service or to locate the record in the NGI System and add the biometric information.

Iris images may be submitted for enrollment by criminal justice agencies, for criminal justice purposes, via bulk or single transmissions. Authorized criminal justice agencies may conduct a one-to-many Iris Image Identification Search (IIDS) without human intervention,¹ enroll iris images along with criminal tenprint fingerprints, or append iris images to existing criminal records through the NGI Iris Service. The Type of Transactions (TOTs) for iris images will follow the same routing over the CJIS Wide Area Network (WAN) as other NGI TOTs. The three methods for enrollment are with a tenprint criminal fingerprint submission, the Biometric Image Submission (FIS) transaction after a criminal identity is established (or identity is established in the criminal file), and a bulk submission of FIS transactions.

2 APPROPRIATE USE OF THE NGI IRIS SERVICE

The NGI Iris Service is intended to provide an identification service for criminal justice agencies that have the need to quickly and accurately identify or confirm the identity of an individual. Identification searches are performed for authorized agencies submitting an iris probe image to the NGI Iris Service repository. The initial deployment of the NGI IIDS feature will be used for an identification search for validation. Example use cases include: correctional facilities to readily identify inmates during movement and release; sheriff's offices and police departments as they house and transport arrestees; courts for defendant appearances; and, probation and parole agencies for parolee check-ins.

The NGI Iris Service will return an identification/non-identification response along with other descriptive information as specified by the submitter. All iris images submitted for enrollment in the NGI Iris Service and available for searching must be associated with tenprint fingerprints. The basic policy and technical requirements for enrollment and search transactions are outlined in Sections 2.1 and 2.2, respectively.

¹ See Section 2.2 of this document for information on how an IIDS can be submitted without any data entry.

2.1 Enrollment

The primary and preferred enrollment transaction for iris images is the criminal tenprint submission with two TYPE 17 iris image records attached. Two iris image records, one for each of the left and right irises, must be provided for all enrollments or the transaction will be rejected.

When either the left or right iris cannot be captured, the reason shall be recorded in Field 17.28 Damaged or Missing Eye, and the record should follow the format provided in C.8 TYPE 17 Record Samples – Iris Image Absent. The transaction will be rejected if this field is not populated.

Iris images enrolled with a tenprint fingerprint submission will receive a Submission Results – Electronic (SRE) response. The submitter will receive one SRE per successful transaction. The iris images are not processed if the tenprint fingerprint submission fails.

There are three methods for iris image enrollment to the NGI Iris Service repository:

1. With a tenprint criminal fingerprint submission using the following TOTs:

Criminal Answer Required (CAR)
 Criminal No Answer (CAN)
 Criminal Fingerprint Direct Route
 Criminal Fingerprint Processing Non-Urgent

2. With the FIS transaction after a criminal identity is established:

The FIS transaction supports the enrollment of additional biometric images (e.g., fingerprint; palmprint; supplemental print; iris image; face photo; and scars, marks, and tattoo photos) for an existing criminal identity.

The FIS requires the submission of the UCN and the iris images. It is used for situations where the iris images are not captured during the initial booking or when higher quality images are captured *after* the initial enrollment. Although not mandatory, it is suggested that the FIS transaction also have a Date Printed (DPR) or Event Identifier (EVI) so the additional biometric image may be associated with the existing EVI. Iris images enrolled with a FIS transaction will receive a FIS response which provides details on each biometric type enrolled by a FIS.

3. With a bulk submission of FIS transactions:

Agencies with an existing iris repository may utilize bulk enrollment, as the existing systems are updated, to perform live enrollments (offline) to the NGI Iris Service. Agencies should coordinate with the FBI CJIS Division and the applicable CJIS Systems Agency (CSA) to coordinate the logistics of a bulk enrollment. The authorized agencies are responsible for ensuring that accurate and complete

biographic and biometric information is submitted in accordance with CJIS data quality standards and operating policies. Bulk enrollments require two iris records with the UCN and either the DPR or EVI. The submitter is required to verify all criminal iris images match the UCN, State Identification Number, and/or Miscellaneous Number, and arrest cycle prior to submission to the CJIS Division.

Iris images sometimes fail to “template” – that is, the images cannot be converted for use in the NGI Iris Service. An error transaction is returned when both images in a submission fail to template. For dual iris submission (enrollments and identification searches) where one image templates and one fails, the requested action is performed, and a successful response is returned with a warning message in the 2.060 Status/Error Message field. The operator should recapture failed images and resubmit.

2.2 Search

The NGI Iris Service provides an identification service in which a subject’s irises may be searched against the NGI Iris Service repository and generate an identification/non-identification response. This is known as the IIDS TOT.

The IIDS transaction provides a method of identifying a subject via a one-to-many, “lights-out” (without human intervention) search. The optimal submitted search transaction will include two iris probe images (right iris/left iris) captured by a near-infrared iris camera in a controlled setting. The submitted probe images are then searched against all iris images in the NGI Iris Service repository. If an eye is missing or damaged, it must be appropriately labeled. Iris images included with the IIDS transaction are not retained within the NGI Iris Service repository, nor will they be added to an existing identity record in the event of an identification search result.

For agencies to take full advantage of the speed of iris capture, they are encouraged to work with their booking station providers to reduce the amount of manual selections required to submit the IIDS TOT. For example, vendors can program interfaces that once a user selects the IIDS TOT, the iris camera can be activated automatically, and the user can capture both irises. Agencies may choose to populate the optional name field with the subject’s name, however, the name field will not be part of the search but will be returned in the search result.

Upon successful capture, the IIDS transaction is automatically submitted. An SRE response is returned for a successful IIDS transaction that indicates either an identification/non-identification response. If an identification occurs, the NGI Iris Service will initiate an automated query of the National Crime Information Center repository with the associated unique identifier, to obtain additional biographic and law enforcement information related to the subject to include in the

SRE. When available, this information will be provided in the Supplementary Identity Information (SII) Field. The results include a list of identifiers and case numbers for the Wanted Person, National Sex Offender Registry, and Immigration Violator Persons Files that contain the identity. The response may also contain the Identity History Summary, if requested. In addition, all identification responses include the following caveat:

“This response is based on a search of the NGI Iris Service repository and does not preclude a record from existing in other biometric or biographic repositories.”

When an iris identification search does not match a UCN on file, the contributor will receive a non-identification response.

When an iris identification search does not contain any iris images suitable for searching, the contributor will receive a reject message:

“The biometric search was not performed. Templates could not be created for the submitted images.”

When an iris identification search results in a match against multiple identities (expected to be a remote possibility), the contributor will receive an error message:

The submitted search requires CJIS to adjudicate the results.

3 ADDITIONAL TYPES OF TRANSACTIONS

3.1 Biometric Image/Feature Retrieval Request (IRQ)

Agencies may request specific image sets in the NGI Iris Service for comparison. The IRQ requires the UCN in the Subject Identifier (SI). If the SI is found, available images for the subject will be returned.

3.2 Biometric Delete Request (BDEL)

Agencies are required to delete biometric images if, for example, an individual is no longer on probation or their record is expunged. The request to delete the biometric image is initiated by submitting a BDEL. The owner is defined as the first Controlling Agency Identifier entry on the enrollment submission. The BDEL requires the UCN and Biometric Set Identifier for the iris images to be deleted.

3.3 Biometric Delete Response (BDEL R)

A BDEL R is returned upon completion of a successful BDEL transaction. If any permission or process errors are encountered, an Administrative Error Response is returned. It is only possible to delete one iris record per BDEL transaction (using the Case Identifiers).

4 PARTICIPATION REQUIREMENTS

Authorized criminal justice agencies may participate in the enrollment and/or search of iris images. User agencies must meet the *Electronic Biometric Transmission Specifications (EBTS)* technical requirements for utilizing the NGI Iris Service, including a secure infrastructure, as discussed in Section 6. User agencies must also meet all requirements of the CJIS User Agreement and the CJIS Security Policy.

It is the responsibility of the user agency, in accordance with the applicable laws and policies of the governmental jurisdiction to which the authorized user agency is subject, to develop appropriate usage policies for the NGI Iris Service. All appropriate use policies must protect the constitutional rights of all persons. Users are prohibited from enrolling or searching iris images in the NGI Iris Service that have been collected in violation of an individual's exercise of rights guaranteed under the First Amendment or in violation of the individual's rights secured under the Fourth Amendment.

5 PROPER IMAGE CAPTURE

The proper capture of iris images is imperative to the performance of an iris recognition system. This includes both the initial enrollment into the NGI Iris Service and probe iris images searching the NGI Iris Service repository. Similar to fingerprints, iris images submitted to the NGI Iris Service must meet or exceed minimum quality requirements. Agencies utilizing the NGI Iris Service for the first time will be able to submit test images prior to working within the live environment. Iris image examples can be found in Appendix C.

5.1 Iris Cameras

Standard iris cameras use a near-infrared light to capture a more useful iris image across a broad range of actual iris colors. Testing has shown that a near-infrared images are required to obtain high accuracy rates.

Iris cameras may be designed to capture images of a single eye or both eyes at one time. Capturing images of the left and right eye separately can introduce transposition/labeling errors

where the left eye may be incorrectly labeled as the right eye and vice versa. Since dual-eye iris cameras (e.g., binocular cameras) can reduce labeling errors and help optimize matcher performance through subject head roll angle measurement, dual-eye cameras should be given preference.

To enable interoperability with other iris recognition algorithms and technology, the imagery collected by such cameras should be capable of retention (subject to policy constraints), in standard, *lossless* image formats (e.g., lossless versions of PNG, BMP, JPEG2000).

Capturing iris images is as simple as capturing conventional photos but is still susceptible to similar errors. Such errors can result in low-quality images that may not be usable for iris recognition. Inclusion of such images into databases can result in poor matching performance. Operators should be trained in the use of iris cameras to avoid the types of errors that are common in regular photography such as occluding (or obstructing) the lens, improper focus, strong back lighting, and poor framing as well as iris camera specific errors.

Guidance for iris image collection should include best practices for image capture and handling. Adherence to the following procedures will ensure high quality samples are collected: eyes must be wide open and looking directly at the camera, the iris is to be centered and fully visible, and the image should be sharp and in focus with few reflections or specular highlights. Problems that occur during image acquisition (e.g., subject was looking down or blinking) will lead to poor quality samples. Such problems are straightforward and easy to correct but require attentiveness on the part of the camera operator.

As part of *Iris Exchange (IREX) V: Guidance for Iris Image Collection*, the National Institute of Standards and Technology (NIST) has developed the following, recommended materials:

- Report: *Guidance for Iris Image Collection*
- Slides: *Best Practices for Iris Image Capture*
- Poster: *Guide to Capturing Iris Images*

As part of an FBI-sponsored activity, the NIST reviewed standards and processes for iris cameras that allow for data exchange between government entities, as permitted by regulation and policy, and that provide cost-effective improvements as technology advances. Information regarding iris cameras may be found in the NIST Technical Note TN 2018, *Iris Cameras: Standards Relevant for Camera Selection - 2018*. Any procurement of iris cameras and associated software should require:

- Conformance to the guidance in Appendix C for image quality.
- Ownership and control of all collected imagery by the agency with the authority for its collection.

5.2 Technical Resources

Criminal justice agencies utilizing the NGI Iris Service are permitted to select the hardware and software to best fit their needs. Selections and implementations are typically constrained by contracts, existing systems, and agency resources. Variations exist between vendors, product lines, and agency specific customizations; however, any system implemented by criminal justice agencies that complies with the CJIS Security Policy and the *EBTS Version 11* can utilize the NGI Iris Service. Typical iris image collection locations tether an iris camera to a booking station with fingerprint, palmprint, and face photo image collection capabilities. The NGI Iris Service is designed to follow existing CJIS Division business practices to minimize both transaction complexity and data entry requirements to simplify user interfaces and lower adoption costs for the user.

6 INFRASTRUCTURE

The main method for transmission of biometric submissions is electronically, via the CJIS WAN, a telecommunications infrastructure that connects authorized agencies to the CJIS host computer systems. The CJIS WAN provides a secure transport mechanism for CJIS criminal history record information and biometric-related information. The NGI Iris Service will utilize this secure infrastructure as other FBI identification services currently do, by providing direct and indirect electronic access for criminal justice agencies. For example, after a sheriff's department captures iris images, the agency will electronically submit the images to the NGI Iris Service. The iris images will then route through the state controlling agency to the FBI. NGI Iris Service responses will travel back to the sheriff's department in the reverse path.

Electronically, the iris images will be supported through the FBI's *EBTS Version 11*, which will provide proper methods for external users to communicate with the CJIS Systems for the transmission of biographic and biometric information.

Authorized criminal justice agencies may enroll iris images with the current CJIS TOTs via the CJIS WAN. Agencies intending to utilize the NGI Iris Service search functionality must program their systems to the proper Iris Service TOT. This programming information will be made available in the *EBTS Version 11*.

Existing systems must generate transactions that comply with the *EBTS Version 11*. Iris submissions will be routed from the local user, to the CSA, to the FBI's CJIS Division. Responses follow the reverse path from the CJIS Division to the CSA to the local agency. The iris image routing within the NGI System is identical to the NGI System fingerprint transaction routing process.

7 CONTACT INFORMATION

For additional information on the NGI Iris Service please contact the CJIS Division, at 304-625-IRIS (4747).

APPENDIX A: ACRONYMS

Acronym	Description
ANSI	American National Standards Institute
APB	CJIS Advisory Policy Board
BDEL	Biometric Delete Request
BDEL R	Biometric Delete Response
BIAU	Biometric Identification and Analysis Unit
BSS	Biometric Services Section
CAR	Criminal Answered Required
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services
CNA	Criminal No Answer
CSA	CJIS Systems Agency
DPR	Date Printed
EBTS	Electronic Biometric Transmission Specification
EVI	Event Identifier
FBI	Federal Bureau of Investigation
FIS	Biometric Image Submission
FISR	Biometric Image Submission Response
IIDS	Iris Image Identification Search
IREX	Iris Exchange
IRQ	Biometric Image/Feature Retrieval Request
ITL	Information Technology Laboratory

NGI	Next Generation Identification
NIST	National Institute of Standards and Technology
SRE	Submission Results Electronic
SI	Subject Identifier
SII	Supplementary Identity Information
TOT	Type of Transaction
UCN	Universal Control Number
WAN	Wide Area Network

APPENDIX B: REFERENCES

[American National Standards Institute (ANSI)/NIST-Information Technology Laboratory (ITL)]

NIST Special Publication 500-290 – ANSI/NIST-ITL 1-2011 --- *Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information*, approved November 2011, <http://Fingerprint.NIST.Gov/Standard/>

[CJIS SECURITY POLICY]

Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, CJISD-ITS-DOC-08140-5.8, <https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/>

[CJIS USERS AGREEMENT]

Appendix D.1, Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, CJISD-ITS-DOC-08140-5.8, <https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/>

[FBI EBTS]

FBI CJIS *Electronic Biometric Transmission Specification (EBTS) Technical and Operational Update 9*, Version 10.0.9, 05/22/2018, <https://www.fbibiospecs.cjis.gov/EBTS/Approved>

[IREX I]

Grother, P., Tabassi, E., Quinn, G.W. and Salamon, W., *IREX I – Performance of Iris Recognition Algorithms on Standard Images*, NIST Interagency Report 7629, 10/30/2009, http://biometrics.nist.gov/cs_links/iris/irexII/irex_report.pdf.zip

[IREX II]

Tabassi, E., Grother, P., and Salamon, W., *IREX II – Iris Quality Calibration and Evaluation – Performance of Iris Image Quality Assessment Algorithms*, NIST Interagency Report 7629, 09/30/2011, http://biometrics.nist.gov/cs_links/iris/irexII/iqce_report.pdf.zip

[IREX III]

Grother, P., Quinn, G. W., Matey, J.R., et al., *IREX III – Performance of Iris Identification Algorithms*, NIST Interagency Report 7836, 04/09/2012

Report: http://biometrics.nist.gov/cs_links/iris/irexIII/IREXIII_full.zip

Appendices: http://biometrics.nist.gov/cs_links/iris/irexIII/IREXIII_appendices.zip

[IREX V MAIN]

IREX V: Guidance for Iris Image Collection, <http://www.nist.gov/itl/iad/ig/irexv.cfm>

[IREX V REPORT]

Quinn, G., Matey, J., Tabassi, E., Grother, P., *IREX V – Guidance for Iris Image Collection*, NIST Interagency Report 8013, 07/02/2014,

http://biometrics.nist.gov/cs_links/iris/irexV/IREX_V_Report.pdf

[THE NIST TECHNICAL NOTE TN 2018]

Iris Cameras: Standards Relevant for Camera Selection - 2018

<https://www.nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2018.pdf>

[NIST IRIS REFERENCES]

Guide to Capturing Iris Images

Poster: https://www.nist.gov/system/files/documents/2017/02/23/irex_v_poster_20140612.pdf

IREXV – Best Practices for Iris Image Capture

Instructional Slides: <https://www.nist.gov/document/irexvslides20140612.pptx>


APPENDIX C: GUIDE TO CAPTURING IRIS IMAGES



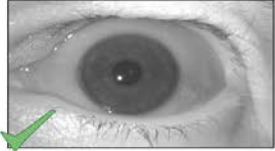
Guide to Capturing Iris Images



CORRECT



Right eye




Left eye

- ✓ Eyes wide open
- ✓ Iris centered and fully visible
- ✓ Eyes looking at camera
- ✓ Sharp, in focus
- ✓ Few reflections or specular highlights
- ✓ Correct left and right labels

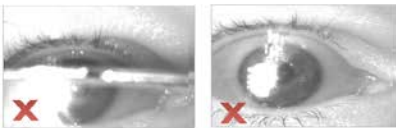
INCORRECT

EYELID: OCCLUSION OF IRIS




Ask subject to open eyes wide. Subject may use fingers to hold eyes open.

EYEGLASSES: OCCLUSION AND REFLECTIONS



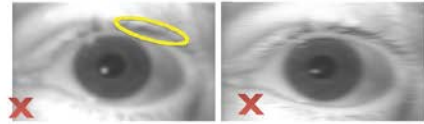
Remove eyewear

IRIS ABSENT



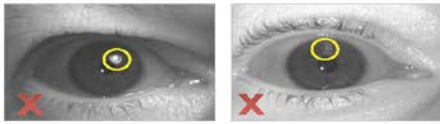
Remove glasses, align camera with eyes

BLUR: FOCUS(L) MOTION (R)




Hold camera still and at proper distance from subject

BACKGROUND REFLECTIONS ON IRIS




Avoid bright scenes in front of the subject

UPSIDE-DOWN




Properly align camera with subject

IMPROPER GAZE ANGLE



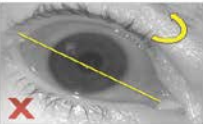
Instruct subject to look directly at the camera or fixation light

IRIS CLOSE TO EDGE




Align camera axis with eye(s)

ROTATION




Align camera with subject

EXCESSIVE DILATION



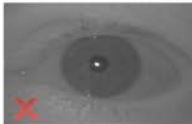
Wait for drugs to wear off; increase ambient light

UNEVEN ILLUMINATION




Verify all LEDs are working and not covered

LOW CONTRAST



PATTERNED CONTACT LENS



Ask to remove, or do not acquire iris

Poster developed by NIST in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. The IREX Program (iris.nist.gov/irex) advances high performance iris recognition through standards development and testing.

APPENDIX D: FREQUENTLY ASKED QUESTIONS

What is the Iris Service?

The NGI Iris Service provides an iris image repository and features an iris search capability. The service enables authorized criminal justice agencies to submit a probe iris image for search and to receive an identification/non-identification response. The NGI Iris Service repository accepts iris images for enrollment, singularly or in bulk, that are obtained during booking, incarceration, or other criminal justice proceedings. Iris images submitted for retention must be associated with a tenprint and/or a UCN.

Why iris recognition?

Automated searches using iris recognition are accurate, contactless, efficient and fast. The iris contains a specific pattern of ridges and folds that are unique to an individual. Agencies are leveraging the NGI Iris Service to improve officer safety, ensure wanted subjects in custody are not erroneously released, and share information in cooperation with federal, state, local, and tribal organizations.

Who can enroll iris images and/or search iris images?

Criminal justice agencies engaged in the administration of criminal justice information.

28 Code of Federal Regulations (CFR) 20.3(b) defines the administration of criminal justice as the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

28 CFR 20.3(g) defines criminal justice agencies as courts or a governmental agency or subunit thereof that performs the administration of criminal justice pursuant to statute or executive order, and that allocates a substantial portion of its annual budget to the administration of criminal justice.

Can a regular camera be used to capture an iris image?

No. The camera must be specifically designed to capture irises for use in automated iris recognition systems. Standard iris cameras use a near-infrared light to capture a more useful iris image across a broad range of actual iris colors. Testing has shown that near-infrared images are required to obtain high accuracy rates.

What are the technical requirements to access this service?

Authorized criminal justice agencies may work with their current service provider to program their systems to handle the TOTs that will be specified in *EBTS Version 11*, for iris biometric enrollment. Agencies intending to utilize the NGI Iris Service must upgrade their systems to generate the proper NGI Iris Service TOTs, connect to the CJIS WAN, and meet all requirements of the CJIS User Agreement and the CJIS Security Policy. Existing systems must generate transactions that comply with the *EBTS Version 11*.

Who do I contact for more information?

For additional information on the NGI Iris Service, please contact the FBI's CJIS Division, at 304-625-IRIS (4747).

Intentionally Left Blank



June 15, 2020

ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION (EBTS)

11.0 REDLINES

SECTION 1 – MESSAGE TO CJIS SYSTEMS OFFICERS, STATE IDENTIFICATION BUREAUS, AND OTHER INTERFACE AGENCIES.....	1-1
SECTION 2 – EBTS FUNCTIONAL CHANGES FOR 11.0.....	2-1
SECTION 3 – AGGREGATE LIST OF CHANGES.....	3-1

SECTION 1 – MESSAGE TO CJIS SYSTEMS OFFICERS, STATE IDENTIFICATION BUREAUS, AND OTHER INTERFACE AGENCIES

The purpose of this document is to identify changes for the Electronic Biometric Transmission Specification (EBTS) version 11.0 with redlines for user clarity. This and all previous **versions of the EBTSs** and associated Technical and Operational Updates (TOUs) can be located at <<https://www.fbibiospecs.cjis.gov>>. The full text of the EBTS version 11.0 is identified through Sentinel Case Number 242-HQ-A6687913-SYSDOCU.

EBTS version 11.0 officially introduces the addition of the iris biometric within the Next Generation Identification (NGI) System. NGI iris deployment is preceded by demonstrated success of the FBI Iris Pilot, endorsement from the FBI CJIS Division Advisory Policy Board, and approval from the FBI Director. Pertinent NGI modifications include changes to existing transactions, for example CAR and FIS, which now allow for enrollment of a subject's iris biometrics in addition to fingerprints, palms, and face images. Of additional significance is the deployment of the new Iris Image Identification Submission (IIDS) transaction. Just as it did in the FBI Iris Pilot, the IIDS transaction provides an easy, rapid, and contactless method of subject identification as the NGI response to the IIDS will provide either an identification or non-identification response. While use cases of iris are numerous for various law enforcement operational scenarios, it proved especially beneficial as a quick, easy, and contactless method of subject identification prior to release from correctional facilities. For additional benefits and information pertaining to the NGI iris services please review the NGI Iris Service Policy and Implementation Guide as well as Appendix S of this document. Additional information pertaining to the NGI Iris Service Policy and Implementation Guide can be located at: <<https://www.fbibiospecs.cjis.gov/Iris>>.

* * * * *

Users are reminded that any questions concerning the distribution of EBTS 11.0 should be directed to the Programs Research and Standards Unit at <<https://www.fbibiospecs.cjis.gov/Comments/Comments>>.

Archived and Active versions of the EBTS and associated TOUs are available via the Internet on the FBI Biospecs Web site at <<http://www.fbibiospecs.cjis.gov>>.

* * * * *

SECTION 2 – FUNCTIONAL CHANGES FOR 11.0

Section 2 contains information concerning the modifications constituting EBTS 11.0. The following table is an overview of the functional modifications for this EBTS version.

Section	Change
Throughout	Grammar, punctuation, and minor style updates
	“Table” and table numbers removed from table titles
Change History	Removed references to EBTS 10 and associated TOUs. Archived versions of the EBTS and its TOUs are available via the internet on the FBI Biospecs web site at www.fbibiospecs.cjis.gov .
1.9 Specific Changes to this Version	Removed references to past EBTS changes Updated section with EBTS 11 information
3.1.1.1 CAR	Updated first paragraph
3.1.1.2 CNA	Updated first paragraph
3.1.1.9 FIDR	Updated first paragraph
3.1.1.22 ERRT	Section moved to 3.7.6 ERRT Removed (Future Capability) from title
3.1.5 Iris Identification Search Submission	Removed (Future Capability) from title
3.1.5.1 IIDS	Removed (Future Capability) from title
	Removed last paragraph
3.1.5.2 IIDS - SRE	Section added
3.3.1.1 IRQ	Added “10. Iris Images” to list
3.3.2.3 ERRI	Section moved to 3.7.3 ERRI
3.4.5 Iris Image Investigation Search Submission	Section removed
3.4.5.1 IIS	Section removed
3.4.6 Biometric Investigation Submission	Section and subsections renumber to 3.4.5
3.4.6.3 EQER	Section moved to 3.7.7 EQER
3.4.6.4 EQRR	Renumbered to 3.4.5.3 EQRR
3.4.6.5 ERRR	Section moved to 3.7.5 ERRR
3.6.15 SPMT	Removed “Tier 2” from first paragraph
3.6.20 RBSCVL	Updated first paragraph
3.7 Error Message Format	Added 3.7.1 ERRA, 3.7.2 ERRB, 3.7.3 ERRI, 3.7.4 ERRL, 3.7.5 ERRR, 3.7.6 ERRT, and 3.7.7 EQER

SECTION 2 – EBTS FUNCTIONAL CHANGES

Section	Change
Appendix A	Added Iris Image Identification Submission to the A-1 NGI Maximum Transaction Response Time Table
	Removed “Future Capability” from Iris Image Identification Search (IIDS) in the A-2 NGI Type of Transaction By Service Table
	Removed Iris Image Investigation Search (IIS) from the A-2 NGI Type of Transaction by Service Table
Appendix C	Updated 2.2028 BID
	Added SI to BID Submitted Values and Results Table
	Updated 2.2029 BSI
	Update 2.051 CSL
	Added 2.2105 FI
	Updated 2.062 IMT Table
	Added note to 2.017 MNU and updated MNU Value Table
	Updated header in 2.065 RBC Values Table
	Updated 2.2040 RBT Values Table
	Updated 2.059 SRF Values Table
	Updated Code 2 of 2.2046 TLI Values Table
	Added Limited Sharing – Not Foreign Dissemination - Code 4 and Federal Sharing – Code 5 to 2.2046 TLI Values Table
Added 2.2105 FI to C-1 Field Edit Specifications for Type-2 Elements Table	
Appendix D	Updated 2.054 SSD, 2.055 SLE in D-1 Summary of Field Lists for Identification and Verification Transactions Table
	Added 2.2105 FI to D-1 Summary of Field Lists for Identification and Verification Transactions Table
	Added IIDS TOT to D-1 Summary of Field Lists for Identification and Verification Transactions Table
	Updated SRE TOT in D-1 Summary of Field Lists for Identification and Verification Transactions Table to include 2.088 NOT and 2.2024 SII
	Removed CSL note and updated remaining notes in Reference Notes
Appendix E	Updated 2.084 AMP fields in E-1 Summary of Field Lists for Investigation, Information, and Notification Transactions Table
	Added footnote to E-1 Summary of Field Lists for Investigation, Information, and Notification Transactions Table
Appendix F	Updated footnote for F-5 Mobile ID IQS Requirements Table
Appendix I	Updated 2.084 AMP, 2.009 OCA, and 2.055 SLE fields in I-1 Summary of Field Lists for Data Management Transactions Table
	Added footnote to I-1 Summary of Field Lists for Data Management Transactions Table
Appendix K	Added new fields 10.200 – 10.249 RSV to Type-10 Data Dictionary
	Added new fields 10.351 – 10.400 RSV to Type-10 Data Dictionary
Appendix L	Added 2.2105 FI to L-1 Complete Element Cross-Reference List by Tag Number Table

SECTION 2 – EBTS FUNCTIONAL CHANGES

Section	Change
	Added FBI allocated fields to L-1 Complete Element Cross-Reference List by Tag Number table
	Added Type-17 fields to L-1 Complete Element Cross-Reference List by Tag Number table
	Updated T17 values to DOCE, EMUF, FANC, FAUF, FNDR, NNDR, NFUE, NFUF, MAP, DEK, DEU, MPR, AMN, and FDSP in L-2 Record Set Requirements Summary by Type of Transaction table
	Removed (Future Capability) form IIDS transaction in L-2 Record Set Requirements Summary by Type of Transaction table
	Removed the IIDS transaction from L-2 Record Set Requirements Summary by Type of Transaction table
	Added Biometric Search Error to Identification Service Responses in L-3 Record Set Requirements Summary by Type of Response table
	Removed (Future Capability) form IIDS transaction in L-4 Transaction/Response/Error TOT Correspondence
	Removed the IIDS transaction from L-4 Transaction/Response/Error TOT Correspondence
	Added L-5 Record Type Fields Allocated by the FBI table
Appendix M	Added new codes IR001, IR002, IR003, IR004, IR005, IR006, IR007, IR008, IR009, IR010, IR011, IR012, IR013, IR014, IR015, IR016, IR017, IR018, IR019, and IR020 to M-1 Transaction Message table
	Updated and added corresponding footnote to L0008 to M-1 Transaction Message Table
	Removed footnote associated with L0008, L0116, L0117, and L0118 in M-1 Transaction Message table
	Added new codes L0062, L0183, L0185, L0186, L0187, L0188, L0189, and L0191 to M-1 Transaction Message table
	Removed messages M0011 from M-1 Transaction Message Table
	Updated M0012 from M-1 Transaction Message table
	Added new codes M0058, M0059, M0060, M0061, M0062, M0063, M0064, M0065, and M0066 to M-1 Transaction Message table
Appendix N	Added new fields 14.201 – 14.400 RSV to Type-14 Data Dictionary
Appendix R	Added new fields 13.200 – 13.400 RSV to Type-13 Data Dictionary
Appendix S	Added new appendix and Data Dictionary for Type-17
Appendix AC	Removed IIDS from acronyms list

Change History

1.9 Specific Changes to this Version

~~This version of the EBTS represents Full Operational Capability of the NGI system and includes the following list of new services (new/modified TOTs in parenthesis):~~

- ~~1. Face image searching (FRS, SRB, UBM, ERRB, UUBD)~~
- ~~2. Face and Scars, Marks and Tattoos (SMT) text based searching (TXTSRCH, SRB)~~
- ~~3. Rap Back services (RBSCRM, RBSCVL, RBSR, RBRN, RBMNT, RBMNTR, RBN, RBIHS, RBIHSR, RBRPT, RBRPTR)~~
- ~~4. Disposition Reporting Enhancements (FDSP, SRE, DSPE, DSPR, SRNRR)~~
- ~~5. Civil event maintenance (CDEL, CDELRL)~~
- ~~6. External system interoperability (XACT, XACTR, XMNT, XMNTR)~~
- ~~7. RISC repository (FIDR, SPMNT, SPMNTR, SPN)~~
- ~~8. Iris image searching (future capability) (IIDS, IIS, SRB)~~

~~In addition to the new capabilities, several existing TOTs were expanded to support biometric types other than friction ridge. These TOTs are:~~

- ~~• IRQ, IRR~~
- ~~• FIS, FISR~~
- ~~• BDEC, BDECR~~
- ~~• BDEL, BDELRL~~
- ~~• BATQ, BATR~~

~~Also, the existing SRE response is modified to include the Biometric Image Enrollment (2.2061 BIE) and Biometric Image Available (2.2031 BIA) fields to inform the user of which biometrics from their submission were successfully enrolled and what biometric types are available for the matched identity respectively. SRE is also modified to reflect Rap Back subscription information, when enrollment into Rap Back is requested within the tenprint fingerprint identification search request.~~

EBTS version 11.0 officially introduces the addition of the iris biometric within the Next Generation Identification (NGI) system. NGI iris deployment is preceded by demonstrated success of the FBI Iris Pilot, endorsement from the FBI CJIS Division Advisory Policy Board, and approval from the FBI Director. Pertinent NGI modifications include changes to existing transactions, for example CAR and FIS, which now allow for enrollment of a subject's iris biometrics in addition to fingerprints, palms, and face images. Of additional significance is the deployment of the new Iris Image Identification Submission (IIDS) transaction. Just as it did in the FBI Iris Pilot, the IIDS transaction provides an easy, rapid, and contactless method of subject identification as the NGI response to the IIDS will provide either an identification or non-identification response. While use cases of iris are numerous for various law enforcement operational scenarios, it proved especially beneficial as a quick, easy, and contactless method of subject identification prior to release from correctional facilities. For additional benefits and Information pertaining to the NGI iris services please review the NGI Iris Service Policy and Implementation Guide as well as Appendix S of this document. Additional information

pertaining to the NGI Iris Service Policy and Implementation Guide can be located at: <https://www.fbibiospecs.cjis.gov/Iris>.

3.1.1.1 Criminal Tenprint Submission (Answer Required) (CAR)

This transaction is a criminal arrest fingerprint submission for which the requester desires an identification decision response. It contains ten rolled and four plain impressions of all ten fingers, biographic descriptor data, as well as information relative to an arrest **and court disposition data. ~~eustody, or supervisory status~~**. The biographical data and fingerprint images are used to determine potential candidates with criminal records at the FBI/CJIS and a positive identification or non-identification **decision** is determined. A response is returned to the contributor. The **successful** response will ~~always~~ contain the positive identification/non-identification decision and may contain the electronic Identity History Summary, if requested.

[Unchanged text not included here for brevity]

3.1.1.2 Criminal Tenprint Submission (No Answer Required) (CNA)

This transaction differs from a CAR request only in that no identification decision response is sent. However, a communication protocol acknowledgment will be returned to the contributor to confirm receipt of the transaction. Like the CAR, it contains ten rolled and four plain impressions, ~~and~~ arrest, **and court disposition ~~eustody, or supervisory status~~** data. The Retention Code (2.005 RET) for this transaction must be set to “Y.”

3.1.1.9 Foreign Information Direct Route (FIDR)

This transaction consists of a fingerprint submission from a federal or international agency that will be directly routed to an FBI/CJIS internal log application for special processing. The submission shall contain ten rolled or flat and four plain impressions, or three identification flat impressions, along with biographic descriptor data. If the FIDR is successfully processed, a new identity will be created in the Foreign Subjects of Interest (FSI) repository. **For those submissions containing a Tier Level of 2 (Contact Information Only) in the 2.2046 TLI field, the 2.2072 POC field will be required on the submission.**

Note: FIDR is a limited-use TOT that requires coordination with FBI/CJIS prior to use.

3.1.1.22 Tenprint Transaction Error Response (ERRT) (Future Capability)

When a Tenprint Transaction Error Response (ERRT) is sent in response to an identification search submission, the Name (2.018 NAM) and Date of Birth (2.022 DOB) from the search submissions are returned as the Submitted Name (2.2008 SNAM) and Submitted Date of Birth (2.2007 SDOB), respectively. Error responses are listed in the Error Message Format Section (Section 3.7).

3.1.5 Iris Identification Search Submission ~~(Future Capability)~~

Iris Identification Search Submissions allow the user to submit ~~one or two iris images from an individual for a one-to-many identification search against the FBI/CJIS ~~Iris Identification File (IIF)~~ NGI Iris Repository ~~using an iris image as the search probe.~~~~

[Unchanged text not included here for brevity]

3.1.5.1 Iris Image Identification Submission (IIDS) ~~(Future Capability)~~

The Iris Image Identification Submission (IIDS) ~~requires two iris records. At least one record must contain an iris image. Iris images must be from the same individual. ~~transaction allows the user to submit the right or and left iris image for a given individual to be used for searching against the IIF NIRS for a possible match identification.~~~~ All searches of the ~~IIF~~ NGI Iris Repository are one-to-many searches. An IIDS that results in a score better than a predetermined match threshold is deemed ~~a match (i.e., a highly probable identification) an identification.~~ In the event of ~~a match~~ an identification, information pertaining to the matched individual is returned in an SRE transaction. ~~By default, IIDS searches that result in a match an identification do not return any iris images.~~ The optional Request Photo Record (2.096 RPR) field may be set to “Y” to request a front face image to be returned with the SRE for an identification. If the IIDS contains any errors, an ERRB is returned.

No data entry is necessary unless an iris cannot be imaged. Missing iris images require submission of a Damaged or Missing Eye (17.028 DME) code.

[Unchanged text not included here for brevity]

~~Iris image search functionality is currently in the pilot phase. Therefore the IIDS is a limited use TOT that requires coordination with the FBI/CJIS prior to use.~~

3.1.5.2 IIDS Submission Results (IIDS-SRE)

This transaction is returned by NGI in response to an IIDS. The SRE will contain an identification/non-identification decision. For submissions which result in an identification decision, the SRE will return the Master Name (2.018 NAM), Master FBI Number/UCN (2.014 FBI), Master State Identification Number (2.015 SID), Supplementary Identity Information (2.2023 SII) if available, and electronic Identity History Summary (2.075 ERS) if requested. Additionally, if the IIDS included a photo request and a photo is available for the identity, a front face image will be included in the identification response.

The Supplementary Identity Information (2.2023 SII) contains the results of an NCIC search using the FNU/UCN for the identity. The results include a list of identifiers and case numbers for each person file that contains the identity (e.g. Wants/Warrants, Sex Offenders, etc.). The SII contains caution and medical codes (e.g. armed and dangerous, seizures) and handling caveats for Known or Appropriately

Suspected Terrorists (KSTs) when available. The KST data will be returned in accordance with existing dissemination authorities. Additionally, if an active want/warrant is found, the offense (e.g. parole violation), original offense (e.g. assault), and wanting agency are included.

A non-identification response will return the submitted name and submitted SID. Non-identified iris images are not retained in the NGI system. For further information, please refer to the Identification Services section, Submission Results – Electronic (SRE) subsection.

Values of NAM, FBI Number/UCN and SID Returned in the SRE for IDS

Type of Submission	Result	Value of Returned Field			Special Exceptions
		Name	FBI Number/UCN	SID	
Iris Identification Search Submission	Ident	Master NAM	Master FBI Number/UCN	Master SID	SII if available
Iris Identification Search Submission	Non-Ident	NAM Submitted	None	Submitted SID	

3.2.2 Fingerprint Verification Response (SRE)

This transaction is returned by the FBI/CJIS in response to a Fingerprint Verification request. A Match response will be returned when the images on file for the submitted FBI Number/UCN (2.014 FBI) match the submitted images and will contain the electronic Identity History Summary (2.075 ERS), if requested. A No Match response will be returned when the images submitted do not match the images on file for the quoted UCN. **Table-3** The “Values of NAM, FBI Number/UCN and SID Returned in the SRE for FVR” table describes which NAM, FBI Number/UCN, and SID are returned in the SRE for the Fingerprint Verification request. For further information, please refer to the Identification Services section, Submission Results – Electronic (SRE) subsection.

3.3.1.1 Biometric Image/Feature Retrieval Request (IRQ)

[Unchanged text not included here for brevity]

This transaction enables users to retrieve images from the FBI/CJIS databases so a comparison can be made by the requester at user facilities. The requester identifies the subjects whose biometric images are being requested. The requester may also include additional parameters to specify particular modalities or image types of the subjects. Up to 1,000 subject records may be requested per transaction **in the Biometric Image Description (2.2028 BID) field**. Specific fingerprint, supplemental fingerprints, palm print images or the complete set may be requested. Other images, such as facial and SMT photos which are associated with the records, may also be requested. The transaction will be processed, and requested images on file at the FBI/CJIS will be transmitted in the response. Each subject record identifier number in the request and each set of biometrics

being returned for the subject will be addressed in a separate Image Request Response (IRR). **The default response condition in the IRR will return the representative biometric set(s) for the identity specified.**

Alternately, this transaction may be used to request images from external repositories. The Name of Designated Repository (2.098 NDR) field is added to IRQ where only a single external system value is valid. The ~~Biometric Image Description (2.2028 BID)~~ field information item UCN (2.2028A) has been changed to Subject Identifier (SI) in order to support external system identifiers.

[Unchanged text not included here for brevity]

The following biometric and descriptive record types may be retrieved:

1. Tenprint FP Images from an Event using the Biometric Set Identifier (2.2029 BSI)
2. Tenprint FP Features associated with a retrieved image
3. Palm Print Images from an Event using the Biometric Set Identifier (2.2029 BSI)
4. Palm Print Features associated with a retrieved image
5. Supplemental (joint and tip) Prints from an Event using the Biometric Set Identifier (2.2029 BSI)
6. Supplemental (joint and tip) Features associated with a retrieved image
7. Latent Friction Ridge images and associated Features
8. Facial Photos
9. SMT Photos
10. **Iris Images**

In order to support multiple biometric sets and multiple image types for an identity, ~~a new field,~~ the Biometric Image Description (2.2028 BID), has been created. If the ~~new~~ BID field is populated, then the FBI Number/UCN (2.014 FBI) and Finger Numbers Requested (2.057 FNR) fields will be ignored; therefore, UCN and FNR are optional. The BID field is a set type that allows users greater flexibility in defining what images are requested. Please see Appendix C, Type-2 Element Data Dictionary, for a full description of the use of BID.

[Unchanged text not included here for brevity]

3.3.1.3 Image Request Response (IRR)

This transaction is returned by the FBI/CJIS to provide requested images on file at the FBI/CJIS, or the specified external system, to the requester. Each image set identified in the IRQ request will cause a separate IRR response. The response will include either the subject record identifier number (2.014 FBI) or the External Subject Identifier (2.2037 ESI) and the requested image set in the format in which they were enrolled. **As noted in 3.3.1.1, the IRR default response condition will return the representative biometric set(s) for the identity specified, along with the associated biometric feature set, if requested.**

~~The IRR response will return one biometric image set, along with the associated biometric feature set, if requested.~~ The new Biometric Image Available (2.2031 BIA) field is added to reflect the biometric image types available for the Identity. The IMT field in the IRR corresponds to the IMT within the BID field in the request (for composite results, where no BSI is provided in the request) or is equivalent to the image type of the BSI requested (for event results, where BSI is included in the request). When a composite set is returned, no Biometric Set Identifier (2.2029 BSI) is returned in the message.

~~3.3.2.3 Information Transaction Error (ERRI)~~

~~If the requestor does not own any of the images selected by the Biometric Audit Trail Query (BATQ) request criteria, this will result in an Information Transaction Error (ERRI), including the reason for the error in the Status/Error Message (2.060 MSG) field. An ERRI is also generated if the submitted Biometric Set Identifier (2.2029 BSI) or Image Type (2.062 IMT) is not associated with the submitted FBI Number/UCN (2.014 FBI). Error responses are described in the Error Message Format Section (Section 3.7).~~

~~3.4.5 Iris Image Investigation Search Submission (Future Capability)~~

~~Iris Image Investigation Search Submissions allow the user to submit a one to many investigation search against the FBI/CJIS Iris Identification File (IF) using an Iris image as the search probe. As opposed to an identification search, the iris investigation search results consist of a list of candidates that must be adjudicated by the user.~~

~~The following TOT will be accepted by the FBI/CJIS for Iris Image Investigation Search Submissions:~~

~~TOT TRANSACTION~~
~~IIS Iris Image Investigation Search~~

~~The FBI/CJIS response to electronic submissions will provide search results or indicate an error via the following TOTs:~~

~~**TOT RESPONSE TRANSACTION**~~

~~SRB—Search Results—Biometric~~

~~ERRB—Biometric Search Error Response~~

~~Error messages are described in Section 3.7~~

~~**3.4.5.1 Iris Image Investigation Search (IIS) (Future Capability)**~~

~~The Iris Image Investigation Search (IIS) transaction allows the user to submit the right or left iris image for a given individual to be used for searching against the IIF for possible investigative leads. Such iris images may be extracted from a visible light facial photo obtained under less than ideal conditions, such as iris images from photos extracted from video surveillance footage.~~

~~Subsequently, images submitted with an IIS transaction are likely to be of relatively poor quality. All IIS searches of the IIF will be one to many investigative type searches. An IIS transaction will result in up to the 50 best scoring candidates returned in an SRB transaction. The enrolled iris image associated with each matched candidate will be returned. If the IIS contains any errors, an ERRB will be returned.~~

~~Iris image search functionality is currently in the pilot phase. Therefore, the IIS is a limited use TOT that requires coordination with FBI/CJIS prior to use.~~

~~**3.4.6 3.4.5 Biometric Investigation Submission**~~

~~[Unchanged text not included here for brevity]~~

~~**3.4.6.1 3.4.5.1 External Query History Request (EQHR)**~~

~~[Unchanged text not included here for brevity]~~

~~**3.4.6.2 3.4.5.2 External History Request Response (EHRR)**~~

~~[Unchanged text not included here for brevity]~~

~~**3.4.6.3 External Query History Error Response (EQER)**~~

~~When the External Query History Request contains errors, such as missing mandatory information~~

~~or invalid contents, the External Query Error Response (EQER) will be returned to the contributor. The response will include the Status/Error Message (2.060 MSG) field indicating the type(s) of error(s) encountered. See the Error Message Format Section for more detail on how this response is formatted (Appendix M).~~

3.4.6.4 3.4.5.3 External Query History Request Response - Summary (EQRR)

An External Query History Request Response – Summary (EQRR) will be returned as a summary report of the number of candidates returned from the search and the UCN of each candidate. The number of EHRR and ERRR messages returned for the search, up to 20, will be equal to the number of candidates stated in the EQRR message.

3.4.6.5 Transaction Error (Electronic Response) (ERRR)

~~When the result of the External Query History Request contains candidate(s) where the Identity History Summary is not available, the Transaction Error (Electronic Response) (ERRR) will be returned to the contributor. The ERRR will include a Status/Error Message (2.060 MSG) field indicating the status of the record. If the DOB in the EQHR is omitted or invalid, an ERRR indicating the error will be the only response. (See Section 3.7)~~

3.6.15 Special Repository Maintenance Request (SPMNT)

The Special Repository Maintenance Request (SPMNT) is used to manage identities within the Special Population Cognizant (SPC) and Foreign Subjects of Interest (FSI) repositories. Identities may be created within an SPC using the SPMNT with a Maintenance Action Indicator (2.2052 MAI) of “ADD”, while identities are created in the FSI using the FIDR TOT. SPC and FSI identities may be removed using SPMNT by supplying the FBI Number/UCN (2.014 FBI) of the identity and the Name of Designated Repository (2.098 NDR) with the “DELETE” MAI value. Values for Tier Level Indicator (2.2046) TLI, Hit Notification Indicator (2.2051 HNOTI), and/or ~~Tier-2~~ Point of Contact (2.2072 POC) may be updated for an FSI identity using SPMNT with the “REPLACE” MAI value, the UCN of the identity, and the new values to be applied to the identity.

3.6.20 Rap Back Subsequent Subscription Request – Civil (RBSCVL)

Any authorized agency may establish a Civil Rap Back Subscription by submitting a ~~civil~~-UCN (2.014 FBI) and either a full Tenprint Fingerprint image set or ~~an~~ the Event Identifier (2.2035 EVI) from a previously submitted Civil Tenprint Fingerprint Identification Search. A Subscription also requires the Name (2.018 NAM), Date of Birth (2.022 DOB) of the Subscription subject, and the Subscription Rap Back Category (2.2065 RBC). Allowable Civil Rap Back Categories are as follows:

3.7 Error Message Format

When a transmission is rejected because one or more data fields ~~does~~ do not pass internal editing criteria, an error response will be transmitted back to the submitting agency. Each reason for rejection will be detailed in the Status/Error Message (2.060 MSG) field. Up to 11 errors for a transaction can be recorded in the MSG field. If the error is related to a field that contains invalid data, the field tag and first 30 characters of the data in the invalid field will be returned.

The FBI/CJIS will validate all incoming data prior to its use within the system. If any mandatory **data fields are missing or incorrect**, the transaction will be rejected. If any optional data are in error, the data will not be stored in the FBI/CJIS repository.

The error response will be included in the appropriate error transaction. The following is a non-exhaustive list of the types of error messages:

- Mandatory field missing
- Invalid field for transaction
- Field discrepancy
- Field out of range
- Request not on file
- Fingerprints do not allow extraction of characteristics
- Non-standard native-mode fingerprint characteristics
- Inadequate quality of biometrics

3.7.1 Administrative Transaction Error Response (ERRA)

When any permission or processing error is present in a data management transaction, the Administrative Transaction Error Response (ERRA) will be transmitted back to the submitting agency. Each reason for rejection will be detailed in the Status/Error Message (2.060 MSG) field. Up to 11 errors for a transaction can be recorded in the MSG field.

ERRA Transaction

Error Transaction	Error TOT	Generating TOT
Administration Transaction Error Response	ERRA	LRSQ
		FIS
		BDEL
		CDEL
		BDEC
		DSPE
		SPMNT
		RBSCRM

		RBSCVL
		RBMNT
		XMNT
		XACT
		SRNR

3.7.2 Biometric Search Error Response (ERRB)

NGI returns a Biometric Search Error Response (ERRB) to the submitting agency when a transaction is rejected due to one or more data fields not passing internal editing criteria. Each reason for rejection will be detailed in the Status/Error Message (2.060 MSG) field. Up to 11 errors for a transaction can be recorded in the MSG field. If the error is related to a field that contains invalid data, the field tag and first 30 characters of the data in the invalid field will be returned.

ERRB Transaction

Error Transaction	Error TOT	Generating TOT
Biometric Search Error Response	ERRB	IIDS
		FRS
		TXTSRCH

3.7.3 Information Transaction Error Response (ERRI)

If an information service transaction contains any invalid field values or is missing any required fields, an Information Transaction Error (ERRI) will be returned, including the reason for the return in the Status/Error Message (2.060 MSG) field. Errors associated with individual subject identifier numbers, such as an image set not being on file, will be reported in the MSG field of the Image Summary Response (ISR).

ERRI Transaction

Error Transaction	Error TOT	Generating TOT
Information Transaction Error Response	ERRI	IRQ
		CPR
		BATQ
		RBRPT
		RBIHS

3.7.4 Latent Transaction Error Response (ERRL)

If a latent friction ridge transaction contains any invalid field values or is missing any required fields, an Information Transaction Error (ERRL) will be returned, including the reason for the return in the Status/Error Message (2.060 MSG) field.

ERRL Transaction

Error Transaction	Error TOT	Generating TOT
Latent Transaction Error Response	ERRL	LFIS
		LFFS
		LPNQ
		ULD

3.7.5 Transaction Error (Electronic Response) (ERRR)

When the result of the External Query History Request contains candidate(s) where the Identity History Summary is not available, the Transaction Error (Electronic Response) (ERRR) will be returned to the contributor. The ERRR will include a Status/Error Message (2.060 MSG) field indicating the status of the record. If the DOB in the EQHR is omitted or invalid, an ERRR indicating the error will be the only response.

ERRR Transaction

Error Transaction	Error TOT	Generating TOT
Transaction Error (Electronic Response)	ERRR	EQHR

3.7.6 Tenprint Transaction Error Response (ERRT)

When a tenprint identification search submission is rejected, a Tenprint Transaction Error Response (ERRT) will be returned to the submitting agency. The ERRT will include the Name (2.018 NAM) and Date of Birth (2.022 DOB) from the search submissions as the Submitted Name (2.2008 SNAM) and Submitted Date of Birth (2.2007 SDOB), respectively.

ERRT Transaction

Error Transaction	Error TOT	Generating TOT
Tenprint Transaction Error Response	ERRT	CAR
		CNA
		CPDR
		CPNU
		DOCE

		EMUF
		FANC
		FAUF
		FNDR
		NNDR
		NFUE
		NFUF
		MAP
		DEK
		DEU
		MPR
		AMN
		RPIS
		FIDR
		FDSP
		FVR
		TPIS
		TPRS

3.7.7 External Query History Error Response (EQER)

When the EQHR contains errors, such as missing mandatory information or invalid contents, the External Query Error Response (EQER) will be returned to the contributor. The response will include the Status/Error Message (2.060 MSG) field indicating the type(s) of error(s) encountered.

EQER Transaction

Error Transaction	Error TOT	Generating TOT
External Query History Error Response	EQER	EQHR

The field requirements for these error messages are detailed in Tables D-1, E-1 and I-1.

Appendix M contains further details on contents of the Status/Error (2.060 MSG) field for error conditions.

SECTION 2 – EBTS FUNCTIONAL CHANGES

[Unchanged text not included here for brevity]

Appendix A: Transaction Response Times

A-1 NGI Maximum Transaction Response Times

Transaction	Priority	10 sec	20 sec	30 sec	2 min	5 min	10 min	15 min	30 min	1 hour	2 hours	4 hours	24 hours	48 hours	15 days
[Unchanged text not included here for brevity]															
Iris Image Identification Submission								.							
[Unchanged text not included here for brevity]															

A-2 NGI Type of Transaction By Service

SERVICE	TRANSACTION	TOT	DESCRIPTION
[Unchanged text not included here for brevity]			
Identification Services	Iris Image Identification Search (Future Capability)	IIDS	Iris Image Identification Submission
[Unchanged text not included here for brevity]			
Investigation Services	Iris Image Investigation Search (Future Capability)	IIS	Iris Image Investigative Search
[Unchanged text not included here for brevity]			

Appendix C: Descriptors and Field Edit Specifications for Type-2 Logical Records

BID 2.2028 Biometric Image Description

[Unchanged text not included here for brevity]

The SMT (2.2028G) information item holds the NCIC designation code for a scar, mark, or tattoo. The SMT is required when an SMT image is to be retrieved. If the BSI (2.2028C) information item is not present, the representative biometric set(s) are retrieved for the identity specified in the Subject Identifier (SI) item. The representative set for fingerprints will be a composite fingerprint set of images, while the **representative set of any additional biometrics (i.e., supplemental fingerprint, palm print, face image, iris set)** ~~representative set of palm prints or supplemental fingerprint and palm print iris set~~ will be the latest set enrolled.

[Unchanged text not included here for brevity]

BID Submitted Values and Results

BID Field Values Submitted	Biometric Images Returned
SI	Composite fingerprint set for the identity specified
SI, IMT	Representative set for image type specified
SI, BSI	Specific image set indicated by the BSI
SI, IMT, FNR	The friction ridge position image of the representative set for the image type specified
SI, BSI, FNR	The finger position image of the specific image set indicated by the BSI

BSI 2.2029 Biometric Set Identifier

This numeric field will uniquely identify each biometric image set or photo, such as a facial photo, a fingerprint set, a palm print set, ~~or~~ a supplemental print set **or iris set**.

CSL 2.051 Court Segment Literal

[Unchanged text not included here for brevity]

When submitting a custody **data in the Supervised Release Notification Request (SRNR) tenprint**, use this field for custody information. In the event that there is no arrest information available when submitting a custody **data tenprint**, the COL and CDD must be copied to the corresponding AOL and DOO fields of the Arrest Segment Literal (ASL), ~~which are is mandatory in all criminal tenprint submissions.~~

[Unchanged text not included here for brevity]

FI 2.2105 Foreign Information

This field contains descriptive data related to the collection of the fingerprint capture for the FIDR TOT. The field may contain alphanumeric and special characters with a limit of 300 characters.

IMT 2.062 Image Type

[Unchanged text not included here for brevity]

IMT Values

Image Type	Value
<i>[Unchanged text not included here for brevity]</i>	
Iris (Future)	11
Fingerprints on Front of Palm Card (Future)	12
<i>[Unchanged text not included here for brevity]</i>	

MNU 2.017 Miscellaneous Identification Number

[Unchanged text not included here for brevity]

NOTE: For all U.S. Military personnel (as their Identifying Agency), the 10-digit U.S. Department of Defense Identification Number on the service member’s Identification Card or Common Access Card (CAC) will be the primary number used as one of the MNU’s. (Ex: U.S. Army, AS-0000000000).

MNU Values

Identifying Agency	Code
Air Force Serial Number , Air Force Reserve, Air National Guard	AF
Non-Immigrant Admission Number	AN
Alien Registration Number	AR
Air National Guard Serial Number , U.S. Army Serial Number , Army Reserve, Army National Guard Serial Number	AS

SECTION 2 – EBTS FUNCTIONAL CHANGES

Bureau Fugitive Index Number	BF
Canadian Social Insurance Number	CI
U. S. Coast Guard Serial Number, Coast Guard Reserve	CG
Fingerprint Identification Number (DHS only)	FN
Identification Order Number	IO
U.S. Marine Corps Serial Number, Marine Corps Reserve	MC
Mariner's Document or Identification Number	MD
RCMP Identification or Fingerprint Section Number	MP
National Agency Case Number	NA
U.S. Navy Serial Number, Navy Reserve	NS
Originating Agency Police or Identification Number	OA
Personal Identification Number (State Issued Only)	PI
Passport Number (U.S. Only)	PP
Port Security Card Number	PS
Selective Service Number	SS
Veterans Administration Claim Number	VA

RBC 2.2065 Rap Back Category

[Unchanged text not included here for brevity]

RBC Values

Rap Back Category	Category Code	Purpose Code
<i>[Unchanged text not included here for brevity]</i>		

RBT 2.2040 Rap Back Trigger

[Unchanged text not included here for brevity]

RBT Values

RBT Code Value	Format Description
1	Criminal Retain Submission
2	Dispositions
3	Civil Retain Submission
4	Expungement/Partial Expungement
5	Want Addition
6	Want Deletion
7	Want Modification
8	Sexual Offender Registry Addition
9	Sexual Offender Registry Deletion

SECTION 2 – EBTS FUNCTIONAL CHANGES

10	Sexual Offender Registry Modification
11	External
12	Death Notices with Fingerprints
13	Death Notices without Fingerprints
13 14-40	Reserved for FBI Future Use

SRF 2.059 Search Results Findings

[Unchanged text not included here for brevity]

SRF Values

Value	Definition	TOT
C	Inconclusive	BDEC, LSR
D	Deferred for manual processing	FDSP-SRE
G	Green - No Hit	RPISR
I	Identification	BDEC, LSR, IDSS-SRE , SRE
M	Match of Images Submitted	FVR-SRE
N	Non-Identification	BDEC, LSR, IDSS-SRE , SRE
P	Pending Verification of Identification	BDEC, LSR
R	Red - Hit on Potential Candidate, High Confidence Match	RPISR, UHN
Y	Yellow - Probable Candidate, Potential Match	RPISR, UHN, BDEC
X	Not a Match of Images Submitted	FVR-SRE
Z	Disposition posted but no biometric search was performed.	FDSP-SRE

TLI 2.2046 Tier Level Indicator

[Unchanged text not included here for brevity]

TLI Values

Definition	Code
Share ALL	1
Share POC (ATN) Limited Sharing	2
Silent Hit	3
Limited Sharing – Not Foreign Dissemination	4
Federal Sharing	5

Appendix C: Descriptors And Field Edit Specifications For Type-2 Logical Records

[Unchanged text not included here for brevity]

SECTION 2 – EBTS FUNCTIONAL CHANGES

Table C-1 Field Edit Specifications for Type-2 Elements

Field Number	Identifier	Field Name	Character	Field Size		Occurrences		Example	Comments/Special Characters
				(not including Character Separators)		Min ¹	Max		
				Min	Max				
<i>[Unchanged text not included here for brevity]</i>									
2.2030	PPD	PRINT POSITION DESCRIPTOR	SET				+10	2.2030:02{US}FV1{GS}	
A	FGP	FRICTION RIDGE GENERALIZED POSITION	N	1	2	1	1		
B	FIC	FFFINGER IMAGE OCDE	AN	3	3	1	1		
2.2105	FI	FOREIGN INFORMATION	ANS	1	300		999	2.2105:CAPTURED DURING RAID{GS}	

Appendix D: Summary of Logical Record Layouts for Type-2 Identification and Verification Transactions

[Unchanged text not included here for brevity]

SECTION 2 – EBTS FUNCTIONAL CHANGES

Table D-1 Summary of Field Lists for Identification and Verification Transactions
(Minimum/Maximum Occurrences of Each Element for Each Logical Record Type)

Tag Elem	AMN	CAR	CNA	CPDR	CPNU	DEK	DEU	DOCE	EMUF	ERRT	FANC	FAUF	FDSP	FIDR	FNDR	FVR
<i>[Unchanged text not included here for brevity]</i>																
2.054 SSD		0..1	0..1	0..1	0..1											
2.055 SLE		0..1 ⁹	0..1 ⁹	0..1 ⁹	0..1 ⁹											
<i>[Unchanged text not included here for brevity]</i>																
2.2105 FI														0..999		

Tag Elem	IIDS
2.001 LEN	1
2.002 IDC	1
2.006 ATN	0..1
2.007 SCO	0..9
2.009 OCA	0..1
2.014 FBI	0..1
2.015 SID	0..1
2.017 MNU	0..4
2.018 NAM	0..1
2.070 RAP	0..1
2.073 CRI	1..3
2.096 RPR	0..1

Tag Elem	SRE
2.088 NOT	0..1
2.2023 SII	0..1

Appendix D – Reference Notes

1. For this transaction, this field must contain a ‘Y’.
2. The DOO portion of this field is optional, but should be provided if known. ASL is required when the submission contains a RET = ‘Y’.
3. This field is mandatory for applicant submissions from DIS and OPM.
4. It is obviously not expected that full Name and Date of Birth of Unknown Deceased and Amnesia victims will be known. These fields, however, must be submitted with formatted information.
5. FBI number must be present if known for inquiry prints.
6. Field is mandatory if fingerprint submission is from an NFF State.
7. This field is mandatory if any finger is either amputated or a rolled impression was not made.
8. An UCN may be returned depending upon transaction results. No FBI number is returned when none is assigned (e.g., Non-Identification with RET = ‘N’). UCN will be returned for any submission resulting in an Identification against the Criminal File or when a Non-Identification results in an add to the Criminal File or Civil file.
9. This field will be returned in the response if subject identification is made.
10. Field is optional unless Identification has been made and subject criminal history was requested in submission.
11. CDD and CCT are mandatory fields for this TOT.

[Unchanged text not included here for brevity]

Appendix E: Summary of Logical Record Layouts for Type-2 Investigation, Information, And Notification Transactions

[Unchanged text not included here for brevity]

SECTION 2 – EBTS FUNCTIONAL CHANGES

Table E-1 Summary of Field Lists for Investigation, Information, and Notification Transactions

Tag Elem	RBRPTR	SPN	SRB	SRL	SRT	TPIS	TPRS	TPRR	TXTSRCH	UBM	UHN	ULM	UUBD	UULD
<i>[Unchanged text not included here for brevity]</i>														
2.084 AMP		0..13			0..13	0..13 ²	0.13 ²					0..13		
<i>[Unchanged text not included here for brevity]</i>														

¹The number of candidates returned may be less than the maximum specified as a result of thresholds determined by trade study tests and the algorithm used to determine potential matches.

² This field is mandatory if any finger is either amputated or a rolled impression was not made.

Appendix F: FBI/CJIS Image Quality Specifications

[Unchanged text not included here for brevity]

F-5 Mobile ID IQS Requirements

Fingerprint Acquisition Profile (FAP)	Minimum Image Dimensions (WxH in inches)	IQS Specification Requirements	Simultaneous # of Fingers
10	0.5 x 0.65	PIV	1
20	0.6 x 0.8	PIV	1
30	0.8 x 1.0	PIV	1
40	1.6 x 1.5	PIV	1-2
45	1.6 x 1.5	App F	1-2
50	3.2 x 2.0	App F	1-4
60	3.2 x 3.0	App F	1-4

NOTE: Although the RISC will accept submissions from Mobile Fingerprint Scanners that do not meet these requirements, the FBI/CJIS Division reserves the right to enforce these, or any other, scanner requirements deemed necessary to meet accuracy levels established by the FBI/CJIS Division’s Advisory Policy Board. NGI RISC participants should refer to the FBI/CJIS Biometric Specification (<https://www.fbibiospecs.cjis.gov>) ~~IAFIS~~ Certified Products List/Mobile ID Category for a list of mobile identification devices which have been certified by the FBI/CJIS as tested and in compliance with the FBI/CJIS’s Next Generation Identification (NGI) initiatives and ~~Integrated Automated Fingerprint Identification System (IAFIS)~~ Image Quality Specifications (IQS). The certification process is not intended to endorse one product over a competitor’s product but merely to certify that the product meets FBI/CJIS standards and that, between two products that meet FBI/CJIS standards, the FBI/CJIS does not recommend one over the other.

[Unchanged text not included here for brevity]

Appendix I: Summary of Logical Record Layouts For Type-2 Data Management Transactions

[Unchanged text not included here for brevity]

SECTION 2 – EBTS FUNCTIONAL CHANGES

I-1 Summary of Field Lists for Data Management Transactions
(Minimum/Maximum Occurrences of Each Element for Each Logical Record Type)

Tag Element	BDEC	BDECR	BDEL	BDELR	CDEL	CDELR	CPD	DSPE	DSPR	ERRA	FIS	FISR	PDR	RBSCRM	RBSCVL
<i>[Unchanged text not included here for brevity]</i>															
2.084 AMP											0..13 ³				0..13 ³
<i>[Unchanged text not included here for brevity]</i>															

³This Field is mandatory if any finger is either amputated or a rolled impression was not made.

Tag Element	RBSR	RBMNT	RBMNTR	SPMNT	SPMNTR	SRNR	SRNRR	ULD	ULDR	XACT	XACTR	XMNT	XMNTR
<i>[Unchanged text not included here for brevity]</i>													
2.009 OCA	0..1			0..1	0..1	0..1							
<i>[Unchanged text not included here for brevity]</i>													
2.055 SLE						0..1							
<i>[Unchanged text not included here for brevity]</i>													
2.084 AMP				0..13 ³									
<i>[Unchanged text not included here for brevity]</i>													

[Unchanged text not included here for brevity]

³This Field is mandatory if any finger is either amputated or a rolled impression was not made.

Appendix K: Descriptors And Field Edit Specifications For Type-10 Logical Records

Type-10 Data Dictionary

[Unchanged text not included here for brevity]

RSV 10.200 – 10.249 Reserved For Future Use

Reserved

RSV 10.351 – 10.400 Reserved For Future Use

Reserved

Appendix L: Summary Tables

[Unchanged text not included here for brevity]

L-1 Complete Element Cross-Reference List by Tag Number

EBTS Tag Number	Element ID	Element Name
2.0001 – 2.0099	RSV	FBI USE
2.0100 – 2.0208	RSV	CA USE
2.0210 – 2.0234	RSV	MA USE
2.0235 – 2.0269	RSV	PA USE
2.0300 – 2.0309	RSV	CA USE
2.0310 – 2.0379	RSV	IL USE
2.0380 – 2.0399	RSV	KING CO, WA USE
2.0400 – 2.0409	RSV	CA USE
2.0410 – 2.0460	RSV	TX USE
2.0475 – 2.0530	RSV	WESTERN IDENTIFICATION NETWORK USE
2.0531 – 2.0542	RSV	NC USE
2.0550 – 2.0589	RSV	FL USE
2.0590 – 2.0609	RSV	WESTERN IDENTIFICATION NETWORK USE
2.0610 – 2.0650	RSV	VA USE
2.0700 – 2.0750	RSV	ME USE
2.0700 – 2.0750	RSV	LA USE
2.0751 – 2.0799	RSV	WASHINGTON STATE POLICE USE
2.0800 – 2.0899	RSV	ROYAL CANADIAN MOUNTED POLICE USE
2.0900 – 2.0999	RSV	WESTERN IDENTIFICATION NETWORK USE
2.1000 – 2.1099	RSV	NY USE
2.1100 – 2.1399	RSV	DEPARTMENT OF DEFENSE USE
2.1400 – 2.1499	RSV	NIST – OLES – LITS STANDARD
2.2000 – 2.7999	RSV	FBI USE

SECTION 2 – EBTS FUNCTIONAL CHANGES

2.8000 – 2.999	RSV	DEPARTMENT OF DEFENSE USE
2.2105	FI	FOREIGN INFORMATION
10.200 – 10.249	RSV	RESERVED FOR FUTURE USE
10.250 – 10.349	UDF	USER DEFINED FIELDS
10.351 – 10.400	RSV	RESERVED FOR FUTURE USE
10.401 – 10.900	UDF	USER DEFINED FIELDS
13.200 – 13.400	RSV	RESERVED FOR FUTURE USE
13.401 – 13.900	UDF	USER DEFINED FIELDS
14.201 – 14.400	RSV	RESERVED FOR FUTURE USE
14.401 – 14.900	UDF	USER DEFINED FIELDS
15.201 – 15.400	RSV	RESERVED FOR FUTURE USE
15.401 – 15.900	UDF	USER DEFINED FIELDS
16.200 – 16.400	RSV	RESERVED FOR FUTURE USE
17.001	LEN	LOCIGAL RECORD LENGTH
17.002	IDC	INFORMATION DESIGNATION CHARACTER
17.003	ELR	EYE LABEL
17.004	SRC	SOURCE AGENCY
17.005	ICD	IRIS CAPTURE DATE
17.006	HLL	HORIZONTAL LINE LENGTH
17.007	VLL	VERTICAL LINE LENGTH
17.008	SLC	SCALE UNITS
17.009	THPS	TRANSMITTED HORIZONTAL PIXEL SCALE
17.010	TVPS	TRANSMITTED VERTICAL PIXEL SCALE
17.011	CGA	COMPRESSION ALGORITHM
17.012	BPX	BITS PER PIXEL
17.013	CSP	COLOR SPACE
17.014	RAE	ROTATION ANGLE OF EYE
17.015	RAU	ROTATION UNCERTAINTY
17.016	IPC	IMAGE PROPERTY CODE
17.017	DUI	DEVICE UNIQUE IDENTIFER
17.019	MMS	MAKE/MODEL/SERIAL NUMBER
17.020	ECL	EYE COLOR
17.021	COM	COMMENT
17.025	EAS	EFFECTIVE ACQUISITION SPECTRUM
17.028	DME	DAMAGED OR MISSING EYE
17.031	IAP	SUBJECT ACQUISITION SPECTRUM
17.032	ISF	IRIS STORAGE FORMAT
17.200 – 17.400	RSV	RESERVED FOR FUTURE USE
17.999	DAT	DATA
18.200 – 18.400	RSV	RESERVED FOR FUTURE USE
19.200 – 19.400	RSV	RESERVED FOR FUTURE USE

SECTION 2 – EBTS FUNCTIONAL CHANGES

L-2 Record Set Requirements Summary by Type of Transaction

Transaction	Enrollment TOT	T1	T2	T4 ¹	T7	T9	T10	T13	T14 ³	T15 ²	T17 ²
Identification Service Transactions											
[Unchanged text not included here for brevity]											
DEPARTMENTAL ORDER CHANNELING ELECTRONIC	DOCE	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
ELECTRONIC IN/MANUAL OUT USER FEE	FMUF	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
FEDERAL APPLICANT (NO CHARGE)	FANC	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
FEDERAL APPLICANT USER FEE	FAUF	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
FEDERAL NO CHARGE DIRECT ROUTE	FNDR	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
NON-FEDERAL NO CHARGE DIRECT ROUTE	NNDR	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
NON-FEDERAL USER FEE EXPEDITE	NFUE	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
NON-FEDERAL APPLICANT USER FEE	NFUF	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
MISCELLANEOUS APPLICANT CIVIL	MAP	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
KNOWN DECEASED	DEK	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
UNKNOWN DECEASED	DEU	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
MISSING PERSON	MPR	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
AMNESIA VICTIM	AMN	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
[Unchanged text not included here for brevity]											
ELECTRONIC FINGERPRINT DISPOSITION SUBMISSION	FDSP	1	1	0-14	0-2	0	0	0	0-46	0-10	0-2
IRIS IMAGE IDENTIFICATION SEARCH (<i>FUTURE CAPABILITY</i>)	IIDS	1	1	0	0	0	0	0	0	0	2
[Unchanged text not included here for brevity]											
Investigation Search Transaction											
[Unchanged text not included here for brevity]											
<i>IRIS IMAGE INVESTIGATION SEARCH (FUTURE CAPABILITY)</i>	IIS	+	+	0	0	0	0	0	0	0	+
[Unchanged text not included here for brevity]											

SECTION 2 – EBTS FUNCTIONAL CHANGES

L-3 Record Set Requirements Summary by Type of Response

Transaction	TOT	T1	T2	T4*	T7	T9	T10	T13	T14*	T15**	T17**
Identification Service Responses											
RAPID FINGERPRINT IDENTIFICATION SEARCH RESPONSE	RPISR	1	1-2	0	0	0	0-2	0	0	0	0
SUBMISSION RESULTS - ELECTRONIC	SRE	1	1	0	0	0	0-1	0	0	0	0
LATENT SUBMISSION RESULTS	LSR	1	1	0	0	0	0	0	0	0	0
TENPRINT TRANSACTION ERROR	ERRT	1	1	0	0	0	0	0	0	0	0
BIOMETRIC SEARCH ERROR	ERRB	1	1	0	0	0	0	0	0	0	0

L-4 Transaction/Response/Error TOT Correspondence

Transaction	TOT	Response TOTs	Error TOTs
Identification Service Transactions			
[Unchanged text not included here for brevity]			
IRIS IMAGE IDENTIFICATION SEARCH- (FUTURE CAPABILITY)	IIDS	SRE	ERRB
[Unchanged text not included here for brevity]			
Identification Service Transactions			
[Unchanged text not included here for brevity]			
IRIS IMAGE INVESTIGATION SEARCH (FUTURE CAPABILITY)	IIS	SRB	ERRT
[Unchanged text not included here for brevity]			

SECTION 2 – EBTS FUNCTIONAL CHANGES

L-5 Record Type Fields Allocated by the FBI

Record Type Number	Fields Allocated by the FBI	Element ID	Element Name
Type-2 (NGI)	2.0001 – 2.0099	RSV	FBI USE
Type-2 (NGI)	2.0100 – 2.0208	RSV	CA USE
Type-2 (NGI)	2.0210 – 2.0234	RSV	MA USE
Type-2 (NGI)	2.0235 – 2.0269	RSV	PA USE
Type-2 (NGI)	2.0300 – 2.0309	RSV	CA USE
Type-2 (NGI)	2.0310 – 2.0379	RSV	IL USE
Type-2 (NGI)	2.0380 – 2.0399	RSV	KING CO, WA USE
Type-2 (NGI)	2.0400 – 2.0409	RSV	CA USE
Type-2 (NGI)	2.0410 – 2.0460	RSV	TX USE
Type-2 (NGI)	2.0475 – 2.0530	RSV	WESTERN IDENTIFICATION NETWORK USE
Type-2 (NGI)	2.0531 – 2.0542	RSV	NC USE
Type-2 (NGI)	2.0550 – 2.0589	RSV	FL USE
Type-2 (NGI)	2.0590 – 2.0609	RSV	WESTERN IDENTIFICATION NETWORK USE
Type-2 (NGI)	2.0610 – 2.0650	RSV	VA USE
Type-2 (NGI)	2.0700 – 2.0750	RSV	ME USE
Type-2 (NGI)	2.0700 – 2.0750	RSV	LA USE
Type-2 (NGI)	2.0751 – 2.0799	RSV	WASHINGTON STATE POLICE USE
Type-2 (NGI)	2.0800 – 2.0899	RSV	ROYAL CANADIAN MOUNTED POLICE USE
Type-2 (NGI)	2.0900 – 2.0999	RSV	WESTERN IDENTIFICATION NETWORK USE
Type-2 (NGI)	2.1000 – 2.1099	RSV	NY USE
Type-2 (NGI)	2.1100 – 2.1399	RSV	DEPARTMENT OF DEFENSE USE
Type-2 (NGI)	2.1400 – 2.1499	RSV	NIST – OLES – LITS STANDARD
Type-2 (NGI)	2.2000 – 2.7999	RSV	FBI USE
Type-2 (NGI)	2.8000 – 2.999	RSV	DEPARTMENT OF DEFENSE USE
Type-10 (Photo)	10.200 – 10.249	RSV	RERSERVED FOR FUTURE USE
Type-10 (Photo)	10.351 – 10.400	RSV	RERSERVED FOR FUTURE USE
Type-13 (Latent)	13.200 – 13.400	RSV	RERSERVED FOR FUTURE USE
Type-14 (Fingerprint)	14.200	ISC	IMAGE SOURCE CODE
Type-14 (Fingerprint)	14.201 – 14.400	RSV	RERSERVED FOR FUTURE USE
Type-15 (Palm)	15.200	ISC	IMAGE SOURCE CODE
Type-15 (Palm)	15.201 – 15.400	RSV	RERSERVED FOR FUTURE USE
Type-16 (Test)	16.200 – 16.400	RSV	RERSERVED FOR FUTURE USE
Type-17 (Iris)	17.200 – 17.400	RSV	RERSERVED FOR FUTURE USE
Type-18 (DNA)	18.200 – 18.400	RSV	RERSERVED FOR FUTURE USE
Type-19 (Foot)	19.200 – 19.400	RSV	RERSERVED FOR FUTURE USE

Appendix M: Transactions Messages

[Unchanged text not included here for brevity]

SECTION 2 – EBTS FUNCTIONAL CHANGES

M-1 Transaction Message

Code	Condition for Message	Description	Count	Insert #1	Insert #2	Insert #3
IR001	Mislabeled Images - Enrollment	The biometric image enrollment contains mislabeled images (ex. 2 right eyes). The iris images were not enrolled.				
IR002	Missing Type-17 - Enrollment	The biometric image enrollment requires 2 Type 17 records to be submitted. Only one was submitted.				
IR003	No Enrollment Images	The biometric image enrollment requires at least one iris image. No images were provided.				
IR004	Unable to Generate Templates - Enrollment	The submitted iris images were not enrolled. Templates could not be created for the submitted images.				
IR005	Unable to Template One Image - Enrollment	One of the submitted iris images was not enrolled. A template could not be created for image. %1 %2		ELR	Field Value	
IR006	Below Quality Threshold - Enrollment	The submitted iris images fail to meet NGI Minimum Iris Image Quality Standards and were not enrolled.				
IR007	Below Quality Threshold One Image - Enrollment	One of the submitted iris images fails to meet NGI Minimum Iris Image Quality Standards and was not enrolled. %1 %2		ELR	Field Value	
IR008	Invalid AUD - Enrollment	Could not enroll iris images. UCN %1 is not criminal.		UCN		
IR009	Missing Iris Image - Search	The biometric search contains only one iris image. %1 %2 did not contain an image. Search was performed using only one iris image.		ELR	Field Value	
IR010	No Search Images	The biometric search requires at least one iris image. No images were provided.				
IR011	Mislabeled Images - Search	The biometric search included mislabeled images (ex. 2 right eyes). Search was performed using the mislabeled images.				

SECTION 2 – EBTS FUNCTIONAL CHANGES

IR012	Unable to Generate Templates - Search	The biometric search was not performed. Templates could not be created for the submitted images.				
IR013	Unable to Template One Image - Search	One of the submitted iris images was not searched. A template could not be created for image. %1 %2		ELR	Field value	
IR014	Below Quality Threshold - Search	The submitted iris images fail to meet NGI Minimum Iris Image Quality Standards and were not searched.				
IR015	Below Quality Threshold One Image - Search	One of the submitted iris images fails to meet NGI Minimum Iris Image Quality Standards and was not included in the search. %1 %2		ELR	Field value	
IR016	Missing Iris Image – Enrollment	The biometric image enrollment contains only one iris image. %1 %2 did not contain an image.		ELR	Field value	
IR017	Manual Review - Search	The submitted search requires CJIS to adjudicate results.				
IR018	Non-Ident Quoted UCN	The submitted iris images identified to a different UCN than provided.				
IR019	Undefined Eye - Enrollment	The submitted iris images contain an undefined eye position (ELR). The biometric image enrollment must be a known eye position. The iris images were not enrolled.				
IR020	Deceased UCN - Search	The submitted search resulted in an identification to an identity that has been confirmed deceased by %1 on %2		ORI	DOD	
‡L0008	Characteristics quality low	The quality of the characteristics is too low to be used. ¹ The quality of the characteristics is too low to be used. Candidate(s) were found. Please resubmit a new set of fingerprints for comparison to the candidates(s). ²	0			
L0062	Reject Count Not Found	The element of %1 provided for reference in this maintenance request is not present in this record.	1	CCT #		

SECTION 2 – EBTS FUNCTIONAL CHANGES

‡L0116	Fingerprint Pattern Quality Error	Fingerprint pattern (s) not discernable	0			
‡L0117	Fingerprint Pattern Area Error	Insufficient pattern area(s) recorded for identification purposes	0			
‡L0118	ITN Image Quality/Sequence Error	Erroneous or incomplete fingerprint(s) on images, fingers or hands out of sequence, printed twice, missing, and not reason given.	0			
L0183	Mandatory UCN not provided on subsequent arrest submission from A-NFF state	Necessary to differentiate when ANFF states are not complying with the NFF Quals to provide UCN on 2nd or subsequent criminal submissions.	0			
L0185	Multiple Images	Rolled and/or plain fingerprint block(s) contain multiple images. See finger(s).	0			
L0186	Multiple Subject	Rolled and/or plain fingerprint image appears to be from multiple subjects. See finger(s).	0			
L0187	Invalid Plain Impressions	Plain impressions are not printed simultaneously and/or same hand printed twice in plains. See finger(s).	0			
L0188	Invalid Pattern Area	Fingerprint image contains shadowing/gray areas with ridge detail throughout or surrounding the pattern area. See finger(s).	0			
L0189	Invalid Pattern Area	Fingerprint image contains text and/or lines running through the pattern area. See finger(s).	0			
L0191	Non Visible Plains	Non Visible Plains Fingerprint images not visible/printed in the plain impression block(s). Unable to determine correct sequence. See finger(s) 0	0			
M0011	Biometric Sample Quality Below Threshold	The %1 biometric for UCN %2 fails to meet NGI Minimum Image Quality Standards and has not been enrolled	2	IMT	UCN	
M0012	Biometric Sample Failed Validation	The %1 biometric for UCN %2 has failed validation with Fingerprints on file and was not enrolled The palm print biometric for UCN %1 has failed segmentation or validation with fingerprints on file.	2	IMT	UCN	

SECTION 2 – EBTS FUNCTIONAL CHANGES

M0058	The palm print image is distorted/smeared/blurred	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) is distorted/smeared/blurred.	1	UCN		
M0059	The palm print image is a plain impression	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) is a plain impression.	1	UCN		
M0060	The palm print image(s) is mislabeled	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) is mislabeled.	1	UCN		
M0061	The palm print image is missing all fingers	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) is missing all fingers.	1	UCN		
M0062	The palm print image contains multiple/overlaid images	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) contains multiple/overlaid images.	1	UCN		
M0063	The palm print image contains insufficient ridge detail	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) contains insufficient ridge detail.	1	UCN		
M0064	The palm print images contain a scanning error	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) contains a scanning error.	1	UCN		
M0065	The palm print images contain white/gray/blank box	The palm print biometric for UCN %2 has failed segmentation or validation with fingerprints on file; The palm print image(s) contains white/gray/blank box.	1	UCN		

SECTION 2 – EBTS FUNCTIONAL CHANGES

M0066	The palm print images are associated with a Non-Ident/Non-Retain tenprint	The palm print biometric for UCN%2 is associated with a Non-Ident/Non-Retain tenprint and was not enrolled.	1	UCN		
-------	---	---	---	-----	--	--

[Unchanged text not included here for brevity]

* These error messages will include a formatted response reflecting “Candidates(s) were found. Please resubmit a new set of fingerprints for comparison to the candidate(s).” when a candidate was associated with the submission.

¹ A name check request should not be submitted

² A name check can be submitted after second submission

Appendix N: Descriptors And Field Edit Specifications For Type-14 Logical Records*[Unchanged text not included here for brevity]***Type-14 Data Dictionary***[Unchanged text not included here for brevity]***RSV 14.201 – 14.400 Reserved For Future Use**

Reserved

Appendix O: Place of Birth (POB) Code Table*[Unchanged text not included here for brevity]*

Table O-1 POB Code			
CODE	CTZ	DESCRIPTION	DATE AHEAD FLAG
BP	*	Bosnia (Herzegovenia , for Reference only)	
CK	*	Czechoslovakia	
FT		Eastern Shoshone Tribe WY	
FU		Ely Shoshone Tribe of NV	
FV		Paiute- Shoshone Tribe of the Fallon Rsvn and Colony, NV	
FW		Flandreau Santee Sioux Tribe of SD	
HC	*	Herzegovenia	
HN	*	New Hebrides (now Vanuatu)	
IZ		Kootenai Tribe of ID	
JX		Mississippi Band of Choctaw Indians	
KF		Nez Perce Tribe, ID (Frmrly Listed Nex Perce Tribe of ID)	
KQ		Ohkay Owingeh, NM (Formerly the Pueblo of San Juan)	
PC		Pitcairn, Henderson, Ducie, and Oeno Islands	
QV		Shoshone -Bannock Tribes of the Fort Hall Rsvn of ID	
QW		Shoshone -Paiute Tribes of the Duck Valley Rsvn of NV	
RX		Te-Moak Tribe of W. Shoshone Indians of NV	
SJ	*	South- West Africa (Namibia)	
UC		Turtle Mtn Band of Chippewa Indians of ND	
UI		Tunica -Biloxi Indian Tribe of LA	
UU		Wampanoag Tribe of Gay Head (Aquinnah) of MA	
VF		Yakama Nation, WA	
WM		Duckwater Shoshone Tribe of the Duckwater Rsvn, NV	

WP		Fort McDermitt Paiute & Shoshone Tribes of F.M. Indians Rsvn, NV & OR	
YZ		Northwestern Band of Shoshoni Nation of UT (Washakie)	

Appendix R: Descriptors And Field Edit Specifications For Type-13 Logical Records

[Unchanged text not included here for brevity]

Type-13 Data Dictionary

[Unchanged text not included here for brevity]

RSV 13.200 – 13.400 Reserved For Future Use

Reserved

Appendix S: Descriptors And Field Edit Specifications For Type-17 Logical Records

This appendix contains the descriptors and field specifications for Type-17 logical records, defined by ANSI/NIST-ITL, as iris image records.

Iris enrollment requires an iris set, defined as two Type-17 iris image records, be submitted with a CAR, FIS, CNA, CPNU, or CPDR transaction. For detailed information pertaining to the enrollment of iris images into the NGI, please review the NGI Iris Service Policy and Implementation Guide located at <<https://www.fbibiospecs.cjis.fbi/Iris>>.

Refer to the ANSI/NIST-ITL for complete usage and descriptions of the Type-17 fields. The Data Dictionary in this appendix has been organized to display Identifier, Field Number, Field Name, and Field Description.

Type-17 Data Dictionary

The Type-17 Data Dictionary only includes those fields that have been constrained by NGI/CJIS functionality. All other fields defined in the ANSI/NIST-ITL will be used as defined in that standard.

NGI/CJIS accepts two different configurations for the Type-17 record. One is used when an iris image is present and the other when an image is absent. The exact layout, including allowed fields can be found in table S-1 and S-2 of this appendix.

ELR 17.003 Eye Label

This field is mandatory for all iris transactions submitted to NGI for enrollment or search. For enrollment TOTs, (1) an ELR value of '0' for 'unknown' is not permissible, and (2) mislabeled iris

images (i.e. two right eyes) will cause the iris records to be rejected. For an IIDS with mislabeled iris images within the Type-17 records, the transaction will be processed but an error message will be returned along with the search response.

CGA 17.011 Compression Algorithm

This field is mandatory if an image is present in Field 17.999. It shall specify the algorithm used to compress the transmitted iris image. Permitted values for this field are “NONE”, “PNG”, “JP2”, and “JP2L”. Lossless compression or no compression is preferred to preserve image quality. Typically, image submissions use the PNG format.

Note that the baseline JPEG algorithm (*ISO/IEC 10918*) is not acceptable for iris images and shall not be used.

CSP 17.013 Color Space

This field is mandatory if an image is present in Field 17.999. The NGI/CJIS restricted value for Field 17.025 EAS is “NIR”; therefore this field is restricted to “GRAY”.

MMS 17.019 Make/Model/Serial Number

This field is mandatory if an image is present in Field 17.999. The MMS contains the make, model, and serial number for the capture devices. Each information item shall be 1 to 50 characters. Any or all information items may indicate that information is unknown with the value “0”.

ECL 17.020 Eye Color

This optional field is used to record the subject’s eye color as it appears in the image. Due to restrictions for fields 17.013 CSP and 17.025 EAS, which only permit gray scale iris images, the only NGI/CJIS acceptable value for ECL shall be “XXX.”

EAS 17.025 Effective Acquisition Spectrum

This optional field indicates the acquisition spectrum used in capturing the iris image. NGI/CJIS transactions are restricted to the “NIR” (near-infrared) value.

DME 17.028 Damaged or Missing Eye

This field is mandatory for all iris transactions submitted to NGI for enrollment or search when either the left or right iris image cannot be captured. Enrollment TOTs not following this requirement will be rejected. The IIDS TOT will still process, but an error message will be returned along with the search results. This field shall contain a code from the Missing and Damaged Eye Codes below. “UC” should be entered if the eye is physically present, but a usable iris image cannot be captured. An example is when the eye is swollen shut due to injury.

SECTION 2 – EBTS FUNCTIONAL CHANGES

Missing and Damaged Eye Code

Descriptor	Code
Missing or Artificial Eye	MA
Unable to Capture Image	UC

S-1 Iris Transaction with Image

Filed Number	Identifier	Field Name	EBTS Value Constraints	Min	Max
17.001	LEN	Logical Record Length		1	1
17.002	IDC	Information Designation Character		1	1
17.003	ELR	Eye Label	“1” or “2”	1	1
17.004	SRC	Source Agency		1	1
17.005	ICD	Iris Capture Date		1	1
17.006	HLL	Horizontal Line Length		1	1
17.007	VLL	Vertical Line Length		1	1
17.008	SLC	Scale Units		1	1
17.009	THPS	Transmitted Horizontal Pixel Scale		1	1
17.010	TVPS	Transmitted Vertical Pixel Scale		1	1
17.011	CGA	Compression Algorithm		1	1
17.012	BPX	Bits Per Pixel		1	1
17.013	CSP	Color Space	“GRAY”	1	1
17.014	RAE	Rotation Angle of Eye		0	1
17.015	RAU	Rotation Uncertainty		0	1
17.016	IPC	Image Property Code		0	1
a	IHO	Horizontal Orientation Code		1	1
b	IVO	Vertical Orientation Code		1	1
c	IST	Specific Scan Type		1	1
17.017	DUI	Device Unique Identifier		0	1
17.019	MMS	Make/Model/Serial Number		1	1
a	MAK	Make		1	1
b	MOD	Model		1	1
c	SER	Serial Number		1	1
17.020	ECL	Eye Color	“XXX”	0	1
17.021	COM	Comment		0	1
17.025	EAS	Effective Acquisition Spectrum	“NIR”	0	1
17.031	IAP	Subject Acquisition Profile - Iris		0	1
17.032	ISF	Iris Storage Format		0	1
17.999	DAT	Data		1	1

S-2 Iris Transaction without Image

Filed Number	Identifier	Field Name	EBTS Value Constraints	Min	Max
17.001	LEN	Logical Record Length		1	1
17.002	IDC	Information Designation Character		1	1
17.003	ELR	Eye Label	“1” or “2”	1	1
17.004	SRC	Source Agency		1	1
17.005	ICD	Iris Capture Date		1	1
17.017	DUI	Device Unique Identifier		0	1
17.019	MMS	Make/Model/Serial Number		0	1
a	MAK	Make		1	1

SECTION 2 – EBTS FUNCTIONAL CHANGES

b	MOD	Model		1	1
c	SER	Serial Number		1	1
17.021	COM	Comment		0	1
17.028	DME	Damaged or Missing Eye	“MA” or “UC”	1	1

Appendix AC: Acronyms

Acronym	Description
<i>[Unchanged text not included here for brevity]</i>	
IIS	Iris Image Investigation Search
<i>[Unchanged text not included here for brevity]</i>	

SECTION 3 – AGGREGATE LIST OF CHANGES

Section 3 – Aggregate List of Changes

This section records the changes made for EBTS 11.0.

EBTS	Date
11.0	6/15/20

Section	TOU Number	Change
1.9 Specific Changes to this Version	11.0	Removed references to previous versions of the EBTS
3.1.1.1 CAR		Updated first paragraph
3.1.1.2 CNA		Updated first paragraph
3.1.1.9 FIDR		Updated first paragraph
3.1.1.22 ERRT		Section moved to 3.7.6 ERRT
3.1.5 Iris Identification Search Submission		Removed (Future Capability) from title
3.1.5.1 IIDS		Removed (Future Capability) from title
3.1.5.2 IIDS - SRE		Section added
3.3.1.1 IRQ		Added “10. Iris Images” to list
3.3.2.3 ERRI		Section moved to 3.7.3 ERRI
3.4.5 Iris Image Investigation Search Submission		Section removed
3.4.5.1 IIS		Section removed
3.4.6 Biometric Investigation Submission		Section and subsections renumbered to 3.4.5
3.4.6.3 EQER		Section moved to 3.7.7 EQER
3.4.6.4 EQRR		Section renumbered to 3.4.5.3 EQRR
3.4.6.5 ERRR		Section moved to 3.7.5 ERRR
3.6.15 SPMNT		Removed “Tier 2” from first paragraph
3.6.20 RBSCVL		Updated first paragraph
3.7 Error Message Format		Added sections 3.7.1 ERRA, 3.7.2 ERRB, 3.7.3 ERRI, 3.7.4 ERRL, 3.7.5 ERRR, 3.7.6 ERRT, and 3.7.7 EQER
Appendix A		Updated A-1 NGI Maximum Transaction Response Times Removed (Future Capability) from IIDS transaction in A-2 NGI Type of Transaction By Service table Removed from the IIDS transaction in A-2 NGI Type of Transaction By Service table

SECTION 3 – AGGREGATE LIST OF CHANGES

Section	TOU Number	Change
Appendix C		Updated 2.2028 BID Added SI to BID Submitted Values and Results table Updated 2.2029 BSI Updated 2.051 CSL Added 2.2105 FI Updated 2.062 IMT table Added note to 2.017 MNU and updated MNU Values table Updated header in 2.2065 RBC Values table Updated 2.2040 RBT Values table Updated 2.059 SFR Values table Updated Code 2 and added Code 4 and 5 2.2046 TLI Values table Added 2.2105 FI to C-1 Field Edit Specifications for Type-2 Elements table
Appendix D		Updated 2.054 SSD, 2.055 SLE in D-1 Summary of Field Lists for Identification and Verification Transactions table Added 2.2105 FI to D-1 Summary of Field Lists for Identification and Verification Transactions table Added IIDS TOT to D-1 Summary of Field Lists for Identification and Verification Transactions table Updated SRE TOT to D-1 Summary of Field Lists for Identification and Verification Transactions table Removed CSL note and updated remaining notes in Reference Notes
Appendix E		Updated 2.084 AMP fields in E-1 Summary of Field Lists for Investigation, Information, and Notification Transactions table Added footnote to E-1 Summary of Field Lists for Investigation, Information, and Notification Transactions table
Appendix F		Updated footnote for F-5 Mobile ID IQS Requirements table
Appendix I		Updated 2.084 AMP, 2.009 OCA, and 2.055 SLE fields in I-1 Summary of Field Lists for Data management Transactions table Added footnote to I-1 Summary of Field Lists for Data Management Transactions table
Appendix K		Added new fields 10.200 – 10.249 RSV to Type-10 Data Dictionary Added new fields 10.351 – 10.400 RSV to Type-10 Data Dictionary

SECTION 3 – AGGREGATE LIST OF CHANGES

Section	TOU Number	Change
Appendix L		<p>Added 2.2105 FI to L-1 Complete Element Cross-Reference List by Tag Number table</p> <p>Added Type-17 fields to L-1 Complete Element Cross-Reference List by Tag Number table</p> <p>Added FBI Allocated Fields to L-1 Complete Element Cross-Reference List by Tag Number table</p> <p>Updated T17 values to DOCE, EMUF, FANC, FAUF, FNDR, NNDR, NFUE, NFUF, MAP, DEK, DEU, MPR, AMN, and FDSP in L-2 Record Set Requirements Summary by Type of Transaction table</p> <p>Removed (Future Capability) from the IIDS transaction in L-2 Record Set Requirements Summary by Type of Transaction table</p> <p>Removed the IIS transaction in L-2 Record Set Requirements Summary by Type of Transaction table</p> <p>Added Biometric Search Error to Identification Service Responses in L-3 Record Set Requirements Summary by Type of Response table</p> <p>Removed (Future Capability) form IIDS transaction in L-4 Transaction/Response/Error TOT Correspondence</p> <p>Removed IIS transaction from L-4 Transaction/Response/Error TOT Correspondence</p> <p>Added L-5 Record Type Fields Allocated by the FBI table</p>
Appendix M		<p>Updated and added corresponding footnote to L0008 in M-1 Transaction Message table</p> <p>Removed footnote associated with L0008, L0116, L0117, and L0118 in M-1 Transaction Message table</p> <p>Added new codes IR001, IR002, IR003, IR004, IR005, IR006, IR007, IR008, IR009, IR010, IR011, IR012, IR013, IR014, IR015, IR016, IR017, IR018, IR019, and IR020 to M-1 Transaction Message table</p> <p>Updated and added corresponding footnote for L0008 to M-1 Transaction Message table</p> <p>Added new codes L0062, L0183, L0185, L0186, L0187, L0188, L0189, and L0191 to M-1 Transaction Message table</p> <p>Removed code M0011 from M-1 Transaction Message table</p> <p>Updated M0012 from M-1 Transaction Message table</p> <p>Added new codes M0058, M0059, M0060, M0061, M0062, M0063, M0064, M0065, and M0066, to M-1 Transaction Message table</p>
Appendix N		<p>Added new fields 14.201 – 14.400 RSV to Type-14 Data Dictionary</p>
Appendix R		<p>Added new fields 13.200 – 13.400 RSV to Type-13 Data Dictionary</p>
Appendix S		<p>Added new appendix and Data Dictionary for Type-17</p>
		<p>Added S-1 Iris Transaction with Image table</p>
		<p>Added S-2 Iris Transaction without Image table</p>

SECTION 3 – AGGREGATE LIST OF CHANGES

Section	TOU Number	Change
Appendix AC		Removed IIIS from acronyms list

(Appendix B)
Law Enforcement LEOs Killed and Assaulted Program
LAW ENFORCEMENT SUICIDE
DATA COLLECTION

Form 1-701
Suicide or Attempted Suicide

Version 2.0
 Document Date: 07/24/2020

Prepared by:
 Global Law Enforcement Support Section
 Crime Statistics Management Unit
 Law Enforcement LEOs Killed and Assaulted (LEOKA) Program

FOR FBI USE ONLY

File Number	Date Entered/Initials	Population Group
Reference Number	Date edited/initials	Region/Division
Date received	Date QR'd/initials	FBI field office

Definitions

Incident – Occurrence of the suicide.

Incident Date – Date the incident occurred, or the beginning of the time-period in which it occurred, as appropriate.

Law enforcement LEO – Any current or former LEO (including corrections LEO) agent, or employee of the United States, a state, Indian tribe, or a political subdivision of a state authorized by law to engage in, or supervise the prevention, detection, investigation, or prosecution of any violation of the criminal laws of the United States, a state, Indian Tribe, or a political subdivision of a state.

Line of duty – Any action which an LEO, whose primary functions are crime control or investigations, reduction, enforcement of the criminal law and keeping public order, is obligated and authorized by law to perform in the course of performing his/her functions. The LEO is compensated by the public law enforcement agency which he or she serves.

On duty – An LEO is working their assigned shift at the time of incident.

Off duty – An LEO who is not working their assigned shift at the time of incident.

Policy - A standard course of action that has been officially established by an organization, business, political party, etc.

Position Status - Job status of LEO at time of death.

- Active Duty – Full time on-duty.
- Reserve – Full time training duty.
- Suspended – Out of work for disciplinary reasons.
- Medically Separated – Medical condition which renders the LEO unfit to perform their required duties.
- Retired – Withdrawn from occupation.

Suicide – The act of taking one's own life.

Traumatic – Emotionally disturbing or distressing. Relating to or causing psychological trauma.

Law Enforcement LEOs Killed and Assaulted Program SUICIDE DATA COLLECTION

This report is authorized by the Law Enforcement Suicide Data Collection Act, Title 34, Section 50701 and Title 28, Section 534, U.S. Code. Please use this form to report circumstances and other details regarding law enforcement LEOs who have committed suicide. Information provided throughout this form should apply to data that was available at the time of form completion. The FBI will use this critical information for statistical purposes related to law enforcement, including research, training, and publication in reports such as *Law Enforcement LEOs Killed and Assaulted*. Based on legislation requirements, data submitted within this questionnaire will be reported to the United States Congress and will be accessed on the Internet at <https://ucr.fbi.gov/leoka>. Your accuracy, cooperation, effort, and time are critical to our mission and appreciated.

The goal of this collection is to develop, implement, collect, report, and maintain statistics on federal, state, local and tribal law enforcement suicides.

 Suicide
 Attempted Suicide

PART 1 – ADMINISTRATIVE DATA PERTAINING TO VICTIM LEO

1.1 Type of agency:

- | | | | |
|--|---------------------------------|---|--|
| <input type="checkbox"/> Federal | <input type="checkbox"/> State | <input type="checkbox"/> City/Municipal | <input type="checkbox"/> Port authority (airport, transit) |
| <input type="checkbox"/> County/Parish | <input type="checkbox"/> Tribal | <input type="checkbox"/> College/University | |
| <input type="checkbox"/> Other (Specify) _____ | | | |

Agency Headquarters:
1.2 Originating Agency Identifier (ORI): _____ **Unknown**
1.3 Address of headquarters: _____

(Mailing address)
(City)
(State)
(Zip code)
1.4 Telephone (____) _____ **1.5 Email address:** _____

1.6 Please indicate the number of sworn LEOs in your agency:

- | | | | | |
|------------------------------------|------------------------------------|------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> 1-20 | <input type="checkbox"/> 21-50 | <input type="checkbox"/> 51-100 | <input type="checkbox"/> 101-200 | <input type="checkbox"/> 201-500 |
| <input type="checkbox"/> 501-1000 | <input type="checkbox"/> 1001-5000 | <input type="checkbox"/> 5,001-10K | <input type="checkbox"/> 10,001-20K | <input type="checkbox"/> 20,001-30K |
| <input type="checkbox"/> 30,001-up | | | | |

Victim LEO's assigned office: (Complete for Federal or State agencies only. If not applicable, skip to question 2.1)
1.7 Was victim LEO assigned to the headquarters? **Yes** **No**
If No:
ORI for assigned office: _____ **Unknown**
Barracks, district, precinct, region, troop, etc.: _____

Agency address: _____

(Mailing address)
(City)
(State)
(Zip code)

PART II – PERSONAL DATA PERTAINING TO VICTIM LEO

2.1 Age at time of attempt/death: _____

2.2 Gender:

-
- Male
-
-
- Female

2.3 Race:

- White
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Other Pacific Islander

2.4 Ethnicity:

- Hispanic or Latino
- Not Hispanic or Latino

2.5 Total sworn law enforcement experience at time of incident (include previous law enforcement experience):

- 0 – 5 years
- 6 – 15 years
- 16 – 25 years
- Over 25 years

2.6 Position status

- Active Duty
- Reserve
- Suspended
- Medically Separated
- On approved leave (annual/sick)
- Retired

2.7 Occupation

- Agent
- Technician
- Officer/Patrol/Detective
- Corporal
- Sergeant
- Lieutenant
- Captain
- Deputy Police Chief
- Chief of police
- Deputy
- Major
- Colonel
- Chief Deputy Sheriff
- Sheriff
- Correctional Officer/Juvenile CO
- Prison Warden
- 911 Operator

2.8 Marital status

- Single/Never married
- Married
- Divorced/Not remarried
- Divorced/Remarried
- Widowed/Not remarried
- Widowed/Remarried
- Separated
- Living with significant other

2.9 Children

- Yes
- No
- Unknown

2.10 Military Veteran

- Yes
- No
- Unknown

PART III – GENERAL DATA PERTAINING TO INCIDENT

3.1 Agency incident or case number: _____

3.2 Date of incident:

(mm/dd/yyyy)

3.3 Time of incident:

(Military hh:mm)

3.4 Attempt/suicide occurred:
 On Duty
 Off Duty

3.5 Location of incident: _____
City County State Country

3.6 Type of location of incident:

- Commercial (place of business and surrounding property, e.g., parking lot)
- Government (government building and surrounding property, e.g., parking lot)
- Public space (highway/road/alley/sidewalk)
- Public space (lake/river/park)
- Other public space (specify) _____
- Residential (place of dwelling and its property, e.g., yard, private driveway)
- Other location (specify) _____

3.7 Was the LEO found in an official police vehicle?

- Yes
- No

3.8 Manner of attempt/death (check all that apply):

- Service weapon
- Firearm other than service weapon
- Hanging
- Overdose prescription drugs
- Overdose illicit drugs
- Alcohol
- Knife/Cutting instrument
- Suffocation
- Jumping from high elevation
- Death caused by what would otherwise be deemed accidental (specify) _____
- Other (specify) _____

3.9 Was this a murder/suicide or an attempted murder/suicide?

- Yes
- No
- Unknown

3.10 Did the LEO leave notice of the attempt/suicide? (If yes proceed to question 3.12)

- Yes
- No (skip to Part IV)
- Unknown (skip to Part IV)

3.11 What type of notification was left behind?

- Note/written correspondence
- Text message
- Social media
- Phone call/voice message
- Video
- Audio recording
- Email correspondence
- Other (Specify) _____

PART IV- CIRCUMSTANCES OF THE INCIDENT

4.1 Did the LEO report - or was known to have experienced - any of the following within the last year? (check all that apply)

	YES	NO	UNKNOWN
Line-of-duty death or injury of fellow LEO(s)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Line-of-duty incident that injured/killed a bystander	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Experienced the death of a close colleague, friend or family member	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Involved in an incident in which a LEO discharged a weapon	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Injured or assaulted in line-of-duty incident	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Present at the scene of an incident resulting in casualty/casualties	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Involved in an active shooter incident or hostage situation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify)			

4.2 Did the LEO report if a Protection Order (is/was) in effect against them?

- Yes
- No

4.3 Did the LEO report a pending investigation against the agency?

- Yes
- No
- Unknown

4.4 Did the LEO report if his/her unit (is/was) under investigation?

- Yes
- No

4.5 Did the LEO report that he/she (is/was) the target of an investigation?

- Yes
- No

4.6 Did the LEO report if he/she (is/was) a witness in an investigation involving other LEOs?

- Yes
- No

4.7 Did the LEO report if he/she (is being/has been) indicted recently for a crime?

- Yes
- No

4.8 Did the LEO report if he/she (is/was) scheduled to stand trial?

- Yes (proceed to next question)
- No (skip to question 4.11)
- Unknown (skip to question 4.11)

4.9 Would a guilty verdict preclude further service by the LEO?

- Yes
- No
- Unknown

4.10 Are you aware if the LEO was on a promotional list?

- Yes
- No
- Unknown

4.11 Did the LEO report if he/she (is/was) denied a promotion or transfer?

- Yes
 - Within the last 0-3 months
 - Within the last 3-6 months
 - Within the last 6-9 months
 - Within the last 9-12 months
- No
- Unknown

4.12 Did the LEO report he/she (is/was) suffering from any of the following? (check all that apply)

	YES	NO	UNKNOWN
Post-traumatic stress disorder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Depression	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alcohol/Drug abuse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical Illness impacting the ability to perform in the capacity of the job	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern over impending retirement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Domestic violence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chronic illness	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial problems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Relationship problems (pending divorce, affairs)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify)			

4.13 Are you aware if the LEO exhibited any mental health/warning signs prior to the incident? (check all that apply)

	YES	NO	UNKNOWN
Making threats to harm or kill themselves	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Seeking access to drugs, weapons, or other items that could cause harm	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Talking or writing about death and dying	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Expressing hopelessness, rage, anger or anxiety	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Engaging in reckless or risky behavior	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Increasing use of alcohol or drugs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chronic absence from work	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Showing signs of mood changes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Prior suicide attempts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PART V LEO WELLNESS POLICY AND TRAINING

5.1 Does the agency provide training on suicide prevention/LEO wellness?

- Yes (proceed to next question)
- No (skip to question 5.3)
- Unknown (skip to question 5.3)

5.2 How often is training on suicide prevention/LEO wellness provided?

- At orientation only
- Annually
- Upon request
- Unknown

5.3 Does the agency provide guidance on the availability of mental health services to its LEOs?

- Yes
- No
- Unknown

5.4 Are you aware if the victim LEO had taken advantage of the services offered?

- Yes
- No
- Unknown

Prepared by: _____

Date: ____/____/____
(mm/dd/yyyy)

Email address: _____

Telephone: _____

NOTE: If there are any questions concerning the completion of this form, contact the staff of the FBI LEOKA Program at 304-625-3521. The completed form should be forwarded to the FBI LEOKA Program via email to leoka.statistics@fbi.gov; or mail to FBI, Criminal Justice Information Services Division, Attention: LEOKA Program, Module E-3, 1000 Custer Hollow Road, Clarksburg, WV 26306-0159. Under the Paperwork Reduction Act, you are not required to complete this form unless it contains a valid OMB control number. The form takes approximately 30 minutes to complete.

Privacy Act Statement

Authority: The collection of this information is authorized under the Law Enforcement Suicide Data Collection Act, 34 U.S.C. § 50701; 28 U.S.C. § 534; 34 U.S.C. § 10211; 44 U.S.C. § 3101; and the general record keeping provision of the Administrative Procedures Act (5 U.S.C. § 301). Providing your contact information is voluntary; however, failure to provide your contact information may inhibit the FBI's ability to verify or clarify information in your LEOKA incident submission.

Principal Purpose: Providing your contact information allows the FBI to contact you with any clarifying questions regarding your LEOKA submission. This allows the FBI to verify submitted information and ensure the accuracy of the LEOKA data.

Routine Uses: All contact information will be maintained in accordance with the Privacy Act of 1974. Your information may be disclosed with your consent, and may be disclosed without your consent as permitted by all applicable routine uses as published in the *Federal Register* (FR), including the routine uses for *The FBI Central Records System* (JUSTICE/FBI-002), published at 63 FR 8659, 671 (Feb. 20, 1998) and amended at 66 FR 8425 (Jan. 31, 2001), 66 FR 17200 (Mar. 29, 2001), and 82 FR 24147 (May 25, 2017), and the *FBI Online Collaboration Systems* (JUSTICE/FBI-004), published at 82 FR 57291 (Dec. 4, 2017). Routine uses may include sharing information with other federal, state, local, tribal, or territorial law enforcement agencies.

DRAFT

Appendix B—Example of UCR Police Employee Collection if Option 1 (Changes to Race Ethnicity and Gender Expression) is accepted:

UCR Police Employee Collection

Please provide totals for the following categories of employees on your payroll as of October 31 and worked a normal workweek.

Race/Ethnicity and Gender Expression	Law Enforcement Officers			Civilian Employees			Total
	Full-time	Part-time	Reserve/ Auxiliary/ Other	Full-time	Part-time	Reserve/ Auxiliary/ Other	
Hispanic or Latino, of any race							
Male							
Female							
Non-binary							
Unknown/Unreported							
American Indian or Alaska Native, not Hispanic or Latino							
Male							
Female							
Non-binary							
Unknown/Unreported							
Asian, not Hispanic or Latino							
Male							
Female							
Non-binary							
Unknown/Unreported							
Black or African-American, not Hispanic or Latino							
Male							
Female							
Non-binary							
Unknown/Unreported							
Native Hawaiian or Other Pacific Islander, not Hispanic or Latino							
Male							
Female							
Non-binary							
Unknown/Unreported							

White, not Hispanic or Latino							
Male							
Female							
Non-binary							
Unknown/Unreported							
Two or more races, not Hispanic or Latino							
Male							
Female							
Non-binary							
Unknown/Unreported							
Unknown/Unreported Race							
Male							
Female							
Non-binary							
Unknown/Unreported							
Total employees							
Male							
Female							
Non-binary							
Unknown/Unreported							

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC K

Fiscal Year 2020 Audit Results Summary

PURPOSE

To inform the Working Groups of results from fiscal year 2020 National Crime Information Center (NCIC), National Sex Offender Registry (NSOR), Information Technology Security (ITS), Next Generation Identification (NGI) (previously known as National Identity Services or NIS), National Instant Criminal Background Check System (NICS), and National Data Exchange (N-DEx) audits and Uniform Crime Reporting (UCR) Quality Assurance Reviews (QARs).

AUTHOR

Global Law Enforcement Support Section, Criminal Justice Information Services (CJIS) Audit Unit (CAU)

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

This paper summarizes the most common results from audits conducted by the CAU staff from October 1, 2019, through September 30, 2020. Due to the COVID-19 pandemic and its impact on the Federal Bureau of Investigation's (FBI) CJIS Division information sharing partners, the CAU canceled all scheduled CJIS systems audits in March 2020. Each program's audit results are reported under the respective program heading. It should be noted for each deficiency found during agency audits, the CAU staff informed agency personnel of the deficiencies, provided the assessed policy and source references, explained how to comply with the policy, and discussed corrective measures to achieve policy compliance. The CAU plans to resume all CJIS systems audits in March 2021, beginning with the audits that were canceled in March 2020, and completing the remaining 2020 audits in 2021.

Information Only Topic K, Page 1

Users of the CJIS systems are required to abide by all applicable policies. Compliance is essential to safeguard public and officer safety, as well as to protect the privacy of United States citizens. Failure to comply may result in potential sanctions, to include loss of service, which may jeopardize these safeguards and protections. It is critical for the agencies that provide CJIS systems access to receive the appropriate level of resources and support in order to achieve full compliance. If a CJIS Systems Agency (CSA) has difficulties in creating a plan for corrective actions or identifying how to become compliant, they should contact the CAU at cjisaudit@fbi.gov or the Compliance Evaluation Subcommittee Chair at CESUB@fbi.gov as a resource for guidance.

NCIC

The CAU staff conducted six NCIC audits of federal and state CSAs.

Five (83.33 percent) of the six CSAs had a recommendation to ensure the use and dissemination of the Interstate Identification Index (III) is authorized.

Three (50.00 percent) of the six CSAs had a recommendation to ensure NCIC validation requirements are met.

Three (50.00 percent) of the six CSAs had a recommendation to ensure Missing Person File records, for individuals under age 21, are entered within two hours.

Three (50.00 percent) of the six CSAs had a recommendation to ensure locates are placed on corresponding NCIC records after confirming hits.

Two (33.33 percent) of the six CSAs had a recommendation to ensure the clear/cancel transaction is programmatically available and/or local agencies use the correct transaction to remove the records from NCIC.

Two (33.33 percent) of the six CSAs had a recommendation to ensure NCIC records contain all available information.

Two (33.33 percent) of the six CSAs had a recommendation to ensure Extradition Limitation Field codes are correctly used.

One (16.67 percent) of the six CSAs had a recommendation to ensure records meet the criteria for entry into NCIC.

One (16.67 percent) of the six CSAs had a recommendation to ensure the memorandum of understanding clearly articulates redress procedures and identifies which NCIC files will be used for disqualification into the Critical Infrastructure Facility.

One (16.67 percent) of the six CSAs had a recommendation to ensure purpose codes are correctly used for III transactions.

One (16.67 percent) of the six CSAs had a recommendation to ensure reasons for all III transactions can be provided.

NSOR

The CAU staff conducted six NSOR audits of the CSAs' Sex Offender Registries (SORs).

Six (100.00 percent) of the six SORs had a recommendation to ensure that NSOR records are entered into the NCIC with all available information.

Five (83.33 percent) of the six SORs had a recommendation to ensure that NSOR records are entered into the NCIC with accurate information.

Two (33.33 percent) of the six SORs had a validation recommendation to ensure NSOR records are validated in accordance with NCIC policy.

One (16.67 percent) of the six SORs had a recommendation to ensure NSOR records are modified in a timely manner.

One (16.67 percent) of the six SORs had a recommendation to ensure NSOR records that are no longer valid are removed from the NCIC in a timely manner.

ITS

The CAU staff conducted eight ITS audits of federal and state CSAs. It should be noted that the applicability of policies is dependent upon the CSA's network/computer configuration and capabilities.

Four (50.00 percent) of the eight CSAs had a recommendation to ensure advanced authentication is utilized for personnel who access and/or manage information systems containing criminal justice information (CJI) from non-secure locations.

Four (50.00 percent) of the eight CSAs had a recommendation to ensure audit and accountability controls are implemented on information systems accessing CJI.

Four (50.00 percent) of the eight CSAs had a recommendation to ensure all account management, identification policies, and procedures are implemented on system accounts accessing CJI.

Four (50.00 percent) of the eight CSAs had a recommendation to ensure all security awareness training requirements of the *CJIS Security Policy* are documented and implemented.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure CJI transmitted or stored outside the boundary of the physically secure location is immediately protected via encryption to comply with *CJIS Security Policy* requirements.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure written agreements are implemented prior to exchanging CJI with each agency.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure appropriate agreements are implemented and signed with each noncriminal justice agency.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure security controls are implemented for virtual environments hosting CJI.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure all physical protection policy requirements are documented and implemented.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure the CJIS Security Addendum is adequately documented, implemented, and signed with all private contractor personnel.

Three (37.50 percent) of the eight CSAs had a recommendation to ensure an operational information security incident response policy is documented and implemented.

NGI

The CAU staff conducted two NGI audits of non-National Fingerprint File (NFF) state repositories.

There were no reportable findings of the two non-NFF state repositories. The CAU staff recognizes this as a significant accomplishment and encourages all CSAs to continue to strive for this attainable goal.

NICS

The CAU staff conducted six NICS audits of state CSAs. It should be noted that the applicability of policies is dependent upon the CSA's participation to the NICS.

Three (50.00 percent) of the six CSAs had a recommendation to ensure NICS Indices records are accurate and valid.

Two (33.33 percent) of the six CSAs had a recommendation to ensure access to the NICS is used only for authorized purposes in accordance with Title 18, U.S.C., § 922(t).

Two (33.33 percent) of the six CSAs had a recommendation to ensure local agencies transmit the request for a background check via the NCIC interface to the NICS.

One (16.67 percent) of the six CSAs had a recommendation to ensure NICS Indices records are entered under the correct Originating Agency Identifier (ORI) number.

One (16.67 percent) of the six CSAs had a recommendation to ensure a NICS check is conducted prior to the issuance of a Bureau of Alcohol, Tobacco, Firearms and Explosives or ATF qualified alternate permit valid to purchase a firearm.

One (16.67 percent) of the six CSAs had a recommendation to ensure individuals are denied who are unlawful users of or addicted to any controlled substance per Title 18, U.S.C., § 922(g)(3).

One (16.67 percent) of the six CSAs had a recommendation to ensure individuals are denied who have been convicted in any court of a crime punishable by a term exceeding one year in accordance with Title 18, U.S.C., § 922(g)(1).

One (16.67 percent) of the six CSAs had a recommendation to ensure individuals are denied who are under indictment or information for a crime punishable by imprisonment for a term exceeding one year in accordance with Title 18, U.S.C., § 922(n).

One (16.67 percent) of the six CSAs had a recommendation to ensure individuals are denied who are adjudicated as a mental defective or committed to a mental institution per Title 18, U.S.C., § 922(g)(4).

One (16.67 percent) of the six CSAs had a recommendation to ensure individuals are denied who have been convicted in any court of a misdemeanor crime of domestic violence per Title 18, U.S.C., § 922(g)(9).

One (16.67 percent) of the six CSAs had a recommendation to ensure only those individuals who are subject to a court order of protection meeting the federal definition are denied per Title 18, U.S.C., § 922(g)(8).

One (16.67 percent) of the six CSAs had a recommendation to ensure NICS background checks are conducted solely for the sale of a firearm, issuance of a permit to possess or acquire, a permit to carry, or an explosive permit in accordance with Title 18, U.S.C., § 922(t).

One (16.67 percent) of the six CSAs had a recommendation to ensure audits are conducted for all agencies with direct access to CJI.

Three (50.00 percent) of the six CSAs had no recommendations. The CAU staff recognizes this as a significant accomplishment and encourages all CSAs to continue to strive for this attainable goal.

N-DEx

The CAU staff conducted six N-DEx System audits of federal and state CSAs.

Three (50.00 percent) of the six CSAs had a recommendation to ensure the N-DEx System is used only for authorized purposes.

One (16.67 percent) of the six CSAs had a recommendation to ensure agencies utilized the correct use code.

One (16.67 percent) of the six CSAs had a recommendation to ensure the user identifier-employer ORI was for the user's assigned agency.

Three (50.00 percent) of the six CSAs had no recommendations. The CAU staff recognizes this as a significant accomplishment and encourages all CSAs to continue to strive for this attainable goal.

QAR

The CAU staff conducted nine QARs of state UCR programs.

Five (55.56 percent) of the nine state UCR programs had a recommendation to ensure Group A offenses were reported according to the FBI's UCR Program guidelines.

Four (44.44 percent) of the nine state UCR programs had a recommendation to ensure cargo theft was implemented or valid incidents were reported to the FBI's UCR Program.

Three (33.33 percent) of the nine state UCR programs had no recommendations. The CAU staff recognizes this as a significant accomplishment and encourages all state UCR programs to continue to strive for this attainable goal.

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC L

Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program Beyond 2021 Task Force Update

PURPOSE

To summarize the recent activities and initiatives of the Beyond 2021 Task Force.

AUTHOR

Global Law Enforcement Support Section, Crime Statistics Management Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. CJIS will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

Established in 2019, the Beyond 2021 Task Force was charged with the creation of the FBI UCR Program Roadmap after the transition from a summary-based data collection to a National Incident-Based Reporting System (NIBRS) data collection. The purpose of the Beyond 2021 Task Force is to engage the stakeholder community through the Criminal Justice Information Services (CJIS) APB process using subject matter expert (SME) groups and create recommendations for enhancements to the FBI UCR Program's data collections.

The Beyond 2021 Task Force consists of a small group of individuals who are dedicated to the FBI UCR Program's mission. The task force is supported by SME groups who create recommendations based on specific areas of expertise. The information is then provided to the task force who use SME feedback to create recommendations for enhancements to FBI UCR Program data collections. All recommendations created through the Beyond 2021 Initiative will be presented through the CJIS APB process for consideration and recommendation for approval by the FBI Director.

Since the Beyond 2021 Task Force was initiated, the Task Force has met monthly to discuss topics and ideas proposed by the SME groups. Areas of consideration have included:

- Data Publication – Ensuring future FBI UCR Program data publication strategies accommodate the expansion of data.
- Edward J. Byrne Justice Assistance Grants – Collaborating with the Bureau of Justice Assistance and the Bureau of Justice Statistics to determine if the NIBRS transition will impact grant funding. The FBI UCR Program presented an information paper discussing these findings during the Fall 2020 round of the CJIS APB.
- NIBRS Data Elements – Examining methods to enhance and modify NIBRS data elements to produce a more comprehensive view of crime data.
- FBI UCR Program Data Collection Strategies – Determining how to ensure uniformity amongst the data collections within all FBI UCR Program data collections.
- National Academy of Sciences – Modernizing Crime Statistics Study (NAS) – Reviewing the recommendations from the NAS and assessing the impact implementation will have on crime data.
- Law Enforcement Officers Killed and Assaulted (LEOKA) – Enhancing the data collected within LEOKA.

Through research and analysis, the Beyond 2021 Task Force has created recommendations for action and consideration, to include 16 recommendations for enhancements to NIBRS data elements, in addition to policy and operational enhancements that will not require systematic changes.

DISCUSSION AND ANALYSIS

FBI UCR Program Publications

The FBI UCR Program produces six publications from the data provided by federal, state, local, and tribal law enforcement agencies from across the nation. In addition to these publications, the FBI UCR Program produces annual tables on incidents of cargo theft, federal crime, and human trafficking data. Historically, the FBI UCR Program has produced topical reports highlighting the utility of UCR data, and more specifically NIBRS data, on an intermittent basis. These special reports showcase the usefulness of NIBRS data, demonstrating the granularity of the data and providing additional insight in elements of specific offenses.

The FBI UCR Program will shift from data publications on www.FBI.gov to all crime data being presented on the Crime Data Explorer (CDE). Launched in June 2017, the CDE is an interactive web-based tool presenting UCR data differently to users than traditional, static tables. The CDE provides data consumers with the ability to easily access, view, and understand UCR data.

Enhancing Crime Data through NIBRS

Through the Beyond 2021 Initiative, the FBI UCR Program staff identified SMEs to conduct analysis and recommend a path forward for the FBI UCR Program publications. The FBI UCR Program staff used the information generated by the SME group to create a publication strategy defining future publications by focusing on how to display, promote, and use NIBRS data. Through the work of these individuals, the FBI UCR Program developed methods to ensure the continuity of previous years, while demonstrating the utility of the granularity provided by the

NIBRS transition. The FBI UCR Program can provide a more robust view of crime data due to enhancements including:

- The transition to a NIBRS-centric data collection
- Technology afforded by an enhanced UCR system

The shift to an all-NIBRS data publication will allow data consumers to view data not possible with a summary-centric view. Summary reporting allows data consumers to receive details about offense, arrest, and police employee data. Through summary data, users can view limited information regarding offenses known to law enforcement at an aggregate level. In contrast, NIBRS allows submitters to provide additional data on separate offenses within one incident, information on the victims, known offenders, the relationships between victims and offenders, arrestee information, and the property involved in crimes. In addition, NIBRS allows for a disaggregated view of the data displayed.

The NIBRS affords data submitters the ability to supply additional information, and details not available within a summary view. This allows the FBI UCR Program to highlight additional data points through a NIBRS-centric presentation. The granularity available within NIBRS data, gives the FBI UCR Program the ability to present more data than historically provided within its annual publications. This additional detail has been provided to data consumers since 2011, through the annual release of the *National Incident-Based Reporting System* publication. The static tables created for this publication provide data consumers with a preview of the vast amount of data available within a NIBRS dataset and focuses on highlighting data points a summary-centric data collection cannot provide.

Impact to UCR Publications

Quarterly data releases are occurring on a regular schedule: Mid-June (presenting data from January – March), mid-September (presenting data from January – June), mid-December (presenting data from January – September), and mid-March (presenting data from January – December). Quarterly publications consist of national trend tables, provided by population group, region, and five consecutive two-year trends as well as information on the “Most in Population” (municipal law enforcement agencies covering areas with a population of 100,000 or more) offense data. Each quarterly data release will be a cumulative report for the calendar year. The FBI UCR Program will release current year crime data through these quarterly data pushes prior to releasing crime data from the previous year in the annual publication of *Crime in the United States*.

Initial Differences - After the NIBRS Transition

In 2021, the FBI UCR Program will simplify how data consumers obtain national crime data by presenting all crime data on the CDE. The shift from housing crime data in two locations (on www.FBI.gov and on CDE) will allow for the creation of the UCR Program data journey, highlighting all data submitted by law enforcement partners. In addition to current year data available via quarterly release, the legacy annual publication containing the previous year’s data will continue to be available as downloadable files for users wishing to continue to access these annual data products on the CDE. Furthermore, this shift to the CDE will provide data users

with access to raw data files, Part I¹ crime trends, data downloads, and NIBRS data, as well as the static tables required for the annual publication of crime data in a single location. The CDE gives the FBI UCR Program the opportunity to enhance the delivery of information beyond the static tables published annually using the Explorer pages. In addition to the year-over-year view similar to the data tables published in *Crime in the United States*, data consumers will be able to easily access and view data visualizations, downloadable data, spreadsheets, master files, and other tools to enhance the data consumer experience.

Based on the current publication schedule of *Crime in the United States* the first data release after the NIBRS transition will have minimal changes. The 2021 release of *Crime in the United States* will consist of data from calendar year 2020, the last year the FBI UCR Program is accepting SRS data. Therefore, there will be no significant changes within the data tables presented. The 2021 data release will highlight SRS data, as it has historically. Data consumers will notice the static tables displaying data submitted on cargo theft and human trafficking offenses will be absorbed into the *Crime in the United States* data release. These tables have historically been highlighted within separate links located on www.FBI.gov.

In 2021, the FBI UCR Program will highlight NIBRS data through the release of the *National Incident-Based Reporting System*, which the FBI UCR Program will continue to release for the foreseeable future. Data released on a quarterly basis in 2021 will be no different from the 2020 data releases. Since the quarterly data releases contain trend tables and the FBI UCR Program must maintain trends, quarterly data will be converted to SRS for the foreseeable future. However, there will not be trend tables for data published from quarter one and quarter three because the data for the quarters has not been released before and there is no trend table to publish. Second quarter trends will mimic the previous *Preliminary Semiannual Publication* and fourth quarter trends will mimic the annual *Crime in the United States* data release.

Initial data releases highlighting crime in the nation will be lacking data previously available if agencies are unable to make the deadline for the NIBRS transition. Since the FBI UCR Program will not accept SRS data from those agencies not meeting the NIBRS transition deadline their data will not be included in the publications. The FBI UCR Program has continued to promote the NIBRS transition through various outreach strategies, securing commitments from thousands of law enforcement agencies that they will meet the deadlines.

Continued Expansion - Crime Data Presentation 2022 and Beyond

The FBI UCR Program will gradually condense the number of publications released while providing more information with dynamic views. The FBI UCR Program will implement all modifications in phases, communicating with data contributors and consumers throughout the process to ensure all stakeholders have a clear understanding of the benefit of the enhancements.

¹ Part I Offenses – The first of two main groupings of crime classifications within SRS data and consisting of eight offenses (criminal homicide, forcible rape, aggravated assault, robbery, burglary, larceny-theft, motor vehicle theft, and arson). (Summary Reporting System (SRS) User Manual v.1, p. 174).

Maintaining Rates and Trends - Presentation of Summary Data after the NIBRS Transition

Although the FBI UCR Program will not accept SRS data after January 1, 2021, the FBI UCR Program will continue to present SRS data for the foreseeable future. The FBI UCR Program produces tables showcasing rates and trends of crimes known to law enforcement over a five-year and twenty-year period and will continue publishing these tables. To preserve trends, the FBI UCR Program will convert NIBRS data to a summary view. To ensure data users begin to experience the benefits of the NIBRS-only collection, the FBI UCR Program will begin creating rate and trend tables consisting of only NIBRS data after the first two years. These rates and trends will be based upon estimates² derived from a sample of NIBRS agencies representing the nation. These tables will be released in conjunction with the SRS-NIBRS hybrid tables to allow data consumers time to acclimate to the new view of crime data within the trend tables.

The FBI UCR Program anticipates the conversion of NIBRS data into an SRS view for twenty years. This will ensure the current rates and trends are preserved while providing data users with adequate time to acclimate to NIBRS-only views. During this time, the FBI UCR Program will continue to educate data contributors and consumers on the benefits and updated views of NIBRS data.

Reduction in Data Publications

The FBI UCR Program releases six publications annually. It is the desire of the FBI UCR Program to reduce the number of publications by half. Through the NIBRS transition and the push to release crime data on a quarterly basis, the goal of the FBI UCR Program is to publish three annual reports, while maintaining the same tables the nation expects for national crime and law enforcement data. Within the next ten years, the FBI UCR Program will only release *Crime in the United States*, *Law Enforcement Officers Killed and Assaulted*, and *National Use of Force Data Collection*.

The reduction in the number of data publications will take place gradually. First, the FBI UCR Program will no longer need to publish the *Preliminary Semiannual Crime Report*, as the data historically provided in this publication will be released as part of the quarterly crime data report. Next, the FBI UCR Program will begin to transition the tables currently published within the publication *National Incident-Based Reporting System*. This publication will be absorbed into the annual publication of *Crime in the United States*. As the FBI UCR Program transitions the nation to become more familiar with NIBRS data and create NIBRS trend tables, the tables released in *National Incident-Based Reporting System* will also transition to *Crime in the United States*. The FBI UCR Program staff is also creating a plan to absorb the data that is published within *Hate Crime Statistics* into *Crime in the United States*.

Law Enforcement Officers Killed and Assaulted (LEOKA)

Historically the FBI UCR Program has released its publication of *Law Enforcement Officers*

² The FBI UCR Program is actively collaborating with the Bureau of Justice Statistics to develop a statistically robust method to calculate national estimates of key measures and indicators of the NIBRS data that will account for missing or incomplete data.

Killed and Assaulted in two installments. The first installment containing information about officer deaths is released in May during Police Week. The second installment containing officer assaults and injuries is released in September. The goal of the FBI UCR Program is to work toward a single publication for *Law Enforcement Officers Killed and Assaulted* which will be released to coincide with Police Week.

The LEOKA Data Collection is examining the expansion of the data collected to include health related deaths. The FBI UCR Program is working to determine how to include and present this data with the existing publications. As the LEOKA Data Collection continues to expand and evolve, the publication will reflect these changes.

National Use-of-Force Data Collection

In July 2020, the first data release containing information on the National Use-of-Force Data Collection was available via the CDE. This data collection is the newest publication released by the FBI UCR Program, highlighting law enforcement use of force and is the first FBI UCR Program publication released exclusively via the CDE. The first release of *The National Use-of-Force Data Collection* provides data contributors with a glimpse of how future data publications will be presented once the FBI UCR Program transitions all data publications to the CDE. Held to the Office of Management and Budget (OMB) publication thresholds, this data publication will continue to expand as additional law enforcement agencies submit data.

Enhancing Data Publications through Visualizations and Data Stories

Through the expansion of the data collections, the transition to NIBRS, quarterly data releases, and the transition to CDE, the FBI UCR Program will maintain its status as the authoritative source for law enforcement data. The FBI UCR Program is planning to enhance the experience for data consumers by including data visualizations and data stories to CDE.

The FBI UCR Program will create data visualizations to expand on the information shared in the data stories. Similar to the infographic produced to highlight LEOKA data, these visualizations will highlight NIBRS data. The FBI UCR Program will use the LEOKA Infographic as the basis for additional data visualizations highlighting NIBRS data. In addition to the data visualizations highlighting the information within the data stories, the FBI UCR Program will begin publishing data visualizations highlighting hate crime offenses.

The FBI UCR Program will begin publishing data stories highlighting specific NIBRS data on the CDE. These data stories will provide high-level overviews of portions of NIBRS data providing data use cases for consumer review. These data stories will replace the historical topical crime reports released by the FBI UCR Program and will highlight varying topics of interest. The following table provides an overview of publication enhancements and the anticipated years of implementation.

Year(s)	Anticipated Enhancement
2021	<ul style="list-style-type: none"> • Transition all publications to CDE • Tables highlighting Cargo Theft and Human Trafficking will be absorbed into the annual release of <i>Crime in the United States</i> • Continued expansion of the <i>National Use-of-Force Data Collection</i> publication
2022 and Beyond	<ul style="list-style-type: none"> • Continued publication of trends and tables highlighting summary data • Gradual transition of <i>Crime in the United States</i> to highlight NIBRS data – phasing out the <i>National Incident-Based Reporting System</i> publication • Continued expansion of LEOKA data • The FBI UCR Program will highlight NIBRS data through data visualizations and data stories on CDE • Through consolidation, reduce annual publications released by the FBI UCR Program

Governance

As part of the Beyond 2021 Initiative, the FBI UCR Program leveraged the work of a SME group to assess and recommend enhancements to improve program processes and outreach to stakeholders. The Governance SME group assisted the Beyond 2021 Task Force in creating recommendations to enhance how the FBI UCR Program shares information with all stakeholders and obtains feedback on potential future enhancements. The Beyond 2021 Task Force acknowledges there are many stakeholders interested in the data the FBI UCR produces. Because of this, it is important the FBI UCR Program promotes transparency and accessibility to FBI UCR Program data and receives input from the appropriate stakeholder groups when proposing enhancements or modifications to the data. Through the work of the SME and Beyond 2021 Task Force a recommendation to promote transparency and access to the CJIS APB Process is recommended to enhance stakeholder access and promote use of the FBI UCR Program data. This will be accomplished by:

- Inviting the Bureau of Justice Statistics to be represented on the UCR Subcommittee.
- Increasing awareness of the CJIS APB process within the research community, such as engagement with the American Society of Criminology (ASC), the Academy of Criminal Justice Sciences (ACJS), or the American Statistical Association (ASA)
- Determine opportunities to share FBI UCR Program topic papers on the webpage www.fbi.gov.
- Seeking opportunities to reach out to subject matter experts and external stakeholders throughout the early research process of topic papers.
- Enhance CJIS Systems Officer (CSO) Training.
- Explore options for non-law enforcement SME to provide input on best practices for data quality and methodology during the UCR Subcommittee discussions.

Proposed Timeline

The FBI UCR Program will begin immediately enhancing how data is shared with stakeholders, via modifications to UCR Subcommittee membership, enhancements to CSO training, and exploration into obtaining additional input from stakeholders. In addition, the FBI UCR Program will leverage groups such as the ASC, ACJS, and ASA to promote the CJIS APB

process through articles in the organizations' newsletters. The FBI UCR Program will collaborate with these groups to ensure information on the CJIS APB process is included. The FBI UCR Program anticipates continuing outreach and promotion of the CJIS APB process and FBI UCR Program data for the foreseeable future.

NIBRS Business Rules

Ensuring the accuracy of the data released by the FBI UCR Program is of the utmost importance. To ensure high-quality data outputs, each data submission is checked against a programmed set of data validation rules, known as the NIBRS business rules. The FBI UCR Program uses the NIBRS business rules as a mechanism to ensure the data received from contributors meets the standards set forth within the *National Incident-Based Reporting System Technical Specification* and the *National Incident-Based Reporting System User Manual*. When contributors submit data to the FBI UCR Program it is automatically validated against programmed NIBRS business rules. Should an agency submit data that does not meet the FBI UCR Program criteria, the submitting agency will receive a warning or an error notifying the submitter to review the data and correct the noted issues to comply with the NIBRS business rules.

The FBI UCR Program set a goal of using the Beyond 2021 Initiative to review the NIBRS business rules. The goal was to create recommendations and improve state-level implementation of the NIBRS business rules and determine which rules are required and which can be removed given technological enhancements within records management systems (RMS). Prior to the NIBRS Business Rules SME implementation, delays created by the COVID-19 pandemic caused an inability to effectively gain information from state UCR programs and the vendor community to fully assess the impact modifications to the NIBRS business rules will have on law enforcement data. However, it is the desire of the Beyond 2021 Task Force to continue with research and analysis of the NIBRS business rules. In addition, the Beyond 2021 Task Force desires to leverage the work of the Data Quality Working Group and conduct outreach to the stakeholder community to conduct a thorough examination of all NIBRS business rules and analyze how modifications can create high-quality data outputs.

The FBI UCR Program has identified areas that must be addressed to conduct a thorough analysis of the NIBRS business rules.

- Data Quality Working Group Analysis – Leveraging the work of the Data Quality Working Group to identify gaps within the data that are impacted by the current NIBRS business rules.
- Feedback from state UCR programs and the vendor community – Conducting outreach with data contributors and those building RMS to determine how current NIBRS business rules are being interpreted and implemented.

By combining the information from these areas, the FBI UCR Program can provide recommendations for enhancements to the NIBRS business rules. The Beyond 2021 Task force recommends allowing additional time for a thorough analysis of the NIBRS business rules.

Data Submissions Methods

The FBI UCR Program is aware of multiple implementation methods to enforce NIBRS business rules. Most often, these methods fall into two categories. The first is integration of the rules within the User Interface at the point of collection, best categorized as an active implementation requiring the user to address the error prior to moving onto the next field or presenting a list of errors and warnings for the user to address prior to enabling the submit function. The second method is a more passive collection mechanism, where the rules are enforced after the collection of agency-specific data elements are extracted from the database and transformed to compile a monthly incident-based reporting submission to the state UCR program.

Additional considerations must be made given the differences in data submission mechanisms. Data contributors can submit data to the FBI UCR Program in two ways: flat file submissions and via Extensible Mark-Up Language (XML). With flat file submissions, agencies must provide data within specific parameters (for example, the Arrestee Segment must contain a specific number of characters or spaces) whereas XML submissions provide agencies with flexibility for formatting data submissions. To accommodate XML data submissions, the FBI UCR Program must determine what revision mechanism should be supported to manage the changes within literal codes. For example, using flat file submissions agencies submit the code 11B to report a sodomy offense whereas XML data submitters use the literal code Sodomy, if there is a literal code change or retirement, the traceability of the offense is removed within an XML data submission (in this example the retirement of sodomy would then be counted as rape).

Data Quality Working Group

The FBI UCR Program established the Data Quality Working Group as to review all current NIBRS business rules. This group consist of internal stakeholders from the FBI UCR Program, the Law Enforcement Technology Services Unit, and the CJIS Audit Unit. The purpose of this group is to process data quality issues, create strategies for improving submitted data, and address other quality related efforts for all FBI UCR Program data collections. The Data Quality Working Group meticulously reviews anomalies within data and analyzes how the data are impacted by the current business rules and identifies process improvement opportunities ensuring high-quality data from submitters.

State and Vendor Outreach

Outreach to state UCR programs and the vendor community is imperative because of the varying methods for data submissions across the nation. The FBI UCR Program must determine how to ensure high-quality data outputs without straining the resources of data contributors. Varying implementation methods for the business rules, different data submission methods, and response rates to the errors and warnings received must be considered prior to making significant changes to the NIBRS business rules. State UCR program managers were represented with the Beyond 2021 Task Force and the supporting SME groups. Initial feedback from these individuals indicates that additional research on the impact of the NIBRS business rules on the data is needed. A common theme among Beyond 2021 Initiative participants is the relaxation of NIBRS business rules to allow FBI UCR Program staff time to conduct analysis on the impact

relaxation has on the data. The Beyond 2021 Task Force identified the need for additional time and resources to ensure all stakeholder input is considered prior to making modifications to the NIBRS business rule.

In addition to state UCR program personnel and the vendor community, the FBI UCR Program must have time to communicate with RMS and crime data repositories personnel. Prior to these communications, the FBI UCR Program needs to determine the best path forward and obtain approval for these communication methods. There is potential to leverage groups such as SEARCH and the Integrated Justice Information Systems Institute and obtain feedback. Through such communications, the FBI UCR Program can determine which methods of business rule implementation are being used and obtain feedback on how the current NIBRS business rules are being coded within law enforcement agency RMS.

Proposed Timeline

The FBI UCR Program anticipates completing the NIBRS business rules analysis for presentation during the Spring 2022 round of the CJIS APB. Providing one year for analysis prior to recommendations will allow the FBI UCR Program to conduct a complete outreach to stakeholders and analysis. The Data Quality Working Group will leverage the work currently in progress to analyze the NIBRS Business Rules with a focus on:

- Examine strategies for improving data submissions.
- Determine if relaxation of business rules increases data submissions.

Allowing a one-year research period will also provide the FBI UCR Program with the opportunity to review NIBRS data after the NIBRS transition is complete. In addition, outreach to the vendor community will require approval. The FBI UCR Program must identify the best mechanism for contacting and communicating with the vendor community. Through this outreach, the FBI UCR Program wants to obtain additional information to:

- Determine RMS vendors implement the NIBRS business rules.
- Determine if the FBI UCR Program can provide clarification or additional assistance with NIBRS business rules implementation.

Upon completion of outreach and analysis the FBI UCR Program will be able to provide an update and recommendations for consideration through the CJIS APB. It is anticipated all outreach and analysis will be completed for presentation by mid-2022.

Additional Analysis of the NIBRS Property Segment

The data presented within NIBRS provides a more granular view of crime data than SRS can provide. While this is evident throughout all data reported by the FBI UCR Program, NIBRS can provide more insight into property crimes than ever before. Within NIBRS, the Property Segment describes the type, value, and in the case of drug seizures, the quantity of property involved in an incident. Property information is submitted to the FBI UCR Program for specific offenses, including those within the Crimes Against Property category, Kidnapping/Abduction, Drug Narcotic, and Gambling offenses. The FBI UCR Program documentation provides guidelines on reporting property data, noting a law enforcement agency should submit a separate

Property Segment for report up to 10 types of property for each property loss.

Through the Beyond 2021 Initiative, the FBI UCR Program held discussions to address the need for enhancements to the NIBRS Property Segment. Discussions focused on what data is reported by law enforcement agencies with a particular emphasis on highlighting this data at a national level. The Measures of Harm for Crimes Against Property and Crimes Against Society SME was responsible for creating recommendations, which support the modification or creation of data elements to provide greater context within incidents that have property and society offenses. To complete this task, Task Force members and supporting SME group examined the collection and reporting of property information within NIBRS.

The Beyond 2021 Task Force recommends additional analysis, outside of the work of the Beyond 2021 Initiative be conducted. The goal of additional analysis is to determine how to enhance the Property Segment and enhance the quality of the data submitted to and published by the FBI UCR Program including:

- Continue research on restructuring the NIBRS incident to ensure property information collected is of the highest quality. This includes examination of the NIBRS business rules.
- Increase the focus on publishing property crime information.
- Determining what if any property categories can be added to NIBRS to enhance crime data.

Proposed Timeline

The FBI UCR Program anticipates providing additional information and recommendations for modifications to enhance NIBRS property information in mid-2021. This will allow the FBI UCR Program to conduct additional research and address additional requests received for review after the SME group examining crimes against property and crimes against society was established. After the Beyond 2021 Task Force made the recommendation to conduct additional research on the NIBRS Property Segment to enhance crime data, an additional request was received to expand the property codes collected when property data is submitted with an incident. When the FBI UCR Program received the request to expand NIBRS property descriptions, the SME group focused on Crimes Against Property and Crimes Against Society was given additional time to conduct further review and additional recommendations will be presented in the Fall 2021 round of the CJIS APB.

Additional Enhancements

In addition to the other enhancements and additional research recommended by the Beyond 2021 Task Force the FBI UCR Program was recommended to research the possibility of making those offenses created for federal agencies open to all law enforcement. In 2017, the FBI Director approved the addition of 21 Group A offense codes and two Group B offense codes within NIBRS for tribal and federal reporting. Through discussions and research for the Beyond 2021 Initiative, a recommendation will be forthcoming requesting opening these offenses for use by all data contributors. This request comes from research and feedback from states showing some of the offense codes can be used by state and local law enforcement agencies. Making the tribal

and federal offense codes available for all data contributors will provide uniformity amongst the data collections, meeting one of the original goals of the Beyond 2021 Initiative.

In addition to the expansion of federal offenses for all law enforcement, the Beyond 2021 Task Force recommends examining the addition of computer facilitated or cybercrime to NIBRS. The FBI UCR Program consulted with staff from the Internet Crimes Complain Center (IC3) as part of the Beyond 2021 Initiative to determine potential ways to expand the collection of offenses to include additional cybercrimes. The Beyond 2021 Task Force determined the expansion of NIBRS offenses to collect additional information on computer facilitate and cybercrimes will provide additional context to modern crimes investigated by law enforcement agencies. The FBI UCR Program anticipates presenting these topics to the CJIS APB during the Fall 2021 round.

The LEOKA data collection was also reviewed as part of the Beyond 2021 Initiative's scope. However, during this time additional factors including the passing of The Law Enforcement Suicide Data Collection Act, mandating the collection of officer suicides have impacted review of the data collection. The FBI UCR Program requires additional time for a thorough review and analysis through the work of SME groups prior to making formal recommendations for additional modifications to the LEOKA data collection. The FBI UCR Program will also be bringing forth a paper in the Fall 2021 round of the CJIS APB outlining the proposed enhancements to the LEOKA data collection.

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC M

National Data Exchange (N-DEx) Program Update

PURPOSE

To provide a program status update on activities and initiatives.

Author

Global Law Enforcement Support Section / Data Sharing Services Unit (DSSU)

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

The DSSU is currently planning, developing, and implementing numerous initiatives, which will further support the growth and effectiveness of the N-DEx System. The DSSU is providing the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) with status updates on the following program activities and initiatives:

- N-DEx System Participation
- Strategic Partnerships
- Technical Management
- Outreach Resources
- Success Story Program

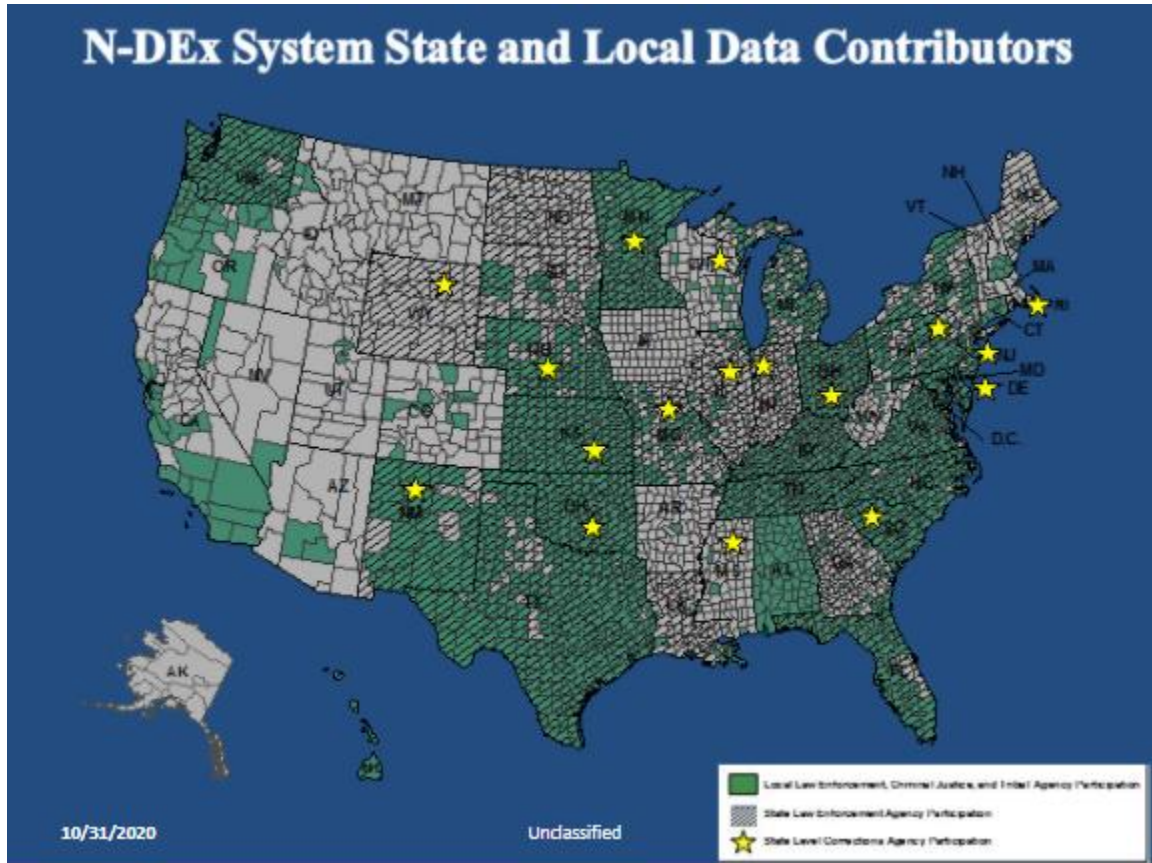
N-DEX SYSTEM PARTICIPATION

As of October 31, 2020:

- Agencies: 7,641 (Increase of 197 in fiscal year 2020 [FY20])
 - Largest (“Top 100”) law enforcement agencies: 76*
 - State Departments of Corrections: 17
- Searchable records: 880+ million (+43.4 million in FY20)
- Active FY20 users: 42,000+
- Searches: 1.6 million+ monthly average (nearly 20 million in FY20)

- Single searches: 7.8 million
- Batch searches: 12 million
- Average monthly search response time: 1.5 seconds

*Represents the largest 100 city/county law enforcement agencies by population served, per Uniform Crime Reporting population estimates.



STRATEGIC PARTNERSHIPS

The DSSU is actively leveraging strategic partnerships with additional large-scale information sharing systems outlined below to enhance the N-DEx System’s visibility and increase system use and criminal justice data.

Naval Criminal Investigative Service Law Enforcement Information Exchange (LInX)

The Naval Criminal Investigative Service (NCIS) manages LInX, an initiative designed to enhance information sharing between federal, state, and local law enforcement in areas of strategic importance to the Department of the Navy. Member agencies contribute information from their individual law enforcement records management systems to a regional system. The NCIS has partnered with the N-DEx Program Office (PO) to promote the national sharing of N-DEx and LInX data.

- All 15 LInX regions participate as a user and/or data contributor.

- 1,399 LInX agencies have contributed data.
- LInX currently contributes incident and arrest activities.
- 312 LInX agencies are not sharing data with the N-DEx System.
- The DSSU is working with LInX, CJIS Systems Officers (CSOs), and agencies to encourage broad information sharing.
- The DSSU has developed a user orientation distance learning session for new N-DEx System LInX users.
- The DSSU and LInX PO meet monthly for technical discussions.

COPLINK

Deployed in multiple states with more than 50 active regional nodes, Forensic Logic COPLINK is a law enforcement database designed to consolidate information from multiple agencies, aiding in generating tactical leads and collaboration between departments in different jurisdictions. COPLINK received grant funding through a cooperative effort with the Los Angeles Sheriff's Department to enable N-DEx System participation for all requesting COPLINK nodes, at no cost to the agency, enabling COPLINK and N-DEx System users to seamlessly search data from both systems.

- The N-DEx System is currently working with 11 known node connections.
- Nine nodes are connected for users and data contribution.
- Oregon Regional Automated Information Network is pending cloud analysis for data contribution.
- There have been no new user or data connections since 2018.
- The new COPLINK X Exporter data passed N-DEx Quality Assurance. We are currently awaiting data refresh from participating nodes.
- The COPLINK strategy will be revisited in the coming months.

Regional Information Sharing Systems (RISS)

Since 2013, the Regional Information Sharing Systems (RISS) Program has partnered with the N-DEx PO to promote and enhance national information sharing. Participating RISS users have access to the N-DEx System, making available all N-DEx System data and N-DEx System features to the RISS user.

- 38 States have approved to allow users to access the N-DEx System through RISSNET.
- Three states allow RISS Center Analysts N-DEx System access by this method.
- Three states have denied this access method.
- The Web Service (machine to machine connection) RISSIntel project is expected to begin in January 2021.
- The DSSU continues to maintain contact with RISS Regional Directors, as well as the state RISS Law Enforcement Coordinators.
- Attend quarterly teleconferences.
- Attend RISS conferences in person or via Microsoft Teams.
- Collaborated trainings in person or via Microsoft Teams.
- The DSSU conducts quarterly N-DEx System Skype sessions for RISS users.

High Intensity Drug Trafficking Areas (HIDTA)

High Intensity Drug Trafficking Area (HIDTA) Centers provide assistance to federal, state, local, and tribal agencies operating in areas determined to be critical drug trafficking regions of the US. There are 29 designated HIDTAs in the United States, cutting across all 50 states, the District of Columbia (DC), Puerto Rico, and the U.S. Virgin Islands. Two HIDTA centers currently partner with the N-DEx System, allowing access to national information sharing of N-DEx System and HIDTA data. The remaining centers are on a path for future connectivity.

- Northern California Regional Intelligence Center HIDTA
 - Identity Provider (IdP) direct N-DEx WebPortal user connection to the N-DEx System.
 - Currently submitting data to the N-DEx System.
- Washington/Baltimore HIDTA
 - IdP Web Services Logical Entity eXchange Specification Search and Retrieve (LEXS-SR) connection to the N-DEx System.
 - All 29 HIDTA Centers intend to be an IdP to the N-DEx System for direct user access.

TECHNICAL MANAGEMENT

Information Exchange Package Documentation (IEPD)

An IEPD is a compilation of documents and artifacts which provide participating agencies documentation on data specifications used for the exchange of criminal justice information. The DSSU is releasing the newest IEPD version 4.0 at <https://www.fbi.gov/services/cjis/ndex>. One of the main features is aligning the N-DEx IEPD to the National Incident-Based Reporting System (NIBRS), to allow the use of the N-DEx IEPD for NIBRS mapping tasks. The IEPD was implemented in December 2020.

Migration to the Amazon Web Services (AWS) Government Cloud (GovCloud)

The Information Technology Management Section (ITMS) is migrating the N-DEx System from the on-premise Common Compute Platform to the AWS GovCloud. The document search component of the N-DEx System has been migrated to the AWS GovCloud. The next phase of AWS GovCloud migration is entity correlation and searching. The N-DEx System migration to the AWS GovCloud is planned for completion by December 31, 2021.

Technical and Policy Engagement Process

The DSSU recently made changes to strengthen the technical and policy engagement process with the APB and N-DEx System user community. Through a focus group initiative, DSSU examined and recommended changes to improve both internal and external processes related to technical and policy changes and/or enhancements. As a result, the DSSU has identified the following for potential areas of improvement:

- Update N-DEx Analysis Review Board purview to include a pipeline of all major user facing enhancement activities.
- Leverage DSSU’s JusticeConnect service to create communities.
- Explore modernized Train-the-Trainer option with a JusticeConnect “Expert Corner” resource.
- Create a JusticeConnect "What's New?" resource for N-DEx System users.
- Email enhancement snippets related to N-DEx System interface and performance changes.
- Enhance the messaging ticker on the N-DEx System to include a larger character limit and attachment ability for portable document format (PDFs).
- Research "What's New?" 15-minute workshop rotations as an addition to distance learning.
- Include a detailed technical enhancement attachment within the N-DEx Program Status topic paper.
- Submit relevant technical enhancement and policy topics through the APB process.

OUTREACH RESOURCES

Engagement Tools

The DSSU offers a tiered approach to outreach by providing multiple levels of resources designed to complement and enhance system awareness and user education. Web-based and on-demand resources provide concise and dynamic digital resources, while leveraging technology to provide specific outreach to meet the needs of the users. Registration links are provided via email to CSOs and stakeholders, as well as in newsletters. Training resources include:

- Computer Based Training Modules
- User Workshops
- Video Tutorials
- Quick Reference Cards
- Web-based Workshop Sessions via Skype for Business

Distance Learning Workshops

The N-DEx System distance learning workshops are approximately 15 minutes to an hour in duration and include a PowerPoint presentation and an N-DEx System demonstration via Microsoft Teams. Distance learning topics rotate monthly and are offered to a variety of users with multiple access methods. N-DEx System distance learning workshop topics include:

- N-DEx System Overview and Demonstration - offered to FBI, RISS, and general users the first month of each quarter.
- N-DEx System Search Workshop - offered to FBI, RISS, and general users the second month of each quarter.

- N-DEx System Batch Search Workshop - offered to FBI, RISS, and general users the third month of each quarter.
- N-DEx System New User Orientation - offered monthly to general and LInX users.
- N-DEx System Subscription/Notification Quick Bite - offered monthly to general and RISS users.
- N-DEx CSO Workshops - include a variety of topics related to CSO functions and are offered the first month of each quarter.
- N-DEx Agency Coordinator (NAC) Workshops - include a variety of topics related to NAC functions and are offered the second month of each quarter.

The following chart provides a schedule showing the many different web-based workshops available to the N-DEx System user community for the next several months.

N-DEx Distance Learning Calendar March 2021 – September 2021							
FY21	New User Orientation	N-DEx Overview & Demonstration	N-DEx Search Workshop	N-DEx Batch Search Workshop	Quick Bite Workshop	CSO Workshop	NAC Workshop
Mar 2021	General LInX			FBI General RISS	Subscription & Notification		
Apr 2021	General LInX	FBI General RISS			Subscription & Notification	User Admin	
May 2021	General LInX		FBI General RISS		Subscription & Notification		User Administrator
June 2021	General LInX			FBI General RISS	Subscription & Notification		
July 2021	General LInX	FBI General RISS			Subscription & Notification	Training Admin	
Aug 2021	General LInX		FBI General RISS		Subscription & Notification		Training Administrator
Sept 2021	General LInX			FBI General RISS	Subscription & Notification		

The distance outreach workshops have proven to be highly successful. The following chart reflects the number of sessions offered over the course of FY20 to FBI field offices (FOs), CSOs, and external users, as well as the overall participation for those sessions. Note participation includes DC, Guam, Saipan, American Samoa, and Singapore users.

FY 20 N-DEx Distance Learning Workshop Participation			
FY20	FBI	CSO	External
October 2019	4 Sessions 176 Attended	3 Sessions 24 Attended	8 Sessions 36 Agencies 48 Attended
November 2019	4 Sessions 110 Attended	1 Session 3 Attended	6 Sessions 60 Agencies 72 Attended
December 2019	5 Sessions 17 Attended		5 Sessions 32 Agencies 49 Attended
January 2020	4 Sessions 67 Attended	2 Sessions 31 Attended	4 Sessions 25 Agencies 33 Attended
February 2020	5 Sessions 36 Attended		8 Sessions 44 Agencies 109 Attended
March 2020	1 Session 5 Attended		6 Sessions 27 Agencies 63 Attended
April 2020	1 Session 5 Attended	2 Sessions 21 Attended	19 Sessions 115 Agencies 484 Attended
May 2020	On hold		19 Sessions 111 Agencies 284 Attended
June 2020	On hold		20 Sessions 96 Agencies 540 Attended
July 2020	On hold	2 Sessions 33 Attended	21 Sessions 157 Agencies 399 Attended
August 2020	On hold		14 Sessions 133 Agencies 263 Attended
September 2020	On hold		16 Sessions 158 Agencies 355 Attended
FY20 Participation	24 Sessions 416 Attended 35/56 FOs	10 Sessions 112 Attended 35/50 States (plus DC)	143 Sessions 994 Agencies 2699 Attended 50/50 States (plus DC, Guam, Am. Samoa, Singapore, and Saipan)

N-DEx System Points of Contact

For more information about user engagement resources or N-DEx System participation, please contact the respective point of contact outlined below:

N-DEx Liaison Specialists
Rita Jo Willis, Acting Supervisor <riwillis@fbi.gov> 304-625-4822

Region	Specialist	Contact Information
WESTERN & DoD	Jay Summers	<jsummers@fbi.gov> 304-625-2455
NORTH CENTRAL	John Bush	<jbush@fbi.gov> 304-625-7053
SOUTHERN	Dale Smith	<dasmith6@fbi.gov> 304-625-4826
NORTHEASTERN	John Tittle	<jmtittle@fbi.gov> 304-625-7641
FEDERAL AGENCIES (Except DoD)	Bellinda Cumpston	<bcumpston@fbi.gov> 304-625-4398

The map shows the following regional assignments:
- **Western (Yellow):** WA, OR, ID, MT, WY, NV, UT, CO, AZ, NM, TX, CA, HI, GU, AK, MP, Commonwealth of the Northern Mariana Islands.
- **North Central (Green):** ND, MN, WI, MI, SD, IA, IL, IN, OH, NE, KS, MO.
- **Southern (Blue):** KY, WV, VA, NC, TN, AR, MS, AL, GA, SC, OK, LA, FL.
- **Northeastern (Orange):** NY, PA, NJ, DE, DC, MD, CT, RI, MA, VT, NH, ME.
- **Other:** PR - Puerto Rico, VI - Virgin Islands.

Updated: 05/20/2020

CELEBRATING SUCCESS

The N-DEx Success Story of the Year Award was created to recognize the best success story, as submitted by N-DEx System users and selected by CJIS Division Executive Management. The concept of the Success Story of the Year Award began in 2013, and the first award was presented in January 2015. The first Success Story of the Year was given jointly to the Maryland State Police and the Bureau of Alcohol, Tobacco, Firearms, and Explosives for their success on discovering thousands of cartons of counterfeit cigarettes. Last year's recipient, a case involving a child predator posing online as a wealthy prince, was awarded to Wayland Police Department in Michigan. This year's award was chosen from 32 stories submitted by N-DEx System users from searches conducted in 2019.

Winner of the 2020 Success Story of the Year

United States (U.S.) Department of Housing and Urban Development (HUD), Office of Inspector General (OIG)

A special agent with the U.S. HUD OIG had been conducting an international money laundering investigation since 2014, involving over 100 subjects. The investigation was initiated based on information indicating an agency employee had been suspected of laundering money. The investigation confirmed the employee was laundering money, and her boyfriend illicitly received millions of dollars. The pair was linked to an organized crime group, which involved money laundering, interstate human trafficking, drug transportation, and real estate fraud. The agent broke the case after using the N-DEx System to search phone numbers contained in N-DEx System records. The N-DEx System returned police reports from across the country, mostly from the Las Vegas Metro Police Department (LVMPD), linking previously identified prostitution victims to the boyfriend. The victims were interviewed and provided crucial information about the operation's key players, structure, and methods of illicit activities. The money laundering organization spanned coast to coast, including major cities, such as Chicago, Miami, Dallas, Las Vegas, and San Francisco. In addition, money was traced internationally via online casinos. The agent stated, "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. The investigation is coming to an end and will involve major indictments." The agent concluded to say, "N-DEx has been there by my side the whole time. However you are getting the information in there, keep doing it, and we will keep solving investigations."

Excellence in Information Sharing Awards

The DSSU also recognized four Excellence in Information Sharing Award recipients. Each recipient and their respective scenarios are detailed here:

- **FBI-specific award for the Atlanta FO**

Operation Safe Summer was led by the FBI's Metro Atlanta Child Exploitation and Human Trafficking (MATCH) task force, where the N-DEx System, via its batch search feature, assisted in locating 14 missing children and multiple sex offenders.

- **LVMPD**

The LVMPD received a call requesting a welfare check. When the officers went to the location the victim was found unconscious in the bathtub face down in her own blood. The N-DEx System assisted in finding the suspect in the attempted murder, which was the ex-husband of the victim. Using a name and physical descriptors, the investigators used the N-DEx System to positively identify the subject and obtain several addresses in Texas, where he could be located. He was arrested several weeks later in Texas and extradited for prosecution.

- **San Pasqual, California, Police Department**

A tribal member and employee of the San Pasqual Band of Missions Indians did not show up for work as scheduled. Co-workers went to check on him at his residence and found him deceased, as a result of an accidental overdose. The San Pasqual Police Department used the N-DEx System to ultimately locate the drug supplier, who was apprehended while in a vehicle actively selling drugs. Within the vehicle, agents seized two hundred OxyContin laced with Fentanyl, as well as an additional 200 OxyContin, 84 grams of heroin, 14 grams of cocaine, cash, and a firearm from the residence.

- **Shreveport, Louisiana, Police Department**

The Shreveport, Louisiana, Police Department used the N-DEx System to help locate the witness to a 2016 rape and murder case. No further details can be released at this time.

The DSSU expresses its sincere appreciation and recognition to all recipients and their agencies for furthering the mission of protecting the U.S., promoting public safety, and supporting information sharing efforts across the nation. Please remember the DSSU is actively gathering successes for the next Success Story of the Year Awards. Please submit N-DEx System successes via the N-DEx System's User Feedback link or via email ndex@leo.gov.

Appendix: Technical Build Schedule

COMPLETED ENHANCEMENTS

SUMMARY/REQUEST	DESCRIPTION	DEPLOYMENT DATE
Implemented LEXS-SR 4.0 Search and Notification	Ability to search the N-DEx System using IEPD 4.0.	Summer 2020
Implemented LEXS-SN 4.0 Subscribe and Notify	Ability to set notifications using IEPD 4.0.	Summer 2020
Batch Search Templates	Removed Batch Search templates.	Spring 2020
Batch Search Counts	Added a column on user interface with the total number of Batch Search terms.	Spring 2020
IEPD 4.0 LEXS 5.0	Upgraded the system to allow agencies to submit data using the latest IEPD.	Winter 2020
Alfresco Collaboration/ JusticeConnect	Replaced Alfresco Collaboration software with link to the Law Enforcement Enterprise Portal Justice Connect.	Summer 2020
Entity Correlation	Upgraded Entity Correlation to newer version.	Summer 2020

UPCOMING ENHANCEMENTS

SUMMARY/REQUEST	DESCRIPTION	DEPLOYMENT DATE
CSO New User Notification	Modify CSO New User Notification to include new users searching via LEXS-SR.	Spring 2021
Automated Welcome for New Users	New users will receive a welcome notification when signing on for the first time. This can include training and tips for using the system.	Spring 2021
Highlight Search Terms	The user's search term will be highlighted in the returned document.	Summer 2021

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC N

National Crime Information Center (NCIC) Enterprise File Transfer Service (EFTS) Migration Update

PURPOSE

To advise the NCIC user community of the Criminal Justice Information Services (CJIS) Division's progress on migration from the NCIC File Transfer Protocol (FTP) server to the EFTS.

AUTHOR

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

The NCIC FTP server facilitates the transfer of large data files from the NCIC system to its users. CJIS System Agencies (CSAs) and direct connect agencies interface with the FTP server to access and download requested files. Files are then dispersed by the interfacing agency to end users as necessary. Examples of files transferred via the FTP server include lists of records to be validated, requested NCIC data extracts, statistical reports, and offline search results.

During the NCIC 3rd Generation (N3G) Canvass, users requested an improved method of large file retrieval. Users desired a user-friendly and intuitive process for downloading files. Additionally, agencies suggested a service be developed with decreased manual interaction. The user requests were considered by the N3G Task Force and resulted in functional requirement ***12.02.TF03 NCIC shall explore additional methodologies to facilitate file transfers.*** By approving the functional requirement, the N3G Task Force acknowledged the need to improve the current mechanism and reserved the selection of the solution for the CJIS Division.

Security deficiencies have been identified in the NCIC FTP Server. Due to its critical standing, the CJIS Division justified the continued use of the FTP server. However, the security concerns

expedited the selection of a suitable replacement file transfer server.

The EFTS was selected to provide convenient file transfer and to address the outstanding security issues. Interfacing agencies can access the NCIC EFTS server through the interface on the Law Enforcement Enterprise Portal (LEEP) or a machine-to-machine connection. The EFTS allows large data files to be rapidly transferred to users in a secure fashion. The EFTS also offers a user-friendly and intuitive interface. Furthermore, agencies can automate file retrieval if using the machine-to-machine connection.

DISCUSSION

The CJIS Division initially engaged the user community concerning the migration to EFTS during the Spring 2020 Working Group Meetings. At that time, the migration effort was in its infancy and information was limited. During the subsequent months, the CJIS Division has made significant strides to ensure external users can access valuable information through the EFTS. CSAs and direct connect agencies can already retrieve the following files:

- Monthly lists of records to be validated
- Biennial Originating Agency Identifier validation file
- License Plate Reader extract
- Pawn Gun and Article data extracts
- Authorized CSA or agency specific extracts
- NCIC offline search results

The CJIS Division anticipates all files downloaded by external agencies will be successfully migrated from the NCIC FTP server to EFTS by March 31, 2021.

The CJIS Division also improved the ability to select and retrieve relevant files. In July 2020, validation lists were made available to all CSAs in both the \$.C. Request for Validation Notification format and the fixed format. By allowing access to both formats, CSAs may easily determine the format best suited for their validation procedures. Additionally, the CJIS Division reviewed the NCIC data extracts and created new naming conventions for many EFTS files. The new file names describe the files' contents in greater detail.

In September 2020, the CJIS Division provided a product demonstration for the N3G Task Force in accordance with the N3G Project's agile friendly Advisory Process. The demonstration highlighted the LEEP user interface and rapid download of large data files. The N3G Task Force determined the EFTS met the intent of FR 12.02.TF03 and was a suitable replacement file transfer server for the needs of the NCIC user community.

Several state and federal agencies have already obtained access to the EFTS server and successfully downloaded NCIC data files. All files will continue to be housed on both the NCIC FTP Server and EFTS until a sunset date is established. The *Sunset Date for FTP* action topic paper will leverage the CJIS Advisory Process to determine the sunset date.

CSAs and direct connect agencies interested in transitioning to EFTS should contact their NCIC Regional Representative for additional information. The most recent EFTS User Manual and account request form are accessible via LEEP on the NCIC JusticeConnect community to assist the transition.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC O

Criminal Justice Information Services (CJIS) Division National Crime Information Center (NCIC) Status

PURPOSE

To provide a status report on the NCIC System.

AUTHOR

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

STATISTICS

- End of Fiscal Year 2020 statistics are as follows:
 - Average number of transactions processed per day was 7,922,014. There has been a decline in daily transactions due to COVID-19, but transactions are starting to increase.
 - Average response time per transaction was 0.0069 seconds.
 - System availability was running at approximately 99.70 percent with planned maintenance.

- The NCIC System record processing day remains the same. The NCIC System processed 18,617,237 on Thursday, April 6, 2017, with an average response time of .0216 seconds.

REGULARLY SCHEDULED MAINTENANCE

The regularly scheduled maintenance for the NCIC System occurs the first Tuesday of each month from 4 a.m. to 6 a.m., Eastern Standard Time. Please note, in addition to the regularly

scheduled maintenance in July, the CJIS Division will conduct a disaster recovery drill, adding an additional hour to the maintenance time starting at 3 a.m.

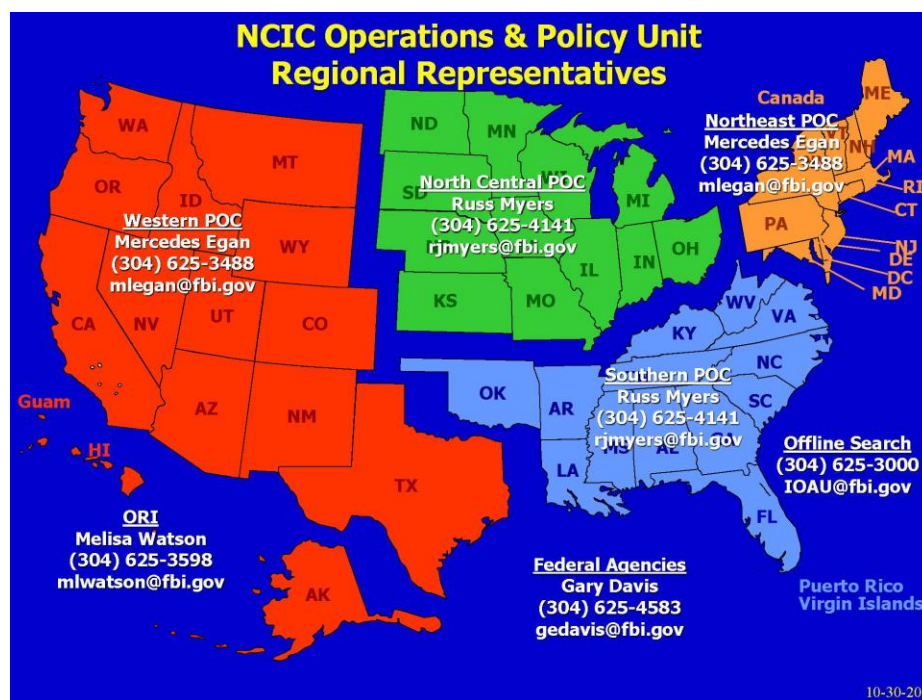
Maintenance Date	From	To	Total Hours	Out of Service
10/06/2020	04:00 a.m.	06:00 a.m.	2	YES
11/03/2020	No Planned Outage		0	NO
12/01/2020	04:00 a.m.	06:00 a.m.	2	YES
01/05/2021	04:00 a.m.	06:00 a.m.	2	YES
02/02/2021	04:00 a.m.	06:00 a.m.	2	YES
03/02/2021	04:00 a.m.	06:00 a.m.	2	YES
04/06/2021	04:00 a.m.	06:00 a.m.	2	YES
05/04/2021	04:00 a.m.	06:00 a.m.	2	YES
06/08/2021	04:00 a.m.	06:00 a.m.	2	YES
07/13/2021	03:00 a.m.	06:00 a.m.	3	YES
08/10/2021	04:00 a.m.	06:00 a.m.	2	YES
09/14/2021	04:00 a.m.	06:00 a.m.	2	YES

TESTING

The CJIS Division maintains two test environments for NCIC users to conduct testing with the NCIC System. The first test system, Operational Test, can be accessed by using the appropriate header which starts with a “T”. Test records are currently accepted as TN01 transactions. This test system should be accessed for user training purposes only.

The second system, First Level Integration (FLI), uses a different Internet Protocol address than the operational environment and can be accessed using the standard header data, 1N01 or the Operational Test header, TN01. The test transactions in the FLI do trigger notifications. This test system should be accessed for any type of testing whether for user training or for software development purposes. The testing environments are operational 24/7, excluding infrequent maintenance activity.

Questions concerning the test environments and their usage may be directed to the appropriate NCIC Regional Representative listed below. Technical issues with the NCIC test environments may be directed to the CJIS Division Help Desk at 304-625-HELP (4357).



NCIC EXTENSIBLE MARKUP LANGUAGE (XML)

- The NCIC National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD) version 2.0, located in the NCIC Community within JusticeConnect via the Law Enforcement Enterprise Portal, was released in August 2020. This version will be available in the FLI in February 2021, and will move to the operational environment in August 2021. Some noteworthy changes in the IEPD include Unified Modeling Language diagrams, a change log file to document all major updates, and updated sample messages to include missing Message Field Codes.

The NCIC Regional Representatives notified all CJIS System Officers (CSOs) of the new version. Please contact your Regional Representative if you have any questions.

- One CJIS System Agencies (CSA) is currently testing NIEM XML, and one CSA has completed testing and is currently operational.

All CSOs are encouraged to contact their NCIC Regional Representative listed above and move towards NIEM. The representative will provide the necessary documentation and will coordinate a teleconference with the CSO and/or technical staff to obtain required information and answer any questions that arise.

- Based on user requests and feedback, the CJIS Division is developing XML presentation style sheets for NCIC system responses that will assist CSOs and local users in their transition to NIEM XML. These presentation style sheets will be available to CSOs and local agencies for modification, but will not be maintained by the CJIS Division. The

Presentation Style Sheets are expected to be available in early calendar year 2021.

- There was an overwhelming concern regarding support for users who are not ready to transition to NIEM XML, as well as the cost associated with developing style sheets for that support. Therefore, the CJIS Division is developing Transformation Style Sheets, which will be used to transform the NCIC NIEM XML format into NCIC dot-delimited format for those users. The Transformation Style Sheets are on track to be completed in early 2021, and will be provided as requested.
- As a reminder, dot-delimited and Global Justice XML Data Model (GJXDM) XML formatted messages, along with Transmission Control Protocol/Internet Protocol (TCP/IP) socket and message queue series protocols, will no longer be supported after September 30, 2022.

NCIC ENHANCEMENTS

- Below is a list of NCIC enhancements, including pending enhancements, since the last round of Working Group meetings. The NCIC Build schedule constantly evolves due to programming requirements, manpower, and overall impact on the NCIC database baseline. Please note, when a Technical and Operational Update is published supporting an NCIC Build, the one year notification process occurs, and it is followed by a reminder letter in six months. For enhancements not affecting state programming, during the December 2002 CJIS Advisory Policy Board meeting, a motion passed to limit the minimum notification to three months.

PENDING NCIC ENHANCEMENTS AS OF 10/01/2020						
ENHANCEMENT		PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	FBI TENTATIVE WORK TIMELINE	IMPLEMENTATION DATE
255	Inclusion of Blue Alert in the NCIC	3H	12/2019	Yes	2020	Implemented in the operational environment on January 5, 2021. This topic is now closed.
256	Endorse the creation of a new NCIC file specifically for the entry of Extreme Risk Protection Orders (ERPOs)	3H	12/2019	Yes	2021	The ERPO File Concept of Operations is being presented to the Advisory Process in spring 2021. Once approved by the APB and the FBI Director, the file will be created and begin with availability in the FLI.

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC P

Programs Research and Standards Unit (PRSU) Update on Contactless Fingerprint Collection Studies

PURPOSE

To summarize the recent activities related to the study of contactless fingerprint matching capability with legacy contact prints and status on certification of contactless collection devices.

AUTHOR

Global Law Enforcement Support Section, PRSU

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office (APMO) via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. The APMO will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

Contactless fingerprint technology may offer a rapid and hygienic alternative to conventional fingerprint capture equipment, such as live-scan devices. However, there are challenges in using contactless capture of fingerprints. The biggest challenge is the images are not of forensic quality. While it is easy to distinguish topographical highs (ridges) and lows (valleys) in a contact collection, this is not the case with contactless fingerprints. The illumination of a three-dimensional (3D) object, as is done with contactless collection, creates complicating factors such as over-illumination, shadows, and reversal of polarity (ridges appearing as valleys and vice versa). Additionally, although most contactless devices were designed to record the entire friction ridge surface nail-to-nail, analogous to a rolled fingerprint, the lighting challenges, curvature of the finger, and depth of focus limitations may only yield a portion of the fingerprint that would be more analogous to a flat impression.

In a previous update to the APB, the PRSU presented evaluation results of contactless device performance obtained through PRSU's work with the National Institute of Standards and Technology (NIST). The following diagram, taken from the *NIST Interagency/Internal Report*

Information Only Topic P, Page 1

(NISTIR) 8307, shows the performance of various contactless devices supplied by vendors participating in NIST’s contactless Cooperative Research and Development Agreement (CRADA), compared against devices certified to meet NGI image quality specifications as outlined in Appendix F of the FBI’s *Electronic Biometric Transmission Specification (EBTS)* document. The threshold of 4100 was determined to be the best measure of operational performance for the fingerprint matcher. It is important to note the following results are based on a small set of 200 subjects with a gallery dataset of 3 million, which are representative of the FBI database, and the fingerprints were taken under controlled laboratory conditions.

Table 1 - True Positive Identification Rate/False Positive Identification Rate (%) at threshold 4100 - from NISTIR 8307

	Single Finger		Fingers 02, 03		Fingers 02, 07		Fingers 02, 03, 07, 08		Fingers 02, 03, 04, 05		Fingers 07, 08, 09, 10		Eight Fingers	
	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR	TPIR	FPIR
Dev01	96.00	0.26	98.97	1.55	98.97	1.55	99.48	1.55	98.97	1.55	98.97	1.55	99.81	1.55
Dev02	91.49	0.19	97.95	1.54	98.97	1.54	99.49	1.53	98.47	1.53	98.98	1.53	99.49	1.53
Dev03	83.73	0.19	94.97	1.51	96.48	1.51	98.99	1.51	95.98	1.51	96.48	1.51	98.49	1.51
Dev04	68.83	0.25	86.80	1.52	84.34	1.52	89.39	1.52	92.89	1.52	88.78	1.53	91.92	1.52
Dev05	45.51	0.19	75.88	1.51	77.00	1.50	86.00	1.50	81.91	1.51	74.37	1.51	88.00	1.50
Dev06	45.84	0.19	76.80	1.55	77.84	1.55	78.87	1.55	76.80	1.55	78.35	1.55	78.35	1.55
Dev07	20.42	0.19	48.73	1.52	55.05	1.52	59.60	1.52	51.78	1.52	52.53	1.52	63.13	1.52
Dev08	53.28	0.19	86.87	1.52	90.91	1.52	92.42	1.52	87.88	1.52	85.35	1.52	89.39	1.52

Dev01 & Dev02 (Certified Contact Devices), Dev03 & Dev04 (Stationary Contactless), Dev05 – Dev08 (Mobile Contactless)

Analysis of the above table shows contactless matching is much improved when considering multiple fingers, but still yields lower True Positive Identification Rates (TPIR) than legacy contact devices. Matching performance appears to fall into three tiers of performance. The two contact devices fall into the highest performing tier. The second tier, with a slightly lower performance, consists of the two stationary contactless devices. Finally, the third tier, with inconsistent performance across devices, consists of the mobile smartphone contactless devices.

CONTINUED TESTING

NISTIR 8315, published September 15, 2020, shows contactless results using a fingerprint matcher configured in tenprint mode and mobile identification (Mobile ID) mode. The testing was done using eight fingerprints of a subject. Thumbs were excluded because many contactless devices cannot collect thumbs in a timely manner due to its anthropometric positioning. The evaluation showed the Mobile ID matcher handles the contactless images better than a matcher configured for tenprint. This could be because Mobile ID matchers are built to operate on cropped fingerprint images, which are smaller than a full fingerprint impression and operate on fewer than a full set of ten fingerprints.

The highlighted areas in the table below show the accuracy (as False Negative Identification Rate [FNIR] at two operational thresholds) of contactless probes against a contact database, since that is the most relevant use case for law enforcement. As a reference, the worst performing contact-to-contact (contact probe against a contact database) performs at 0.5 FNIR using a matcher configured for tenprint. The relatively small size of the dataset (193 subjects) in this study allows for a meaningful examination of FNIR behavior, but generation of statistically significant false positive error rates would require a contactless data set of at least 2,000 subjects. PRSU is actively pursuing larger data sets to support such testing; however, at the current time none are available.

The devices used in the study are identified as follows:

- D1 – An optical (Frustrated Total Internal Reflection [FTIR]) contact-based Appendix-F-certified capture device.
- D2 – An electroluminescent (EL) contact-based Appendix-F-certified capture device.
- D3 – A tabletop (stationary) contactless capture device.
- D4 – A tabletop (stationary) contactless capture device.
- D5 – A mobile (phone) contactless capture device.
- D6 – A mobile (phone) contactless capture device.
- D7 – A mobile (phone) contactless capture device.
- D8 – A mobile (phone) contactless capture device.

Note: Subjects processed on D1 were captured twice, Encounter 1 (E1) and Encounter 2 (E2).

Test cases are summarized in the following format (second column):

(Device Number Populating Database) ◀ (Probe Device Number)
 or
 (Device Number Populating Database) ◁ (Probe Device Number)

The symbol “◀” denotes control cases where both probe and biometric reference database contain ONLY contact captured fingerprints. The symbol “◁” denotes all other cases (can be a mix of contactless versus contact or contactless versus contactless).

Table 2 - Calculated Accuracy Data – Mobile ID Matcher at Operational Thresholds, Sorted in Ascending Order of FNIR at T=4100.

		Best performing stationary contactless	
		Another stationary contactless device	
		All mobile contactless devices	
Trial #	Database ◁ Probe	FNIR (%), T=3000 (Mobile ID Green)	FNIR (%), T=4100 (Mobile ID Yellow)
1	D1-E1◀D1-E2	0	0
2	D1-E1◀D2	0	0
3	D1-E1◁D3	0	0
4	D1-E2◀D1-E1	0	0
5	D1-E2◀D2	0	0

6	D1-E2<D3	0	0
7	D2<D1-E1	0	0
8	D2<D1-E2	0	0
9	D2<D3	0	0
10	D3<D1-E2	0	0
11	D3<D2	0	0
12	D3<D6	0	0
13	D4<D6	0	0
14	D6<D2	0	0
15	D6<D5	0	0
16	D6<D8	0	0
17	D7<D2	0	0
18	D7<D6	0	0
19	D8<D6	0	0
20	D1-E1<D4	0	0.5
21	D3<D1-E1	0	0.5
22	D4<D8	0	0.5
23	D7<D1-E1	0.5	0.5
24	D7<D1-E2	0.5	0.5
25	D7<D3	0	0.5
26	D7<D8	0	0.5
27	D8<D1-E1	0.5	0.5
28	D1-E2<D6	0.6	0.6
29	D5<D6	0.6	0.6
30	D6<D1-E2	0.6	0.6
31	D6<D3	0	0.6
32	D6<D4	0.6	0.6
33	D4<D2	0	0.8
34	D8<D2	0.8	0.8
35	D2<D6	1	1
36	D3<D4	0.5	1
37	D4<D1-E1	0	1
38	D4<D1-E2	0	1
39	D4<D3	0	1
40	D4<D5	0	1
41	D5<D4	0	1
42	D7<D4	0.5	1
43	D8<D1-E2	0.5	1
44	D8<D3	0.5	1
45	D6<D1-E1	0	1.2
46	D1-E1<D8	0.5	1.5
47	D1-E2<D4	0	1.5
48	D3<D8	0.5	1.5
49	D5<D1-E1	0.5	1.5
50	D2<D8	0.8	1.6
51	D5<D2	0	1.6
52	D2<D4	0.8	1.7
53	D1-E1<D6	0.6	1.8
54	D6<D7	0.6	1.8
55	D1-E2<D8	0	2
56	D5<D3	0.5	2
57	D7<D5	1.5	2
58	D8<D4	1	2
59	D1-E2<D5	0.5	2.5
Trial #	Database < Probe	FNIR (%), T=3000 (Mobile ID Green)	FNIR (%), T=4100 (Mobile ID Yellow)
60	D2<D5	0	2.5
61	D3<D5	0.5	2.5
62	D3<D7	0.5	2.5
63	D5<D1-E2	1	2.5
64	D5<D7	1	2.5
65	D8<D5	0	2.5
66	D1-E2<D7	1	2.6
67	D8<D7	1	3
68	D1-E1<D5	1	3.1
69	D2<D7	0.8	3.3
70	D1-E1<D7	2	3.6
71	D4<D7	3	4
72	D5<D8	2	4

Information Only Topic P, Page 4

Analysis of the above table shows the best performing stationary contactless device does quite well matching against a contact database using a Mobile ID configured matcher. However, apart from a few exceptions, the accuracy of using fingerprints from contactless devices matching against a contact database, taken as a whole, generally perform worse than the worst performing contact-to-contact results (0.5 FNIR) on the tenprint matcher. All contact-to-contact had a 0.0 FNIR using the Mobile ID matcher)

In evaluating the same data using the matcher configured for tenprint matching (not shown- Table 5 from *NISTIR 8315*), results showed the contact-to-contact cases emerged as most accurate, with the FNIR ranging from 0 percent to 0.5 percent. The best performing contactless device was a stationary device, which yielded an FNIR of 1.6 percent. While this error rate is small taken by itself, this jump in error for the contactless biometric reference database utilization represents a 320 percent increase in FNIR versus the worst performing contact-to-contact case (FNIR of 0.5 percent for contact biometric reference database vs contact probe, versus FNIR of 1.6 percent for contactless database vs contact-probes)¹. While the 1.6 percent FNIR represents the best performance when using contactless images as the gallery, typical error rates are much higher. The FNIR rates using a gallery of contactless images range from a best of 5% to a worst of 39.7 percent. A 5 percent FNIR would represent a 1000 percent increase in error rate versus the worst performing contact-to-contact case.

Also, of note, the post-capture, proprietary digitization processes used to create grayscale or binary images, which more closely resemble legacy contact fingerprints, cannot be easily explained and could erode confidence if used in a courtroom.

CERTIFICATIONS AND STANDARDS

In order to enable certification of contactless devices, new test methods and test targets are needed. The PRSU is currently funding the development of both in collaboration with the NIST. Test targets are needed to provide a quantitative measure of image quality and ensure the testing of contactless collection resembles the use of these devices in operational scenarios.

Current device certifications are based on the configuration of hardware and software. With the turnover rate of smartphone devices, each change of platform would require a separate certification. However, from documented test results, contactless fingerprint devices are unable to achieve the same match performance level as FBI certified fingerprint devices. Once comparable performance is attained, the PRSU will take a more active position on this subject.

The NIST has been working on a specification for the evaluation of the matching capability of contactless fingerprint acquisition devices. The protocol, when approved and fully implemented, will use a suite of 3D targets fabricated from polycarbonate and later replicated in polydimethylsiloxane (PDMS) to measure the fidelity of two-dimensional (2D) legacy

¹ An example of this effect using FY2020 NGI total receipts of 45,734,030 would be missed identifications rising from 228,670 (0.5 percent) to 731,744 (1.6 percent).

compatible image output of the devices to exemplars captured using contact technology. In essence, images collected from contactless devices of these 3D targets will be compared against images collected from certified contact devices to evaluate matching capability.

The 3D test targets will be machine engraved with various testing patterns, such as:

- Horizontal and Vertical Ronchi rulings – to evaluate geometric distortion in what should be evenly spaced bars of constant width relative to contact exemplars of the artifact.
- Concentric circles - for testing for contrast reversal.
- Fingerprint Engravings – for comparison of images from contactless and contact.
- Smooth Polycarbonate Rod – to reveal “feature noise” created by errors in ridge reconstruction algorithms.

The test procedures being drafted by the NIST will allow the PRSU to determine contactless device matching capability against legacy databases. Image quality, as defined in Appendix F of the *EBTS* or Personal Identity Verification specifications, were deemed inappropriate for evaluating contactless images. This is because 2D targets cannot account for aspects such as illumination effects on a 3D surface. The finalized procedures document is expected to be delivered by the third quarter of fiscal year 2021.

INTERAGENCY COLLABORATION/DISCUSSION

The PRSU has been in communication with the Michigan State Police and New Jersey State Police about possible pilot projects to evaluate the usefulness of contactless images for criminal searches.

The PRSU has also had communication with the Department of Homeland Security about the prospect of using contactless collection for civil pre-check screenings. An interagency working group has been established to review policy, process, technology issues, and challenges involving contactless prints.

NEXT STEPS

The PRSU will continue to assess and evaluate contactless technology to ensure matching capability with existing databases and to develop a certification pathway for evaluating contactless devices. The PRSU continues to welcome communication and collaboration with other agencies to determine ways to further the advancement of contactless technology.

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC Q

FBI Programs Research and Standards Unit (PRSU) Update

PURPOSE

The purpose of this staff paper is to provide an update on PRSU projects and activities.

AUTHOR

Program Research and Standards Unit (PRSU), Global Law Enforcement Support Section (GLESS)

FEEDBACK

Please send all questions or comments concerning this topic to the Advisory Process Management Office (APMO) at facsimile, (304) 625-5090 or e-mail: AGMU@leo.gov. Feedback can also be submitted via the electronic feedback form found on the Law Enforcement Enterprise Portal's Special Interest Group (SIG) service under the CJIS SIG, Advisory Process Information tab, Upcoming Meeting Information and Topic Papers. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

Part of the PRSU's mission is to research, develop, and implement technology to increase efficiencies and productivity in the fight against crime and terrorism. The PRSU strives to enhance stakeholder capabilities by promoting biometric and identity management capabilities while also supporting multimodal system development and interoperability. The PRSU provides a range of services including the testing and evaluation of biometric technologies; performing various research and development projects; developing biometric prototypes, pilots, and toolsets; promoting and developing biometric standards and biometric best practices; and addressing privacy and policy issues as needed. While PRSU is currently engaged in several biometric research and development projects, the following activities have been a primary focus of the PRSU and will hopefully provide useful insight into the areas of forensic iris adjudication, biometric algorithm evaluations, and postmortem biometrics. The PRSU also collaborates with the FBI Laboratory Division regarding deoxyribonucleic acid (DNA) research activities. As such, an overview of the Laboratory Division's research and development activities with regard to DNA have also been included in this paper.

DNA Forensic Analysis

The FBI and the National Institute of Standards and Technology (NIST) have worked successfully for over 30 years to drive the improvement of DNA analysis as a forensic discipline. The collaboration continues with Booking Station Rapid DNA integration and the development of Rapid DNA for crime scene analysis. More recently, the two groups have been working on methods to assess DNA mixture interpretation with probabilistic genotyping software. New collaborations are under way to expand FBI population datasets and investigate the combining of forensic DNA markers to increase the discrimination power of forensic DNA matching statistics. The investigation of next generation sequencing as an emerging method for DNA analysis has resulted in updated population allele frequencies to support improved one-to-one matching statistics. Sequencing has also been assessed for utility in analyzing degraded samples and the prediction of biogeographical ancestry, as well as eye and hair color. Finally, the groups continue to work on research for direct-to-DNA workflows involving DNA quantification, direct polymerase chain reaction (PCR) methods and DNA extraction optimization.

Forensic Iris Adjudication Efforts

The PRSU developed and managed the FBI's Iris Pilot from 09/20/2013 until iris functionality was integrated into the Next Generation Identification (NGI) System on 09/29/2020. In addition to this effort, PRSU has conducted various research activities to support iris adoption within the law enforcement and criminal justice communities as well as bolster the relevance of iris in the biometric and forensic communities at large.

The PRSU, in conjunction with the NIST, formed the Iris Experts Group (IEG-II) in 2015. IEG-II consists of individuals from federal, state, and local agencies, research entities, and vendors with a vested interest in iris recognition technology. Collaboration between these groups allows information sharing and cross fertilization of ideas pertinent to iris related issues. Two ongoing efforts within the group include "Iris Examiner Training" and "Iris Camera Selection Guidance". These two groups meet monthly with the goal of creating guidance to develop human examiner skills specific to iris and to provide recommendations on what types of iris cameras agencies should purchase based on their use case (e.g. mobile identification versus booking station). Anyone interested in iris is welcome to join IEG-II regardless of background or technical knowledge. For more information on IEG-II and to subscribe to the mailing list, please visit <https://www.nist.gov/programs-projects/iris-experts-group-ii-homepage>.

In addition, PRSU has undertaken multiple forensic iris identification efforts. The PRSU is working to establish an ontology of markable iris features to assist human examiners. This ontology will determine if a detectable feature is properly defined and can be used to effect identification or an exclusion. Once these features are defined, PRSU plans to develop prototype software to assist examiners in locating those features in an iris image. This software will then be incorporated into the PRSU's prototype iris analysis tool, which allows side-by-side iris comparisons. Findings from this project will help directly contribute to overall acceptance of iris comparison techniques from biometric and forensic communities.

Ongoing Biometric Algorithm Evaluations

The FBI has a long-standing relationship with NIST, wherein NIST provides critical validation of FBI operational technology. As an example, PRSU has continually sponsored NIST to conduct biometric algorithm vendor tests. For decades, NIST has demonstrated subject matter expertise for conducting these tests for the biometrics community. These evaluations provide valuable insight into the performance capabilities of automated biometric matching products. Both federal and state governments leverage these products in their automated biometric identification systems; the FBI NGI System is one example.

In the past, these vendor tests were typically held every three years. Going forward, NIST will be making “ongoing” vendor tests available. This platform enables vendors to submit new biometric matching algorithms to NIST at their discretion. This approach better aligns with vendor development schedules and affords the law enforcement and criminal justice community near real-time awareness of state-of-the-art biometric accuracy and performance capabilities.

Currently, “ongoing” vendor testing is available for face, iris, and latent fingerprint algorithms. How does the “ongoing” platform work and how can an agency stay informed on results? It is simple. The vendor community is actively submitting their algorithms to NIST for evaluation. Once the NIST receives the algorithm submission from the vendor, in most cases they are able to publish performance results to the corresponding modality leaderboard within 60 days. The modality leaderboards can be found by visiting the following NIST web site at <https://www.nist.gov/programs-projects/biometrics>. Never before has access to such valuable information been possible. Now agencies can easily check the modality leaderboards to determine who is at the top and, more importantly, the position of their vendor’s product.

Technology is rapidly advancing every day across all industries. “Ongoing” vendor algorithm testing provides a mechanism for the law enforcement and criminal justice community to maintain awareness of advancements within the automated matching sector of the biometrics industry. This information can be leveraged to assist in planning algorithm updates, development of requests for proposal packages, and long-term strategy development. The FBI is proud to sponsor these activities and hopes its law enforcement and criminal justice partners are able to take full advantage of the outputs from this valuable program.

Quality Metric for Face Biometrics

For all biometric modalities, better quality samples generally equate to better results from both automated matching systems as well as human comparison. Fingerprints have benefited from nonproprietary quality products such as the NIST Fingerprint Image Quality (NFIQ) tool. Products like the NFIQ can be implemented throughout the biometric lifecycle, which improves the chances of making an accurate identification. Nearly all vendors within the biometric community offer proprietary biometric quality products in conjunction with the products they sell, such as matching algorithms and biometric capture equipment. While these proprietary biometric quality products can be effective, many are tuned to work with a specific algorithm and most have several settings that can generate confusion for the system owner.

As part of their Face Recognition Vendor Test (FRVT) program, NIST is actively engaged in the development of international face image quality standards and is conducting tests of existing face image quality tools. Two of the standards, ISO/IEC 24357 and ISO/IEC 29794-5, aim to establish functional requirements on quality assessment algorithms reporting numerical image quality values and establish requirements for a quality vector which will convey quantitative quality values for both subject and image properties. These standards, if adopted by the face recognition industry, could simplify management of face quality tools by alleviating some of the concerns noted in the previous paragraph. A third standard, ISO/IEC 24385, aims to address the fact that unlike nearly all fingerprint capture devices, most cameras used to capture mugshots or portrait-like photos are blind to the fact that the officer or user is trying to capture a face image. The standard will address new capabilities, which should be leveraged for all face image capture stations, such as built-in face detection and pose estimation.

Although the standards mentioned above have not been officially published and are in draft form, knowledge of them and their applications can be leveraged for the generation of future requests for proposal documentation associated with system upgrades. If vendors start building products, which conform to all three standards, the users of face recognition technology would likely see an overall performance boost. If mug shot cameras become ‘face aware’ and standardized quality metrics are incorporated throughout the biometric pipeline, overall database quality would be improved which will lead to higher system accuracies.

As previously mentioned, NIST is conducting tests of existing face image quality tools. The effectiveness of quality assessment algorithms is important, because they can make two kinds of errors: (1) designating an image as poor quality when it is not and conversely (2) designating an image as good quality when it is not. Ultimately, an image quality metric should be able to accurately predict recognition failure, which is what NIST is currently testing. Initial test results can be found by visiting the NIST FRVT Quality web page. A notable initial observation is that match predictability from vendor A’s quality algorithm performs considerably worse when the matching is done by vendor B’s algorithm. In other words, image quality tool interoperability is difficult. This finding directly supports the need to develop and implement face image quality standards. Tracking the development of these standards and available test results is certainly recommended to any agency who currently either leverages or is planning a future deployment of face recognition technology.

Forensic Face Examiner Efforts

The law enforcement and criminal justice communities have been performing manual examination and comparison of face images in the furtherance of criminal investigations for decades. However, it has only been within the last few years that these technology advancements have made taking photos and capturing video ubiquitous within society. As such, more of this data is being made available to the law enforcement and criminal justice agencies. With the ever-expanding presence and utility of this information, there will be a continued need for both trained face examiners and scientific community validation of face examination technique. While the FBI and others currently offer face examination training, PRSU is actively engaged in obtaining scientific community validation.

From 2016 to 2018, PRSU sponsored a forensic face examiner ‘black box’ evaluation conducted by NIST. Being completely independent from the FBI and having the necessary skills and expertise, NIST is perfectly suited to perform these types of evaluations. This project resulted in the first substantial set of quantitative data confirming trained forensic face examiners out-perform all non-specialist groups and had the ability to score perfect results during the test. These findings provided a strong foundation for the practices put in place by the FBI and its partners and will help lead to overall scientific community support. The final report on this evaluation can be found by visiting the following the NIST web site at <https://www.nist.gov/programs-projects/face-projects>.

In a ‘black box’ evaluation, participants are only asked to make match/no match decisions and denote a confidence rating in that decision. No additional information is obtained regarding factors contributing to the final decision, thus examiners are seen as a ‘black box.’ These evaluations are performed first because they provide a cost effective means of confirming initial hypotheses and require minimal participant effort. With initial hypotheses confirmed that trained examiners perform at a high degree of accuracy, the next step is to perform a ‘white box’ evaluation. A ‘white box’ evaluation requires participants to not only make match/no match decisions with a noted degree of confidence, but they also require participants to catalog additional factors that contributed to the final decision rendered. For example, for each image set compared participants will document specific items about the face photo they leveraged for the comparison, such as the mouth and periocular region. Analysis of this data from all participants in conjunction with accurate match/no match decisions will provide extremely valuable quantitative data further contributing to scientific community support of face examination practices. The data will show what face landmarks are used most often to make accurate decisions on face comparisons. These important findings will then be leveraged to both enhance face examination training programs, as well as contribute to image quality standards and face capture best practices.

The ‘white box’ test platform is currently under development and is expected to undergo beta testing in late summer 2021. Agencies who currently have face examination programs are encouraged to participate when the evaluation becomes available. High volume participation will affect meaningful evaluation results, which will directly foster acceptance of face examination practices by both the scientific community and the public.

Academic Community Research Initiatives

The PRSU entered into a Cooperative Agreement with West Virginia University’s Research Corporation in 2008. This agreement gives PRSU the ability to fund universities with specific areas of expertise and abilities across the United States to conduct research and analysis for the FBI. While there are multiple projects conducted every year, PRSU has decided to highlight the following two ongoing projects.

The Automatic Face Recognition Best Practices (AFRB) project, a collaboration between the Florida Institute of Technology and the University of Notre Dame, is a project aimed at addressing concerns that bias exists in face recognition algorithm results. Their analysis is

focused on the relation of skin tone and gender to false match rates, why these problems appear to exist, and what can be done to mitigate the issues. Initial project results show that skin color alone does not create an increase in false match rates. This finding opposes recent publications claiming face recognition technology is specifically biased to certain racial or ethnic groups and confirms other image property variables must be included when conveying accuracy results. Though not an applicable application or use of the NGI System's face recognition, the study did confirm that using face recognition technology to automatically classify a person's gender from a photo does generate errors which varies between demographic groups.

The Postmortem Variability of Biometrics (PVB) project supports the collection of biometrics (fingerprints, face, and iris) from volunteers who have donated their bodies to University of Tennessee's Forensic Anthropology Center (also known as The Body Farm) for forensic science research after their death. These donors often participate in antemortem events where their biometrics can be collected prior to death. Once donors are deceased, their bodies are transported to the University of Tennessee where their biometrics are collected every day until they are no longer viable for identification. This unique dataset will allow agencies to better understand biometric viability after death by supporting ongoing academic research and future algorithm testing. The most surprising initial results of this work show that iris can be used to identify individuals after death. These findings are contrary to previously published assumptions that the iris structure begins to degrade immediately once an individual is deceased, making them invalid for identification purposes. In one specific case, the individual died six days prior to transport to the university, but her iris images collected at intake were identified to the iris images collected while she was still alive.

Electronic Biometric Transmission Specification (EBTS)

Through calendar year 2020, PRSU drafted *EBTS 11.0*, which introduced Appendix S: Descriptors and Field Edit Specifications for Type-17 Logical Records. The *EBTS 11.0* was routed and approved through the APB process and in early 2021 was officially published on the FBI Biometric Specifications (FBIBiospecs) Web Site at <https://www.fbibiospecs.cjis.gov/EBTS/Approved>.

Table M-1 "Transaction Messages" of the *EBTS* lists the transaction message codes, message condition for each code, and a description of the code. In the past, comprehensive lists of the transaction messages were only available in the *EBTS* and new messages were only added when new versions of the *EBTS* were published. To better support NGI System users, a 'living' version of Table M-1 has been added to the *EBTS* page of the FBIBiospecs Web Site. This table will be updated as new message codes are approved, providing users an up-to-date list of transaction messages.

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC R

National Instant Criminal Background Check System (NICS) Operational Update

PURPOSE

The information outlined in this paper provides an update of the NICS.

AUTHOR

NICS Section, NICS Business Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

The Brady Handgun Violence Prevention Act of 1993 (Brady Act) required the U.S. Attorney General to establish the NICS for federal firearms licensees (FFL) to contact so information may be supplied immediately on whether the transfer of a firearm would violate federal or state law. The NICS became fully operational on November 30, 1998.

When an FFL initiates a background check through the NICS, the prospective firearm transferee's name and descriptive information is searched. The NICS queries three national databases for possible matches when conducting a NICS check. These databases are: (1) the National Crime Information Center (NCIC), which contains records of wanted persons, subjects of protection orders, and other persons who pose a threat to officer and public safety; (2) the Interstate Identification Index (III), which provides access to criminal history records; and (3) the NICS Indices, which contain information on prohibited persons as defined in Title 18, United States Code, Section 922(g) or (n). Records contributed to these national databases are modified, cancelled, and added daily. In addition, a query of the applicable databases of the Department of Homeland Security's U.S. Immigration and Customs Enforcement is conducted on all prospective firearm transferees who indicate a non-U.S. citizen status on the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Form 4473.

NICS TRANSACTIONS

From November 30, 1998, through December 31, 2020, a total of 372,699,381 firearm and firearm-related permit background checks have been processed through the NICS. Of these:

- 223,098,834 background checks were processed by state agencies.
- 149,600,547 background checks (resulting in 1,885,942 denials) were processed by the FBI CJIS Division’s NICS Section.

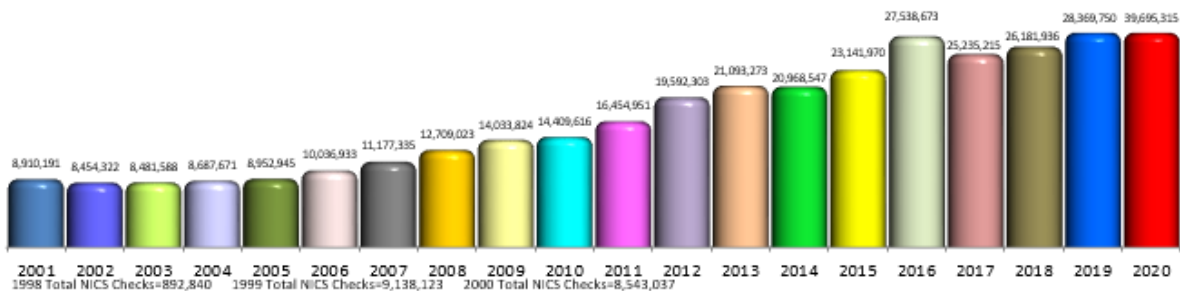
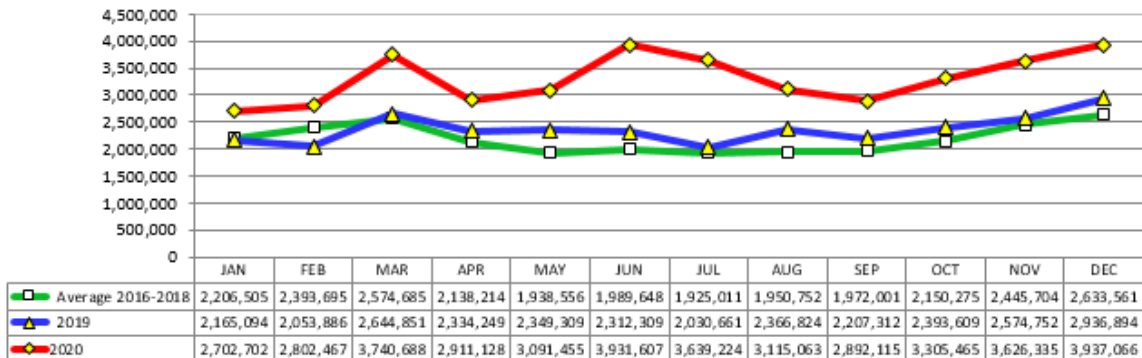
In calendar year (CY) 2020, the NICS experienced the highest volume of background checks since its inception. The first half of CY 2020 resulted in 19,180,047 background checks being submitted, which was an increase of 38.39 percent from the first half of CY 2019. The second half of CY 2020, the volume reached 20,515,268 (as of December 31, 2020), which was an increase of 41.38 percent. The total volume for CY 2020 climbed to 39,695,315 (as of December 31, 2020), which is an increase of 39.92 percent when compared to the second highest volume year CY 2019.



Total NICS Checks

November 30, 1998–December 31, 2020

Program-to-date **372,699,381**



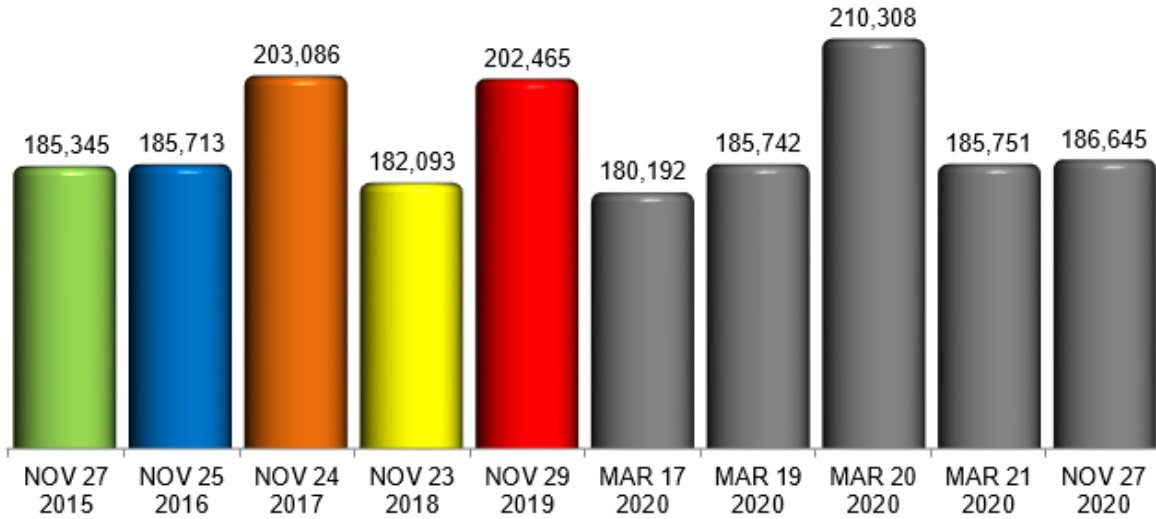
The following charts represent the top 10 highest days and the top 10 highest weeks for background checks processed through the NICS since November 30, 1998.



NICS Firearm Background Checks Top 10 Highest Days



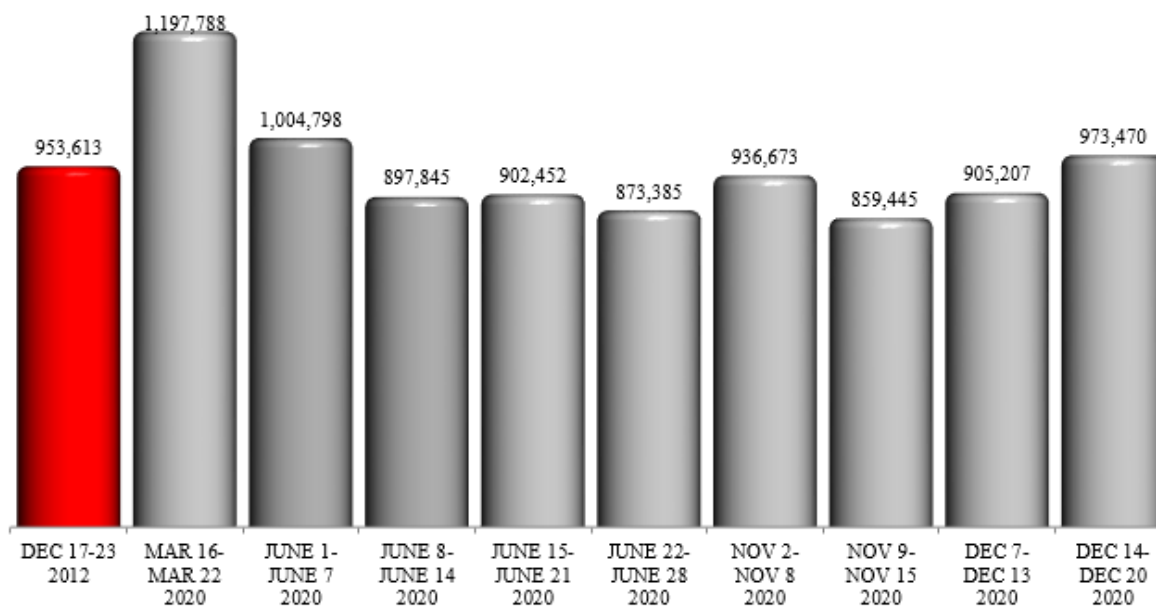
November 30, 1998–December 31, 2020



NICS Firearm Background Checks Top 10 Highest Weeks



November 30, 1998 – December 31, 2020



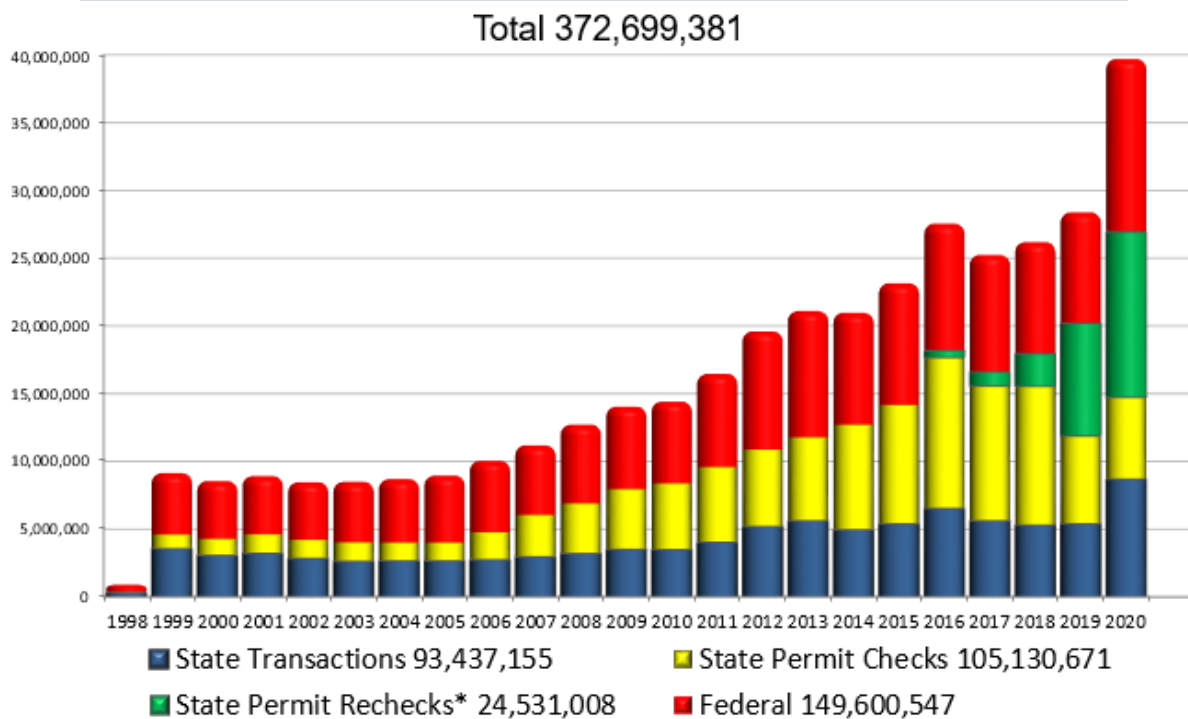
The chart below represents federal and state background checks processed by state agencies and the NICS Section since November 30, 1998. Included in this chart are the total of those firearm-related permit checks submitted for both firearm permit identification (Purpose ID) numbers of 14 (new and renewals) and 34 (revocations, rechecks, and similar permit transactions).

Mandatory use of Purpose ID 34 became effective on May 26, 2017. However, those states not yet programmed to use Purpose ID 34 had until June 30, 2019, to be programmed and comply.



State and Federal NICS Checks

November 30, 1998–December 31, 2020



*Began capturing these statistics in 2016

NICS SECTION DENIALS

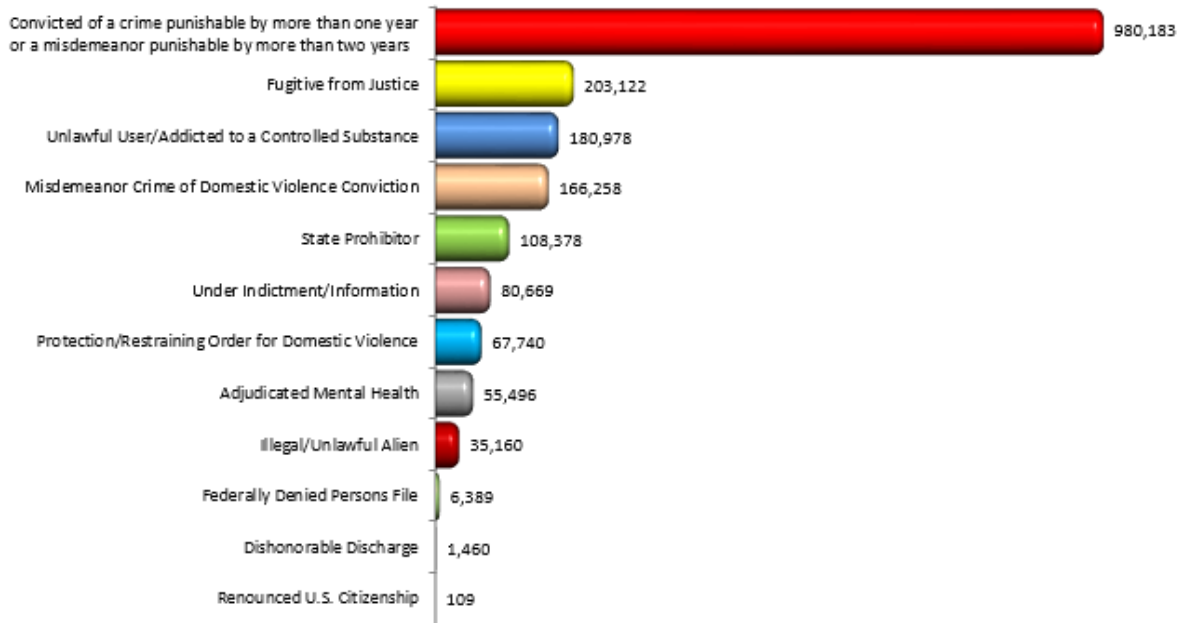
Program-to-date, from the inception of the NICS on November 30, 1998, through December 31, 2020, a total of 1,885,942 background checks have been denied by the NICS Section. The following chart represents a breakdown of the federal-issued denials, by prohibiting category.



Federal Denials

November 30, 1998–December 31, 2020

Program-to-date **1,885,942**



INSTANT DENIALS

On October 27, 2016, the NICS Section implemented a feature that allows the system to return instant deny responses on federal background check transactions based upon hits to the NICS Indices which meet certain pre-determined parameters. On September 26, 2017, this same functionality was implemented to also instantly deny NICS transactions based upon the III records that have the Identification for Firearm Sales Flag (IFFS) set to disqualification. The Predictable Learning Automation of the NICS (the PLAN) was then implemented at the end of 2018, and the first instant denial was made through the PLAN automation in June 2019. Again, these transactions must meet certain pre-determined parameters to be eligible for an instant denial. This functionality created efficiencies in processing for the NICS Section by removing a manual process and providing additional time for NICS Legal Instruments Examiners to engage in necessary research in other areas of the background check process while still providing an accurate determination. As of December 31, 2020, there have been 99,171 federal background check transactions instantly denied by the NICS.

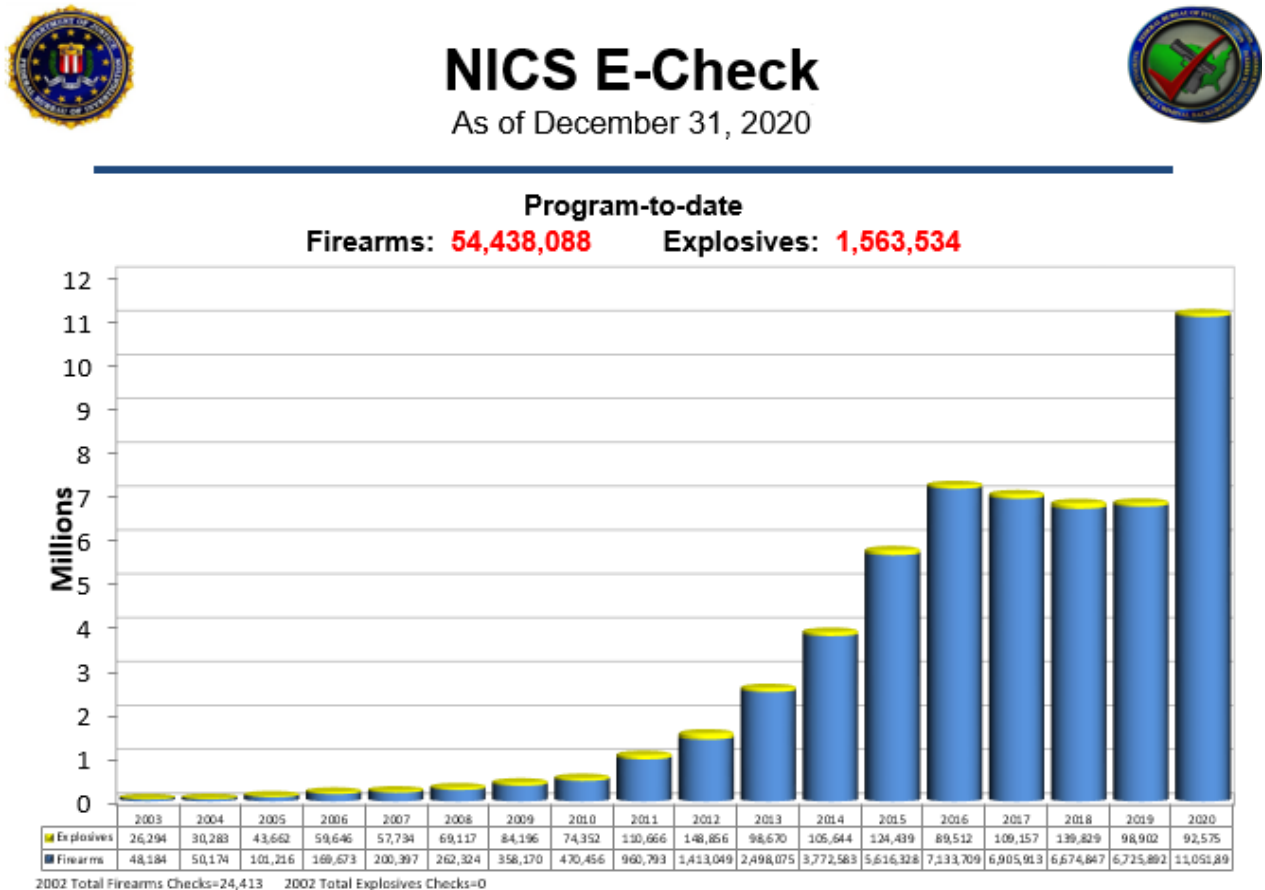
NICS E-CHECK

The NICS E-Check provides FFLs and other approved entities with efficiencies, such as the capability to initiate unassisted background checks through the NICS. The use of the NICS E-Check continues to expand as more and more users realize the benefit and ease of using

this resource. As of December 31, 2020, of all federal NICS background checks initiated, 86.6 percent were via the NICS E-Check. This is higher than the 82.25 percent that ended CY 2019. Approximately 34,541 FFLs (or 69.8 percent) are registered users of the NICS E-Check out of the 49,470 FFLs actively enrolled with the NICS. The NICS Section has confirmed that staff can process more NICS E-Check transactions than phone calls received via the NICS Contracted Call Center, making the NICS E-Check the quickest method for the FFLs to receive a response to a firearms background check. Therefore, promotional efforts by the NICS Section continue. In addition to promoting the NICS E-Check, the following indicates how the NICS Section supported and serviced FFLs between July 1, 2020, and December 31, 2020:

- The NICS Section continues to offer the NICS web service process of submitting firearm background checks electronically via extensible mark-up language. The NICS provides an application programming interface allowing corporations and FFLs to automate their entire background check process.

The following chart illustrates the growth of the NICS E-Check since it began in 2002:

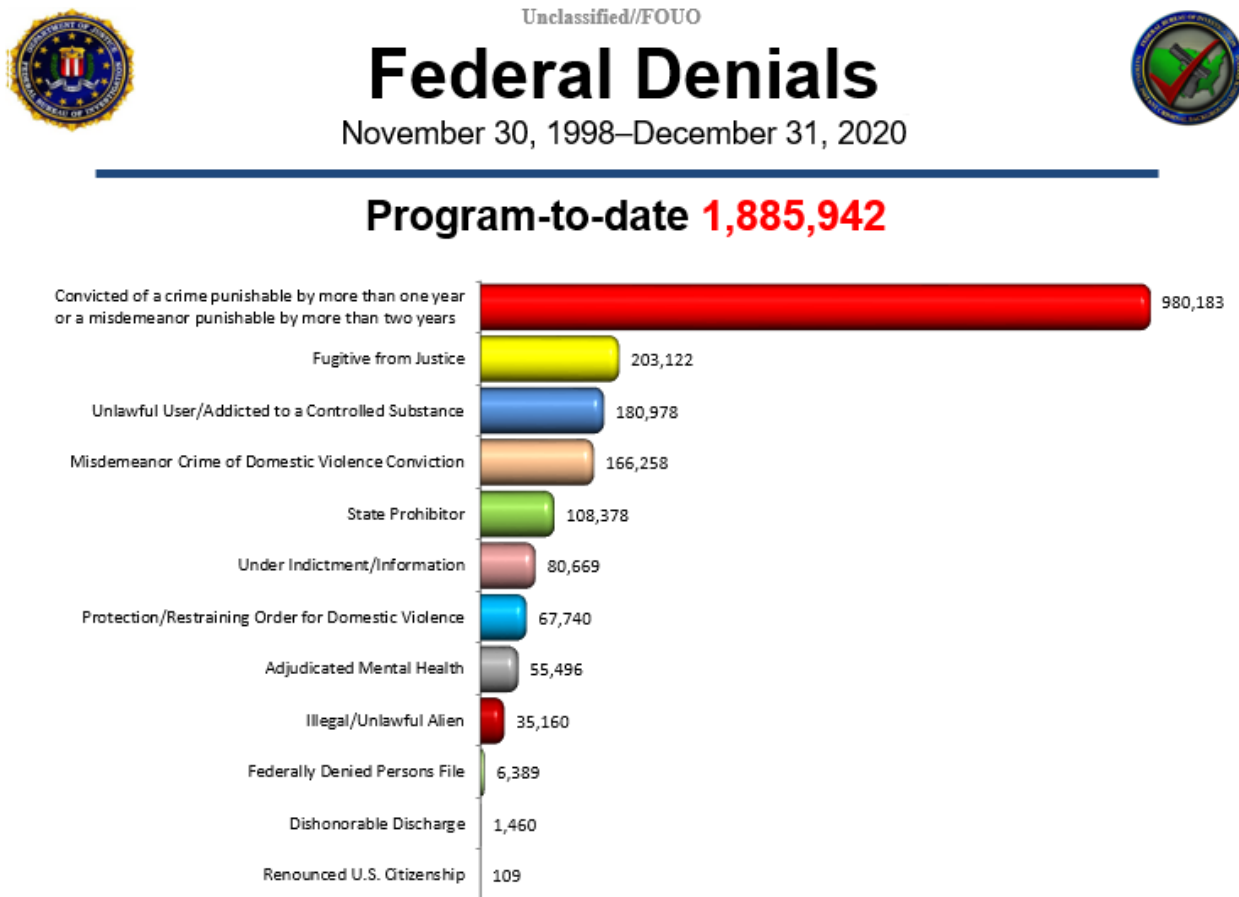


NICS INDICES

The NICS Indices contain descriptive information about persons prohibited (per federal and state law) from possessing or receiving firearms. The entries contained in the NICS Indices are contributed by federal, state, local, and tribal agencies. There are two main methods for making

an entry into the NICS Indices. The first method is through the NCIC interface and the second method is via batch data transfer or single entry through the Law Enforcement Enterprise Portal Internet-based connection using the NICS E-Check.

As of December 31, 2020, there were 23,377,233 entries maintained in the NICS Indices for availability to NICS users at a national level, which is a 11.7 percent increase from December 31, 2019. A breakdown of the records maintained in the NICS Indices, ranked by prohibiting category, is illustrated as follows:



Of the entries maintained in the NICS Indices (as of December 31, 2020):

- Approximately 49 percent were contributed by the states.
- Approximately 51 percent were contributed by federal agencies.

In 2020, most states continued to make entries to the NICS Indices in the mental health category. In addition, since December 31, 2019, states have increased their submissions to other categories such as the fugitive from justice, state prohibitor, and the under indictment/information categories.

- Fugitive from Justice—entries have increased by nearly 64 percent.
- State prohibitor—entries have increased by 13.6 percent.
- Under indictment/information—entries have increased by 17 percent.

With states passing extreme risk protection order (ERPO) laws or red flag laws that could qualify for a firearms prohibition, some states have contributed information to the NICS Indices for this category of prohibited individuals within the State Prohibitor File. Individuals with an active and served ERPO, that includes a firearms prohibition, are prohibited from possessing or receiving a firearm. In most cases, ERPO information is not reported within the NCIC; therefore, the NICS Indices is the best option for this information to respond during a NICS check. The NICS Section worked with several states throughout 2020 to aid in the sharing of this information to the NICS Indices. The NICS Section continues to provide information and promote the sharing of records, to not only the NICS Indices, but to the NCIC and III databases as well.

As with the states, the NICS Section has worked with federal agencies to address the lack of contributing records to the NCIC, the III, and/or the NICS Indices.

As a result, many federal agencies are performing self-audits of their data and filling the gaps in the criminal history records they originated by making the information available to a database searched during a NICS check. Since June 30, 2020, federal records reported to the NICS Indices continue to increase.

The NICS Section continues to provide statistical support to the federal and state agencies upon request and participates in task force meetings, conferences, and other training venues to educate NICS Indices contributors on the process and benefits of entering prohibited individuals.

DISPOSITION OF FIREARMS (DOF)

The NICS may be accessed by criminal justice agencies prior to disposing/returning firearms currently under the agency's control to a prospective transferee. The NICS check assists the agencies in determining an individual's eligibility to possess or receive firearms in accordance with federal and state law. Currently state criminal justice agencies, within 43 states and the District of Columbia, access the NICS for DOF purposes. The DOF background checks are also conducted by 68 federal agencies, such as the military, FBI, and ATF offices, as well as 95 tribal agencies. From July 1, 2020, through December 31, 2020, a total of 47,898 DOF background checks were conducted. Approximately, 2,322 DOF background check denials, equating to a 4.85 percent denial rate, were reported to the NICS Section during this time frame.

NICS QUERY OF THE NATIONAL DATA EXCHANGE (N-DEx)

Due to the unprecedented volume of incoming background checks, the NICS Section has had to focus all technical resources on automation efforts to help manage the current workload, therefore is not currently searching N-DEx as a secondary search. However, the NICS Section does continue to conduct data analysis on the N-DEx data to efficiently retrieve pertinent information that may assist with the processing of those background checks identified as having potential prohibitions. In September 2020, states that opted in were given the ability to access the N-DEx via the portal for all permissible uses of the NICS.

EXTERNAL TRAINING

State entities serving as a point of contact (POC) or partial-POC for their respective state must provide a basic level of service to the FFLs. Efficient and effective execution of the provisions set forth in the Brady Act requires close cooperation between the FBI and state agencies. The NICS Section offered training opportunities for state NICS users from January 1, 2020 through December 21, 2020. The various training methods included on-site, teleconference, Skype for Business, Microsoft Teams, and Train-the-Trainer. Throughout this time period, the NICS Section, as well as our users, experienced a drastic change in our workplace due to the COVID-19 pandemic. This change greatly affected the way the NICS training instructors provided training and outreach to our users. During this time period, there was also a large increase in firearm-related transactions across the country affecting not only the NICS Section, but also the POC, partial-POC, and the ATF-qualified alternate permit states. The increase in workload along with the workplace changes experienced by our users enhanced the need to provide training and support to ensure the consistent application of the federal prohibitions nationwide.

The NICS training instructors worked diligently to alter the training curriculum to function on a virtual platform that encouraged attendee engagement, promoted understanding and execution of presented concepts, and increased retention of information. In April 2020, the training platform utilized for training was Skype for Business; however, in September 2020, the CJIS Division moved to the Microsoft Teams platform. The move to a virtual platform was embraced by several states and agencies and has provided the NICS training instructors the opportunity to reach small and rural agencies that have not been able to attend previous in-state training sessions.

The NICS Section provided training to the following agencies:

- Kentucky State Police Carry Concealed Deadly Weapon Unit received in-state training in February 2020.
- Various Kentucky law enforcement agencies for DOF received in-state training in February 2020.
- Illinois State Police Firearms Services Bureau received training via Skype for Business in May 2020.
- Ohio State Patrol and various law enforcement agencies across the state received training via Skype for Business beginning May 2020 through July 2020. (Webinar series)
- North Carolina State Bureau of Investigation, local sheriffs' offices, and police departments received training via Skype for Business in July 2020.
- Florida Department of Law Enforcement's state-designated trainer received training in July 2020.
- Pennsylvania State Police Firearms Unit received training via Skype for Business in August 2020.
- Naval Criminal Investigative Service received training via Skype for Business in August 2020.
- Illinois State Police Firearms Services Bureau received Train-the-Trainer review session in August 2020.

- Nebraska State Patrol, local sheriffs' offices, and police departments received training via Microsoft Teams in September 2020.
- California Department of Justice received training via Microsoft Teams in September 2020.
- North Carolina Association for Property and Evidence members received training via Microsoft Teams in November and December 2020.

During this time period, the NICS Section's staff provided training to approximately 1,000 individuals from over 280 federal, state, and local agencies. The NICS Section's staff provided continuous support to all attendees throughout this time period to assist with the processing of firearm or firearm permit-related background checks.

CHANGES AND ENHANCEMENTS

The NICS Section has implemented numerous system builds this year, and there are several more scheduled for deployment. A few notable impacts are shared below.

- ATF Form 4473 Updates
 - Buyer information on the Submit a Search screen updated to match the new version of the ATF Form 4473.
 - The system provides the ability to select between the old form (Revision Date October 2016) and the new form (Revision Date May 2020).
 - The "Sex" field will have a third choice of "Non-Binary."
- External Requests
 - Enhancements were made to auto-populate external requests with fbinicsrequests@services.fbi.gov replacing personal e-mail addresses with the ability to choose a personal e-mail for agencies that send encrypted responses.
 - Originating Agency Identifiers (ORI) will now be automatically added to the top of the NICS transmittal cover sheet. This was done to assist agencies that require an ORI on responses back to the NICS.

Efforts continue to optimize capabilities within the NICS Section. Research and development on various software applications continue to further enhance the NICS process.

NICS FRONT OFFICE

The innovative use of resources between the FBI CJIS Division's Information Technology Management Section (ITMS) and the NICS Section were instrumental in deploying NICS staff to work from remote locations due to the COVID-19 pandemic. It was through the efforts of the NICS Strategy and Systems Unit of the NICS Section and the Technology Integration and Support Unit of the ITMS that NICS employees and contract staff were able to quickly access the NICS remotely.

The teams worked in conjunction with each other to prepare and distribute the government furnished equipment (GFE). While this effort was taking place, additional staff transitioned the materials needed to work NICS transactions to the cloud so that employees could gain access

remotely and an additional group of staff provided support to the users while they were attempting to log on.

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC S

National Instant Criminal Background Check System (NICS) Enhancements Status

PURPOSE

To provide a status update of pending and recently completed NICS Enhancements

AUTHOR

NICS Section, NICS Business Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. A copy of any comments and questions (with corresponding responses) will be provided to all members and registered meeting attendees.

BACKGROUND

The Brady Handgun Violence Prevention Act of 1993, Public Law 103-159, required the U.S. Attorney General to establish the NICS for Federal Firearms Licensees to contact for information to be supplied immediately as to whether the transfer of a firearm is in violation of federal or state law. The NICS began operations on November 30, 1998.

Over the years, the NICS Section, in collaboration with CJIS Division technical experts, has identified, developed, and implemented numerous technical system enhancements to improve the overall efficiency and effectiveness of the NICS when processing background checks. All proposed recommendations for the NICS process and system changes are submitted to the APB for review and, if approved, are submitted to the FBI Director for final approval.

Once approval is obtained, the pending enhancements specific to the NICS are assigned to the NICS Section, and their progress is tracked by the CJIS Division. Historically, this tracking mechanism has primarily been used internal to the CJIS Division. To ensure that external users are kept informed as to the status of the NICS enhancements, the NICS Section will provide status updates to the CJIS advisory process members. The NICS Enhancements build schedule

will track the progress of all impending, future, and/or upcoming NICS enhancements as well as those enhancements which have been completed since the last update. This tracking mechanism is a living document that will continuously evolve as NICS enhancements are added, reprioritized, and completed. The NICS Enhancements build schedule will also assist advisory process members in determining how the progression may impact state users.

NICS Enhancement Status as of November 2019

NICS Enhancement Status as of November 2019						
Enhancement		Priority Level	Date Approved by APB	User Impact	Status Level	Implementation Date/Comments
1	Point-of-Contact (POC) state access to the complete Interstate Identification Index (III) criminal history record— Implement III changes to provide an expanded response to POC states using the Purpose Code “F.”	5	12/2008	Other: User impact has not yet been determined	Pending	An information Topic Paper, "NGI Purpose Code F responses vs Purpose Code C responses" is being drafted to go to APB in spring 2021.
2	Access for authorized federal, state local, and tribal agencies to the Disposition Document File (DDF) via existing CJIS Division Systems— Making the DDF available on an existing CJIS system via separate query.	5	12/2009	Optional	Pending	TBD—A task force including employees from the NICS Section, the Information Technology Management Section, the BSS, and the Criminal Justice Information Law Unit continues to review internal processes as part of the overall evaluation of possible options. The task force is continuing its efforts to find a long-term solution that preserves the value of the data and allows access by other entities to whom the data may be relevant. In addition, the CJIS Division is currently working to remove non-relevant data.

3	Expanding access of the NICS to permit criminal justice agencies and/or other authorized agencies to conduct a NICS check during the hiring process and/or during the reinvestigation of criminal justice professionals or other persons authorized by law to carry a firearm.	5	06/2013	Optional	Pending	The NICS Section is working with the FBI's Office of General Counsel to finalize proposed regulation changes for submission to the Department of Justice to expand the use of the NICS to include background checks for criminal justice professionals or other authorized persons.
4	Permanent expansion of the NICS to query the National Data Exchange (N-DEx) System as a secondary source.	3	12/2016	Yes	Pending	The NICS Section's management determined that the section will not begin searching the N-DEx until all technical requirements for an automated machine-to-machine search are complete. In addition, the NICS Section is pursuing the capability to filter the results so the NICS only receives records relevant to the background check. In September 2020, states, that opted in, were given access to search the N-DEx, via the portal, for all permissible uses of the NICS.

NICS ENHANCEMENTS KEY

Priority Description

0	Typically used for all new unassigned work requests; tabled topics
1	Critical project: system recovery, production failure
2	Essential project: no effective work around, legislative mandates, data integrity problems
3	Important project: system enhancement/efficiencies, cost saving, adequate work around, no data integrity programs
4	Desirable/operational enhancement
5	Implement as resources permit

User Impact

Yes	Mandatory Information Technology (IT) changes necessary on the external user's system
No	No IT changes necessary on the external user's system
Optional	IT changes necessary on the external user's system to participate in the change
Other	Further description on impact/no impact within the Impact column

System Enhancement Status Levels

NICS Section Analysis	Creating a concept of operations document/detailed request to forward to IT development
IT Development	Defining system requirements, development, and testing
Pending	Further description of why the change is pending within the Implementation Date column
Complete	Implementation on the Operational Environment; functionality delivered

Implementation Date/Comments

Tentative	<insert tentative date> When a build is scheduled through IT
TBD	When a build is not yet scheduled through IT
Actual	<insert implementation date> When a build is implemented and the Status is marked as complete

Intentionally Left Blank

**CJIS ADVISORY POLICY BOARD (APB)
SPRING 2021 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS**

STAFF PAPER

INFORMATIONAL TOPIC T

Uniform Crime Reporting (UCR) Program Status Report

PURPOSE

The purpose of this paper is to provide a status report on the Crime Statistics Management Unit (CSMU) UCR Program.

AUTHOR

Global Law Enforcement Support Section, Crime Statistics Management Unit

FEEDBACK

Direct any questions regarding this topic to the Advisory Process Management Office via e-mail at agmu@leo.gov. Submit feedback via the feedback form provided. CJIS will provide a copy of any comments and questions (with corresponding responses) to all members and registered meeting attendees.

BACKGROUND

The Federal Bureau of Investigation (FBI) UCR Program's primary objective is to generate reliable information for use in law enforcement administration, operation, and management; over the years, however, the data has become one of the country's leading social indicators. The program has been the starting place for law enforcement executives, students of criminal justice, researchers, members of the media, and the public at large seeking information on crime in the nation. The program was conceived in 1929 by the International Association of Chiefs of Police to meet the need for reliable uniform crime statistics for the nation. In 1930, the FBI was tasked with collecting, publishing, and archiving those statistics. Today, data is received from more than 18,000 federal, state, county, city, university and college, and tribal law enforcement agencies voluntarily participating in the program.

The data is submitted either through a state UCR program or directly to the FBI UCR Program. The FBI UCR Program publishes four publications: *Crime in the United States (CIUS)*, *Hate Crime, Law Enforcement Officers Killed and Assaulted (LEOKA)*, and *National Incident-Based Reporting System (NIBRS)*. The FBI UCR Program also releases data on a quarterly basis through the *Quarterly Uniform Crime Report*. In addition, the FBI UCR Program manages the National Use-of-Force Data Collection and the FBI's interactive Crime Data Explorer (CDE).

The CDE serves as the digital front door for UCR data, enabling law enforcement and the public to more easily use and understand the UCR data collected. The CDE can be accessed at www.fbi.gov/cde.

In 2015, the FBI CJIS Division was tasked with a Director's Priority Initiative to improve the nation's UCR statistics for reliability, accuracy, accessibility, and timeliness and to expand the depth and breadth of data collected. In December 2018, the Crime Data Modernization (CDM) Initiative was transitioned to a CJIS Strategic Initiative. The mission of CDM is to improve the nation's UCR crime statistics reporting standard for federal, state, local and tribal law enforcement agencies (LEAs) and to provide richer data to inform, educate, and strengthen communities. This effort is being achieved through the completion of five identified initiatives. The first initiative is to transition state, local, and tribal LEAs from the Summary Reporting System (SRS) to NIBRS. The second is to collect use-of-force incidents, which result in the death or serious bodily injury of a person, as well as firearm discharges at or in the direction of a person. The third and fourth initiatives both include federal LEA compliance with the Uniform Federal Crime Reporting Act (UFCRA) of 1988, which mandates all federal agencies with a law enforcement component report their crime statistics to the national UCR Program. Strategically, the third initiative specifically addresses FBI participation with the FBI UCR Program. Finally, the fifth initiative relates to technical efforts to create the CDE, which is designed to ensure crime data publication is timely and accessible. The CDM provided the groundwork for the FBI UCR Program to evolve and the goals set forth will continue to grow through the initiatives established as part of the CDM as well as through future initiatives.

DISCUSSION AND ANALYSIS

APB Topic Update

The FBI UCR Program provides an updated status report during each spring and fall round of the CJIS APB meetings, highlighting initiatives and on-going activities within the program. Due to the COVID-19 pandemic, the Spring 2020 subcommittee and APB meetings were postponed until Fall 2020, which included finalizing motions on the Spring 2020-topic papers. The Spring 2020 topics and their associated motions were presented during the Fall 2020 subcommittee and APB meetings. Below are the Fall 2020 action topics and the Spring 2021 topics the FBI UCR Program submitted for 2021 APB meetings.

Fall 2020 Action Topics:

- **Modification of NIBRS Rape Definition** – request guidance on pursuing modifications to the NIBRS sex offense nomenclature.
- **Addition of Case Disposition Information to NIBRS** – present information on additional case statuses to be collected in NIBRS, such as administratively closed.
- **FBI UCR Program adding Unfounded to NIBRS** – present options for adding unfounded case status to the NIBRS data collection.
- **Expansion of Exceptional Clearance Category** – request guidance if the FBI UCR Program should pursue modification of the nomenclature used with Data Element 4 (Cleared Exceptionally) and the public reporting of clearance data for sex offenses.
- **Modification of NIBRS Arson Victims** – request guidance on pursuing modifications to

the NIBRS data collection to allow for the collection of firefighters and law enforcement officers as victims of Murder, Non-negligent Homicide and Aggravated assaults in Arson related incidents.

- **Changing the Anti-Mormon Bias Type to Anti-Church of Jesus Christ** – present a proposal for revising the Anti-Mormon bias type to Anti-Church of Jesus Christ.
- **Police Employee Collection: Addition of "Unknown" Category for Capturing Race-Ethnicity** – request the addition of an “Unknown” category for capturing race and ethnicity for Police Employee collection.
- **Recommendation for Gender Non-Binary Classification for Uniform Crime Reporting** – request recommendations to address non-binary gender classification within the UCR Program and in consistency with other CJIS systems.
- **Law Enforcement Suicide Data Collection** – request for the establishment of a central repository for the capture and analysis of data points for law enforcement officer suicide incidents.

Fall 2020 Discussion and Information Topics:

- **Impact of NIBRS Transition on the Eligibility to Apply for Justice Assistance Grant (JAG)** – discuss any potential impact of the NIBRS transition to JAG fund eligibility.
- **National Use-of-Force Data Collection Update** – provide an update on the National Use-of-Force Data Collection, as well as to provide information on publication of data.
- **Status of NIBRS Transition** – provide an update on the nation’s status of transitioning to NIBRS.
- **UCR LEOKA Program Health-Related Line-of-Duty Deaths** – provide a plan for initiating a data collection for officer deaths resulting from duty-related health conditions.

Spring 2021 Action Topics:

- **Expansion of Property Descriptions in NIBRS Data Element 15**
- **Expansion of Location Types within NIBRS Data Element 9**
- **Expansion of Victim to Offender Relationships in NIBRS Data Element 35**
- **Addition of New “Criminal Offense in Progress” Data Element to the NIBRS Victim**
- **Beyond 2021 Update - Creation of NIBRS Offense Crosswalk repository**
- **Beyond 2021 Update - Addition of Geolocation to NIBRS**
- **Beyond 2021 Task Force Update NIBRS Sex Offense Nomenclature**
- **Changes to Race Codes within the FBI UCR Program**
- **Beyond 2021 Initiative update – NIBRS Data Elements**

Spring 2021 Discussion and Information Topics:

- **Beyond 2021 Initiative Update**
- **UCR Program Expansion to Support Lawful Access Initiative**
- **National Use-of-Force Collection Update**
- **Status of NIBRS Transition**
- **Uniform Crime Reporting Program Update**

CDE

For nine decades, the FBI has collected nationwide crime data under the FBI UCR Program. In June 2017, the program launched the CDE. Considered the FBI UCR Program's digital front door for presenting crime data, the core goal of CDE is to foster more transparency in law enforcement and better, more informed conversations about crime.

Since the last update, CDE has continued to evolve in user experience and functionality. Recent additions include:

- A new homepage to differentiate between crime and law enforcement data collections;
- Preliminary Quarterly data for the current year, updated data will be available March, June, September, and December. Updated preliminary data will include January through most recent quarter, so Quarter 2 data will include January through June of the current year;
- 2019 UCR data has been added to CDE to coincide with the *CIUS* publication;
- National Use-of-Force Data Collection participation data is available.

Current developments underway for CDE include:

- Adding a Hate Crime Reporting Explorer page;
- Development of a "Custom Table and Chart Builder" that will replace the UCR data tool;
- Development of crime pages to display federal data and tribal data, respectively;
- Refactoring the entire site to provide a new look and feel that will enhance the user experience of the site and allow ease of navigation.

The CDE team is also in the process of creating a *CDE Product Vision Alignment* for UCR publication migration and proposed NIBRS roadmap. This vision will be the basis of development for the CDE from current efforts to beyond 2021.

CDE can be located at www.fbi.gov/cde. Additional questions and/or comments may be sent to UCR@fbi.gov or by completing the "Feedback" form located at the bottom of the CDE website

Operations

Today, data releases are produced from data received from more than 18,000 state, county, city, university and college, and tribal law enforcement agencies voluntarily participating and federal agencies mandated to report based on UFCRA Act of 1988.

The data is submitted through a federal or state UCR program or directly to the FBI UCR Program. The FBI UCR Program publishes four annual data releases each fall. The following will be released in the fall of 2021:

- *Crime in the United States (CIUS), 2020*
- *Hate Crime Statistics, 2020*
- *Law Enforcement Officers Killed and Assaulted (LEOKA), 2020*
- *National Incident-Based Reporting System (NIBRS), 2020*

In 2020, quarterly reporting launched with releases in September and December. In 2021, there will be four quarterly releases:

- *Quarterly Uniform Crime Report, January–December 2020 (releasing in March 2021)*
- *Quarterly Uniform Crime Report, January–March 2021 (releasing in June 2021)*
- *Quarterly Uniform Crime Report, January–June, 2021 (releasing in September 2021)*
- *Quarterly Uniform Crime Report, January–September 2021 (releasing in December 2021)*

LEOKA

Through the FBI’s LEOKA Data Collection, the FBI UCR Program strives to collect and report reliable statistical information for use in law enforcement administration, operation, and management. Data about officers who were killed – either feloniously or accidentally – or assaulted are derived from reports voluntarily submitted by the officers’ employing agencies to the FBI’s LEOKA Data Collection.

The purpose of this collection is to:

- Identify situations and trends in which officers are killed and assaulted in the line-of-duty.
- Report preliminary statistical data to the law enforcement community.
- Aid law enforcement agencies in developing operational and tactical policies to improve officer safety.
- Assist law enforcement by providing current statistical data to improve officer safety training.
- Publish line-of-duty death and assault statistical data and written narratives for felonious killings and selected assault with injury incidents for integration into law enforcement training programs.

The LEOKA Data Collection releases data twice yearly. The Spring publication produces data reported on officers who are feloniously killed in the line-of-duty and supporting narrative information on select incidents. The Fall publication covers assault incidents and strives to break down aggravated incidents causing injury as a result of the weapon types of knife or cutting instrument and/or firearm.

To release data in a timely manner and, to better serve our customers, LEOKA also releases a monthly infographic. The infographic was created to display line-of-duty death information for the previous reporting year and preliminary data for the current reporting year. The infographic serves as a quick reference for officer deaths without waiting for a publication and is updated on a monthly basis. The infographic, and supporting LEOKA resources and information, including real-time statistics, may be accessed on the FBI UCR Program’s CDE at <https://crime-data-explorer.fr.cloud.gov/officers/national/united-states/leoka>.

Hate Crime Statistics

The FBI UCR Program will continue to offer hate crime training sessions via webinars throughout 2021. Three separate interactive webinars will be offered that focus on training

record managers, law enforcement officers, and law enforcement administrators. The webinars allow for direct contact between the FBI UCR Program and the state program managers or administrators of the non-participating and zero reporting agencies.

The webinars also permit the FBI UCR Program to continue outreach strategies and training sessions with state UCR program agencies and the local agencies experiencing safety travel constraints due to the COVID-19 pandemic.

Beyond 2021 UCR Program Roadmap

In February 2019, the CJIS APB Executive Committee approved the formation of the Beyond 2021 Task Force. The Beyond 2021 Task Force was established to create recommendations for the FBI UCR Program roadmap after the January 1, 2021, transition to NIBRS. All recommendations created by the task force will be vetted through the CJIS APB process. On September 29, 2020, the Beyond 2021 Task Force conducted its final formal meeting. During this meeting, the task force reviewed all proposals generated by the supporting Subject Matter Expert (SME) groups and determined which proposals will be included in proposals brought forth for consideration by the CJIS APB. The Beyond 2021 Task Force developed actions and topics of interest for review and prioritization by the UCR Subcommittee in the five areas below:

- Data Publication – examining methods to enhance the data publications. This includes determining how to optimize the use of CDE to provide dynamic data views for the user community. Topics of interest include ensuring continuity of rates and trends while highlighting NIBRS data.
- Edward J. Byrne Justice Assistance Grant – Determining the immediate impact of the NIBRS transition on grant eligibility.
- Data Elements – Examining NIBRS data elements to determine how to enhance the data and its usefulness for all stakeholders. Topics of interest include expanding the data collected on weapons used in the commission of crimes and expanding the property information collected for national reporting.
- Data Collection Strategy – Expanding the collection of data available and ensuring uniformity across all FBI UCR Program data collections. Topics of interest include ensuring the data collected is accurate and of the highest quality.
- Governance – Exploring methods to expand understanding of the CJIS APB process and ensuring the FBI UCR Program manages future modifications through outreach to all stakeholders.

Law Enforcement Public Contact Pilot

Representatives from several federal, state, local, and tribal law enforcement agencies throughout the nation, as well as the major law enforcement organizations, requested the FBI develop and manage a national collection regarding law enforcement uses of force.

During the subsequent development of the National Use-of-Force Data Collection, law enforcement leaders believed it was critically important to place use-of-force incidents in the context of the total number of law enforcement interactions with the public.

In response to this request, the FBI UCR Program deployed a pilot project for the “Law Enforcement Public Contact” collection. The Pilot was available for contributors from September 1, 2020, through October 30, 2020.

The objective of the project is to provide context for use of force and other law enforcement statistics already collected by the FBI UCR Program. The Law Enforcement Public Contact collects the number of law enforcement contact with the public for the following categories:

- Citizen calls for service
- Unit/officer-initiated contact
- Court/bailiff activities

Agencies participating in the pilot reported law enforcement public contact that occurred from January 1 – December 31, 2019. Agencies were not expected to create a data system to obtain this information. Instead, agencies were encouraged to use their computer-aided dispatch systems, or other existing systems, to obtain counts for law enforcement contacts with the public that fit into the listed categories. Agencies had the option to submit an actual count, an estimated count, or note the number of contacts with the public are not applicable or are unavailable. The FBI UCR Program will submit the findings of this study by Spring 2021, for review by the Office of Management and Budget. The FBI UCR Program will use the research from the pilot study to evaluate and improve the overall validity and reliability of this data collection. Upon review and approval, the FBI UCR Program will deploy the data collection on January 1, 2022.

National Crime Statistics Exchange NIBRS Estimation Project

In 2020, the Bureau of Justice Statistics and the Research Triangle Institute International continued its collaboration with CSMU to produce national estimates for key indicators that are available in the NIBRS once the SRS retires on January 1, 2021. Current plans involve the finalization of methodology to produce national-level estimates of offense counts/rates, and estimates of other key indicators available in NIBRS (e.g., victim and offender characteristics, weapon involvement, and location type). Significant milestones and points of information for work going into calendar years 2021 and 2022 include:

- The publication of national NIBRS estimates as part of the release of 2021 data during calendar year 2022.
- Continuation of national and subnational estimates using converted NIBRS data for long-term trends using the SRS format.
- Future work to produce the methodology for the same key measures at the state-level once state coverage is sufficient to support them.

Intentionally Left Blank