



# Criminal Justice Information Services

---

Advisory Policy Board

March 5, 2018

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 December 6-7, 2018 Criminal Justice Information Services Advisory Policy Board meeting held in Oklahoma City, Oklahoma.

Sincerely yours,

Mr. John K. Donohue  
Chief of Strategic Initiatives  
Office of the Police Commissioner  
New York City Police Department  
Chairman, CJIS APB

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>

Criminal Justice Information Services (CJIS)  
Advisory Policy Board  
December 6-7, 2017  
Oklahoma City, Oklahoma

Table of Contents

Item #1	Oklahoma City Bombing Briefing.....	2
Item #2	Executive Briefings.....	4
Item #3	Chairman’s Report on the National Data Exchange Subcommittee.....	9
Item #4	Chairman's Report on the National Instant Criminal Background Check System Subcommittee.....	11
Item #5	National Crime Prevention and Privacy Compact Council Report.....	15
Item #6	Nlets, The International Justice and Public Safety Network Update.....	18
Item #7	Biometric Hit of the Year.....	22
Item #8	Chairman's Report on the Identification Services Subcommittee.....	22
Item #9	U. S. ICE Programs Update: Biometrics and Advanced Analytics.....	33
Item #10	Chairman’s Report on the National Crime Information Center Subcommittee...	34
Item #11	NCIC Third Generation Briefing.....	38
Item #12	FirstNet.....	39
Item #13	Operational Applications of National Incident-Based Reporting System.....	41
Item #14	Chairman’s Report on the Uniform Crime Reporting Subcommittee.....	41
Item #15	UCR Program Briefing.....	50
Item #16	National Consortium for Justice Information and Statistics (SEARCH) Update.	51
Item #17	Chairman’s Report on the Security and Access Subcommittee.....	53
Item #18	Tribal Update.....	60
Item #19	Chairman’s Report on the Compliance Evaluation Subcommittee.....	61
Item #20	NICS Section Status Report.....	63



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

December 6-7, 2017  
Oklahoma City, Oklahoma

**Meeting Report**

Mr. John K. Donohue, New York City Police Department and the Federal Bureau of Investigation's (FBI's) CJIS APB Chair, called the meeting to order at 9 a.m., December 6, 2017, at the Cox Convention Center, Oklahoma City, Oklahoma.

Mr. R. Scott Trent, FBI, CJIS Division, and Designated Federal Officer (DFO) for the CJIS Advisory Process, opened the meeting with a moment of silence in honor of former Security and Access (SA) Subcommittee Chairman, Mr. Allen Ferretti, who recently lost his battle with cancer.

Next, Mr. Trent welcomed everyone to the meeting and led the attendees in the Pledge of Allegiance. He then provided housekeeping notes and introduced the head table:

Mr. John K. Donohue, New York City Police Department, and CJIS APB Chair

Mr. Rainer S. Drolshagen, Deputy Assistant Director (DAD), FBI, CJIS Division, Clarksburg, WV

Mr. Christopher M. Piehota, Executive Assistant Director, (EAD), FBI, Science and Technology Branch (STB), Washington, DC

Mr. Michael C. Lesko, Texas Department of Public Safety (TXDPS), and CJIS APB First Vice Chair

Colonel Douglas A. Middleton, Henrico County Manager's Office, and CJIS APB Second Vice Chair

Ms. Kimberly J. Del Greco, DAD, FBI, CJIS Division, Clarksburg, WV

Mr. Joseph F. Klimavicz, Chief Information Officer (CIO), Department of Justice (DOJ), Washington, DC

Chairman Donohue welcomed everyone to the meeting. He encouraged attendees to contribute and make the sharing of the nation's criminal justice information (CJI) better, more secure, and efficient. He then introduced new APB members:

Mr. Kevin C. Cockrell, Montgomery County Attorney, National District Attorneys Association representative

Lieutenant Nicholas DelRomano, Pennsylvania State Police, Northeastern Region representative

Mr. Joseph N. Morrissey, New York State Division of Criminal Justice Services, Compact Council representative

He then called the roll of the CJIS APB members and recognized the Working Group Chairs. *(See Appendix A for the Roll Call.)*

Chairman Donohue introduced special guests, Ms. Kathryn Peterson, Special Agent in Charge (SAC) Oklahoma City Field Office, FBI; Chief Deputy Rickey Barrow, Oklahoma County Sheriff's Office; and Chief William Citty, Oklahoma City Police Department, all who provided opening remarks.

Gallery Introductions were then conducted. *(See Appendix B for a complete Meeting Attendee List.)*

Chairman Donohue briefed on his promise to improve the posture of the APB and awareness in the law enforcement and criminal justice communities of the work of the APB. A newsletter was sent to members of the Advisory Process following the June 2017 APB meeting with a quick synopsis of the work done at the meeting. He indicated this would continue, and encouraged members to share these newsletters with their constituencies, the CJIS Systems Officers (CSOs) in each of their states, as well as those involved in technology and CJIS-related items in each of their police departments, to apprise them of what the Advisory Process is working on.

He mentioned talking points were also provided to help clarify APB members' roles to their colleagues regarding the APB and how it works in CJI sharing. He relayed significant outreach was made to a number of major organizations to ensure awareness of the work of the APB. He stated they will seek opportunities to speak to the National Governors Association about the Advisory Process, as some of the recommended changes may require governors' support, and they need to be aware of how it affects them.

He encouraged APB members to speak to their colleagues and encourage those in law enforcement to submit topic papers. He expressed the importance of continually improving systems, data sharing, and data security.

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 Oklahoma City Bombing Briefing**

Ms. Kari Watkins, Executive Director, Oklahoma City National Memorial and Museum, provided a briefing on the Oklahoma City Bombing.

Ms. Watkins stated when entering the grounds of the Oklahoma City National Memorial there are three flags-- the city flag, the state flag, and the United States flag. These flags are symbolic of city, county, state and federal governments coming together and working through the worst domestic terrorist attack on American soil, and one of the largest crime cases the FBI has prosecuted.

She relayed a considerable amount of the story is told through touch screen. The museum was renovated three years ago, allowing them to give the story more depth than when the museum first opened in 2001.

She advised the memorial museum is a public-private partnership. The park service is on-site, but is owned and maintained by a private foundation. They take pride in this because on the grounds where an American citizen tried to take down government, they can show that government and its people can work together. The museum tells a story from the moment before the bombing occurred to where the city and the country is today. She opined one of the most powerful aspects of the museum is the story it tells about all levels of law enforcement working together.

Ms. Watkins stated the museum is the largest repository for any single event. They have the majority of all the FBI material, as well as the state's and city's collateral work that led to the prosecution of both Timothy McVeigh and Terry Nichols. She expressed the story is told not to glamorize or highlight McVeigh or Nichols, but to show the great work of the people, the government employees, the agents, the police officers, the sheriffs, everyone working in law enforcement, and volunteers. It illustrates how individuals came together and worked together in the very worst of circumstances.

In 1995, computers and the worldwide web were new, and people were not tweeting and texting. School age children today have no perception of a world where cell phones and texting were not an option. Children often ask survivors why they did not text their family to let them know they were okay. This was not a reality in 1995. She expressed how modern technology and communications has affected the responsibility of citizens. She stated, as an institution, it is important to teach the basic lessons of citizenship, responsibility and resilience. The lesson learned from this incident is that one of McVeigh's friends could have made a difference and kept this from happening. If students are taught these stories, then possibly somewhere down the road we will see the fruits of that labor. Since Oklahoma history is first taught to ninth graders, private money has been raised to bring ninth graders to the museum. The museum teaches them about the senselessness of violence, the impact to the common man, of terrorism, what domestic terrorism is, what the lone wolf looks like, and what caused this to happen.

Visitors to the museum learn a lesson and understand lives were changed. Families lost loved ones, and survivors are still wounded by what they lived through. Rescue workers are still living with the fact they could not pull one more body out. Law enforcement still deals with the fact they did not know this was going on, or they couldn't stop what was going on. Those realities are still relevant today, 23 years later.

She advised the story is meant to take you back to 1995 and experience the horror, but also the hope that came out of it and the lessons learned, but most importantly, to teach the lessons of responsibility, resilience and remembrance.

## **APB ITEM #2 Executive Briefings**

Chairman Donohue introduced Mr. Christopher M. Piehota, EAD, FBI, STB. Mr. Piehota provided a PowerPoint Presentation. (*See Appendix E.*)

Mr. Piehota greeted meeting attendees, expressing his appreciation for taking time out of their busy schedules to attend the meeting. He thanked the APB for providing leadership and helping the law enforcement community at large. He also recognized CJIS for providing the forum and helping facilitate the APB's activities. He thanked DOJ CIO Mr. Joseph Klimavicz, for attending to provide alignment and leadership across the department when it comes to how systems are developed and employed.

He briefed on areas he asked the Operational Technology's Laboratory, and CJIS Division, to give extra attention to this upcoming year. One area of focus is identity resolution. He advised biographic information can be manipulated easily, but the hope is that together through the law enforcement community, biometrics can be used as a way to move forward for positive validation, identification, authentication, and ways to promote community safety for officers and citizens. He stressed the importance of ensuring officers know who they are dealing with, and can take appropriate measures when looking at making expedient, accurate, and professional identity resolution.

Another area he briefed on was data collection and data management. He noted massive amounts of data are collected right now, and while the conversations are focused on video data, immense amounts of data are collected across the entire law enforcement community. He noted while it is a good thing, it is also a liability if the data cannot be used to draw conclusions, make the information actionable, and deliverable to front-line investigative and analytical personnel. Along with video, massive amounts of just digitized data and audio data is collected. He pointed out the FBI managed approximately three petabytes of video recordings last year for investigative purposes. It is a challenge to take that type of volume, apply analytics, and then provide that data to our partners and to investigative and analytical personnel to react, predict, respond to, or to develop plans for future operations.

He advised the STB is planning to build an updated, integrated, more sustainable FBI identification approach using all communities' abilities to collect, store, process, and analyze, as well as retrieve and share. He noted it is not enough to get the information. How do we apply analytics, how do we store it, how do we retrieve it, and how do we provide it to our partners? He stated it needed to be done in a timely fashion because certain instances require the information within hours.

He touched on video analytics. He stated they take in much data, but until more advanced video analytics are developed across the law enforcement enterprise, there will be limitations on the ability to extract and exploit intelligence and leads from video and data



evidence. He explained footage from the last couple of tragic events had key video components that helped draw conclusions and clarify situations. He emphasized nothing of any importance happens anymore without some sort of video component. With the presence of cell phones, surveillance cameras, dash cameras, and video cameras, the video component will become more important in the future.

He briefed on technology integration. Along with the DOJ CIO's office, the FBI is looking for a better way to integrate their technology and look at systems compatibility and scalability. He advised the time of building specialized singular scope systems has passed. We have to plan better, and we are looking for that partnership across the enterprise.

He briefed on Rapid Deoxyribonucleic Acid (RDNA). He advised in August, the President signed an act, allowing DNA profiles to be generated outside of an accredited laboratory environment and searched against the Combined DNA Index System (CODIS) database. He stated this technology has significant potential in how it can aid law enforcement. Applicable and appropriate protocols, practices, policies, and infrastructure must be developed to get this done. They do not want to move too quickly and do anything that may negatively affect the credibility or utility of this technology. He advised the FBI has been working with their partners to create test studies and cases, where RDNA would be done in booking station environments in a controlled environment, in which they can develop those practices, protocols, procedures, test the technology, and look for confounding factors that may not be readily available or apparent.

Mr. Piehota advised CJIS is completing a pilot study for criminal justice applications of the iris scanning. He stated there is a lot of interest in this because biometric identification can be accomplished in an expedient, accurate fashion, without touching people. The pilot study will conclude this year. He stated there are 750,000 records, which is a 25 percent increase over last year's database. He advised the pilot resulted in the identification of 372 wanted persons in fiscal year (FY) 2017.

Mr. Piehota then briefed on facial recognition. He pointed out the public is willing to post their pictures and videos on the internet, but are reluctant to share them with law enforcement. He voiced concern that individuals are putting less trust in law enforcement than the internet.

He advised the FBI is still committed to Crime Data Modernization (CDM) and the National Incident-Based Reporting System (NIBRS) transition with the full support of FBI senior leadership. Director Wray has maintained the NIBRS transition as one of his primary priority initiatives. January 2021 is still the target for implementation. He stated society wants to see data and have information. To provide information and drive and guide the conversation, the FBI must be able to collect more data to provide context and relationships. He reported significant sums of grant money have been awarded to law enforcement agencies in need of funding to assist with the transition. He advised the group to work with their partners and their organizations if they think they can benefit from this funding.

He advised the Use of Force (UoF) data collection pilot, which includes over 100 agencies, concludes in December 2017. He noted this is another way to guide an informed and objective conversation on law enforcement activity.

Lastly, he briefed on the development and deployment of the Crime Data Explorer (CDE), which went online in 2017. He advised the site is still being developed and refined, but it was decided the data should be available to the public so they can drive an objective, informed data-enhanced conversation, and not rely as heavily on the internet to characterize what law enforcement is doing in its communities.

Mr. Piehota introduced Mr. Klimavicz, DOJ, CIO. Mr. Klimavicz advised he was serving the APB in two capacities, one as the department CIO, the other as DOJ's CJIS Systems Agency (CSA). As CIO, he is responsible for serving, protecting, and advancing DOJ's goals through information and technology services. As DOJ's CSA, he serves almost 150 Criminal Justice Agencies (CJAs) as well as many others for civil purposes.

From a department perspective, CJIS's investment in technology represents a significant amount of the overall DOJ Information Technology (IT) spend, and CJIS is an important link to DOJ's state, local, and tribal mission partners. The APB provides the FBI and DOJ an unparalleled view into technology as well as the evolving needs of state, local, county, tribal territories, and the national forum focused on improving information sharing.

Mr. Klimavicz first briefed on IT modernization. He pointed out technology is a critical mission enabler in all aspects of their work. Building a modern, secure architecture for federal IT systems is high priority across the entire federal government. It ensures availability to information, when individuals in the field need it, and that the information is accessible only by authorized users. He noted technology is evolving at an increasing rate. The tools for managing this information need to keep pace with American innovation. He stated he is modernizing the way DOJ delivers CJIS services to DOJ components, to other partners, and to federally recognized tribes.

He advised the interconnected nature of CJIS architecture means they all need to consider the cost and time it will take for customers to take advantage of these modernization efforts. He opined modernization would only be successful if there is a solid understanding of the costs for state and local governments to take advantage of these solutions, as well as the time it takes to implement them.

He then briefed on information sharing. He advised his office is in the process of developing an information management, access, and sharing strategic plan, which will focus on three aspects: identity management, data management, and interoperability.

He noted IT services and systems exist to ensure the right users are getting the right information when they need it. The information management strategy will provide a framework for ensuring DOJ technology efforts synchronize with the needs of mission partners, and contribute to a national dialogue about shared long-term vision and strategy for improving national criminal information and information sharing architectures.

The last topic he addressed was identity credential and access management. He opined this continues to be one of the biggest obstacles to effective information sharing. He noted there are many stakeholders and many needs that must be considered. Within the department, his focus is on creating an enterprise level management of identities, credentials, physical access, and logical access, as ways to secure both their systems and their information.

From a data management perspective, they are targeting consistent use of information exchange standards to take advantage of their Integrated Computer Aided Manufacturing (ICAM) enhancements, which is an important step toward better interoperability with their mission partners. A unified ICAM framework based on a federated approach with strong governance will enable users to access systems using existing identity credentials, via simplified sign-on technologies. He stated they would continue to explore promising ICAM technologies and strategies. He encouraged the group to consider how CJIS identity ecosystems might interact with a nationwide ICAM framework.

Chairman Donohue introduced Mr. Drolshagen, DAD, FBI, CJIS Division. Mr. Drolshagen provided an update on CJIS. (*See Appendix F, PowerPoint.*) He advised Assistant Director Douglas Lindquist was unable to attend the APB as he was going before the Senate.

Mr. Drolshagen first briefed on CDM, noting significant progress in 2017. He advised there would be four solicitations in 2018, stressing December 2018 will be the final solicitation. In FY 2017, the Bureau of Justice Services (BJS) provided funding to eight large local agencies, six small and medium agencies, and three state Uniform Crime Reporting (UCR) programs. He touched on the UoF pilot program, which concludes on December 31, 2017. They anticipate it to go live in early 2018, pending Office of Management and Budget (OMB) approval.

He then briefed on the NIBRS transition. There will be an update at the spring APB on how CJIS anticipates the country will be transitioning in 2018. He noted National Crime Information Center (NCIC) Third Generation (N3G) has made significant strides in the last six months, with fourteen high level concepts approved. A nationwide canvass done in 2014 and 2015 resulted in 5,600 user requests. He recognized N3G Task Force Chair, Wyatt Pettengill and the N3G Task Force for leading the effort to work through these requirements. He advised another big step for N3G is the ability to test NCIC functionality in the National Information Exchange Model (NIEM) Extensible Markup Language (XML). This is currently available in a test environment with the anticipation it will be in the operational environment in January 2018. He advised a request for information was sent to the vendor community in November 2017, resulting in an overwhelming response and interest in transitioning N3G. He advised CJIS is reviewing the responses and anticipates they will submit a request for proposal to the vendor community in early 2018.

Mr. Drolshagen briefed on the National Instant Criminal Background Check System (NICS). Black Friday 2017 was a record day with 203,086 transactions, an increase of nine percent from the previous record set on Black Friday 2016. In order to handle the high demand of checks, CJIS NICS alumni assisted and CJIS worked with FBI SACs across the country to enlist their NICS alumni to support NICS checks from the field. He said the response

was positive with overwhelming support and the FBI is dedicated to the endeavor to avoid tragic events when possible.

He then briefed on missing dispositions. He noted the FBI has focused on improving the percentage of resolved dispositions. Ninety percent of their arrests are associated with dispositions. The remaining 10 percent have not had final adjudication. Currently, seven million federal arrests and 65.1 million state and local agency arrests are missing dispositions in the Next Generation Identification (NGI). The FBI hired 30 contractors to address the backlog for federal dispositions, and plan to hire additional contractors to further assist with federal dispositions. He stated they are exploring additional solutions to address the disposition issue, and he hopes the law enforcement community will help find solutions to this problem as well, pointing out missing dispositions is a national challenge.

He advised another area of great improvement this year is requests for identity history summaries. Previously, it was a manual process. He reported Phase 1 of electronic departmental orders is an internet public interface for request submissions. Phase 2 will allow individuals to request their identity history summaries and receive them electronically. He advised the rollout should be in February 2018. Individuals can also submit an appeal via electronic means on the internet. A pilot project with the United States Postal Service is in the works and it will allow individuals to submit their fingerprints at a number of select post offices across the country. This should be available in spring 2018.

He briefed on the Public Access Line (PAL). PAL receives tips from across the country regarding threats and criminal activity. He reported all field offices transitioned to the PAL this year. He stated the FBI takes these tips, collates them, and gets them out to the field. In 2017, PAL answered over 745,000 calls, received over 733,000 electronic or email tips, and forwarded over 20,400 tips to investigators. He advised PAL is not just an FBI service. When major events occur across this country, the tip line 1-800 CALL FBI is established. The FBI is working with their state and local counterparts during these major crises to have a tip line for individuals to use. PAL vets the tips and forwards them to investigators. He provided a few examples of major cases PAL supported in 2017, which included the Las Vegas Shooting and the Delphi, Indiana homicide of two female hikers.

He reported the 2017 CJIS Annual Report has been published and will be posted to the <fbi.gov> website. This report highlights significant accomplishments in 2017 and provides program area updates. He asked the group to not only take note of the statistics and the volume of activity occurring through the systems, but also their information shared across the country. He stated it is a great reflection of the hard work of the APB, individuals at CJIS, and the state, local, tribal, and federal agencies. He recognized Colonel Ed Roessler, Major City Chiefs Association; Chief Bill Denke, tribal agency representative; and Mr. Corey Steel, Conference on Chief Justices; who provided their perspectives which were included in the annual report.

In closing, he stated CJIS relies on the APB to carry out the CJIS perspective and share it with the agencies and groups they represent. Additionally, he asked the group to bring

back input from their peers and their communities and continue to help make sound and solid decisions on the systems and services that affect this nation.

### **APB ITEM #3 Chairman's Report on the National Data Exchange (N-DEx) Subcommittee**

Ms. Carol Gibbs, Illinois State Police, and acting Chair of the N-DEx Subcommittee presented this agenda item. (*See Appendix G, PowerPoint.*)

#### N-DEx Issue #1 N-DEx Program Status

Ms. Gibbs briefed on the N-DEx program status, providing new statistics as of September 30, 2017. She reported N-DEx contains data from over 6,400 criminal justice agencies CJAs, totaling more than 396 million ingested records, with another 308 million federated records available. As of the October 2017 subcommittee meeting, there were over 7.2 million searches performed in FY 2016 and 13.7 million in FY 2017.

She continued with an update on stakeholder outreach and customer support. The subcommittee heard about some of the partnerships with Law Enforcement Information Exchange (LInX) regions. All 15 are connected for user access, with only one, Rocky Mountain Network, that has not completed their data submission link to N-DEx. For COPLINK, nine of the 12 regions are connected for user access, and seven of the 12 for data submission.

She briefed on the Regional Information Sharing System (RISS). Seven of the 12 are connected for users, with the remaining five showing at least half of their agencies connected. The discussion about the RISS centers brought some input from the group about the upcoming proposed intel project for the federation of criminal intel. The discussion revolved around the vetting and training of users, and the technical connection that is involved. Would it be possible for the regional systems to pass the attribute intended for the portal to authenticated users? The subcommittee presented an action item to the N-DEx Program Office (PO) to conduct research to determine if the criminal intel project can allow regional partners to pass the attributes for access, and therefore, not limit it to portal users only.

She next briefed on the International Justice and Public Safety Network (Nlets) pilot. The Illinois and Kansas fusion centers were piloting federated access to Nlets-run data, which is transaction log files. The preliminary feedback was good and the pilot ended in November 2017.

She then discussed the success story awards program. In 2017, there was one success story of the year and five excellence awards. The success story award, involving a human trafficking case, was presented to the Las Vegas Metro Police Department. The recipients of the excellence awards were Jacksonville Sheriff's Office, Florida; Georgia Department of Community Supervision; Washington County Sheriff's Office, Minnesota; Suquamish Tribal Police Department, Washington; and the Tennessee Department of Safety and Homeland Security. The award recipients were featured in a state regional newsletter.

The last portion of the N-DEx program status was on technical enhancements or future enhancements. The first was batch query performance. She advised there has been a significant increase in the use of the batch query. The goal is to ensure the performance is there and the batch query size can be supported. The second enhancement was to return structured elements to the Logical Entity Exchange-Specifications Search and Retrieve (LEXS-SR) customers in addition to what they are already receiving. The third enhancement pertained to the use of NICS code F for N-DEx, and support of those searches through both portal and web service. She stated it must be as automated as possible for those conducting screenings for prohibited individuals.

This topic was accepted for information only.

#### N-DEx Issue #2 Creation of a N-DEx System Use Code for Federal Security Clearances, Suitability, and Fitness for Federal Employment, Credentialing and Related Federal Matters

Ms. Gibbs briefed on an update from the N-DEx PO regarding actions that resulted from Executive Order 13764, which amended two earlier executive orders. The new executive order authorized searches of additional biometric or other databases if deemed appropriate by the entity having control of that data source, and law did not otherwise preclude it. CJIS executive management deemed N-DEx is an appropriate data source, they have completed a review and update of the privacy impact assessment (PIA) and the systems of record notifications (SORN), and it is in the approval process.

She advised the new use code would be no different from the others the law enforcement community is accustomed to today. For instance, the same rules apply to advanced permission and verification, as well as to the agreement of the data contributor. The CSO has many controls in N-DEx, and performs an authorization for an individual or individuals authorized under a new use code, and ultimately that code is only available to those individuals; no one else sees it. She noted it is important for the record owning agency to control the dissemination of their own data.

This topic was accepted as information only.

#### N-DEx Issue #3 N-DEx Institutional and Community Corrections Update

Ms. Gibbs then provided an update on the corrections and probation community. She noted there are currently nine state departments of correction agencies directly contributing, and four other state level contributors that are not necessarily the department of corrections. She provided some statistics on batch use by this group of users. In the first quarter of FY 2016, there were 1,000 searches of N-DEx via batch, increasing to 500,000 by the second quarter of FY 2017. By the third quarter of FY 2017, there were 1.75 million searches.

She briefed on collaborations with corrections, probation, parole, and their use of the batch query capability to monitor absconders in their high-risk populations. Half of all of the submitted 2017 success stories came from the community corrections group. She reported the N-DEx received an endorsement from the National Institute of Corrections in September 2017.

APB Motion: This was accepted as information only.

#### N-DEx Issue #4 Update on Fusion Center Access to CJIS Division Systems

Ms. Gibbs advised the N-DEx Subcommittee discussed this issue completely, and made a recommendation.

APB Motion: This was accepted as information only.

#### N-DEx Issue #5 NICS Searching N-DEx Update

Ms. Gibbs stated technical, training, and outreach categories were discussed. She noted technical work is ongoing. Training, which she groups into outreach, is critical to this implementation. The user of the system needs to be aware there is a new use code.

APB Motion: This was accepted as information only.

Ms. Gibbs then briefed on the subcommittee's two ad hoc discussion items. She advised the N-DEx PO reported a variety of individuals have expressed the opinion yellow responses are lean. She provided an example of a query that returns a large record set, but with limited information in the records. She opined the reason might be the circumstances of that query is a time-bound decision. The program received a suggestion from the outside to take yellow records and tweak them. For instance, a query could include the involved individual's role and add the offense for that particular incident. The subcommittee responded everything done in N-DEx was deliberate. Contributors deemed their records yellow according to the established rules. The subcommittee understood the dilemma; but were unwilling to support changing yellow responses. However, the subcommittee requested the N-DEx PO research the impact of creating a new color for data sharing, and in their research include some of the other things that would include who would be affected, what it would mean, how much of a technical challenge it might create, and also the impact on the PO.

The second ad hoc topic involved the CJIS Division's Bioterrorism Risk Assessment Group (BRAG). BRAG vets individuals who possess, use, or transport biological select agents or toxins. These individuals seek authorization through such bodies as the Center for Disease Control. She noted this ad hoc topic was a heads-up precursor to a spring 2018 topic paper.

#### **APB ITEM #4 Chairman's Report on the NICS Subcommittee**

This agenda item was presented by Ms. Lynn Rolin, South Carolina Law Enforcement Division, and Chair of the NICS Subcommittee. *(See Appendix H, PowerPoint.)*

#### NICS Issue #1 NICS Update

Ms. Rolin advised she would not present the NICS statistical data because it was included in Ms. Robin Stark's NICS Update presentation the previous day. Ms. Rolin briefed on

the disposition of firearms (DOF). She stated there is a denial rate of 5.5 percent associated with DOF background checks. The NICS Section plans to target states not currently utilizing the DOF to convey the benefits of employing this resource.

This topic was accepted as information only.

NICS Issue #2 CJIS Division's NICS Enhancements Status.

This topic was accepted as information only.

NICS Issue #3 Application of Title 18, United States Code, Section 922 (g)(2)-Fugitive from Justice

Ms. Rolin reported there was a fugitive from justice update from NICS, providing a historical overview of some of the changes and information related to processing federal prohibition. NICS is seeking guidance from the NCIC Subcommittee for suggestions to streamline the research process and to see if they could add some elements to NCIC that could benefit processing. A letter currently pending from the Office of the General Counsel (OGC) will be sent to state attorney general (AG) offices throughout the country. The purpose is to advise of the change in processing fugitives from justice and to advise if they are unsatisfied with the changes made at the federal level, they have the discretion to enact laws at the state level to supplement it. Chairman Donohue drafted a letter to send to the United States AG. He plans to share this letter with the APB and working groups, whose members might share with their respective states. She advised the letter is in the approval process and should be sent before the end of 2017.

This topic was accepted as information only.

NICS Issue #4 N-DEx Program Status

Ms. Rolin stated technical requirements are being developed and the framework has been completed for NICS to search N-DEx as a secondary search. The N-DEx point of contact (POC) will be developing training materials for the NICS and N-DEx POCs to ensure understanding between both parties. This topic was presented in the N-DEx Subcommittee Report, N-DEx Issue #5 NICS Searching N-DEx Update.

This topic was accepted as information only.

NICS Issue #5 Re-evaluation of the Expansion of the Information Required with the Submission of a Record to the NICS Indices, Formerly known as the NICS Index, and Potential Fields to be Added

Ms. Rolin reported this issue was a re-evaluation of the expansion of information required with the submission of a record to the NICS Indices, formerly known as the NICS Index, and potential fields to be added. The mandatory and optional fields were re-evaluated within the NICS Indices. The current topic for vote is related to reevaluation of the mandatory



and optional fields within NICS Indices that were approved by the APB in 2012. In 2012, a topic paper was presented to the APB with the purpose of discussing whether the minimal information required when adding information to the NICS Indices should be changed or remain the same. The approval of the mandatory requirement in some of the data fields and the addition of new data fields warranted a system change in the NICS. At that time in 2012, changes to the NICS were constrained during the New NICS development to prevent cost and schedule impacts of re-planning. The initiative was deemed a post-New NICS enhancement. Now the New NICS is functional, the enhancements may be implemented, if necessary.

***Option 1: State Identification Number (SID)***

APB Motion 1: The APB moved to accept Option 1a: Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices.

***Option 2: Henry Fingerprint Classification***

APB Motion 2: The APB moved to accept Option 2b: Rescind the 2012 decision by the APB to create an option field for the Henry Fingerprint Classification. Contributors will be advised that they may continue to enter this information in the MIS field.

***Option 3: Eye Color/Hair Color***

APB Motion 3: The APB moved to accept Option 3a: Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

***Option 4: Weight***

APB Motion 4: The APB moved to accept Option 4a: Uphold the 2012 decision by the APB to make no changes to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

***Option 5: Race***

APB Motion 5: The APB moved to accept Option 5b: Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

***Option 6: Date of Birth (DOB)***

APB Motion 6: The APB moved to accept Option 6b: Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

***Option 7: Miscellaneous Field (MIS)***

APB Motion 7: The APB moved to accept Option 7a: Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

***Option 8: Middle Name***

APB Motion 8: The APB moved to accept Option 8a: The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.

***Option 9: Additional Information Available Checkbox***

APB Motion 9: The APB moved to accept Option 9b: No change, the indication of additional information will continue to be notated in the MIS field.

She advised subcommittee members offered opinions both for and against the use of the additional information available checkbox in the NICS Indices. The checkbox could indicate there is more identifying information or research documentation. There were concerns the addition of the box may cause individuals not to reach out for additional information if the checkbox is not checked. NICS clarified the checkbox was for research information that had not been shared; it was not for mug shots. NICS pointed out information may be available at the agency level but statutory restrictions may preclude it from being shared. Another concern was individuals could mistakenly interpret an unchecked box to mean no additional information is available. The subcommittee agreed this checkbox could be valuable, but did not want to cause additional confusion among the states and would rather the states contact the agency, and know that is always an option to do so.

**NICS Issue #6 Importance of the Identification for Firearm Sales (IFFS) Program to the NICS User Community**

Ms. Rolin emphasized the importance of participation in the IFFS program and discussed the status flags available. With the deployment of the New NICS in August 2016, the NICS Section has benefited greatly from many enhancements in efficiency, including the capability to immediately deny a transaction when specific conditions are met. In May 2017, the NICS Section began a lights out Interstate Identification Index (III) denial process involving III records with disqualifying IFFS status flags.

This topic was accepted for information only.

**NICS Issue #7 and Issue #8 The Impact of Pseudo-Pointers on State Outreach in the NGI System and Criminal History Update**

Ms. Rolin advised the impact of pseudo-pointers and criminal history update was provided. She stated the NICS Subcommittee would like to thank the states who contribute and the CJIS Biometric Services Section (BSS) for their efforts, as well. She acknowledged it is a great benefit to all of the user communities, including NICS.

This topic was accepted as information only.

**NICS Issue #9 Submission of an Originating Case Number (OCA) during a NICS DOF Background Check**

Ms. Rolin reported this topic was a reevaluation of the requirement previously set forth by the NICS Section directing CJAs to include an OCA on all DOF checks conducted through the NICS. In 2014, the APB was advised the CJIS Audit Unit (CAU) and the NICS Section would conduct audits on DOF background checks to ensure compliance with federal regulations governing the NICS. The NICS Section originally advised the OCA would be a required field when conducting DOF background checks through the NICS. At that time, the OCA was necessary for auditing purposes to ensure NICS is only accessed for Brady authorized uses. This requirement was delayed until January 2017 to allow states time to make necessary system changes. Since that time, upon receipt of additional information, the CAU determined the OCA was not needed for auditing purposes.

APB Motion: The APB moved to accept Option 2: The OCA remains an optional field on all DOF background checks conducted via the NICS.

#### NICS Issue #10 Update on Outstanding NICS Subcommittee Action Items

Ms. Rolin reported there were 52 action items, 25 of which have been completed. There are three ongoing action items, 20 open action items and four new action items. One action item was the reevaluation of the NCIC Wanted Person (QW) that is now responding on the NICS Denied Transaction File (NDTF). During previous subcommittee meetings, members requested the NICS Section reevaluate the change to the NDTF six months after deployment to determine if the information responding in the QW is effective and efficient in assisting criminal justice efforts. NICS denial data began responding on QWs in August 2017. The NICS Section will provide an update for the subcommittee in spring 2018.

APB Motion: This topic was accepted for information only.

#### NICS Issue #11 Ad Hoc Discussions

Ms. Rolin reported the NICS Subcommittee heard a presentation on the Law Enforcement Enterprise Portal (LEEP). They heard a presentation on how NICS could more uniformly be a part of (TOUs) versus the interface control document (ICD). Another ad hoc discussion was related to NDTF responses and the audit process. The CAU participated in the discussion and one of the subcommittee members pointed out an apparent inconsistency in the audit process. Every auditor is different; therefore, they do not know what to expect from audit to audit. The CAU will take this into advisement.

This topic was accepted for information only.

#### **APB ITEM #5 National Crime Prevention and Privacy Compact (Compact) Council (Council) Report**

Ms. Dawn Peck, Idaho State Police, and Chair of the Compact Council, provided an update on the Compact Council. (*See Appendix I, PowerPoint.*)

Ms. Peck briefed there are 31 states and the federal government that have enacted Compact legislation. Virginia became the 31<sup>st</sup> state to ratify the Compact on July 1, 2017. She congratulated the Virginia State Police since they were instrumental in partnering with legislature to ratify the Compact. Additionally, 12 nonparty states and territories have signed the Council's memorandum of understanding (MOU) as a voluntary recognition of the Council's authority to promulgate rules, procedures, and standards for the noncriminal justice use of the III system.

She advised one of the Council's main goals is to increase the participation of criminal record repositories in exchange of criminal history information for noncriminal justice purposes. In support of that goal, the Council developed the Compact Mentorship Program (COMP) to engage states and territories to ratify the Compact.

The goal of the COMP is to pair nonparty and MOU representatives with a Compact POC. The Compact state POC serves as a resource to the nonparty or MOU representative. She noted many have recently been contacted by their COMP mentor.

She advised the Council is planning to host a Compact Ratification Symposium in conjunction with the May 2018 Council meeting. The symposium will consist of several sessions focusing on Compact ratification. Compact Officers will share lessons learned and the benefits of Compact ratification. Attendees will also learn about the significance of the work of the Council and the value of having a voice in the establishment of policies and procedures for noncriminal justice use of criminal record information. This is an opportunity to meet and collaborate with state Compact Officers and become part of COMP.

In addition to the symposium, nonparty state representatives will be invited to attend the Council meetings on May 16 and 17, 2018. This is a valuable opportunity to see the Council in action. Travel accommodation and expenses will be covered for one representative from each state, and additional state representatives may attend at the state's expense.

Ratifying the Compact brings a state one step closer to providing the most comprehensive criminal record information 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 the state's criminal history record files solely with the state.

NFF participation results in both enhanced individual privacy protection, and better security of our nation's most vulnerable populations. To date, 20 states are NFF states, with several others working on the process.

The Council met in Jacksonville, Florida, November 1-2, 2017. During the meeting, the FBI Compact Officer, Ms. Chasity Anderson, provided a briefing of the Council, detailing some of her observations after serving in the position for a year. Many of these were driven by observing the year in context of four cornerstones the former FBI Compact Officer, Mr. Gary Barron, passed on to her as keys to success. The first cornerstone is the law rules. This serves as a constant reminder that the requirements of the Compact Act are not mere

suggestions; they are the law. The second cornerstone is the FBI controls the Compact Officer's paycheck; the states control the Council. The FBI has a vote and a voice at the table and it must be used. But a strong state presence on the Council was by design. It is imperative that the state representatives in the Council engage their peers in discussion to establish the most well-informed policies and procedures for noncriminal justice use of criminal record information. The third cornerstone was it is not the FBI Compact Officer's Council. The FBI Compact Officer and the Compact team provide invaluable support to the Compact Council all year long, but they cannot be the driving force. The parties of the Compact, those being the federal government and the states who have ratified the Compact, must be aware and engage in the process and with each other, and maintain ownership of the discussions. The fourth cornerstone is to rely on history, not hearsay. With time comes a natural transition in turnover with personnel. The cornerstone is a reminder to look back at the responsibility placed on the Council almost 19 years ago and rely on the well-documented history of the Council's work, not on hearsay. She said we should all feel a responsibility to provide the most accurate and up-to-date criminal history record information for noncriminal justice purposes and the Compact Council has the privilege of being the independent body responsible for ensuring the greatest level of authorization, which occurs to prevent crime and protect privacy. She stated Ms. Anderson reaffirmed her commitment to work towards building new relationships with many of the federal partners who have, over time, become less aware and engaged in the Council, and to continue to support the states in any way she can.

Ms. Peck advised in March 2013, the Standards and Policy (S&P) Committee formally began discussing the rejection of civil fingerprints due to low image quality and the potential negative impact to the states and the federal agencies enrolling these individuals in NGI Rap Back services. With the implementation of the Seven of Ten Solution in November 2016, the statistics for fingerprint quality image quality rejects drastically reduced. Before the solution processing, the ten-print submissions retained the quality scoring assigned by the NGI system with no adjustment and returned L008, a reject message, meaning that the quality of the characteristics was too low to be used if the image quality score did not meet the minimum requirements. With the implementation of the Seven of Ten Processing, up to three low scoring images are now eliminated if scoring does not meet the scoring requirements. When the NGI system removes a low scoring image, the average score increases. This adjustment can result in the quality score increase to a level where the high confidence response can be returned to the contributor.

Based on the data collected after implementation, the first six months reflected at least a 44.79 percent reduction in image quality rejects, with approximately 81 percent of those being civil submissions and 19 criminal submissions. The Council will continue to engage those agencies who submit prints with less than ten good prints, but this program is processing many more prints with positive impacts.

In May 2016, the Council approved the proposal to allow for an alternate path to NFF participation, which will provide all Compact states with an option to submit all criminal fingerprints as Criminal Answer Required (CAR) transactions rather than a mix of CAR and fingerprint image transactions to participate in the NFF program.

During the March 2017 S&P Committee meeting, the discussion focused on adopting A-NFF, or the alternate NFF, workflow chart to review the data, logic, and system decision points throughout the process of submission to the NGI system. As a result, the A-NFF Task force was created to evaluate and provide input in the technical requirements for programming the A-NFF. The A-NFF Task Force met for the first time on August 2, 2017. At that meeting, specific topics were discussed from the May 2017 Council meeting which included an impact of the date-of-arrest cutoff, unsolicited message, rejected message, and responses. Based on discussions with task force members, the workflow chart was revised to reflect the task force's recommendations to the S&P Committee in September 2017. The committee then recommended the FBI CJIS Division move forward with the development of the A-NFF program. The Council concurred with the committee's recommendations during the November 2017 Council meeting. As the development of the A-NFF program continues, updates will be provided via topic papers shared through the APB and Council processes.

Lastly, she announced she completed her second term as the Council chair in November 2017. The Council bylaws limit the terms to two consecutive two-year terms. During the November 2017 Council meeting, Ms. Katie Bower was elected as the new chair and Mr. Wyatt Pettengill was elected as the new vice chair. She also announced the newly appointed state Compact Officers: Ms. Jennifer Bishop, Hawaii Criminal Justice Data Center; Lieutenant Jeremy Kaplan, Virginia State Police; Mr. Eric Wiltanger, Wyoming Division of Criminal Investigation; and Ms. Beverly Wilson, Maryland Division of Public Safety and Correctional Services.

This topic was accepted as information only.

#### **APB ITEM #6 Nlets, The International Justice and Public Safety Network Update**

Mr. Frank Minice, Deputy Executive Director, Nlets, presented this topic. (*See Appendix J, PowerPoint.*) He provided some background on Nlets and briefed on some projects they are currently working on.

He advised Nlets is connected to nearly every law enforcement agency in the United States and Canada, as well as every federal agency with the justice component. He reported there are over a million users and Nlets will have processed 1.8 billion transactions by the end of 2017.

Mr. Minice reported drivers' queries that take place over Nlets constitute about 50 percent of the transactions. These are followed closely by criminal history responses, both from the FBI and the III and from the states through IR and FR messages. Closely after that is the international checks, international wants and warrants, stolen travel documents, and transactions through INTERPOL. About 18 percent of the transactions are made up of 100 other resources available over Nlets.

He explained those 1.8 billion transactions run each year are kept forever. He advised they are available online through the Random Access to Nlets Data (RAND). There is

currently a pilot project with N-DEx, allowing Kansas and Illinois users to run RAND transactions against the Nlets' transaction log through their N-DEx connection.

He advised the Nlets system is up nearly 100 percent of the time thanks mostly to the wireless 4G backup connectivity available for all states and federal agencies that connect to Nlets. It kicks in automatically if they lose their terrestrial circuits. The response time round trip is about a second and a half.

Nlets offers a couple types of hosting within their data center. They have their Colo rack and stack type of hosting, where they provide real estate network connectivity into the network from their secure CJIS-audited environment. He stated Nlets has several federal agencies, state agencies, and strategic partners hosted within the data center.

He advised they have started to provide backup services to state, federal and local agencies. If an agency does not have an off-site backup capability today, Nlets can offer space within their storage environment. Data can be backed up through the network or it can be sent out of band to Nlets.

The second type of hosting they have is their turnkey cloud offering, referred to as NOVA. He explained it is the same as having physical equipment within their data center, but it is a cloud offering in their security cloud that was included in the scope of the CJIS audit. He stated it is a CJIS-compliant space in a cloud environment they offer.

Nlets has a project underway to replicate the NOVA environment in their disaster recovery location, which is in Louisville, Kentucky. They will offer a primary and backup site capability within their cloud environment.

He provided an update on their federated identity management efforts. Nlets is now a member of the National Identity Exchange Federation (NIEF). Nlets completed a pilot project with the Tennessee Dangerous Drug Task Force to share Security Assertion Markup Language (SAML) assertions to log into each other's systems with a single sign-on, which was successful. The next step in the project is to replicate that with Kansas and New York, to allow their users, through their own active directory and their own systems, to have access passing a SAML assertion to Nlets to get to Nlets' justice portal. Nlets' justice portal is their direct graphical user interface, their portal to run transactions directly over to Nlets. This allows access for states and federal agencies that connect to Nlets, in the event of a disaster, when their system is out of service. In addition, he stated they are engaged in a pilot project working with The Georgia Tech Research Institute and the El Paso Intelligence Center (EPIC), to exchange trustmarks. The trustmark program, which essentially allows them, at a resource level, access to certain types of Nlets data. They are hoping to kick this off with EPIC through their open connectivity project and the EPIC portal for EPIC users to get to data over Nlets directly.

There has been some real movement in the area of their multi-state query enhancements. They have leveraged their parsing work. It is now possible for users to send a single transaction to a destination of NL to check all 50 states on certain types of messages.

Mr. Minice said there is a push to move all users towards XML and some real progress has been made in this area. A lot of states are responding to messages in free form text and this information is being parsed by Nlets. States can request that their criminal history records come back parsed in XML from Nlets. Nlets is also able to do this for dot-delimited text formats for everything from license plate readers to stolen vehicles to initiate LoJack beacons. Nlets parsing is also being done for driver's license and registration responses as well as the multi-state queries mentioned previously.

The Nlets Board of Directors passed a motion in 2014 that all of the users that connect to Nlets would need to connect to Nlets through web services or MQ series (MQ) by July 2017. He advised the July 2017 date has passed, but about 70 percent of the users that are connected to them are using either web services or MQ. For the states that are still working towards that, there are Brodie Assistance Fund projects underway where Nlets is paying, through their excess revenue, to have the changes made in the state or federal agency.

Several are deployed a broker box, an appliance that they can put between them and the state or federal agency that will communicate with Nlets in web services and talk to the state switch in the socket protocol. The reason for this is they are moving towards a new system, which is a completely different design. This new system, which is the equivalent of N3G, will be in place around April 2018. It is their active environment between both of their location services running on an enterprise service bus. He stated they could not take advantage of the value of the enhancements if individuals are connected to an old socket to connect to Nlets. He reiterated they are past the deadline, but April 2018 is the drop-dead date.

He advised the Vehicle Identification Number (VIN) assist program was launched over Nlets recently. The VIN assist program has been supported for years by the National Insurance Crime Bureau (NICB), providing this decoding service for investigators. Nlets worked with NICB to turn that into an Nlets transaction that is available to the users. Nlets created a new message key, GVQ. Users can put the VIN in and it will completely decode the VIN just like the VIN assist program would. It provides the make, manufacturer, and color options.

He highlighted a couple of projects Nlets is working on in conjunction with the Department of Homeland Security (DHS). The first one is the Five Eyes project. The goal is to make DHS Automated Biometric Identification System (IDENT) available for law enforcement through an Nlets transaction and to query the other Five Eyes countries. The pilot will include 100 Customs and Border Protection (CBP) and DHS component users. They will be able to run a transaction based on the IDENT number at the border or wherever the case will be, and Nlets will launch that against IDENT and it will send a query to Canada to see if the individual has been denied a visa and entry into Canada. He noted the ultimate goal is to query the other four Five Eyes countries at any time they run transactions. Nlets and DHS have been working on style sheets and how the response will look. They hoped this would be up by the end of December 2017, however, it looks like it will probably be February 2018 before Nlets sees results and starts receiving feedback.



The second project Nlets is collaborating on with DHS is an enhancement to the Law Enforcement Notification System (LENS). When Immigration and Customs Enforcement (ICE) releases a subject based on a criterion, the local agencies receive a notification this person will be released into their community. Those messages are sent over Nlets today as an AM message, which goes directly to an Originating Agency Identifier (ORI). They are on a subscription type of basis with ICE, which is currently manual. It identifies the address where the individual is supposed to be released to and the date they will be released. Nlets' approach to assisting them with this is to leverage criminal history parsing. They will leverage the Nlets justice portal and their partnerships with the National Consortium for Justice Information and Statistics (SEARCH), Pragmatica, DCI, CPI and their strategic partners.

He advised the first thing they will do is assist with the subscription service that takes place today. There is a lot of manual interaction between DHS and the local users on subscribing for releases and specific ZIP codes in their jurisdictions. Nlets will automate all of that. The users will be able to send a message over Nlets and subscribe and unsubscribe based on a set of ZIP codes in their jurisdiction. They will change the way they route Nlets system messages specifically for these LENS notifications where they will be able to send them to Nlets based on ZIP codes or groups of ZIP codes, and all the ORIs or agencies that have subscribed for that ZIP code will receive the notification.

He noted Nlets is engaged with SEARCH on a project to assist with the mapping of the local charges to NCIC codes. Before they send out these notifications, DHS needs to know if the subject meets a criterion for their notification. They run a criminal history check on the individual and determine if the local literal charges meet the NCIC code to send out the alert. He acknowledged NICS, BJS, and other entities are doing something similar to map literal charge codes to NCIC codes.

Nlets is starting with a list of 46,000 state charge codes that were mapped to NCIC codes, primarily by ICE agents, who made phone calls and conducted research before sending out the notifications. Nlets has a contract with SEARCH, who will reach out to the SEARCH community to help authenticate charges. Once Nlets has an authoritative source in place, they will modify their parsing service so the criminal history, as it runs through the network, also runs through Nlets. When they parse it, they will see a state literal charge code, they will map it to NCIC, and give it to DHS so they can make those decisions automatically and speed up the process. They will make a query capability after the database is populated and the states will have the ability to keep it up to date. They will include a query capability for individuals to put in a state literal charge code and receive a response on what NCIC code it maps to.

He reported there is funding through this project to modify state criminal history systems to include that information in the response before it is sent to Nlets. Nlets will work with agency vendors directly, and if agencies are interested they will take those charges and will have the agency include them in the rap sheet before they send them to Nlets. This takes the parsing out of Nlets' hands and it also might be a way for an agency to pay for their state to send NIEM XML to Nlets for the criminal history records. He reported the project must be completed by the end of 2018.

This topic was accepted as information only.

#### **APB ITEM #7 Biometric Hit of the Year**

The Biometric Hit of the Year was presented by Ms. DelGreco, DAD, FBI, CJIS Division and Mr. William McKinsey, BSS Chief, FBI, CJIS Division.

Mr. McKinsey reminded the group that several years ago the APB tasked CJIS to identify unusual identification techniques utilizing biometrics, and to find a way to share them. He introduced award recipients, Ms. Jenny Hall and Ms. Meghan Blackburn, TXDPS, who pulled a fingerprint out of a photo which led to the successful identification of a subject in a pornography investigation. CJIS went to Austin, Texas, to present the award and film a recreation of the events surrounding this success story. It will be shared via meetings, standard publications and the <fbi.gov> website. (*The Biometric Hit of Year video was played.*)

#### **APB ITEM #8 Chairman's Report on the Identification Services (IS) Subcommittee**

Mr. Mike Lesko, TXDPS, and Chair of the IS Subcommittee presented the topic. (*See Appendix K, PowerPoint.*) He advised there were 11 information only topics.

##### **IS Issue #1 Identification Services Coordination Group (ISCG) Update**

This topic was accepted as information only.

##### **IS Issue #2 Impact of Pseudo-Pointers on State Outreach in the NGI System**

Mr. Lesko mentioned everyone in the working groups saw the impact of the pseudo-pointers on the state outreach for the NGI system.

This topic was accepted as information only.

##### **IS Issue #3 A Solicitation to the User Community Regarding their Experiences with Face Recognition Searches of the FBI's NGI Interstate Photo System (IPS) and the Utility of the Responses Received**

Mr. Lesko stressed the importance of outreach for those who are utilizing facial recognition systems to submit success stories, much like the biometric hit of the year. It shows the value of the system and how it is working, but also provides feedback on how it is not working.

This topic was accepted as information only.

##### **IS Issue #4 Require Training for Those Conducting Face Recognition Searches of the NGI/IPS**

Mr. Lesko stated this was a proposal to require training for those conducting face recognition searches of the NGI IPS. The *NGI IPS Policy and Implementation Guide* suggests training, but does not require it. With the concern Congress has had regarding the implementation of the system, it was proposed the training should be a requirement. One of the options was to require training for agencies/states prior to conducting face recognition searches of the NGI IPS. Required training is identified as completion of the FBI's Facial Comparison and Identification Training class, which meets the guidelines and recommendations for facial comparison training to competency as outlined by the Facial Identification Scientific Working Group (FISWG). The other option was to make no change. There was an additional option, which identified required training as completion of the FBI's Facial Comparison and Identification Training class or contractor-supplied training, which meets the "Guidelines and Recommendations of Facial Comparison Training to Competency" as outlined by the FISWG.

The IS Subcommittee reviewed motions from the Working Groups noting the requirement that the FBI provide all of the training would not be possible. There was also discussion that training conducted by contractors may not be a good idea. The IS Subcommittee came up with the following motion: To adopt Option 1 as amended: Require CJAs or State Identification Bureaus (SIBs) approved training for individuals of agencies/states prior to conducting face recognition searches of the NGI/IPS. Training must be consistent with the "Guidelines and Recommendations for Facial Comparison Training to Competency" as outlined by the FISWG. Mr. Lesko stated the motion would open up more opportunities for training ratified by the SIB or the CSA.

One member inquired who would approve the training. Mr. Lesko stated the approval would be by the SIB or the CSA, who would ensure the training is consistent with FISWG recommendations. The member then asked who would train the SIBs. Mr. Lesko opined he thought CJIS would provide outreach if that type of training was desired. The FISWG provides the outline of what needs to be in the training for competency. The same member asked how agencies would know if vendors claiming to be approved are approved. Mr. Lesko opined the vendor would have to approach the SIB or CSA and show how their training meets the requirements articulated in the FISWG documentation.

Another individual inquired if there had been discussion to have the FBI certify the training for consistency. Mr. Lesko responded there was no such discussion. He did note he did not believe the CJIS Division had the bandwidth to conduct and/or certify all training. He relayed this could be taken back as an action item at the direction of the CJIS APB.

A member commented while the FBI does not have the bandwidth to train the potential numbers of students, there are companies that could. For instance, MorphoTrak has a facial recognition trainer who used to work for the FBI Laboratory Division, and was part of the FISWG when it was established. She is one of the authors of the document and is qualified to provide the training. If it is limited to just bureau staff, she would not be able to provide that training.

Another individual inquired if there will be a certification for facial examiners. Mr. Lesko responded the International Association for Identification, which has representation on the IS Subcommittee, is looking into certification for facial identification training.

A member asked if core competencies could be defined so third-party assessors could determine the training is qualified. She opined individuals who do these types of matches will have to testify in court, and will have to validate their training is sufficient. Mr. Lesko stated he is certain that should be something that would be done.

APB Motion: The APB moved to adopt Option 1 as amended: Require CJIS Systems Agency/State Identification Bureau approved training for individuals of agencies/states prior to conducting face recognition searches of the NGI/IPS. Training must be consistent with the “Guidelines and Recommendations for Facial Comparison Training to Competency,” as outlined by the Facial Identification Scientific Working Group.

#### IS Issue #5 Final Seven of Ten Solution Update and Future Concepts

Mr. Lesko reported seventy-one percent of unclassifiable prints were left pinkie fingers and fifty-five percent were right pinkie fingers. He advised they have been able to get at least seven of ten prints, and the solution would benefit both law enforcement and noncriminal justice agencies.

This topic was accepted as information only.

#### IS Issue #6 Criminal History Update

This topic was accepted as information only.

#### IS Issue #7 R-DNA Update

Mr. Lesko advised Mr. Thomas Callaghan provided an update on R-DNA to the IS Subcommittee. He reported a major development includes the need for some devices to be recertified to 20 loci. The FBI moved CODIS from 13 loci to 20 loci.

He noted several local agencies have been utilizing R-DNA devices to develop forensic samples and have expressed interest in entering them into CODIS. However, Mr. Callaghan, as well as the American Society of Crime Laboratory Directors and the Scientific Working Group on DNA Analysis Methods have expressed concerns and reasons this should not be done.

He advised the IS Subcommittee agreed on the option recommended by the RDNA Task Force. A member asked, with regard to the use of R-DNA devices, why the language “limited” was chosen. Mr. Lesko responded it was because the limit was going to be for the booking environments. He advised it was discussed this will not limit the use for the locals; however, with regard to entry into CODIS, there would be a prohibition against using it for forensic development. There has been discussion on best practices for use in a local environment; taking A and B swabs, allowing A to go to a lab, and B may be used by a rapid device to do early detection.

APB Motion: The APB moved to accept Option 2 as recommended by the R-DNA Task Force: The FBI shall issue guidance on the limited use of Rapid DNA devices, including the specific prohibition against enrolling and searching of crime scene evidence developed from R-DNA devices in the CODIS.

#### IS Issue #8 Disposition Task Force (DTF) Update

Mr. Lesko briefed the DTF presented an update. The topic was accepted as information only.

#### IS Issue #9 Update on Fusion Center Access to CJIS Division Systems

Mr. Lesko provided an update on the efforts regarding fusion center access to the FBI's CJIS Division systems. There were 78 nationally recognized fusion centers, eight of which did not have an affiliation with a law enforcement agency and were unable to get access to the systems managed by the FBI's CJIS Division. Previously, the APB voted to allow for the fusion centers to enter into management control agreements (MCAs) and do the same thing CJAs can under 28 Code of Federal Regulations (CFR) Part 20.33(a)(7), which allows agencies to contract with private entities to do pretty much anything they want as long as they have entered into a CJIS Security Addendum. That flexibility is not available for noncriminal justice governmental agencies, and the fusion centers that do not have access are noncriminal justice governmental agencies.

The CJIS APB previously made a provision to move forward and allow those fusion centers to get access through the law enforcement agency by the execution of a MCA, which would allow all 78 agencies to have access to the data they need to conduct their job. He stated the question is whether to make that a permanent solution or seek a different one. Option 1 was to endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 CFR 20.33(a)(6) as a long-term solution to facilitate access to the CJIS Division's systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs, and accept the language as proposed, a modification to (6), To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency. Option 2 was to make no change to the existing regulations and continue the interim solution of granting the fusion centers access to the CJIS Division systems through an MCA. Option 3 was to discontinue the interim solution of granting fusion centers access to CJIS systems through a MCA with CJA, which would cut off access for those agencies that did not have a relationship with a law enforcement agency.

When the topic was routed through the Working Groups, three Working Groups recommended Option 1, with one adding the additional caveat that the FBI should continue to research various scenarios that may result from any proposed regulatory changes, and two Working Groups recommended Option 2. In addition to the IS Subcommittee, the NCIC, N-DEx, and SA Subcommittees also weighed in, with NCIC and N-DEx recommending Option 1, and SA recommending Option 2. The IS Subcommittee reviewed all the recommendations

and made the recommendation to select Option 1, but to revise it to make certain it was understood they were not giving a special right of access to fusion centers, but rather the CJAs have the opportunity to contract with noncriminal justice governmental agencies to provide services that assist in the administration of criminal justice. This would allow fusion centers to have that continued access as long as they had that relationship and the MCA with the CJA.

Members noted since the interim solution had been in place only one of the eight fusion centers had taken advantage of it. One member referenced a letter from Mr. Mark Gwyn, president of the Association of State Criminal Investigative Agencies (ASCIA), noting that Mr. Gwyn and his association were against the interim solution but the letter didn't really say why. (*See Appendix W.*) As a result, he questioned if the CJIS APB really understood why the fusion centers are not taking advantage of the interim solution.

A member opined in regard to Mr. Gwyn's letter he believed the fusion centers disagree with the FBI OGC's interpretation that these other eight nationally recognized centers are not performing the administration of criminal justice, or that they have to be tied to a law enforcement agency as defined in 28 CFR 20.

Another member stated the real issue is determining if fusion centers are performing the administration of criminal justice. He believes the fusion centers are of the opinion they are and the FBI's OGC disagrees. If they are granted access in an acceptable way, they must follow the rules and be audited. If they misuse it, their access would be pulled. He noted this topic has been discussed for several years, and if the APB is talking about the administration of criminal justice by these fusion centers, they should reconsider and create a solution as opposed to trying to change the CFR, which would have to go to Congress. He opined that opening up access to all noncriminal justice governmental entities was overly broad. The APB started out with trying to address fusion centers, and now we couldn't do that so we are going to try and open it up access to any noncriminal justice governmental entity that may think they are performing the administration of criminal justice. He further noted as a CSO he could break a contract with a vendor if that vendor does not perform as stated in his contract and breaks the security addendum. However, he couldn't terminate relationships with other state governmental agencies, all of whom think they perform some level of criminal justice function if this were to pass. The governor could say they are performing that function and grant access and there would be no way for the CSO to prevent it. He opined opening it up to all noncriminal justice governmental entities was too broad and the rush to find a solution that makes a CFR change was not what was needed, but rather a final determination of whether or not fusion centers are performing the administration of criminal justice. If they are not, then they should not get access and if they are there is no issue.

A member countered that argument by noting if you read the language it's for the purpose of performing the administration of criminal justice on behalf of a CJA. While another agency in the state can come forward and say it is performing criminal justice on the CSO's agency's behalf when it is not in the CSO's agency's purview to perform whatever that other sister agency is doing. It is not granting access for those sister agencies, it's granting access for the CJA to contract with that noncriminal justice governmental agency to perform the administration of criminal justice. It doesn't bestow any new authorities. It is just trying to

correct and allow for the same liberties found under (7) with the private contractor for a noncriminal justice governmental entity.

A member rebutted that by noting the fusion centers could enter into a MCA with a criminal justice entity and have access today and some have chosen not to do that. Option 2 allows them to have access. If fusion centers are performing the administration of criminal justice, it needs to be recognized as such. This topic needs to be further researched by the FBI OGC to refine what the definition is for the administration of criminal justice. Otherwise, will not change anything because if you have a criminal justice entity that contracts with an entity that doing work on their behalf, they still have to be doing the work. They still have to be audited. Agencies can do that currently, without a CFR change.

A member asked if the CJA is required to have a physical presence in the fusion center under the MCA. Mr. Lesko responded they may or may not. Another member asked if a CJA could enter into a MCA if the CJA states they perform CJA functions, even though the fusion center isn't performing specific functions for the CJA, but rather the region as a whole? Mr. Lesko responded many of the fusion centers perform these functions for states, regions or territories. The member pointed out the letter from ASCIA stated all fusion centers perform the administration of criminal justice and allocate a substantial portion of their budget to the administration of criminal justice, including the detection, which would qualify them for access. He noted if that is so, they should go get the access and this topic was not necessary.

He pointed out this involves criminal history record information which is national data from all the agencies. Members of the Advisory Process represent all of the criminal information data; therefore, it is their job to ensure the data is used appropriately, while being mindful of officer safety and homeland security. The key is balance and making exceptions that are even somewhat of a stretch is dangerous.

A member stated she assumed a number of the fusion centers must have applied for an ORI, but were denied based on a determination the requirement of being a CJA performing the administration of criminal justice was not met. She stated her agency qualified, but she did not comprehend how signing an agreement with that agency would then bestow the same authority onto another entity.

Another member stated he believed the FBI OGC determined fusion centers do not meet the definition of criminal justice activity, specifically detection.

Mr. Trent advised some fusion centers in their application for an ORI, in the functions they defined, the majority of those functions did not in the FBI CJIS Division's interpretation fall under the current definition of criminal justice activities. That was supported by the FBI's OGC interpretation of what the CFR currently says. Mr. Todd Commodore, Unit Chief, NCIC Operations and Policy Unit (NOPU) agreed and noted it was based on the concern that detection with an articulable suspicion or open case. He noted CJIS looks at fusion centers the same as other entities. They are not all specifically criminal justice agencies, but some have greater than 50 percent of their budget allocated to what CJIS defines as the administration of criminal justice. The fusion centers are falling short of that, our focus purely on detection

without an open case, and if you would allow that type of access, you would be allowing greater access given to them than criminal justice agencies because they can't access the system without the articulable suspicion or open case and that was the concern.

A member commented he was in disagreement with CJIS. The eight fusion centers were nominated by their governors as part of the nationally recognized fusion center program post-9/11. He stated pre-9/11 regulations have not been updated to the current environment. He opined this would not require an open case. They do not have to open up cases in the national security and counterterrorism realms. He suggested a pilot be done with the fusion centers. The fusion center would sign a user agreement with their state CSA, receive full access, and after six months, they would be audited.

Another member opined when looking at fusion centers across the country you can't apply a single definition because fusion centers in different states do different things. There have been studies that indicate in many cases fusion centers are producing information and documentation that has no practical application or purpose, and in many cases compiling information we already know. He further noted when you apply for an ORI you meet certain requirements and obligations and his concern was under this, entities would not necessarily have to meet those now. If we say a fusion center automatically gets an ORI because it is called a fusion center, we are potentially adding risk. However, in the interest of public safety, if fusion centers are providing information, doing things right, and if they had access to information could prevent an event or problem from happening or because they didn't have access and something negative occurred. Public safety should always take priority. The APB has to weigh the risks and determine which decision is better.

Another member commented she was in agreement there did not have to be an open case, but there should be some suspicion of criminal activity; otherwise, you are data mining. She then stated she did not think a pilot would be necessary, as the pilot was put on the table the last time the interim solution was voted on, and only one of eight fusion centers took advantage of that. She stated the APB was not trying to limit access, but trying to ensure it is done the proper way. Another member commented a report by the American Civil Liberties Union, expressed significant concerns about data mining, and cited several things that had gone out from law enforcement agencies, asking for things to be submitted to the fusion centers. The concern with the fusion center not attached to a law enforcement agency is not knowing where the information came from or how the fusion center compiled it.

A member noted perhaps the IS Subcommittee recommendation didn't look to amend the correct portion of the regulation. Would it look at the definition of administration of criminal justice or reexamining the definition of CJA? Another member opined most of the opposing people did not agree the fusion centers were noncriminal justice entities performing a criminal justice function. It further opined it may need to be elevated to the DOJ or FBI OGC to reexamine.

A new APB member stated he had a different perspective, indicating he did not understand the difference between the two motions, because each one requires an agreement allowing the fusion centers access to the data. He stated readdressing whether a fusion center is



a CJA is a different pursuit. He opined the debate was over who they need to enter into that agreement with. When they were given the option the first time, they did not take advantage of it. That option is not being taken away.

Another member commented fusion centers that do not have access, don't have any employees that are authorized to make arrests, and they are probably not submitting cases for prosecution. The focus should be on safety and ensuring the information that needs to go to law enforcement gets to law enforcement. He opined this may not be happening because there are some relationship issues. This agreement would force that relationship with a law enforcement entity, and then the information becomes actionable where an arrest can be made and a case can be forwarded for prosecution. If the governor has created that fusion center, they can enter into that agreement, and that component helps to ensure the information the fusion center is putting together is going to become actionable.

One member agreed with the point made earlier regarding data mining. He noted there was a report done by the American Civil Liberties Union expressing concerns about that, and citing several things that had gone out from law enforcement agencies asking things to be submitted to fusion centers. The concern is the fusion center not attached to a law enforcement agency and the greater risk of information coming back that you can't verify where it came from or how it was compiled. He noted the APB needed to ensure due diligence with regard to community safety and secondly, ensure we are following whatever rules apply.

One of the members commented the group might be splitting hairs over where the fusion center sits. If it sits in a CJA, it is a criminal justice entity; if it does not, it is not a criminal justice entity. Everyone is doing the same thing. They either all have access or they do not have access, and they must have the MCA. Mr. Trent clarified not all fusion centers perform the same duties, but the performance of the duties that are under the jurisdiction of that agency have to be criminal justice, and it would only be for the criminal justice purposes that they should be accessing data.

A member asked if the MCA would have to be sent to the state CSO for approval, and another member confirmed that would be the case.

An individual asked how long it would take to modify a CFR. Chairman Donohue advised the last one requested by the APB has been sitting with the DOJ for seven years. In the current regulatory environment, for every new regulation issued, at least two prior regulations must be identified for elimination. Another individual asked if the interim solution would remain in place. Mr. Trent advised that it would.

A member asked what the language change would open up beyond fusion centers, and the need for a CJA to enter into an agreement with a noncriminal governmental agency to have them assist with the work. Was the interim solution specific to fusion centers? If the motion passed, would anything else fall under the interim agreement in the meantime? Chairman Donohue responded the language does not specifically say fusion center.

Another member stated he also supported a pilot to allow designated fusion centers to participate in a six-month pilot program with a full access ORI followed by a FBI CJIS audit, with the results reported back to the APB. Mr. Trent voiced a concern if the interpretation is that it is not a CJA, a motion is being made to do a pilot to break the CFR. He suggested there might be a way to word a motion to sit down with relevant entities and try to come up with a solution on how to move this issue forward.

A member stated there is an interim solution for those fusion centers on a MCA, for which they are a governmental entity, which flies in the face of a current regulation. How can you say you can break one regulation, and you cannot break another regulation? Mr. Trent stated it was his understanding the OGC felt there is a comfort to interpreting 28 CFR 20.33(a)(6) slightly broader without feeling you were offending the regulation. To grant access to agencies who more clearly don't fall under the definition of criminal justice functions may be more of an offense to the regulation than a broader interpretation of 28 CFR 20.33(a)(6). Mr. Theodore Yoneda, OGC, stated the manner in which 28 CFR 20.33(a)(6) was interpreted to achieve the interim solution is an interpretation that was made to the satisfaction of the OGC.

A member asked if this could be resolved by making a motion for Option 2, no change; maintain the interim solution and not pursue a long-term solution to 28 CFR. Chairman Donohue commented it would take care of the problem as an interim solution, but not a permanent one. A member asked why the interim solution is just an interim solution. Mr. Lesko responded it is an interim solution because it is not supported by 28 CFR 33(a)(6), which only allows for the contracting with noncriminal justice governmental agencies for dispatch and IT processing. He pointed out 28 CFR 33(a)(7) opened it up to vendors where CJA could contract with them, and it is in that spirit, they thought they could broaden 28 CFR 33(a)(6) to make it permanent. He explained an interim solution is an opinion, which could be rescinded when there is a different opinion. If there is a change in statute, it becomes a permanent solution.

Another member stated she could not support the motion, which would give the fusion centers a criminal justice ORI, letting them be independent, not under the purview of a law enforcement agency. She preferred the solution of continuing with the interim solution and having dialogue with those affected, determine what the real issue is, and try to help them become compliant, or put the MCAs in place. It is the information the fusion centers gave to the FBI that led to the decision they did not qualify, so it might be determined what these fusion centers are doing does qualify, but they had presented it incorrectly.

Due to significant concerns raised by board members, with no consensus reached, it was decided they would not come up with a long term solution until they understood why the fusion centers did not take advantage of the interim solution. One of the members proposed an action item that the APB executives, along with CJIS staff, visit the fusion centers that do not have access and determine what assistance can be given to become compliant, or what agreements could be put in place.

Mr. Lesko opined this change fixes some things. If it is the desire of the board to address just the fusion centers, they could go with the interim solution. The fusion centers can

choose to take advantage of it or not. In the interim, they could put a working group together to have discussions and create a more plausible solution.

Mr. Lesko commented there needed to be a determination if the interim solution would continue. Chairman Donohue asked for a voice vote for the interim solution. It was the will of the board that the interim solution would continue during the course of time they were engaged in the action item.

APB Motion 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. 20.33(a)(6) as the long term solution to facilitate access to CJIS Division's systems, which would grant criminal justice agencies to the same authority to contract with noncriminal justice governmental agencies as they currently have to contract with private entities. Accept the language as proposed below:

(6) To noncriminal justice governmental agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.

**Motion failed.**

APB Motion 2: To allow the designated fusion centers to participate in a 6 month pilot program with a full access ORI followed by a CJIS audit. Report back audit results to the APB. Task the APB to create a long-term access solution.

**Motion failed.**

Note: The APB voted to assign the following as an action item:

To create a task force to review the laws, rules, and regulations, associated with CJIS information. The focus of the task force will be to:

1. To examine why any specific fusion center is ineligible for a Criminal Justice (CJ) Originating Agency Identifier (ORI)
2. Define what the basic characteristics of a fusion center must be to qualify for a CJ ORI
3. Recommend what needs to occur for a given fusion center to achieve access.

Results will be reported back to the APB.

APB Motion 3: The APB moved to continue the interim solution noted in the paper of granting fusion centers access to CJIS Division systems through management control agreements with a CJA.

#### IS Issue #10 NGI Facial Recognition Candidate List Accuracy

He provided an update on facial recognition candidate list accuracy. He advised Ms. Del Greco gave testimony in front of Congress regarding this accuracy. He stated the NGI accuracy level is to be 85 percent accurate. Currently, it is hitting above 85 percent from galleries of two to 200 responses.

This topic was accepted as information only.

#### IS Issue #11 Mobile Identification Search of the Full Criminal Master File for the Repository for Individuals of Special Concern (RISC)

Mr. Lesko stressed the importance of having the ability to allow officers utilizing the mobile ID to get the individuals that are in RISC, but also to ID the individual. Often, the officers have exhausted all other methodologies to obtain the individual's identification and they want to know who the individual is.

This topic was accepted as information only.

#### IS Issue #12 Miscellaneous Action Items Update

Mr. Lesko briefed on some miscellaneous action items. One action item the IS Subcommittee is working on is to consider the effect of 1,000 pixels per inch (PPI) on current algorithms. Thousand ppi images are run against Automated Fingerprint Identification Systems (AFISs) or Manual Fingerprint Identification Systems (MFISs), and they are trying to determine if it affects AFISs that were developed as 500 ppi. They are also looking into how it affects devices when the resolution is changed from 1,000 to 500.

He reported the subcommittee will look into the effect of the nonserious offense (NSO) policy, which states the FBI is no longer eligible to retain NSOs in the III. They will conduct research to see how this will impact national security and the National Handgun Violence Prevention Act of 1993 (Brady Act). He relayed this would be a spring 2018 topic paper.

He stated another action item is for the FBI to make expunction and modification forms fillable to make the process more automated. He reported this should also be a topic paper in spring 2018.

He noted the next topic was advice on how disposition notifications will affect the Rap Back responses. Rap Back has started up for both the criminal justice and noncriminal justice sides and there is a concern about dispositions. When they come in, are the people that are subscribed to that individual's record going to be able to get information on a disposition? He noted dispositions are not reported by the NFF states; therefore, there would be no notification to those individuals that are holding subscriptions. The Compact Council is also considering this for the noncriminal justice Rap Back.

He advised there should be a topic paper in spring 2018 regarding the potential use of flats instead of rolled for criminal justice purposes. Typically, flats are used for the fingerprint-based background checks for noncriminal justice purposes, but there has been discussion regarding the use of those flats for criminal justice purposes.

Lastly, he advised the APB moved to request the CJIS Division to review, analyze, and report back to the ISCG the time necessary to expand the RISC searches.

This topic was accepted as information only.

IS Issue #13 Ad hoc Items

This topic was accepted as information only.

IS Issue #14 Legislative Update

This topic was accepted as information only.

#### **APB ITEM #9 U. S. ICE Programs Update: Biometrics and Advanced Analytics**

Mr. Philip T. Miller, Deputy Executive Associate Director, Enforcement and Removal Operations (ERO), ICE, started his presentation by providing a brief description of the ERO and their function as a part of ICE. (*See Appendix L, PowerPoint.*) Mr. Miller said the ERO is charged with civil immigration enforcement, which means they identify people who have had some type of law enforcement encounter. He said the ERO is made up of around 5,700 officers worldwide to handle the estimated 12 to 14 million people in the U.S. who may be in violation of the Immigration and Nationality Act (INA). The ERO has been mandated by the current administration to enforce the INA and this entails many long and dangerous days for ERO officers.

Mr. Miller briefed on the EAGLE Directed Identification Environment (EDDIE). EDDIE is a mobile biometric tool that allows effective identification in the field. This tool allows officers to take slap prints, run them through the full indices, both judicial and DHS, to identify exactly whom they are talking to, what they may have done in their past and what they can be charged with. He said EDDIE has been extremely effective in the nationwide battle with MS-13. This tool has also been used in a mentorship program with the Mexican government to effectively manage their population and has been successful in identifying some high profile cases. Mr. Miller said they have experienced great success with this tool. They are looking at improving on this tool with new technology that could take four slaps simultaneously and improve response time even more.

He also briefed on the Historical Fingerprint Enrollment Project. They are going through more than two million hard prints and enrolling them into the Integrated Automated Fingerprint Identification System (IAFIS). They have had around a dozen hits on suspected terrorists and one on a law enforcement official who obtained their citizenship by fraud. They

have around 700,000 files left to ingest and will continue to work on this program and contribute this resource to the community in terms of having biometric information available as well as possible criminal prosecution.

Mr. Miller briefed on the LENS program, which is a notification at the state level of violent offenders being released from ICE detention when deportation is not an option. Law enforcement at a state level is provided a notification, which includes where the individual is being released from as well as where the individual may be going. LENS 2.0 is in the works based on feedback from sheriffs and chiefs from around the country and it looks to enhance the current notification through a subscription service via Nlets.

Mr. Miller closed by mentioning they are looking at starting a working group possibly through the APB to discuss other opportunities on how to effectively share ICE information with state and local partners.

Chairman Donohue encouraged Mr. Miller to continue to share information with the APB on these important issues. Mr. Miller said previous administrations did not allow them to participate in public events with their law enforcement partners and with the new administration, they are trying to reestablish those relationships. Mr. Miller encouraged anyone interested in hearing more about immigration enforcement to contact him and he would get them in touch with a director in charge of public engagement.

#### **APB ITEM #10 Chairman's Report on the NCIC Subcommittee**

This agenda item was presented by Mr. Walt Neverman, Wisconsin DOJ, and Chair of the NCIC Subcommittee. (*See Appendix M, PowerPoint.*) He reported the NCIC Subcommittee met on October 18, 2017, and discussed seven issues, with five motions to present to the APB. The informational only topics they reviewed were Issue #5 NCIC Status Update; Issue # 6 N3G Update; and the N3G Task Force Update. The subcommittee also had an ad hoc topic, which was a follow-up from the previous meeting, discussing NCIC codes. CJIS has identified what appears to be records that have improper article type codes, so the subcommittee discussed what follow-up action will be occurring and how to streamline new NCIC codes moving forward. States will receive follow-up communication regarding those article type codes sometime after the annual purge in January 2018 for potential records that have been entered incorrectly in each individual state.

#### **NCIC Issue #1 Fugitive from Justice Discussion**

He stated the NICS Section provided an update to the NCIC Subcommittee regarding the change in the fugitive from justice federal prohibitor for firearms. Previously, the prohibitor only required there to be an active warrant for a felony or misdemeanor. With the change of interpretation, there are additional requirements to make a firearm disqualifier determination. These requirements relate to whether the individual has fled the state, and if the individual fled for purposes of avoiding prosecution. The purpose of the discussion was to determine if NCIC could potentially assist with new data fields that could help in those determinations; however, it ultimately comes down to local law enforcement agency participation.

He reported the first action item was the NOPU and the NICS Section would have follow-up discussions following the 12 months of the initial period to determine lessons learned. NOPU will then give their findings to the N3G Task Force to determine if there are potential changes, they can incorporate into the N3G initiative to change NCIC. The second action item was for NICS to provide initial clarification to the state CSOs. Today, during the firearm background checks, if the individual is a fugitive from justice, NICS or any of the POCs must contact local law enforcement agencies and request documentation supporting whether the individual fled the state or fled the state to avoid prosecution. He stated if that communication does not go out to the local agencies, the agencies will not have the information. This communication is important to make them aware of the new process so they can start gathering the information to make it available in the future.

This topic was accepted as information only.

NCIC Issue #2 Update on Fusion Center Access to CJIS Division Systems

Covered under APB Item #8 IS Subcommittee Chairman's Report

This topic was accepted as information only.

NCIC Issue #3 Florida Department of Law Enforcement (FDLE) National Sex Offender Registry (NSOR) Pilot

Mr. Neverman advised in 2007, Florida requested and received an extract of the Sex Offender File following Hurricane Katrina to try to track down potential sex offenders who left the state of Louisiana and potentially gone to Florida. In 2015, Florida asked for its continuation as a two-year pilot project, which was approved through the APB Executive Committee. At the completion of the pilot, Florida asked that it be made permanent. This would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing a MOU with the FBI.

Mr. Charles Schaefer, FDLE, briefed on the pilot. He advised when sex offenders come to Florida, they get a driver's license. FDLE has been comparing the NSOR file to the Department of Motor Vehicle records. They have located several sex offenders hiding in Florida and arrested them.

APB Motion: The APB moved to accept Option 1: Allow FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

NCIC Issue #4 Proposal to Add the Date of Expiration Field in the Wanted Person File

Mr. Neverman advised the expiration field currently exists in the Protection Order File. The state of Georgia requested to add this field to the Wanted Person File, as well. Georgia does not have a tracking process within their state for warrants. The NCIC Subcommittee decided this proposal to the N3G Task Force, who will further explore the addition of the

expiration field in NCIC files, including whether or not the records would be retrievable via direct inquiry. The subcommittee agreed this fell into the purview of the N3G Task Force since they are already looking at all of the files and fields, for consistencies and improvement.

APB Motion: The APB moved for the NCIC Next Generation (N3G) Task Force to further explore the addition of the EXP Field in NCIC Files, including whether or not the records will be retrievable by direct inquiry.

#### NCIC Issue #5 CJIS Division NCIC Status

This topic was accepted as information only.

#### NCIC Issue #6 N3G Task Force Update

This topic was accepted as information only.

#### NCIC Issue #7 N3G Project

Concept 13 – Alternative Access

Concept 4 – Name Search Algorithm

Concept 8 – Enhanced Testing Environment

Concept 2 – Tailored Functionality

Mr. Neverman advised Concept 13, Alternative Access was presented to the subcommittee as an informational only topic. The N3G Task Force reviewed this functional requirement and felt the only option for this implementation would be during a disaster recovery occasion, and it did not want to come down to a functional requirement to limit how, during a disaster recovery, the FBI CJIS and the state CSAs could work together to come up with a solution within the policies that already exist. This concept will not be vetted further through the APB process.

He briefed Concept 4, Name Search Algorithm has two separate issues within it. Issue 1 is the expanded name search, which has ten separate functional requirements. Issue 2 was an improved algorithm, with four functional requirements.

#### **Concept 4**

APB Motion 1: The APB moved to accept Option 1 for Issues 1 and 2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

#### Issue 1 – Expanded Name Search

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.



8. Conduct a name search of alias fields
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

#### Issue 2 – Improved Algorithm

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

Mr. Neverman advised there are two issues with Concept 8 Enhanced Testing Environment. Issue 1 was for an improved testing environment, with two functional requirements. Issue 2 was to provide test records.

#### **Concept 8**

**APB Motion 2:** The APB moved to accept Option 1 for Issues 1 and 2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

#### Issue #1 – Improved Test Environment

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

#### Issue #2 – Test Records

1. Provide test records

Mr. Neverman advised Concept 2 Tailored Functionality has two functional requirements, providing the ability for the users to select content of the data returned from a search in the operational environment, and meet or exceed the improved response times as designated by the APB for searches designated as tactical, investigative, and administrative.

#### **Concept 2**

**APB Motion 3:** The APB moved to accept Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

Mr. Neverman thanked the CJIS NOPU and Mr. Todd Commodore for all their assistance with the NCIC Subcommittee and the N3G Task Force. He also expressed his appreciation to the members of the NCIC Subcommittee and the N3G Task Force.

## **APB ITEM #11 N3G Briefing**

Mr. Wyatt Pettengill, North Carolina State Bureau of Investigation, and Chair of the N3G Task Force presented this agenda item. (*See Appendix N, PowerPoint.*) He explained N3G is the initiative tasked with modernizing NCIC. The N3G Task Force was created to assist with this. He advised the task force consists of federal, state, and local partners. He recognized the members of the task force, most of whom were present at the APB meeting. He expressed his appreciation and confidence in the group. He also recognized Mr. Todd Commodore and NOPU for their guidance.

He stated the 14 high level concepts are: flexible data format, tailored functionality, access data repositories, name search algorithm, enhanced data search, system search, enhanced training resources, enhanced testing environment, record content, enhanced multimedia, improved data management, alternative outbound communication, alternative access, and finally, improved outbound communication.

The 14 high level concepts were previously approved by the APB, which started the process for the N3G Task Force to take a deeper dive into each one and talk through the functional requirements associated with each concept. As the assessments were completed, the concepts were sent back through the Advisory Process.

To date, eight concepts have been presented to the APB for approval. He advised this process will continue until all 14 high level concepts are presented, with anticipated completion in fall 2018.

The N3G Task Force is doing an ongoing review of the functional requirements. The task force has monthly teleconference calls, and they have had several face-to-face meetings. He stated it is difficult to work through these complex topics via teleconference. He emphasized a lot of good work is done in the face-to-face meetings.

The stakeholders canvass conducted by the FBI several years ago resulted in approximately 5,600 suggestions, resulting in 1,200 functional requirements. The task force went through those requirements, and 415 were approved for further exploration. With the completion of the review of the functional requirements, the next step is transitioning the role of the task force.

Mr. Pettengill advised the approved functional requirements for concepts 6, 9 and 14 will be presented to the Working Groups and APB in spring 2018. There will also be a topic paper on the agile development approach.

He stated the task force will continue to provide the CJIS Division guidance with drafting topic papers for the APB Process. As they have gone through this process, there have been some topics that require a more in-depth review. Therefore, there has been discussion about establishing N3G policy groups made up of N3G task force members and CJIS staff who will further discuss these topics and report back to the N3G.

## APB ITEM #12 FirstNet

This agenda item was presented by Mr. Christopher Algieri, FirstNet Federal Consultation Lead. (*See Appendix O, PowerPoint.*) Mr. Algieri briefed that the creation of FirstNet resulted from the identification of challenges in communication capabilities associated with the 9/11 events. The 9/11 Commission's report identified the need for an interoperable public communications capability that was available at all levels of government. As a result, in 2012, Congress passed a statute to create an independent authority within the Department of Commerce called FirstNet. It noted Firstnet should enter into a contractual arrangement with an entity to provide the communications service in an economical and affordable manner in as expeditious a manner as possible.

FirstNet has a board of directors comprised of representatives from public safety, telecommunications industry, entrepreneurs, and the federal government. The board oversees how FirstNet performs and ensures funding is used to deliver capabilities rather than being absorbed into administrative functions. He noted while the mandate exists to build the network, there is no requirement for agencies to use it. FirstNet is working to build a network with technology, capability, and security the public safety organizations want to use. It would include all 50 states, five territories, and the District of Columbia and ensure rural communities were included as well.

He advised Congress allocated 7 billion dollars to FirstNet from auction proceeds. While that amount might sound like a lot, when exploring a nationwide network that would be able to provide the capability, the amount needed is actually more than 40 billion dollars to be comparable. However, Congress advised they could not request additional funding. He stressed there was an urgency for this capability to come to market and be made available. FirstNet developed a business model with the key being public-private partnership. FirstNet partnered with AT&T, who brought 180 billion dollars of network investment to the table, and the necessary telecommunications network operation and security operation centers experience.

FirstNet was also directed to develop and deliver a state plan. They obtained feedback from experts and delivered the plan to each governor regarding how FirstNet planned to deliver radio access network within their state. Coverage was the most important thing they heard feedback on. What coverage would the network provide and how would they get there? FirstNet informed them this would occur over time, with deployment phases run over a five-year period. The states could choose to opt in or opt out. Opting in means FirstNet and AT&T deliver that radio access network within the state. Opting out means the state chooses to enter into an alternative plan and takes responsibility for that radio access network within the state. Mr. Algieri reported the timeline for the state plans and the decision by the governors is December 20, 2017. However, 35 states made the decision for an early opt-in.

He advised FirstNet had to decide if the network core should be a network of networks or a single network with a single network core. The industry standard is a geographically distributed core, but it is still a single network core. They made the decision based on the mandate from Congress for this to be a single network core.

FirstNet is driven to be a standards-based solution. He explained the Long Term Evolution (LTE) standards are developed internationally. They obtain feedback from public safety to ensure it does what it is supposed to before those capabilities are inserted into the FirstNet core. He advised the FirstNet core also allows them to do other things related to prioritization, quality service, and security perspectives. The identification of the FirstNet device the officer is carrying allows them to have priority signaling to access the network. He stated, should there be a challenge or issue with the FirstNet core, operations can be rolled over to the AT&T core.

The services and the priority delivered today prior to the FirstNet core being launched are commercial services delivered through AT&T's network systems. FirstNet's core will be delivered in March 2018, which is when the mission critical capabilities and other services can be inserted into the network and continue to evolve over time. He noted there is a distinct FirstNet Subscriber Identity Module (SIM) card, so the network can identify a user as a FirstNet user.

FirstNet understands there are tools public safety will need in order to understand what is happening on the network. He briefed on the public safety home page, where system administrators can manage the users' priority within the organization, and see the health of the network that will enable them to dynamically manage things during incidents. They can manage those that are responding to an incident to ensure the right applications are being pushed, and those that need priority during that incident have priority. He noted they want to ensure they have applications that meet the needs of public safety. FirstNet also wants to ensure availability on mobile devices to utilize in the field.

FirstNet launched an Application Programming Interface (API) for application developers to develop applications specifically for operation on the FirstNet network. In the future, they will be looking at a certification process for those to operate and run on the FirstNet network.

Chairman Donohue stated he had always heard FirstNet would need to cover the areas in the country with limited cellular service. He asked what would fill those gaps in areas such as the Midwest, Indian country and Alaska. Mr. Algieri responded one of the contractual requirements AT&T has is to deliver 20 percent of any phase of deployment to rural areas. He stated because rural is a relative term, they used the Department of Agriculture's Rural Electrification Act definition of rural in order to provide consistency.

Mr. Mark Marshall commented the project is important to public safety, and part of the premise was to ensure it would be rolled out to areas without coverage. He pointed out Mr. Algieri's statement there was a deliberate move to have one system as opposed to having a network of networks. Mr. Marshall suggested, for those rural areas with no coverage, the FirstNet board should consider partnering with other networks, as well. He opined it should not matter what network it is. Mr. Algieri responded FirstNet has board representation from the rural states and the western U.S. that understand Mr. Marshall's concerns who are trying to leverage what is there and how it is achieved. He advised AT&T is partnering with some of the smaller rural telecommunications companies in order to deliver that.

### **APB ITEM #13 Operational Applications of NIBRS**

This agenda item was presented by Dr. David Bierie, U.S. Marshals Service (USMS), (*See Appendix P, PowerPoint.*)

Dr. Bierie briefed on how the USMS has used NIBRS in the areas of applied science and operational applications. He said NIBRS is great for statistical reporting, scientific research at universities, and for answering descriptive questions about the world we live in, but it also has relevance to everyday policing.

The USMS has used NIBRS data to tackle questions regarding gun violence directed at police officers. Dr. Bierie briefed that fifty-one percent of all DOJ arrests are made by the USMS and deal with extremely dangerous people. In 2011, the nation, including the USMS, saw a significant spike in the number of officers engaged in shootouts. The USMS did many things to assess the reasons behind this spike. They then made multiple changes; for example, they bought more tactical gear and implemented new strategies in terms of entering houses.

Dr. Bierie's team was tasked with identifying everything new in scientific literature regarding the risk of firearm violence directed at police officers. They could not find any studies done on the topic. He stated Law Enforcement Officers Killed and Assaulted (LEOKA) is critically important and has been helpful, but does not answer questions about risk factors, which is needed for training and tactical decision-making. They found NIBRS to be an important tool in predicting who is going to shoot at a police officer. NIBRS provided a random representative sample of all police encounters, those involving shootings and those that did not involve a shooting. The USMS findings are available in a scientific journal and can be found via a Google search. He stated NIBRS helped them rethink some of their training, and what signals identify a risk for officers during contact with fugitives.

Dr. Bierie also briefed on operational tools the USMS has developed using NIBRS data. They included NIBRS e-Profiler, Serial Crime Analysis (S.C.An) and Community Connector (c<sup>2</sup>).

Dr. Bierie closed by stating that NIBRS has had a meaningful impact to the USMS, helping them with political problems, funding and with understanding how to do their job better. He said he hoped the idea that NIBRS is operationally useful and can complement the work of law enforcement now and in the future, would help sell this program to their law enforcement partners.

### **APB ITEM #14 Chairman's Report on the UCR Subcommittee**

This agenda item was presented by Colonel Douglas Middleton, Henrico County Manager's Office, and Chair of the UCR Subcommittee. (*See Appendix Q, PowerPoint.*)

UCR Issue #1 UCR Status Report

- Demonstration of the CDE

- Demonstration of the UoF

This topic was accepted as information only.

## UCR Issue #2 Modification of the Application of the Current Embargo Policy for the Release of UCR Program Data

Colonel Middleton briefed this topic dealt with a modification of the current data embargo policy to allow the FBI UCR program to update data in the CDE program. The CDE went live in June 2017, and the purpose is to allow for the release of information in a more rapid manner so that access and knowledge on crime data is greatly enhanced.

The subcommittee was asked to look at several things, including frequency of data submission, frequency of release, elements to be collected, and any required caveats that might be associated with that data. The subcommittee agreed on option 1, but unanimously agreed further discussion was required; therefore, they created an additional motion.

APB Motion 1: The APB moved to accept Option 1: The UCR Program should cease its application of the data embargo policy allowing for more frequent updates to the CDE.

APB Motion 2: The APB moved prior to the 2017 and later data being published in the CDE, the FBI (in cooperation with local, state, federal, tribal, and academic representatives) will develop the necessary standards on frequency of submission, frequency of release, what data elements are to be collected and released, and what caveats concerning the data that is released. The work of the FBI will be concluded by May 2018.

Chairman Donohue asked if this would be a written document that would be shared with the Advisory Process. Colonel Middleton opined it would be presented as an informational topic.

## UCR Issue #3 Addition of UCR Offenses for Federal Crime Reporting to the NIBRS

Colonel Middleton noted one of the early conversations in UCR was that the inclusion of federal agencies in NIBRS was mandated. Federal agencies have been working on developing a methodology for this to take place. The CDM team has assisted them by identifying four things they needed to consider; types of crimes they investigate, how investigations are managed, length of case investigations, and location of crimes nationwide.

The federal task force identified group A and group B offenses, specific to their work, that needed addressed and included. The subcommittee was presented with accepting all the recommended NIBRS UCR offense codes for federal reporting, and the second option was accepting all NIBRS UCR offense codes for federal reporting, in addition to additional codes.

The subcommittee made the decision to recommend option 2, which included the offense codes identified by the federal task force. However, they felt better definitions were needed for federal liquor offense and federal tobacco offense.

One member asked, with the push for NIBRS and richer data, why several dropped off, particularly the fugitive offense. Colonel Middleton responded he did not think many of the federal agencies were reporting at all in terms of NIBRS. This motion creates codes so they can report them in NIBRS.

APB Motion: The APB moved to accept all recommended NIBRS UCR offense codes for federal and tribal reporting as follows:

NIBRS Group A offenses:

- 26H – Money Laundering (Crime Against Society)
  - The process of transforming the profits of a crime into a legitimate asset.
- 36C – Failure to Register as a Sex Offender (Crime Against Society)
  - The failure to register or update a registration as required as a sex offender.
- 101 – Treason (Crime Against Society)
  - The crime of betraying one’s country, especially by attempting to kill the sovereign or overthrow the government.
- 103 – Espionage (Crime Against Society)
  - The practice of spying or using spies, typically by governments to obtain political and military information.
- 301 – Illegal Entry to the U.S. (Crime Against Society)
  - To attempt to enter the U.S. at any time or place other than as designated; or eludes examination/inspection by immigration officers.
- 302 – False Citizenship (Crime Against Society)
  - Whoever falsely and willfully represents themselves to be a citizen of the U.S.
- 303 – Smuggling Aliens (Crime Against Society)
  - When a person knowingly encouraged, induced, assisted, abetted, or aided another person to enter, or try to enter, the U.S.
- 304 – Re-entry After Deportation (Crime Against Society)
  - Individual who enters, attempts to enter, or has been found in the U.S. after being removed, excluded, deported, or has departed the U.S. while an order of removal exclusion or deportation is outstanding.
- 399 – Other Immigration Violations (Crime Against Society)
  - All other immigration violations.
- 490 – Fugitive (Harboring Escapee/Concealing from Arrest) (Crime Against Society)
  - Harboring or concealing any person for whose arrest a warrant or process has been issued under the provision of any law of the U.S. to prevent his/her discovery and arrest. This

includes any prisoner after his/her escape from the custody of the Attorney General, or from a federal penal or correctional institution.

- 499A – Fugitive (Flight to Avoid Prosecution) (Crime Against Society)
  - Moving or traveling in interstate or foreign commerce with intent to avoid prosecution, custody, confinement, or to avoid giving testimony in any criminal proceedings.
- 499B – Fugitive (Flight to Avoid Deportation) (Crime Against Society)
  - Moving or traveling in interstate or foreign commerce with intent to avoid deportation.
- 500 – Perjury (Crime Against Society)
  - The offense of willfully telling an untruth in a court after having taken an oath of affirmation.
- 580 – Import Violations (Crime Against Property)
  - Any individual who knowingly or willfully, with intent to defraud the U.S., smuggles, imports, or clandestinely introduces, or attempts to smuggle, import, or clandestinely introduce, merchandise that should have been invoiced, received, bought, sold, or facilitates the transportation, the concealment, or sale of such merchandise after importation.
- 581 – Export Violations (Crime Against Property)
  - Any individual who knowingly or willfully, with intent to defraud the U.S., smuggles, exports, or clandestinely distributes, or attempts to smuggle, export, or clandestinely distribute, merchandise that should have been invoiced, received, bought, sold, or facilitates the transportation, the concealment, or sale of such merchandise after exportation.
- 610A – Federal Liquor Offenses (Crime Against Society)
  - The shipment or transportation of any intoxicating liquor of any kind, from one State, Territory, or District of the United States, into any other State, Territory, or District of the United States, which fails to comply with legislation.
- 610B – Federal Tobacco Offenses (Crime Against Society)
  - The sell, transfer, shipment, or transportation of cigarettes or smokeless tobacco for profit into a State, locality, or Indian country of an Indian tribe which fails to comply with legislation.
- 620 – Wildlife Trafficking (Crime Against Society)  
Violations of the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), which regulates exports, imports, and re-exports of wildlife.

Group B additions:

- 90K – Bond Default/Failure to Appear (Crime Against Society)
  - The failure to appear in court without a satisfactory excuse, after bond has been set.



- 90L – Federal Resource Violations (Crime Against Society)
  - Crimes related to the damage or destruction of the nation’s natural resources including land, mineral, air, or water such as the violation of any Act regarding national parks, national monuments, or any natural resource covered by the jurisdiction of federal agencies such as The Lacey Act, Antiquities Act, Wilderness Act, National Historic Preservation Act, etc.

In addition, accept the following further offense codes and additional changes:

- 520A – Firearm (violation of the National Firearm Act of 1934)
  - The violation of federal laws prohibiting the manufacture, importation, sale, purchase, transfer, possession or interstate transportation of unregistered (non-tax paid) weapons including machineguns, firearm mufflers or silencers, short barreled rifles, short barreled shotguns, destructive devices, and any other weapons as defined at 26 USC § 5845 - Definitions.
- 520B – Weapons of Mass Destruction
  - The violation of federal laws prohibiting the unlawful use, attempted use, conspiracy to use, or use of interstate travel or facilities in furtherance of the use of a weapon of mass destruction as defined at 18 U.S. Code § 2332a - Use of weapons of mass destruction
- 526 – Explosives
  - The violation of federal laws prohibiting the manufacture, importation, sale, purchase, transfer, possession, unlawful use, interstate transportation, or improper storage of explosives as defined at 18 USC § 841 (c).

Additionally, the definitions of the below offenses are amended as follows:

- Federal Liquor Offense
  - The violation of federal laws prohibiting the production, importation, distribution, transportation, sale, purchase, or possession of non-tax paid distilled spirits, wine, or beer, and the equipment or devices utilized in their preparation.
- Federal Tobacco Offense
  - The violation of federal laws prohibiting the production, importation, distribution, transportation, sale, purchase, or possession of non-tax paid tobacco products.

UCR Issue #4 The Use of the Judicial District (JD) for Federal Agencies to Report a NIBRS Incident to the UCR Program

Colonel Middleton discussed the difficulty of dealing with a federal agency not operating within the context of a jurisdictional boundary, much as local and state law enforcement does. He stated there may be more than one judicial district in a state, but he

believed most, if not all, of the judicial districts do not cross state boundaries. He commended the federal task force for their work on this issue.

APB Motion: The APB moved to accept Option 1: Create a new data element that exists in the Administrative Segment that captures the JD code for federal agencies to report the location of a NIBRS incident to the UCR Program.

#### UCR Issue #5 Expansion of the UCR Program Police Employee Collection

Colonel Middleton advised this issue was to propose a definition on measuring the number of police contacts with the public in order to relate them to incidents of UoF and assaults against law enforcement officers. The UoF Task Force has determined being able to identify various types of contact with the public will help put UoF incidents in a context.

The concept of adding measures of police and public interaction to the existing police employee collection went through the CJIS Advisory Process in fall 2016. These changes would provide a context in UoF data and potentially be beneficial to the LEOKA data collection, as well. He noted one of the options presented, in consultation with the CSOs and the UCR state program managers, was to add the ability to capture the information on recorded police contacts with the public to the annual police employee data collection. Included in this collection should be the ability to discern the most common types of calls for service or officer-initiated actions recorded by the agency in a computer aided design (CAD) system or other similar record keeping system.

The subcommittee proposed a definition for police contact, as follows: A police contact is considered an incident or occurrence where a law enforcement officer is called to respond to a scene by a citizen, or initiates an activity which results in contact with a citizen. It does not need to include the total number of people encountered at the incident. Law enforcement agencies typically collect the counts for such contacts from CAD system records that capture calls for service or officer initiated activities. Court activities are potential contacts with citizens that occur routinely with court deputies or bailiffs. Court dockets reflecting the number of people with court hearings on any given date are considered an example of a source for reporting this information.

There was considerable discussion by the UCR Subcommittee over how to collect this information. The subcommittee looked at what would get them started with being able to create that context. They decided this can grow in the future if the APB deems it appropriate.

He advised the subcommittee also expanded the predetermined options that can be included. They started out with two options, but the subcommittee felt like actual, estimated, not available, or not applicable were all necessary elements for an agency to mark or identify. Some agencies may not have access to the data and may not be able to report it.

A member inquired about the definition for court and bailiff activities. He stated this is contextual data for the UoF, which is for reporting law enforcement officers. In the police employee count, court deputies are counted as nonsworn. Colonel Middleton opined the

assumption was they are reporting UoF by law enforcement. If they are not being considered as law enforcement, then the locality or state will have to make a decision whether they want to report it or not. The definition is intended to provide guidance in how to report it. Agencies will have to decide if they want to consider that as part of this definition and use it or not. The member stated his sheriff's office has sworn enforcement mixed in with corrections deputies assigned to judicial security. He pointed out it would be difficult to figure out the number of contacts by the sworn law enforcement versus the correctional deputy. Colonel Middleton stated this information was being reported as part of LEOKA. Another member stated she was an advocate for including that because across the nation, being responsible for the courtroom is one of the primary responsibilities for the sheriffs' offices, whether they are the primary law enforcement officer or not. She noted she had never heard of a deputy as not being sworn, so she was a real advocate to include that for a more accurate account for the number of contacts sheriffs' deputies and sheriffs' officers actually have on a given day.

Another member commented there should be weigh-in from local agencies. CSAs would contribute a clear definition of the categories to the FBI prior to implementation. Colonel Middleton informed him the definition was sent to 120 different CSOs and agencies to review. Only eight responses were received from that 120, so they viewed the low response to mean no one felt there was a need to add or change anything.

Chairman Donohue reminded the group this became a topic because they wanted to contextualize the reporting of UoF. When collecting UoF, the board thought it was important to put into context when officers are placed into vulnerable situations. He stated he had a reservation with the definition as presented by the subcommittee attempts to put a degree of accuracy on the counts of the number of interactions law enforcement has. He acknowledged it is an imprecise measure. For instance, a domestic violence incident could involve two individuals, or an entire family. A traffic stop could involve one driver, or many occupants in a vehicle. He stated certain circumstances, specifically to demonstrations, protests, and large scale gatherings are very important to count. He pointed out those gatherings, depending on the circumstances, can turn violent. Acknowledging that police officers and sheriffs' deputies have been injured in those circumstances, and consciously ignoring that fact, is an intentional under count, and he opined it should be captured. He agreed while there is a degree of imprecision, there are ways to count crowd estimates and to present it in reasonable way. He reminded the group they were setting policy, not dictating what anyone is going to actually submit. He asked the APB to consider that at least the demonstrations, protests, or large-scale gatherings be an estimate number that would be part of this count.

Mr. Buckley stated the UCR Subcommittee could not work out how to appropriately account for the mass scale gatherings. The subcommittee is asking it go back through for those they have left off. They could go forward with what they currently have, but the intent was to try to get a better, streamlined definition across the United States.

Colonel Middleton stated this topic was strongly debated, but since they are trying to launch something, they are trying to make it as uncomplicated as possible for agencies to report. He advised there was general agreement that how those counts are achieved could vary considerably, so they would like more time to expand this, much like was done with UoF. They

are only capturing specific types of UoF, not all UoF. They felt as the project moved forward and implemented in January 2018, they will have an opportunity work on reaching a consensus to provide reasonable guidance on how to estimate those types of crowds.

A member reported he sent this topic through his state and only received one response. This response was a concern over the definitions, and whether it would be apples to apples information. This member suggested there should be a lot of outreach since most of this information would be new to many agencies. The information sent to agencies should include the definitions and the tables. He expressed doubt the agencies would have the ability to input the data in the right categories and have the right kind of counts.

APB Motion: The APB moved to add the ability to capture the information on recorded police contacts with the public on an annual basis and revise the table as provided below.

Please provide a count of the following types of recorded police contacts with the public by officers employed by your agency. All counts should include contacts from January 1 to December 31 of the calendar year.

Category	Call/Request/Individuals on the Docket Count
Citizen calls for service	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable
Unit/officer-initiated contacts	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable
Court/Bailiff Activities	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable

UCR Issue #6 Review of the UCR Program’s Definition of a Law Enforcement Officer as it Pertains to the Phrases “Public Governmental Law Enforcement Agency” and “Paid for from Government Funds”

Colonel Middleton advised this came before the December 2017 APB, and the FBI UCR program was asked to review the definition of a law enforcement officer as it relates to paid and unpaid employment. Many law enforcement agencies across the country use auxiliaries or volunteers that are not paid. The UCR Subcommittee came up with a recommendation with modifications.

APB Motion: The APB moved to accept Option 1 with modifications. Law Enforcement Officer-All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of ~~American citizens~~ **individuals**. They must have **statutory** arrest powers and **be members of a law enforcement agency paid from funds set aside specifically for payment to sworn law enforcement** organized and funded for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

### LEOKA Criteria

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**
- ~~Were paid from funds set aside specifically for payment of sworn law enforcement~~
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

### Exclusions from the LEOKA Program's Data Collection

Deaths resulting from the following are not included in the LEOKA Program's statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program's statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

## UCR Issue #7 The FBI's UCR Quality Assurance Review to Resume Operations in Accordance with CJIS Division, CAU's Triennial Audit Schedule

This topic was accepted as information only.

Colonel Middleton briefed on an ad hoc discussion that may eventually come forward. It dealt with the UCR Program conducting internal meetings to discuss the nomenclature of sex offenses. The word "forcible" was removed from sex offenses. However, "nonforcible" remains in the language, which has created confusion. The subcommittee felt it was the intent of the APB, when it approved changing the definition to remove "forcible," that "nonforcible" should have also been addressed. The subcommittee suggested to the FBI this was an administrative change and it should occur immediately.

### **APB ITEM #15 UCR Program Briefing**

This topic was presented by Ms. Amy Blasher, FBI CJIS Division. (*See Appendix R, PowerPoint.*) Ms. Blasher provided an update on the status of the NIBRS transition. The NIBRS transition is part of the CDM effort, which is one of eight Director Priority Initiatives (DPI) for the FBI. She advised this DPI is to improve the nation's UCR crime statistics for reliability, accessibility, accuracy, and timeliness of data. She advised this is achieved through a five-prong approach, the first being the NIBRS transition. The second prong has to do with UoF. The UoF pilot, which began July 1, 2017, will conclude December 31, 2017. The CJIS Division will submit a report, based on analysis of the data, to OMB for approval of the UoF data collection, which may be launched in January 2018. She advised they are still enrolling many agencies despite the conclusion of the pilot. She stated the task force plans to meet in spring 2018 to discuss the data and finalize the publication strategy moving forward.

Ms. Blasher advised the FBI has a mandate to report to UCR. The FBI spent the past year building technical capabilities to report NIBRS. In October 2017, they began training all of the field offices, and then doing a soft rollout of the NIBRS solution. She reported the FBI will be NIBRS-compliant in January 2018.

An AG memo was released on October 27, 2017 to approximately 120 federal agencies that have crime data that should be reported to the UCR program. She advised the CJIS Division has received many inquiries from those federal agencies. Therefore, the team is scheduling agency visits to look at their data, provide assistance to work through what it means to be NIBRS-compliant, and provide technical assistance to move them towards NIBRS.

Ms. Blasher advised they are continually making enhancements to the CDE, which will be the face of the UCR program in the future. She reported all publications currently on the fbi.gov website will be migrated to the CDE.

She briefed further on the NIBRS transition. The Director signed the recommendation in February 2016 to move to an all NIBRS data collection by January 1, 2021. CJIS has partnered with BJS for the National Crime Statistics Exchange (NCS-x), and the FBI is

financially assisting with the transition of the selected 400 agencies in the 20 state UCR programs to become NIBRS-compliant. Between FBI and BJS, funding was allocated for approximately 44 million dollars. She emphasized FBI funding will cease December 2018. There will be four more solicitations in 2018, with the first solicitation anticipated for January. She stated there are 160 agencies and one state still eligible for funding. All other states have already been awarded some type of funding.

CJIS is continuing their engagement with stakeholders. On November 16, 2017, they kicked off a working group for the NIBRS transition to discuss refining strategies and marketing for NIBRS. Secondly, CJIS has been working with the SACs of the FBI field offices. Each SAC received a state profile illustrating their state's progress with the NIBRS transition. Many SACs have begun engaging their chiefs of police, AGs, and governors, to work through the remaining challenges with their states' transition to NIBRS.

She stated they attended an International Association of Chiefs of Police (IACP) meeting to discuss CDM and the NIBRS transition. The IACP offered CJIS monthly space within their Police Chief Magazine to distribute more articles about the NIBRS transition. She advised the articles will focus on user stories of state and local agencies that have made the transition. The articles will also direct readers to the website dedicated to the NIBRS transition. She reported five regional trainings hosted by the FBI concluded in September 2017. Three hundred fifty-five agencies from 34 states, DC, Guam and Saipan participated, with 629 total participants.

A technical team of CJIS data integration specialists has been formed to do code reviews with agencies. They have built XML examples and tools to assist agencies that want to move towards NIBRS through XML. This team can be deployed to work with the agencies' technical staff.

She opined 2018 will be the most critical year with the NIBRS transition. The FBI will reach out to states to find out the status of their transition. The FBI needs this information to enable them to make projections for 2018 and each following year until the deadline. She pointed out this initiative requires a partnership; it cannot be accomplished by the FBI alone. Some of the states have loaned staff to come out and talk to agencies about their transition.

She stated, based on feedback, they have done a great job at the highest levels with major organizations. However, this year they need to focus on reaching agencies at the local level to talk about the transition and help them get to where they need to be.

#### **APB ITEM #16 SEARCH Update**

Ms. Becki Goggins, SEARCH, presented this update. (*See Appendix S, PowerPoint.*) Ms. Goggins reported they would be releasing the *Survey of State Criminal History Information Systems*, 2016 edition, before Christmas 2017.

She provided a brief update on their Quality Assurance Program (QAP). They have revised the QAP checklist to reflect the implementation of NGI and new Compact Council policies. Since the last update, Alaska, Hawaii, Montana, New York, and South Carolina have participated in the QAP. She reported either she or Mr. Dennis DeBacco can be contacted if anyone would like to participate in the program.

She stated SEARCH completed the final publication in a joint series with the National Center for State Courts (NCSC). The four previous publications focused on making records available for firearms background checks. The last publication in the series focuses on illegal drug use records, primarily those entered into the NICS Indices. SEARCH has found, in some states with low-level drug offenses, individuals are not fingerprinted; however, they can still be entered into the NICS Indices.

She advised, in spring 2017, they presented a series of well-attended webinars on auditing practices. It was decided not everyone would sit through four and a half hours of video, so they published a white paper, which summarizes auditing practices. She stated the publication can be located on the SEARCH website.

During the first half of 2018, in cooperation with the FBI, BJS, and NCSC, SEARCH will do a series of regional training sessions, focusing on disposition reporting, NICS prohibitors, and funding applications for National Criminal History Improvement Program (NCHIP) and NICS Act Record Improvement Program (NARIP). Eight states have been tentatively selected for the first round. If successful, SEARCH will continue this training in cooperation with BJS.

She then provided an update on SEARCH's information sharing programs. She reported SEARCH still has funding from the Bureau of Justice Assistance to support technical assistance and development work in states seeking to increase the number of records available for firearms-related background checks.

She stated, in cooperation with the information sharing programs and law and policy, they have done proof of concept of a computerized criminal history (CCH) analytics tool. They wanted to use this tool for the purpose of anomaly detection. If they created an easy user interface, criminal history repository managers could look at some of the measures and assess the health of their criminal history repository. For instance, if a very large court that should be contributing thousands of dispositions, are only contributing a small number, something may be wrong. This tool could make it easier to do early problem identification. This tool could trend analysis and show how dispositions and arrests change over time. It would also be beneficial for stakeholder reporting. She advised, during the auditing webinars, they frequently heard how important communication is to improving the whole system and working well together. They thought this tool would be a good way to help do publications, and let individuals readily see what is going on. Ms. Goggins provided some examples of how the CCH tool can be utilized.

Through the NCS-x, SEARCH has developed some tools that might be useful to states. One is the XML version of the NIBRS precertification tool. She advised the precertification tool does not replace the FBI certification. However, it replicates the process the



FBI uses to do the testing. She demonstrated how easy it is to use and advised it is accessible at <<https://nibrs.search.org/nibrs-web/>>. She highlighted some of the benefits of using the precertification tool. The tool allows agencies, state programs and industry partners to test NIBRS submissions prior to testing with the FBI or a state program. It provides error reports similar to the FBI in a matter of seconds. She noted it may speed up the certification process with the FBI. She then pointed limitations of the tool. They are unable to do comparisons with pre-existing submissions because they do not have the total set the FBI maintains. They cannot check for valid ORIs because they do not have a master listing of ORIs. Certain zero reports cannot be performed, and some rules are not being interpreted in the same way. She advised this will be resolved.

She stated there is a NIBRS analytic tool on the website. Agencies have informed them they would like to know what the data does for them and how to make it useful. SEARCH built an open-source tool. If you have a standard NIBRS data set, it can be ingested, and it has dragging and dropping queries, filtering abilities, and some graphics and charts. The queries can be saved if there is something that needs to be produced on a repetitive basis. A slight limitation is it ingests only the standard NIBRS data. However, it can be modified because it is an open source tool.

Ms. Goggins announced Mr. David Roberts is the new executive director of SEARCH. She then extended an invitation to the SEARCH membership meeting, which will be held January 23-25, 2018, in Birmingham, Alabama.

Chairman Donohue commended SEARCH for their involvement in disposition outreach and trying to clean up the nation's data. He noted incomplete or missing information could lead individuals in the criminal justice community to make bad decisions.

#### **APB ITEM #17 Chairman's Report on the SA Subcommittee**

This agenda item was presented by Mr. Bradley Truitt, Tennessee Bureau of Investigation, and Chair of the SA Subcommittee. (*See Appendix T, PowerPoint.*)

SA Issue #1 *CJIS Security Policy (CSP) Language Changes in Section 5.12*

Mr. Truitt briefed this issue was to propose modifications to the CSP Section 5.12 to permit vetting rules for personnel with access to CJI to be applied consistently among CJA employees and contract personnel.

APB Motion: The APB moved to accept the following recommended changes within the *CJIS Security Policy* Section 5.12 and Appendix B with a Priority Tier 1 as shown in the topic paper (additions in *red, bold italics*, deletions in ~~bold strikethrough~~) and noted below:

#### **A. Proposed *CJIS Security Policy* Section 5.12 Language Changes: 5.12 Policy Area 12: Personnel Security**

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have *unescorted* access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

### **5.12.1 Personnel *Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI* Security Policy and Procedures**

#### **~~5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:~~**

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted ~~within 30 days of assignment~~ *prior to granting access to CJI* for all personnel who have ~~direct unescorted~~ access to *unencrypted CJI and/or unescorted access to physically secure locations or controlled areas (during times of CJI processing)*. ~~those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.~~ However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a Nlets CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
  - (i) 5 CFR 731.106; and/or
  - (ii) Office of Personnel Management policy, regulations, and guidance; and/or
  - (iii) agency policy, regulations, and guidance.

~~(See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.)~~ Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

*See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.*

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
- ~~3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for~~

~~a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.~~

3. ~~4.~~ If a record of any ~~other~~ kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
  - a) *If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.*
  - b) *Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.*
  - c) *If a record of any kind is found on a Contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.*
4. ~~5.~~ If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
- ~~6. If the person is employed by a NCJA, the CSO or his/her designee shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.~~
5. ~~7.~~ If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. ~~8.~~ If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
- ~~9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.~~

***7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.***

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

**5.12.1.2 Personnel Screening for Contractors and Vendors**

**In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:**

- ~~1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.~~**
- ~~2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.~~**
- ~~3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.~~**
- ~~4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.~~**
- ~~5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.~~**
- ~~6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.~~**

**~~Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not~~**

~~warrant disqualification. The CGA may request the CSO to review a denial of access determination.~~

### 5.12.2 Personnel Termination

~~The agency, upon termination of individual employment, shall immediately terminate access to CJI.~~ *Upon termination of personnel employed by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.*

## B. Proposed CJIS Security Policy Appendix J Noncriminal Justice Agency Supplemental Guidance:

### APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

---

...

#### j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have *unescorted* access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring *unescorted* access to *unencrypted* CJI. ~~–listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.2.~~

#### SA Issue #2: CSP Restriction for CJI Stored in Offshore Cloud Computing Facilities

Mr. Truitt advised the purpose of this issue was to propose language changes to CSP Section 5.10.1.5 to restrict where CJI may be stored in cloud computing facilities.

Chairman Donohue highlighted some of the concerns raised by a large cloud computing organization. (*See Appendix X.*) This organization believes this restriction would have a disruptive effect on some agencies already relying on cloud computing services. They believe it would create an unfounded mandate for some agencies looking to leverage cloud computing. It would be more costly, and it would limit choice and competition. In addition, it

would limit innovation and the way to scale cloud computing for law enforcement agencies. Chairman Donohue pointed out there is an argument to be made on all sides, and he felt it was important for the group to hear the concerns. He expressed the cloud is groundbreaking, and it is important to be able to get data rapidly, accurately, and reliably.

One of the members mentioned he sent general information regarding this issue to an individual who works in the private sector in IT security. This individual provided his opinion on data localization. This individual stated, from both a technical and a legal perspective, it matters where the data is physically stored. If a United States law enforcement agency stored its citizens' data in a cloud storage platform with a data center in a country whose laws allow the government to covertly inspect data stored on servers within their borders, then it is possible for such data to fall into the hands of the government and be used against citizens. Large cloud storage providers want to make users' data equally accessible from anywhere in the world, which may involve replicating the data between multiple data centers located around the globe. Data localization laws could complicate such efforts, which may be part of the reason companies are generally opposed to such laws. He opined a data localization policy for law enforcement agencies would be a different matter. It would only affect the agencies' selection processes when looking for cloud service providers, and it would create a competitive marketplace for cloud service providers who want the business of law enforcement agencies. This could lead to competing services more tailored to the needs of law enforcement.

Another member commented there had been a great deal of discussion throughout the process and it is the job of the Advisory Process to secure the data. They need to be concerned about unintended consequences, but the purpose is to ensure the data is secure, and he opined that is what the motion does.

APB Motion: The APB moved to accept Option 1 as a Priority Tier 1 with amended language to replace “foreign criminal justice agencies” with “foreign government agencies” as listed below:

Accept the following recommended changes to CJIS Security Policy Section 5.10.1.5 and Appendix B as shown below (additions in *red, bold italics*, deletions in **bold strikethrough**).

- The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third- party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

*Note: This restriction does not apply to exchanges of CJI with foreign eriminal justice government agencies under international exchange arrangements (i.e., the Preventing and Combatting Serious Crime (PCSC) agreements, fugitive extracts, and exchanges*

*made for humanitarian and criminal investigatory purposes in particular circumstances).*

**Proposed Additions to CJIS Security Policy Appendix B: Acronyms:**

Acronym	Term
<i>RCMP</i>	<i>Royal Canadian Mounted Police</i>

SA Issue #3 Vetting of Non-U.S. Citizen Contractors/Vendors for Access to State Criminal Justice Information Systems

Mr. Truitt advised this topic was presented to raise awareness and to give advice about how one would conduct background checks on contractors or vendors residing outside of the United States.

This topic was accepted as information only.

SA Issue #4 Task Force Updates (Cloud, Mobile, Courts)

Mr. Truitt briefed on the SA Subcommittee's three task forces. The Cloud Task Force, chaired by Mr. Patrick Woods, Missouri State Highway Patrol, worked on the language for SA Issue #3, and they are discussing ideas to make the CSP easily understood in the application to multiple third-party vendors. The Mobile Task Force, chaired by Ms. Brenda Abaya, Hawaii Criminal Justice Data Center, planned to meet by the end of 2017. The Court Task Force, chaired by Mr. Corey Steel, Nebraska Supreme Court, had several conference calls discussing where the CSP applies to CJI when received by the courts. Mr. Scott Trent stated when the Court Task Force started, he was unsure of the direction it needed to go. However, after speaking with Mr. Steele and Mr. Charles Schaeffer, he feels confident there is a plan on how to move forward and ensure the court systems understand when and how to protect the data appropriately.

This topic was accepted as information only.

SA Issue #5 Update on Fusion Center Access to CJIS Division Systems

Mr. Truitt stated the subcommittee heard the update on the fusion center access to CJIS systems. The SA Subcommittee made a recommendation to the IS Subcommittee chair for Option 2.

This topic was accepted for information only.

SA Issue #6 Information Security Officer (ISO) Symposium Review

Mr. Truitt stated the purpose of this topic was to provide an update from the ISO Symposium held in Alexandria, Virginia, and to provide information regarding the 2018

symposium, which will be held in Norman, Oklahoma, for the ISOs and SA Subcommittee members.

This topic was accepted for information only.

### **SA Ad Hoc Discussion Items**

Mr. Truitt stated some of the ad hoc issues discussed were the use of the RISS, and other identity data providers. There was an update on the spring 2017 CJIS action item to provide information to the subcommittee on the process for vetting identity data providers. Mr. Schaeffer provided a briefing to the SA Subcommittee on cloud provider audits his staff is doing and what the audits consist of. There was a FirstNet discussion from SA Subcommittee member, Sergeant T. J. Smith, Los Angeles County Sheriff's Department, and their implementation of a pilot. There was an ad hoc discussion on LEEP identity management. There was an action item to obtain additional feedback regarding LEEP identity management at the federal, state, local, tribal and territorial levels. The purpose of this action item was to discuss noncriminal justice or private entities requesting access to CJIS services, and how to differentiate the categories and the users from the information they should be accessing. There was discussion to request guidance from the subcommittee on how the CAU assesses boundary protection. Lastly, there was an action item for the ISO PO to explore mobile applications taking the place of mobile device management compensating controls.

### **APB ITEM #18 Tribal Update**

This topic was presented by Mr. William Denke, Sycuan Tribal Police Department, and Chair of the Tribal Task Force (TTF) (*See Appendix U, PowerPoint.*)

Mr. Denke thanked Sheriff Kathy Witt, Mr. Brian Wallace and Ms. Dawn Peck for their continued support and value they bring to the TTF.

Mr. Denke reported there is still a disproportionate amount of resources and capabilities with Indian country law enforcement when compared to their non-Indian country counterparts. Either tribal organizations or tribal police departments do not have records management systems, or those that do are not capable of producing NIBRS data. One of the members of the task force is a Bureau of Indian Affairs executive, who has been able to leverage the Department of Interior (DOI) to facilitate tribal access to DOI's Incident Management and Reporting system. This has been rolled out to two tribes as a pilot project. The goal is for this access to be available by the end of 2018 to any tribes needing it in order to meet the 2021 NIBRS transition deadline.

He advised there are continued discussions on the importance of UoF data collection. The Hualapai and Pascua Yaqui tribes are participating in the national UoF pilot project.

Mr. Denke advised dispositions in Indian country continue to be an issue. In June 2017, CJIS staff presented the task force with a draft of a reporting guide for final



dispositions. The task force requested the FBI to include a “how to” section, as well as an explanation of the importance of reporting arrests along with dispositions and relationships, which helps determine if an arrest is related to domestic violence. He stated the goal is for the guide to be published in early 2018.

Mr. Denke then briefed on the Tribal Access Program. This is a DOJ-sponsored program for tribes to gain access to CJIS systems. This kiosk-type system was rolled out to nine tribes in 2016 as a user feedback phase. It was rolled out to an additional ten tribes in FY 2017, and ten more will be rolled out starting in February 2018. In addition, DOJ JUSTNET will be available to tribes that do not need the full hardware solution, but need access to NCIC and Nlets. In 2018, five tribes will gain access to NCIC and Nlets through the DOJ JUSTNET system.

He reported the task force would not meet in person in the immediate future, but would meet via teleconference. It is difficult to get tribal representation at the meetings because individuals cannot afford to be away from their smaller agencies. The TTF will meet via teleconference mid-January 2018. Anyone with tribal issues or concerns related to connectivity to CJIS systems can contact CJIS Division Tribal Liaisons, Ms. Kim Lough or Ms. Kristi Naternicola. They have spoken at tribal conferences in the past, and continue to participate in the IACP Indian country section law enforcement meetings.

#### **APB ITEM #19 Chairman’s Report on the Compliance Evaluation (CE) Subcommittee**

Ms. Dawn Peck, Idaho State Police, and CE Subcommittee Chair, stated the subcommittee is in limbo with Puerto Rico and the Virgin Islands. Due to the destruction from recent storms, these territories are unable to work on resolving their issues. She reported there was an ad hoc discussion on the appropriateness of when they send the letters and to whom they are sent.

Ms. Peck provided the findings of the subcommittee, which are as follows:

**Administrative Office of the United States Courts** – Closure to CSA Head for Security

**Alabama** – Follow-up to CSA Head for Security

**Alaska** – Follow-up to Governor for Security Old Business; and Concern with Follow-up for NCIC and Security, and Commendation for NICS for Recently Conducted Audits

**Arizona** – Concern without Follow-up for NCIC, Concern with Follow-up for Security, Commendation for NICS, and Sanction with Follow-up for N-DEX

**Arkansas** – Follow-up to CSA Head for NCIC

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) – Commendation for NICS

**Colorado** – Follow-up to CSA Head for NCIC and Security Court Services and Offender Supervision Agency (CSOSA) – Commendation for NICS

**Delaware** – Follow-up for Security

**DC Metropolitan Police** – Closure to DC City Mayor for NCIC

**DC Office of the Inspector General** – Closure for Security

**Drug Enforcement Agency (DEA)** – Commendation for NICS

**Florida** – Closure to CSA Head for NCIC and Follow-up to Governor for Security

**Hawaii** – Call/Close or Follow-up to Governor for Security  
**Illinois** – Follow-up to Governor for NCIC and Security for Old Business and Previous Business  
**Interpol** – Closure for NCIC and Commendation for Security  
**Kentucky** – Closure for NCIC, Follow-up for Security and NICS  
**Maine** – Follow-up to Governor for 2010 and 2013 NCIC Old Business; Follow-up for NCIC and Security Previous Business  
**Maryland Repository** – Commendation for Security  
**Michigan** – Follow-up for NCIC and Security  
**Minnesota** – Follow-up for Security to Governor  
**Mississippi** – Follow-up for Security to CSA Head  
**Montana** – Follow-up to AG for Security  
**Nebraska** – Follow-up for NCIC and Security  
**Nevada** – Commendation for NCIC, NICS, and N-DEx, and Concern with Follow-up for Security  
**New Hampshire** – Closure to CSA Head for NCIC  
**New Jersey** – Closure for Security  
**New Mexico** – Follow-up for NCIC, Security, and NICS  
**New York** – Follow-up to Governor for NCIC and Security  
**North Carolina** – Closure to Governor for NCIC and Follow-up to Security for Old Business; and Follow-up to CSA Head for Security for Previous Business  
**North Dakota** – Follow-up for NCIC and Security  
**Ohio Repository** – Closure to Governor for Security  
**Oklahoma** – Closure for NCIC, Security, and N-DEx  
**Oregon** – Follow-up to CSA Head for NCIC and Security  
**Pennsylvania** – Follow-up to Governor for Security  
**Puerto Rico** – TBD  
**Rhode Island** – Concern without Follow-up for NCIC, Sanction with Follow-up for Security, and Commendation for NICS and N-DEx for Recently Conducted Audits  
**Rhode Island Repository** – Concern with Follow-up for Security  
**South Carolina** – Follow-up to Governor for Security Old Business; Sanction with Follow-up for NCIC and Security, and Commendation for NICS and N-DEx for Recently Conducted Audits  
**South Dakota** – Follow-up for NCIC and Security  
**Tennessee** – Follow-up for Security  
**Texas** – Closure for Security and N-DEx  
**U.S. Capitol Police** – Commendation for NCIC, Security, and N-DEx for Recently Conducted Audits  
**U.S. Coast Guard** – Follow-up for N-DEx  
**U.S. CBP** – Follow-up for N-DEx  
**U.S. DOJ Executive Office for the U.S. Attorneys** – Commendation for NICS for Recently Conducted Audit  
**U.S. Virgin Islands** – TBD  
**Vermont** – Follow-up to CSA Head for Security and Closure for N-DEx  
**Virginia** – Follow-up to CSA Head for NCIC  
**Washington** – Closure to CSA Head for NCIC  
**West Virginia** – Follow-up to Governor for NCIC and Security

APB Motion: The APB moved to approve the CE Subcommittee's updates regarding actions and sanctions provided.

## **APB ITEM #20 NICS Section Status Report**

Ms. Robin Stark-Nutter, NICS Chief, FBI CJIS Division, provided this update. (*See Appendix V, PowerPoint.*) Ms. Stark opened her presentation by sharing that any time there is a shooting, NICS runs the biographic data of the shooter through the system to see if they have missed anything that would have prevented the shooting. This allows them to address any issues, close any gaps and mitigate any risks that may happen. Since June of 2016, they have done these types of searches on more than 20 incidents related to law enforcement shootings as well as the Vegas and Texas shootings. NICS was pleased to find out that nothing was missed in any of these shootings that may have prevented them from happening. She said NICS is committed to continually enhancing and improving the NICS system and they appreciate the records that are submitted to them.

Next, she provided statistics for 2017 and said there had been an 8.555 percent decline compared to 2016 with 22.6 million federal and state background checks processed through November 30, 2017 and an 8.09 percent decrease in federal firearms checks. On Black Friday 2017, 203,000 transactions were processed making it the highest day ever in the history of NICS. She also provided information on the NICS denied categories with the highest denial rate being convicted felon prohibitors followed by fugitive from justice, misdemeanor crimes of domestic violence, and drugs.

She also mentioned a 709 percent increase over a 10-year period, in state entries into the NICS Indices and a 120 percent increase in Federal entries. She shared that from October 31, 2017 until November 21, 2017, 26,432 records were added to the NICS Indices by military branches.

She closed by mentioning the NICS backlogs they are currently working on which included NICS Indices, appeals, explosives and voluntary appeals.

A question was raised about a previous APB recommendation allowing additional uses for the NICS Indices particularly regarding the hiring of police officers. Ms. Stark-Nutter said this recommendation is currently with DOJ and NICS is tracking it on a regular basis. It was asked if the APB could do anything to expedite this recommendation. Chairman Donohue said he could possibly write a letter asking for a status from DOJ.

A member mentioned they recently read an article about ATF recovering weapons from individuals who were not qualified to receive them, but a weapon had mistakenly been issued to them. He asked if there was an opinion on whether the three-day deadline should be changed to allow for additional response time. Ms. Stark-Nutter said they follow the federal regulation of three days and they work very closely with ATF to reduce the number of firearm retrievals they have to make. The member said the article did say most retrievals were done without incident. Chairman Donohue said there is a national debate on this topic with involvement from Congress.

Another member asked how many responses go beyond the three days. Ms. Stark-Nutter said she did not have those numbers but reiterated their close relationship with ATF. It was pointed out the article mentioned previously, stated the percentages were low for responses outside the three-day period.

Ms. DelGreco mentioned that, as of that day, NICS had approximately 60,000 delays in their system. She said they are required to purge at 90 days. Many of the records are on employees' desks waiting for final adjudication or dispositions so they can take action before the required purge. Chairman Donohue said it all goes back to the importance of dispositions, which help with crime fighting. They help judges and district attorneys make good decisions. He encouraged everyone to ramp up the importance of getting good, quality data for dispositions on arrest records.

### **Closing Remarks**

Mr. Trent announced Mr. Jim Buckley, the federal APB representative, was retiring. He provided some history of Mr. Buckley's participation in the Advisory Process, beginning with the Working Groups in April 2006. He shared some personal thoughts regarding the time he had known and worked with Mr. Buckley. Chairman Donohue also said a few words about his experience with Mr. Buckley. A video was shown displaying the lighter side of Mr. Buckley and other Advisory Process members over the years. Mr. Buckley was then presented a Director's Certificate in appreciation for his participation and contribution to the Advisory Process. Mr. Buckley shared some words with the group thanking everyone for their friendship, guidance, and mentorship.

Chairman Donohue thanked the members of the APB for their active participation and discussion during the CJIS APB meeting. He pointed out the body is meant to give good recommendations for the management of their data. He reminded the CJIS APB members they would receive a briefing of the meeting in the weeks following the meeting.

Chairman Donohue thanked Colonel Middleton for his work arranging attendance at the basketball game and for setting up the Oklahoma City National Memorial and Museum tour, expressing it was an honor and a privilege to experience that.

Being there were no further agenda items before the CJIS APB, Chairman Donohue asked for a motion to adjourn. Meeting adjourned at 11:18 a.m.

# APPENDICES

# Advisory Policy Board Roll Call

Oklahoma City, Oklahoma -- 12/06-07/2017

<b>Name</b>	<b>Agency</b>	<b>Serving as a proxy for:</b>
<b>Mr. Clifford D. Brophy</b>	Stillwater County Sheriff's Office Columbus, MT	<input checked="" type="checkbox"/>
<b>Mr. James W. Buckley, Jr.</b>	U.S. Immigration and Customs Enforcement Clarksburg, WV	<input checked="" type="checkbox"/>
<b>Mr. Kevin C. Cockrell</b>	Montgomery County Attorney Mount Sterling, KY	<input checked="" type="checkbox"/>
<b>Ms. Veronica S. Cunningham</b>	American Probation and Parole Association Lexington, KY	<input checked="" type="checkbox"/>
<b>Lieutenant Nicholas DelRomano</b>	Pennsylvania State Police Harrisburg, PA	<input checked="" type="checkbox"/>
<b>Mr. William J. Denke</b>	Sycuan Tribal Police Department El Cajon, CA	<input checked="" type="checkbox"/>
<b>Mr. John K. Donohue</b>	New York City Police Department New York, NY	<input checked="" type="checkbox"/>
<b>Ms. Carol A. Gibbs</b>	Illinois State Police Joliet, IL	<input checked="" type="checkbox"/>
<b>Mr. Jeremy Hansford</b>	Ohio State Highway Patrol Columbus, OH	<input checked="" type="checkbox"/>
<b>Mr. Michael C. Lesko</b>	Texas Department of Public Safety Austin, TX	<input checked="" type="checkbox"/>
<b>Mrs. Lynda G. Lovette</b>	Baltimore City Police Department Baltimore, MD	<input checked="" type="checkbox"/>
<b>Mr. Gary M. Lyons</b>	Monroeville Police Department Monroeville, OH	<input checked="" type="checkbox"/>

<b>Name</b>	<b>Agency</b>	<b>Serving as a proxy for:</b>	
<b>Ms. Erin Lyons</b>	National Sheriffs' Association Alexandria, VA	John Thompson	<input type="checkbox"/>
<b>Mr. Mark A. Marshall</b>	Isle of Wight Sheriff's Office Isle of Wight, VA		<input checked="" type="checkbox"/>
<b>Colonel Douglas A. Middleton</b>	Henrico County Manager's Office Henrico, VA		<input checked="" type="checkbox"/>
<b>Mr. Troy A. Miller</b>	U.S. Customs and Border Protection Washington, DC		<input checked="" type="checkbox"/>
<b>Ms. Kathryn M. Monfreda</b>	Alaska Department of Public Safety Anchorage, AK		<input checked="" type="checkbox"/>
<b>Mr. Joseph N. Morrissey</b>	New York State Division of Criminal Justice Services Albany, NY		<input checked="" type="checkbox"/>
<b>Mr. Walt Neverman</b>	Wisconsin Department of Justice Madison, WI		<input checked="" type="checkbox"/>
<b>Mr. Scott G. Patterson</b>	Talbot County State's Attorney Easton, MD		<input checked="" type="checkbox"/>
<b>Ms. Dawn A. Peck</b>	Idaho State Police Meridian, ID		<input checked="" type="checkbox"/>
<b>Colonel Edwin C. Roessler, Jr.</b>	Fairfax County Police Department Fairfax, VA		<input checked="" type="checkbox"/>
<b>Sergeant Robert S. Sage</b>	Augusta Department of Public Safety Augusta, KS		<input checked="" type="checkbox"/>
<b>Mr. Charles Schaeffer</b>	Florida Department of Law Enforcement Tallahassee, FL		<input checked="" type="checkbox"/>
<b>Commissioner James F. Slater, III</b>	Massachusetts Department of Criminal Justice Information Services Chelsea, MA		<input checked="" type="checkbox"/>

<b>Name</b>	<b>Agency</b>	<b>Serving as a proxy for:</b>	
<b>Mr. Corey R. Steel</b>	Nebraska State Court Administrator Lincoln, NE		<input checked="" type="checkbox"/>
<b>Major Jennie Temple</b>	South Carolina Law Enforcement Division Columbia, SC	Vacant Southern Region Rep.	<input type="checkbox"/>
<b>Ms. Sonya Thompson</b>	Federal Bureau of Prisons Washington, DC		<input checked="" type="checkbox"/>
<b>Mr. Jeremy S. Triplett</b>	American Society of Crime Laboratory Directors Frankfort, KY		<input checked="" type="checkbox"/>
<b>Mr. Bradley Truitt</b>	Tennessee Bureau of Investigation Nashville, TN		<input checked="" type="checkbox"/>
<b>Mr. Brian Wallace</b>	Marion County Sheriff's Office Salem, OR		<input checked="" type="checkbox"/>
<b>Mr. Jeffrey Wallin</b>	Vermont Department of Public Safety Waterbury, VT	Mary Kay MacNichol	<input type="checkbox"/>
<b>Honorable Nathan E. White, Jr.</b>	American Judges Association McKinney, TX		<input checked="" type="checkbox"/>
<b>Mr. Anthony Wickersham</b>	Macomb County Sheriff's Office Mt. Clemens, MI		<input checked="" type="checkbox"/>
<b>Ms. Kathy Witt</b>	Office of the Fayette County Sheriff Lexington, KY		<input checked="" type="checkbox"/>





**Meeting Attendee List – Advisory Policy Board – December 6-7, 2017 – Oklahoma City, Oklahoma**

<b><u>NAME</u></b>		<b><u>AGENCY/COMPANY</u></b>
Brenda	Abaya	Hawaii Criminal Justice Data Center
Yusuf	Abdul-Salaam	DHA Group, Inc.
Melissa	Abel	Federal Bureau of Investigation
Richard	Adleson	Decisive Analytics
Justin	Aggus	LeadsOnline
Peter J.	Ahearn	Accenture Federal Services
Christopher	Algieri	First Responder Network Authority/Department of Commerce
Nickole M.	Arbuckle	Department of Justice
Jennifer	Armstrong	U.S. Marshals Service
Karen	Asta	DXC Technology
Rickey	Barrow	Oklahoma County Sheriff's Office
Kimberly	Bartoe	Novetta
Brenda	Beck	Information Builders
Nathan	Beckham	Microsoft
David	Bierie	U.S. Marshals Service
Meghan	Blackburn	Texas Department of Public Safety
Olivia	Blackburn	DMI
Amy	Blasher	Federal Bureau of Investigation
Jay	Bokulic	Google
Catherine	Bolger	Leidos
Buffy	Bonafield	Federal Bureau of Investigation
Katherine	Bond	Federal Bureau of Investigation
Michael	Borden	General Dynamics Information Technology
Mary	Boulware	NCI
Marcus	Bramer	Federal Bureau of Investigation
Jeff	Bristow	Accenture Federal Services
Clifford D.	Brophy	Stillwater County Sheriff's Office
Stacy	Brownstein	Attain
Chad	Bryant	CA Technologies
Keith	Bryars	NTT Data Federal Services
James W.	Buckley, Jr.	U.S. Immigration and Customs Enforcement
Tom	Bush	Tom Bush Consulting
Thomas	Callaghan	Federal Bureau of Investigation
Frank	Campbell	Highland Strategies, LLC
Greg	Carl	Integration Innovation, Inc.
Michael	Carter	IJIS Institute

Alvaro	Castillo	ManTech
Gabe	Chang	IBM
Bill	Chase	Sound Judgment Solutions, LLC
Paul	Christin	Amazon Web Services
William	Citty	Oklahoma City Police Department
Lindsay	Clarke	Arista Networks
Bill	Clinton	Computer Projects of Illinois
Barbara	Clouser	Federal Bureau of Investigation
Kevin C.	Cockrell	Montgomery County Attorney
Todd	Commodore	Federal Bureau of Investigation
Alex	Corley	Amazon Web Services
Tyler	Cox	Federal Bureau of Investigation
Veronica S.	Cunningham	American Probation and Parole Association
David	Cuthbertson	Independent Consultant
Roy	Davis	Unisys Federal Systems
Patrick	Dawson	CA Technologies
Dennis	DeBacco	SEARCH
Kimberly	Del Greco	Federal Bureau of Investigation
Jon	Dellaria	IBM
Nicholas	DelRomano	Pennsylvania State Police
William J.	Denke	Sycuan Tribal Police Department
Magruder	Dent	Aware, Inc.
Ted	DeRosa	Colorado Bureau of Investigation
Karen	DeSimone	NTT DATA
Christopher	DeWitt	IBM
Kelley	Doane	Tygart Technology, Inc.
Atacan	Donmez	CSRA
John K.	Donohue	New York City Police Department
Don	Dougherty	Micro Focus Government Solutions
Reinoehl	Dougherty	NCI
Gena	Dowell	Federal Bureau of Investigation
Rainer	Drolshagen	Federal Bureau of Investigation
Jeffrey	Dunn	IDTechnology Partners
Matt	Egan	CA Technologies
Michael	Entrekin	U.S. Customs and Border Protection
Valerie	Evanoff	Independent Consultant
Michael	Evanoff	Northrop Grumman
Mark	Fabian	CA Technologies
Barry	Fagan	Federal Bureau of Investigation
Patrick	Fagan	Vigilant Solutions, LLC
Su	Fan	Systems Integration, Inc.
Michelle	Farris	Texas Department of Public Safety

Dave	Finley	LeadsOnline
Amy	Fleming	Federal Bureau of Investigation
Amanda	Foster	Amazon Web Services
Leon	Frederick	Iowa Department of Public Safety
Ken	Frosch	Leidos
Cathy	Gallagher	Red Hat
Gerard	Gallant	Motorola Solutions, Inc.
Josh	Garner	Norseman Defense Technologies
Ronnie	George	Federal Bureau of Investigation
Dwight	George	NCI, Inc.
James	Gerst	Federal Bureau of Investigation
Berhane	Gherezgiher	Oklahoma State Bureau of Investigation
Craig	Gibbens	Diverse Computing, Inc.
Carol A.	Gibbs	Illinois State Police
Neal	Gieselman	Aware, Inc.
Becki	Goggins	SEARCH
Nichole	Gohman	Peraton, Inc.
Mayukh	Gon	PerfectCloud Corporatoin
Mary	Gostel	Tygart Technology, Inc.
Robert	Grabow	TMC Technologies
Todd	Graham	AnaVation, LLC
John	Gray	PsPortals, Inc.
Larry	Grund	Computer Projects of Illinois
William K.	Guy	Rhode Island State Police
Michael W.	Haas	U.S. DOJ
Chris	Hagewood	Diversified
Harry	Halden	Idemia-Morpho Trak
Jenny	Hall	Texas Department of Public Safety
Jeremy	Hansford	Ohio State Highway Patrol
Thomas	Harrigan	CACI International
Zachary	Hartzell	Federal Bureau of Investigation
David A.	Hastings	Peraton Corporation
Rachel	Herger	Micro Focus Government Solutions
Donna	Hill	ASRC Federal
Frederick B.	Hoffman	Sotera Defense Solutions
Robert	Holman	Federal Bureau of Investigation
Alan	Hoyt	Micro Focus Government Solutions
Betsey	Hutton	Octo Consulting
Arthur	Ibers	Leidos
Alexander	Isaac	MarkLogic Corporation
Mclean	John	Veritas
Kendra	Jones	Georgetown-Scott County 911

Christopher	Jones	Federal Bureau of Investigation
George	Kantsios	Zolon Tech, Inc.
Christopher	Kastl	Leidos
Lee	Kicker	NEC
David	Kim	Amazon Web Services
Jared	Kim	Anavation
Joseph	Klimavicz	U.S. Department of Justice
Tobey	Knight	Federal Bureau of Investigation
Thomas	Kohler	Full Visibility
Drew	Kudrick	ClearShark
Pete	Lamont	INTEGRITYOne Partners
Thomas	Lehosit	Federal Bureau of Investigation
Michael C.	Lesko	Texas Department of Public Safety
Andy	Levitt	HP, Inc.
Kristen	Lillard	Grant Thornton
Douglas	Lindquist	Federal Bureau of Investigation
Lauren	Linger	KeyLogic
Brad	Long	Datamaxx Applied Technologies, Inc.
Jason	Love	Engility Corporation
Lynda G.	Lovette	Baltimore City Police Department
Erin	Lyons	National Sheriffs' Association
Gary M.	Lyons	Monroeville Police Department
Kim	Mackey	Splunk
Brian	Mahoney	CA Technologies
Stephanie	Manson	Federal Bureau of Investigation
Celia	Marino	Ernst & Young
William	Marosy	National Background Investigations Bureau
Mark A.	Marshall	Isle of Wight Sheriff's Office
Sherrie	Masden	Louisville Metro Police/MetroSafe Communications 9-1-1
Jeff	Matthews	Watch Systems
Peter	McCarthy	Presidio
Andrea C.	McCarthy	HARP
Michael	McDonald	Intellicheck, Inc.
Channing	McGuffin	Microsoft
Donna	McIntire	Google
Michael	McIntyre	Federal Bureau of Investigation
Stuart	McKee	Microsoft Corporation
William	McKinsey	Federal Bureau of Investigation
Aimee	Medonos	AnaVation, LLC
Douglas A.	Middleton	Henrico County Manager's Office
Roland J.	Mignone	PricewaterhouseCoopers Public Sector, LLP

Roberta	Miller	Federal Bureau of Investigation
Johnny	Miller	Presidio
Roger	Miller	Federal Bureau of Investigation- TSC
Philip T.	Miller	Immigration and Customs Enforcement
Troy A.	Miller	U.S. Customs and Border Protection
Joe	Mills	Servicenow
Frank	Minice	Nlets
Michael	Miscio	General Dynamics Information Technology
Kathryn M.	Monfreda	Alaska Department of Public Safety
Jill	Montgomery	Federal Bureau of Investigation
Andrea	Moon	IDEMIA NSS
Randy	Moon	Kansas Highway Patrol
Nichole	Moore	Diverse Computing
Leslie	Moore	Kansas Bureau of Investigation
Todd	Morris	Attain
Joseph N.	Morrissey	New York State Division of Criminal Justice Services
Brian	Mortweet	ASRC Federal
Tracey	Mullins	Federal Bureau of Investigation
Brian	Myers	Tenable Network Security
Timothy	Neal	Federal Bureau of Investigation
Walt	Neverman	Wisconsin Department of Justice
Brian	Nichols	Federal Bureau of Investigation
Chip	Nickerson	Systems & I.D. Solutions, Inc.
Kevin	Nugent	CACI International, Inc.
Jim	Oehm	Kansas Highway Patrol
Kathleen	Oldaker	Federal Bureau of Investigation
Andrew	Overheu	LeadsOnline
Kimberly	Parsons	Federal Bureau of Investigation
Chirag	Patel	Innovative Management & Technology Services, LLC
Scott G.	Patterson	Talbot County State's Attorney
Darrin	Paul	Federal Bureau of Investigation
Dawn A.	Peck	Idaho State Police
Daniel	Pedowitz	IBM Corporation
Kathryn	Peterson	Federal Bureau of Investigation
Wyatt	Pettengill	North Carolina State Bureau of Investigation
Kevin	Phan	Splunk
Christopher	Piehota	Federal Bureau of Investigation
Shanon	Pitsenbarger	Fusion Technology
Brian	Pittack	Department of Homeland Security-OBIM
Jillana	Plybon	Federal Bureau of Investigation
Benton Lawrence	Polzak	The Rehancement Group, Inc.
Kim	Portik	Canyon State Reporting Services

Deborah Lea	Post	Federal Bureau of Investigation
Mark	Potter	Ernst & Young
Charles	Prouty	General Dynamics
Steve	Psarakis	Dorrean, LLC
Anthony	Pun	Diverse Computing, Inc.
Tom	Puskarich	Splunk
Dan	Radke	Gigamon, Inc.
Scott	Rago	Federal Bureau of Investigation
Kevin	Razzaghi	Koniag
James F.	Reed	BAE Systems
J. Kevin Reid	Reid	Fusion Technology
Ryan	Reynolds	Amazon Web Services
Michelle	Richards	Federal Bureau of Investigation
Bryan	Rizzi	Oklahoma State Bureau of Investigation
David J.	Roberts	SEARCH
Edwin C.	Roessler, Jr.	Fairfax County Police Department
Evelyn "Lynn"	Rolin	South Carolina Law Enforcement Division
Lou	Ronca	Akima, LLC
Jason	Rosa	Microsoft Corporation
Brian	Rosenthal	Full Visibility
Jaleh	Sadeghzadeh	CA Technologies
Robert S.	Sage	Augusta Department of Public Safety
Roble	Sahra	Department of Justice
Donnie	Sawin	Computer Projects of Illinois
Damian	Sawle	CA Technologies
Charles	Schaeffer	Florida Department of Law Enforcement
Scott	Schneiderman	Aveshka, Inc.
Chris	Schraf	Microsoft Corporation
Rich	Schramke	Northrop Grumman
Whitney	Shafer	Leidos, Inc.
Warren	Shannon	LeadsOnline
Anil K.	Sharma	IBM
Holly	Shenk	Oracle, National Security Group
Angela	Sheppard	Federal Bureau of Investigation
Glen	Skinner	CSRA
James F.	Slater, III	Massachusetts Department of Criminal Justice Information Services
Barbara	Slayton	Leidos
Craig	Sleight	Accenture Federal Services
Marc	Smith	Computer Projects of Illinois
Barry	Smith	BAE Systems
Eric	Smith	Unisys

Tadgh	Smith	Immigration and Customs Enforcement
Robin	Stark-Nutter	Federal Bureau of Investigation
Corey R.	Steel	Nebraska State Court Administrator
Gary	Stroupe	Federal Bureau of Investigation
Rodrick	Summers	Federal Bureau of Investigation
Scott	Swann	IDEMIA-NSS
Erik	Swanson	BAE Systems
Sam	Swenson	ASRC Federal Mission Services
William	Tatun	Diverse Computing, Inc.
Jennie	Temple	South Carolina Law Enforcement Division
Gene	Thaxton	Oklahoma Department of Public Safety
Sonya	Thompson	Federal Bureau of Prisons
Randy	Tirado	Maricopa County Adult Probation Department Data Systems Unit
Daniel	Tovar	Federal Bureau of Investigation
Chris	Trainor	IBM
Scott	Trent	Federal Bureau of Investigation
Jeremy S.	Triplett	American Society of Crime Laboratory Directors
Bradley	Truitt	Tennessee Bureau of Investigation
Johnathon	Trumble	Oracle NSG
Amaha	Tsegaye	DHA Group, Inc.
Robert	Turnbaugh	Peraton, Inc.
Robert	Turner	CommSys, Inc.
Percy	Turner	Microsoft Corporation
Thomas	Turner	Consultant
Anthony	Vanchieri	Buchanan & Edwards
Chuck	VanDyck	IBM
Brandon	Vincent	Federal Bureau of Investigation
Brian	Wallace	Marion County Sheriff's Office
Jeffrey	Wallin	Vermont Department of Public Safety
Troy	Walter	DMI
Kurt	Walter	Splunk
Roland	Walters	Oracle NSG
Flint	Waters	Google
Kari	Watkins	Oklahoma City National Memorial Museum
John	Weatherly	Federal Bureau of Investigation
Colleen	Weltz	ASUCRP/ND Attorney General's Office
Tony	West	Forcepoint
Charlotte	Whitacre	First Responder Network Authority/Department of Commerce
George	White	Federal Bureau of Investigation
Nathan E.	White, Jr.	American Judges Association



Anthony	Wickersham	Macomb County Sheriff's Office
Paul	Wilkinson	1901 Group
Jim	Willard	Koniag
Missy	Willett	Red Hat
Michelle	Wingate	Guide Point Security
Kathy	Witt	Office of the Fayette County Sheriff
Brian	Wodarski	PricewaterhouseCoopers Public Sector, LLP
Carl	Wolf	Wolf & Associates Consulting, LLC
Glenn	Wood	Oracle
Casey	Workman	Federal Bureau of Investigation
Richard	Wyffels	Alexandria Police Department
Michael	Yates	Federal Bureau of Investigation
John A.	Yearty	Peak Performance Solutions
Theodore	Yoneda	Federal Bureau of Investigation
Derek	Zaugg	Ingersoll Consulting, Inc.
Paula	Zirkle	Federal Bureau of Investigation
Matthew	Zirpoli	Peraton, Inc.
Larry	Zmuda	Sutherland Government Solutions

---

**Criminal Justice Information Services (CJIS)  
Advisory Policy Board (APB)  
December 6-7, 2017  
Oklahoma City, Oklahoma**

**AGENDA  
as of 11/27/2017**

---

**Wednesday, December 6, 2017**  
**9:00 a.m.**

**Board Convenes**

**Opening Announcements**

Mr. R. Scott Trent  
Designated Federal Officer  
CJIS Division  
Federal Bureau of Investigation

**Roll Call**

Mr. John K. Donohue  
APB Chairman  
Assistant Chief  
Office of the Police Commissioner  
New York City Police Department

**Introduction of Attendees and Special Guests**

Mr. John K. Donohue

**Welcoming Remarks**

Ms. Kathryn Peterson  
Special Agent in Charge  
Oklahoma City Field Office  
Federal Bureau of Investigation

Mr. Rickey Barrow  
Chief Deputy  
Oklahoma County Sheriff's Office

Mr. William Citty  
Chief of Police  
Oklahoma City, Oklahoma Police Department

**CJIS Advisory Policy Board**  
**Wednesday, December 6, 2017**

**Item #1\***  
**Oklahoma City Bombing Briefing**

Ms. Kari Watkins  
Executive Director  
Oklahoma City National Memorial & Museum

**Item #2\***  
**Executive Briefings**

Mr. Christopher M. Piehota  
Executive Assistant Director  
Science and Technology Branch  
Federal Bureau of Investigation

Mr. Douglas E. Lindquist  
Assistant Director  
CJIS Division  
Federal Bureau of Investigation

Mr. Joseph F. Klimavicz  
Chief Information Officer  
U.S. Department of Justice

**Item #3**  
**Chairman's Report on the National Data Exchange (N-DEx) Subcommittee**

Ms. Carol Gibbs – **Vice Chair**  
Bureau Chief  
Program Administration Bureau  
Illinois State Police

**Item #4**  
**Chairman's Report on the National Instant Criminal Background Check System (NICS) Subcommittee**

Ms. Lynn Rolin – **Chair**  
Program Coordinator  
IT CJIS Liaison  
South Carolina Law Enforcement Division

**Item #5\***  
**National Crime Prevention and Privacy Compact Council Report**

Ms. Dawn A. Peck - **Chair**  
Manager  
Bureau of Criminal Identification  
Idaho State Police

**CJIS Advisory Policy Board**  
**Wednesday, December 6, 2017**

**Item #6\***

**Nlets, The International Justice and Public Safety Network Update**

Mr. Frank Minice  
Deputy Executive Director  
Nlets

**Item #7\***

**Biometric Hit of the Year**

Mr. Doug Lindquist

**Item #8**

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

Mr. Michael C. Lesko - **Chair**  
Director  
Law Enforcement Support Division  
Texas Department of Public Safety

**Item #9\***

**U.S. Immigration and Customs Enforcement (ICE) Programs Update: Biometrics and Advanced Analytics**

Mr. Philip T. Miller  
Deputy Executive Associate Director  
Enforcement and Removal Operations  
U.S. Immigration and Customs Enforcement

**Item #10**

**Chairman's Report on the National Crime Information Center (NCIC) Subcommittee**

Mr. Walter M. Neverman- **Chair**  
Director  
Crime Information Bureau  
Wisconsin Department of Justice

**Item #11\***

**NCIC Third Generation (N3G) Briefing**

Mr. Wyatt Pettengill –**N3G Task Force Chair**  
Special Agent in Charge  
Criminal Information and Identification Section  
North Carolina State Bureau of Investigation

**CJIS Advisory Policy Board**  
**Wednesday, December 6, 2017**

**Item #12\***  
**FirstNet**

Mr. Christopher Algieri  
Federal Consultation Lead  
FirstNet

**Item #13\***  
**Operational Applications of NIBRS**

Dr. David M. Bierie  
U.S. Marshals Service

**CJIS Advisory Policy Board**  
**Thursday, December 7, 2017**

**Day Two - Board Reconvenes**

**Item #14**  
**Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee**

Colonel Doug Middleton – **Chair**  
Deputy County Manager for Public Safety  
Henrico County Manager's Office  
Henrico, Virginia

**Item #15\***  
**UCR Program Briefing**

Ms. Amy C. Blasher  
Chief, Crime Statistics Management Unit  
CJIS Division  
Federal Bureau of Investigation

**Item #16\***  
**National Consortium for Justice Information and Statistics (SEARCH) Update**

Ms. Becki Goggins  
Director of Law and Policy  
SEARCH

**Item #17**  
**Chairman's Report on the Security and Access (SA) Subcommittee**

Mr. Bradley D. Truitt - **Chair**  
Information Systems Director  
Tennessee Bureau of Investigation

**Item #18\***  
**Tribal Update**

Mr. William J. Denke – **Tribal Task Force Chair**  
Chief of Police  
Sycuan Tribal Police Department  
El Cajon, CA

**Item #19\***  
**Chairman's Report on the Compliance Evaluation (CE) Subcommittee**

Ms. Dawn A. Peck – **Chair**

**CJIS Advisory Policy Board**  
**Thursday, December 7, 2017**

**Item #20\***  
**NICS Section Status Report**

Ms. Robin A. Stark-Nutter  
Chief, NICS Section  
CJIS Division  
Federal Bureau of Investigation

**Recognition of Members**

**Other Business**

**Adjourn Advisory Policy Board**

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)  
ADVISORY POLICY BOARD (APB)  
OKLAHOMA CITY, OK  
DECEMBER 6-7, 2017**

**STAFF PAPER**

**APB ITEM #3**

**Chairman's Report on the National Data Exchange (N-DEx) Subcommittee**

**N-DEx ISSUE #1\***

N-DEx Program Status and System Demo

**N-DEx ISSUE #2**

Creation of a N-DEx Use Code For Federal Security Clearances, Suitability, and Fitness for Federal Employment, Credentialing and Related Federal Matters

**N-DEx ISSUE #3\***

N-DEx Institutional and Community Corrections Update

**N-DEx ISSUE #4**

Update on Fusion Center Access to CJIS Division Systems

**N-DEx ISSUE #5\*\***

National Instant Criminal Background Check System Searching N-DEx Update

**Ad Hoc Discussion Items\*\***

- Displaying Additional Fields in Yellow Point of Contact Data
- New Use Code for CJIS Bioterrorism Risk Assessment Group (BRAG)

\*Delivered with the information only staff papers

\*\*No staff paper





**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL DATA EXCHANGE (N-DEx) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**N-DEx ISSUE #2**

Creation of a N-DEx System Use Code for Federal Security Clearances, Suitability, and Fitness for Federal Employment, Credentialing, and Related Federal Matters

**PURPOSE**

To present for discussion the implementation of an N-DEx System Use Code for Federal Security Clearances, Suitability, and Fitness for Federal Employment, Credentialing, and Related Federal Matters.

**POINT OF CONTACT**

Law Enforcement Support Section, N-DEx Program Office

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**BACKGROUND**

For many years, the N-DEx Program Office has explored proposals to expand the use of the N-DEx System. In the Spring of 2011, the APB considered the expansion of access to N-DEx and recommended "...that N-DEx shall allow access following 28 Code of Federal Regulations (CFR) Part 20 definition for criminal justice agencies." While the national security mission was discussed, it was not ultimately included within the final recommendation. In the Fall of 2012, the Federal Working Group discussed having "CJIS convene a group of Subject Matter Experts to look for a solution to allow access to the CJIS Systems for agencies who, post 9/11, have a national security or counter intelligence mission and do not meet the current guidelines to be issued a criminal justice ORI [Originating Agency Identifier]." One solution within existing policy allowed such agencies to partner with law enforcement to conduct N-DEx searches, when appropriate, on behalf of a law enforcement agency. In the Spring of 2013, the CJIS Division provided an Information Only Topic Paper stating a federal criminal justice agency may extend their N-DEx system's access to OPM for Purpose Code J inquiries. The OPM was required to use the ORI of the federal criminal justice agency for which the employment background investigation was being performed. Additionally, OPM had to enter into a Management Control Agreement with the respective federal criminal justice agency. This solution imposed logistically difficult requirements on OPM.

In January 2017, President Barack Obama signed Executive Order 13764, addressing many of the conversations started in recent years about the federal security clearance process and the standards that agencies should use to measure an employee's trustworthiness and suitability to serve in government. The order amends the Civil Service Rules, Executive Order 13488, and Executive Order 13467 - the governance structure and processes for issuing federal security clearances, as well as suitability and fitness status for employment. The order also revokes Executive Order 10450 effective since 1953, "Security Requirements for Government Employment."

Executive Order 13764 states that "The Government's tools, systems, and processes for conducting these background investigations and managing sensitive investigative information should keep pace with technological advancements, regularly integrating current best practices to better anticipate, detect, and counter malicious activities, and threats posed by external or internal actors who may seek to do harm to the Government's personnel, property, and information."

Specifically, Executive Order 13764 continues the Federal executive agency FBI fingerprint-based records check requirement of Executive Order 10450 for making fitness determinations. However, additional authority was included to authorize searches of additional biometric or other databases if deemed appropriate by the entity having control of that database and not otherwise precluded by law:

**"PART 2—VETTING ENTERPRISE, RECIPROCITY, CONTINUOUS PERFORMANCE IMPROVEMENT, AND GOVERNANCE"**

(o) Section 2.1 of Executive Order 13467 is revised to read as follows:

Sec. 2.1. (e):

Vetting shall include a search of records of the Federal Bureau of Investigation, including a fingerprint-based search, and any other appropriate biometric or database searches not precluded by law."

On July 17, 2017, the CJIS Assistant Director, in response to and accordance with President Obama's Executive Order, deemed the N-DEx System an "appropriate database". As a result, the N-DEx Program Office will incorporate an N-DEx System Use Code for Federal Security Clearances, Suitability, Fitness for Federal Employment, Credentialing, and Related Federal Matters, into the *N-DEx Policy and Operating Manual*, as well as the implementation of associated functionality into the N-DEx System. This capability will be implemented so the N-DEx System Use Code is not automatically visible to existing N-DEx System users. The CJIS Systems Officer (CSO) will navigate to the CSO Role and assign the N-DEx System Use Code capability to users from the qualifying federal agencies as defined by Executive Order 13764 and section 105 of title 5, United States Code. The N-DEx System Use Code will then be visible only to those users.

In addition, the N-DEx Program Office will partner with the FBI's Office of the General Counsel (OGC) to accomplish the implementation by creating specific policy language to be inserted into

the *N-DEx Policy and Operating Manual*. The N-DEx Privacy Impact Assessment (PIA) and System of Record Notice (SORN) will be revised to permit this N-DEx System Use Code. Federal agencies utilizing the N-DEx System Use Code will be required to provide notice to and gain consent from individuals to be checked through the N-DEx System as is currently required for Use Code “J” searches. Federal agencies will also be required to provide individuals with an opportunity to challenge and/or correct records if adverse action is taken based on information obtained from the N-DEx System.

Finally, it is important to note that the N-DEx System record-owning agencies will be provided with the capability to “Opt-Out” of having their data searchable for the N-DEx System Use Code purposes. The N-DEx System Use Code queries will be subject to the same audit policies as are other use code searches. N-DEx System information shall be used only for the purpose indicated by the N-DEx System Use Code and used consistently with the coordination required by the Advanced Permission Requirement and Verification Requirement in accordance with the N-DEx Policy and Operating Manual. Terms of N-DEx System information use must be obtained from the record-owning agency prior to reliance or action upon the information, or secondary dissemination of the information. N-DEx System information may only be relied or acted upon, or secondarily disseminated within the limitations specified by the record-owning agency. Reliance or action upon, or secondary dissemination of N-DEx System information beyond the original terms requires further permission from the record owning agency. N-DEx System information must be verified with the record-owning agency for completeness, timeliness, accuracy, and relevancy, prior to reliance upon, action, or secondary dissemination. Additionally, audits on the N-DEx System Use Code queries will be subject to the policy language developed jointly by the N-DEx Program Office and OGC, and will verify that the search involved an investigation to measure an employee’s trustworthiness and suitability to serve in government in accordance with the Executive Order. The N-DEx System will return results for the N-DEx System Use Code queries based on sharing rules set by the N-DEx System data owner. These results are restricted based on the user’s ORI utilized for N-DEx System access.

**FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

**FALL 2017 N-DEx SUBCOMMITTEE ACTION:**

Accepted as information only.



**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL DATA EXCHANGE (N-DE<sub>x</sub>) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**N-DE<sub>x</sub> ISSUE #4**

Update on Fusion Center Access to Criminal Justice Information Services (CJIS)  
Division Systems

**PURPOSE**

To provide an update regarding the CJIS Division's efforts to fulfill the CJIS APB's recommendations regarding fusion center access to CJIS Division systems.

**POINT OF CONTACT**

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**

The Subcommittee is requested to review the information presented in this paper, and provide comments and recommendations to the APB.

**BACKGROUND**

There are currently 78 fusion centers recognized by the Department of Homeland Security (DHS) operating within the United States and its territories. The National Fusion Center Association (NFCA) reports a small number (less than nine) of these fusion centers lack direct access to the systems managed by the Federal Bureau of Investigation's (FBI's) CJIS Division. This lack of direct access, as reported, creates difficulties from an information-sharing standpoint. The vast majority of fusion centers are either established directly within a criminal justice agency (CJA), and that CJA controls the terminal access within the fusion center, or the fusion centers leverage a partnering CJA's access. As research indicates, other partnering CJAs, (e.g., police departments, sheriff's offices, etc.) working within a fusion center also establish their own terminal access within that fusion center to support their criminal investigation needs.

Access to CJIS Division systems is governed by Title 28, Code of Federal Regulations (C.F.R.), Part 20, which stipulates the types of agencies and the functions those agencies must perform to qualify for access. To qualify for access to CJIS Division systems, an agency must be a CJA or a subunit of a noncriminal justice agency, performing the administration of criminal justice as a primary function (interpreted by the Department of Justice (DOJ) to mean more than 50 percent of the agency's annual budget supports criminal justice functions). The functions which are considered the administration of criminal justice are specified in 28 C.F.R. §20.3(b), and include detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

The primary function of these fusion centers is to compile and share information to support the detection of criminal and terrorist activity. The term "detection" as it relates to the administration of criminal justice must be predicated on an "articulable suspicion" to justify a query of CJIS Division systems. Under the CJIS Division's review, the functions of the fusion centers lacking access did not conclusively meet the threshold requirements in 28 C.F.R. §20.3(b) to be considered the administration of criminal justice.

The compilation, analysis, and sharing of generalized or nonspecific threat information is not considered the administration of criminal justice. The fusion centers lacking direct access which have directly engaged the CJIS Division have been unable to provide documentation to support their primary function is the detection of articulable or specified criminal or terrorist activity. In some cases, the CJIS Systems Agencies (CSAs), for the states of the fusion centers in question, do not support granting direct access to those fusion centers and recommend for a CJA to control the access. For information, CSAs control access to CJIS Division systems for all agencies within their state or territory.

## **DISCUSSION AND ANALYSIS**

A topic was presented at the Spring 2016 Advisory Process meetings. The APB recommended for the CJIS Division and FBI's Office of General Counsel (OGC) to identify a long-term solution to fusion centers lacking direct access to CJIS Division systems and bring the solution(s) back through the Advisory Process for consideration. The APB also moved, pending the outcome of the FBI's review of a long-term solution, to grant fusion centers interim access through the use of management control agreements. This would facilitate access to CJIS Division systems through the management control of a CJA. The CJIS Division is aware of at least one state where this interim solution is currently being implemented.

Throughout this process, the CJIS Division has been engaged with the criminal justice community, the NFCA, the DHS, and the International Association of Chiefs of Police. In addition, the CJIS Division's Assistant Director served on the DOJ Criminal Intelligence Coordinating Council and provided substantial input on the topic of fusion center access.

To fulfill the APB’s recommendation, the CJIS Division and the OGC have collaborated to propose the option to formalize the interim solution stated above by clarifying the existing language in the regulation. The regulation changes will clarify language to definitively authorize a criminal justice agency to enter into a management control agreement with a noncriminal justice governmental agency to perform criminal justice functions on its behalf. A modification to the definition of a CJA under 28 C.F.R. §20.3(g) to include fusion centers was originally discussed during the Spring 2016 Advisory Process discussions, but the APB requested further exploration before making a final recommendation. After consideration of the discussion during the Advisory Process meeting and other engagement with the user community, the CJIS Division and the OGC determined a clarification of the language within 28 C.F.R. §20.33 (a)(6) may be a better option to accomplish this goal. Currently, 28 C.F.R. §20.33 (a)(6) reads, “To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies.” The proposed changes to 28 C.F.R. §20 will memorialize the ability for noncriminal justice governmental agencies, such as the small number of fusion centers lacking direct access, to enter into agreements with CJAs to perform the administration of criminal justice functions on behalf of the CJA. Should this proposed regulation change be endorsed, it should be noted it is a lengthy administrative process that could take many years to accomplish.

Another point to consider is the current administration’s Executive Order 13771 to limit new regulations. On January 30, 2017, the President signed Executive Order 13771, which states “that for every one new regulation issued, at least two prior regulations be identified for elimination . . . .” This Order affects not only the Department of Justice, but all Federal Executive Agencies, and it has brought the federal regulatory amendment process to a near halt. The APB can be assured that if the proposed language under Option 1 is accepted, the FBI will perform due diligence to move the proposed language change forward.

The Subcommittee is requested to provide input on the information provided in this paper and provide recommendations regarding the following options.

## **OPTIONS**

### **Option 1**

Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*



## **Option 2**

No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

## **Option 3**

Discontinue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

### **RECOMMENDATION**

The NCIC Operations and Policy Unit recommends Option 1.

### **FALL 2017 WORKING GROUP ACTIONS:**

#### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

#### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA. FBI Action: FBI should continue to research various scenarios which may result from any proposed regulatory change. Continue with the interim solution.

**Action:** Motion carried with 11 Yay/11 Nay, Chair broke the tie with a Yay vote

#### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2. No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1. Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

**IS SUBCOMMITTEE ACTION:**

**Motion:** To accept a revised Option 1: “Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a) (6) as the long term solution to facilitate access to CJIS Division systems, which would grant criminal justice agencies the same authority to contract with noncriminal justice governmental agencies as they currently have to contract with private entities. Accept the language as proposed below:

*6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.”*

**Action:** Motion carried.

**N-DEx SUBCOMMITTEE ACTION:**

Accepted as information only.

**NCIC SUBCOMMITTEE ACTION:**

**Motion:** Recommendation to the Identification Services Subcommittee for Option 1: Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as

private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**SA SUBCOMMITTEE ACTION:**

**Motion:** To recommend Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)  
ADVISORY POLICY BOARD (APB)  
OKLAHOMA CITY, OK  
DECEMBER 6-7, 2017**

**STAFF PAPER**

**APB ITEM #4**

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

**NICS ISSUE #1\***

NICS Update

**NICS ISSUE #2\***

CJIS Division's NICS Enhancements Status

**NICS ISSUE #3**

Application of Title 18, United States Code, Section 922 (g)(2)-Fugitive from Justice

**NICS ISSUE #4\***

National Data Exchange Program Status

**NICS ISSUE #5**

Re-evaluation of the Expansion of the Information Required with the Submission of a Record to the NICS Indices, Formerly known as the NICS Index, and Potential Fields to be Added

**NICS ISSUE #6\***

Importance of the Identification for Firearm Sales Program to the NICS User Community

**NICS ISSUE #7**

Impact of Pseudo-Pointers on State Outreach in the Next Generation Identification System

**NICS ISSUE #8**

Criminal History Update

**NICS ISSUE #9**

Submission of an Originating Case Number during a NICS Disposition of Firearms Background Check

**NICS ISSUE #10\*\***

Old Action Items

**NICS ISSUE #11\*\***

Ad Hoc

\* Delivered with the information only staff papers

\*\* No staff paper



**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL INSTANT CRIMINAL BACKGROUND  
CHECK SYSTEM (NICS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**NICS ISSUE #3**

Application of Title 18, United States Code (U.S.C.), Section 922(g)(2) – Fugitive from Justice

**PURPOSE**

To provide information regarding the new guidance for the application of the Fugitive from Justice prohibition.

**POINT OF CONTACT**

National Instant Criminal Background Check System (NICS) Section, NICS Business Unit

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**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 to contact for information to be supplied immediately as to whether the transfer of a firearm to an unlicensed person would violate 18 U.S.C. § 922(g) or (n), or state law. Since the inception of the NICS, the federal prohibition fugitive from justice has been used to deny a firearms transfer whenever a prospective transferee is the subject of a verified outstanding arrest warrant.

The Office of Inspector General made a recommendation, in September 2016, that the Department of Justice (DOJ) resolve the long-standing disagreement between the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) regarding the definition of the fugitive from justice category of persons that forms the basis for referrals to ensure the law is being applied appropriately and as intended pursuant to 18 U.S.C. § 922(g)(2).

The DOJ reviewed the fugitive from justice prohibition and the application of the prohibition in NICS background checks. The DOJ provided information to the FBI, in January 2017, which concluded the Brady Act does not authorize the denial of firearm transfers under the prohibition based on the mere existence of an outstanding arrest warrant. The ATF regulation at Title 27, Code of Federal Regulations (C.F.R.), Section 478.11, defines the term fugitive from justice to include not just “any person who has fled from any State to avoid prosecution for a felony or misdemeanor crime” and “any person who leaves the State to avoid giving testimony in any criminal proceeding,” but also “any person who knows that misdemeanor or felony charges are pending against such person and who leaves the State of prosecution.”

To comply with the DOJ determination, the FBI implemented a new policy for applying the fugitive from justice prohibition. This policy requires the NICS user to establish that the prospective purchaser: (1) is subject to a current or imminent criminal prosecution or testimonial

obligation; (2) has fled the state; and (3) has done so to avoid prosecution for a crime or giving testimony in a criminal proceeding.

On February 21, 2017, the NICS Section implemented a processing change to ensure each of the criteria identified in the regulations is met before applying the fugitive from justice prohibition. To ensure compliancy with this criteria, all NICS Indices, formerly known as NICS Index, entries with the Prohibited Category Code (PCA) of B, fugitive from justice, were removed. This was to avoid automatic denials based on NICS Indices entries with the PCA of B, entered under the previous criteria. The NICS Section has asked the NICS Indices contributors having records in the fugitive from justice category to evaluate previous entries under the new standard, and reenter disqualifying records under the PCA of B.

Further clarification regarding the application of the fugitive from justice elements is provided below:

- 1) A warrant that is still active for a felony or misdemeanor arrestable offense or a criminal testimonial obligation (e.g., expert witness, material witness, victim, or informant) will meet the element for a person that is subject to a current or imminent criminal prosecution or testimonial obligation.
- 2) In order to determine if an individual has fled the state, it must first be determined whether a warrant is deemed in-state or out-of-state. If the State of Purchase (SOP) and the issuing state of the warrant are the same, the warrant is considered an in-state warrant. If the SOP and the issuing state of the warrant are not the same, the warrant is considered an out-of-state warrant.

An out-of-state warrant provides evidence the individual left the issuing state and therefore establishes the fled element, whereas an in-state warrant does not. An in-state warrant where the individual's State of Residence and the issuing state of the warrant are not the same, the inferred conclusion is the individual has left the issuing state; thereby, establishing the fled element. Or, if the previous standard does not apply for an in-state warrant, then it must be determined if the individual has, at some point, left the issuing state in which they face a potential prosecution or criminal testimonial obligation.

- 3) The determination of whether the individual has fled the state to avoid prosecution or criminal testimonial obligation can be inferred if the person has left the state with knowledge they are subject to pending/potential criminal charges, a criminal testimonial obligation, or the person was aware of the warrant for the underlying criminal obligation before leaving the issuing state.

The NICS Section is aware some states have laws that prohibit an individual from receiving or possessing a firearm or firearm-related permit based on the existence of an active warrant. Other states define the term fugitive more broadly than the federal definition set forth in 18 U.S.C. § 921(a)(15) and 27 C.F.R. § 478.11. If the federal fugitive from justice prohibition cannot be established, yet a state law exists which prohibits an individual from receiving or possessing a firearm or firearm-related permit when an active warrant is present, the NICS Indices contributors should reenter the warrant-related records to the State Prohibition category, PCA of J.

In summary, the prior practice of the denial of firearm transfers under the fugitive from justice federal prohibition based on the mere existence of an outstanding arrest warrant is no longer valid. The NICS users are now required to establish the aforementioned new standard for a fugitive from justice federal prohibition.

If you have any questions or need assistance in this matter, please contact Dorothy L. Riddle, Legal Administrative Specialist, at 304-625-7416 or Joy L. Jarrett, Supervisory Legal Administrative Specialist, at 304-625-7345.

### **FALL 2017 WORKING GROUP ACTIONS**

#### **FEDERAL WORKING GROUP ACTION:**

This topic was accepted as information only.

#### **NORTH CENTRAL WORKING GROUP ACTION:**

This topic was accepted as information only.

#### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** Request the APB Chairman to facilitate the drafting of a letter expressing the Northeastern Working Group's concerns regarding the DOJ guidance issued in January 2017 pertaining to NICS determinations that permit fugitives from justice, i.e. persons with active warrants, to purchase a firearm.

**Action:** Motion carried.

#### **SOUTHERN WORKING GROUP ACTION:**

This topic was accepted as information only.

#### **WESTERN WORKING GROUP ACTION:**

**Motion:** Request the APB Chairman to facilitate the drafting of a letter to the Attorney General, with a copy to all Working Group members, expressing the Western Working Group's concerns regarding the DOJ guidance issued in January 2017 pertaining to NICS determinations that permit fugitives from justice, i.e. persons with active warrants, to purchase a firearm.

**Action:** Motion carried.

#### **FALL 2017 NICS SUBCOMMITTEE ACTION:**

This topic was accepted as information only.





**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL INSTANT CRIMINAL BACKGROUND  
CHECK SYSTEM (NICS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**NICS ISSUE #5**

Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, formerly known as the NICS Index, and Potential Optional Fields to be Added.

**PURPOSE**

To re-evaluate mandatory and optional fields within the NICS Indices that were approved by the CJIS APB in 2012, as well as additional information to determine if benefits remain for both the National Instant Criminal Background Check System (NICS) Section and external customers utilizing the NICS to conduct firearms- or explosives-related background checks.

**POINT OF CONTACT**

NICS Section, NICS Business Unit

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the information provided in this paper and provide appropriate comments, suggestions, and/or make further recommendations.

**BACKGROUND**

The Brady Handgun Violence Prevention Act of 1993 (Brady Act), Public Law 103-159. Required the U.S. Attorney General to establish the NICS for Federal Firearms Licensees (FFL) to contact for information supplied immediately as to whether the transfer of a firearm is in violation of state or federal law. When a NICS background check is conducted, a prospective firearm transferee's name and descriptive information is searched against the names and descriptive information contained in criminal history records maintained in the Interstate Identification Index (III); information specific to warrants, protection orders, etc., maintained in the National Crime Information Center (NCIC), and information maintained in the NICS Indices pertaining to persons who are prohibited the transfer of and/or possession of firearms (and/or the issuance of firearm permits) pursuant to the Brady Act and the NICS Regulations (or explosives permits pursuant to the Safe Explosives Act). The information in the NICS Indices is typically not available in the III or the NCIC.

## **DISCUSSION AND ANALYSIS**

As part of a NICS background check, all possible matches of information in the NICS Indices to the prospective firearm transferee (by name and descriptors) is returned to the user who determines if a valid match exists. The valid match to a NICS Indices hit to a prospective firearms transferee allows the user to render an immediate denial determination, as all NICS Indices information is pre-validated as prohibiting, prior to the submission to the database. This pre-validation in turn, provides greater efficiency to a user by eliminating the user's need to conduct additional research to determine if the information is prohibiting for firearm possession/transfer.

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 name and descriptive information stored within the NICS Indices. Candidates are scored on the full name, Date of Birth (DOB), Social Security Number (SOC), and Miscellaneous Number (MNU). The scores are heavily weighted on the name and DOB. Anything that scores below a set threshold is not returned.

As outlined in the NICS Interface Control Document (ICD),<sup>1</sup> the data currently required for a NICS Indices submission is listed in Table 1.

Table 1

<b>Mandatory Data Fields for NICS Indices Entry</b>
First Name
Last Name
Gender
DOB, SOC, MNU <sup>2</sup> (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.<sup>3</sup> 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 with the NICS Indices submission enhances the user's ability to more accurately determine if a valid 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.

<sup>1</sup> NICS Document Number NICS-DOC-02456-1.1, dated November 30, 2016, is available via the Law Enforcement Enterprise Portal.

<sup>2</sup> The allowable MNU categories are outlined in the NICS ICD.

<sup>3</sup> The allowable values for optional data is outlined in the NICS ICD.

Table 2

<b>Optional Data Fields for NICS Indices Entry</b>	
Middle Name	Expiration Date
Cadence	Originating Agency Case Number (OCA)
Place of Birth	Universal Control Number (UCN) (AKA FBI Number)
Height	SOC
Weight	MNU
Hair	Race
Eye	Scars/Marks/Tattoos
Also Known As (AKA)	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 valid match between a firearms applicant and a NICS Indices hit and has aided in identity issues during the appeal 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 optional data fields available. The contributor can also provide additional information specific to the individual by denoting it in the MIS field. Since the NICS background check is a name-based check, 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 valid matches to prospective firearm applicants occur.

In 2012, a topic paper was presented to the CJIS APB with the purpose of discussing whether the minimal information required when adding information to the NICS Indices should be changed or remain the same. As a result, the CJIS APB approved the following enhancements to the data fields in the NICS Indices:

- **State Identification Number (SID)**  
Approved to be added as an optional field in the NICS Indices
- **Henry Fingerprint Classification**  
Approved to be added as an optional field in the NICS Indices
- **Eye Color/Hair Color**  
Approved to remain as optional fields in the NICS Indices
- **Weight**  
Approved to remain as an optional field in the NICS Indices
- **Race**  
Approved to become a mandatory field in the NICS Indices

- **DOB**  
Approved to become a mandatory field in the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC).
- **MIS**  
Approved to expand this field to allow for the maximum amount of characters
- **FBI Number (AKA UCN)**  
Approved to be an optional field in the NICS Indices

The approval of the mandatory requirement of some of the data fields and the addition of new data fields warranted a system change in the NICS. At that time in 2012, changes to the NICS were constrained during the New NICS development, so to prevent cost and schedule impacts of replanning, this initiative was deemed a post-New NICS enhancement. Now that the New NICS is functional, the enhancements may be implemented. However, prior to submitting the enhancements, they will be discussed again in this paper to determine if they remain feasible and to assess if benefits remain for both the NICS Section and external customers utilizing the NICS to conduct firearms- or explosives-related background checks.

In reviewing the approvals of the CJIS APB in 2012, the NICS Section offers the following information for further consideration based on field being added to and searched in the NICS Indices:

- **SID** (Approved by the CJIS APB to add as an optional field)

Currently, the only fields available within the NICS Indices to place the SID is the MIS or OCA field. An optional field of entry to specifically capture the SID with the NICS Indices submission could assist the end user when trying to determine a valid match. Typically, a SID is associated with a state criminal history record. If the criminal history record possesses more person-descriptive information than the data entered in the NICS Indices, the association of the SID with the NICS Indices entry could direct an individual to that SID and the additional information.

- **Henry Fingerprint Classification** (Approved by the CJIS APB to add as an optional field)

The NICS background check is not a fingerprint-based check, nor is the NICS Indices. The Henry Fingerprint Classification is derived from fingerprints. A Henry Fingerprint Classification could serve as a resource for further analysis to assist in determining a valid match. With a Henry Fingerprint Classification, there is often a UCN which can presently be included in the NICS Indices entry. If a UCN is available, the need for the Henry Fingerprint Classification diminishes.

- Physical Descriptors (Approved by the CJIS APB to keep eye/hair color, and weight as optional fields)

Currently, a subject's eye color, hair color, and weight can be captured with a NICS Indices submission as an optional field. These fields are not evaluated during the NICS Indices search. Since an individual's eye color and hair color can change and weight can fluctuate over time, these data fields are not considered by the NICS Section to be as reliable for record-matching purposes because this information does not add to the algorithmic score.

- Race (Approved by the CJIS APB to make this a mandatory data field)

An individual's race, collected by the FFL when completing the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Form 4473, is required when submitting a NICS background check. An allowable value within the Race field is "unknown." Currently, the individual's race is not a required field for NICS Indices submissions. In 2012 when the race field was approved to become a mandatory field, the race was used in the search algorithm when searching for viable matches. The race category is no longer part of the search algorithm (only the name, DOB, SOC, and MNU are used in the search algorithm).

- DOB (Approved by the CJIS APB to make this a mandatory data field)

In 2012, the CJIS APB voted to make the DOB a mandatory field with the provision that if a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC).

The DOB plays a major role when searching for viable matches. The DOB, as part of the NICS search algorithm, is the only numeric identifier required by the NICS when conducting a NICS background check. If the only numeric-based information captured in a NICS Indices entry is a SOC or MNU (in lieu of the DOB), there is the possibility the NICS, during a background check search, could miss a potential match to a NICS Indices record. If the NICS Indices entry does not contain the DOB and the individual does not provide a SOC or MNU (which is not required) on the ATF Form 4473, the NICS Indices entry lacking the DOB information or containing the partial DOB information will most likely not return based on the search algorithm.

- MIS (Approved by the CJIS APB to expand this field to allow for the maximum amount of characters)

The MIS section is an area where other information can be entered if there is not an applicable field. Expanding the comments section can allow for more detailed information to be entered. The NICS Section recommends limiting the maximum number of characters to 2500, which is standard for NCIC informational fields.

- UCN (Approved by the CJIS APB as an optional field)

The UCN is already an optional field for NICS Indices entry. If a contributor has this information, it can be entered in the UCN field. The UCN could serve as a resource for further analysis to assist in determining a valid match.

In addition to the information provided from the prior 2012 paper, the NICS Section would like to offer the following information for consideration:

- Middle Name

The middle name is currently an optional field on NICS Indices submissions. When source documentation contains either an individual's middle name or middle initial, it is very helpful to add that information to the NICS Indices entry for accurate identification. Additional data points, such as the middle name, assists NICS users in accurately comparing potential buyer's descriptive data to NICS Indices records. As demonstrated earlier, the NICS search algorithm is based on a full name. If a middle name is included, this could strengthen this search which would result in a higher score for a match or a lower score which may exclude a non-identical record. As of April 18, 2017, there were 16,497,141 NICS Indices entries. Of these entries, 13,306,824 or 81 percent did not include a middle name or middle initial.

It should be noted that there are individuals who legally have no middle name. Adding an indication of no middle name (NMN) to the NICS Indices entry does not add value to the entry nor does it bolster the search algorithm; in fact, the NMN designation could become a hindrance when the search is performed.

- Additional Information Available Checkbox

Research has determined there are times when a NICS Indices contributors may have additional information not readily captured in the NICS Indices format (e.g., photo available, an individual's address, mother's maiden name, father's name). Although, additional information may be included in the MIS field, often the information is sensitive and/or only available as outlined under state law. In these situations, a checkbox would alert a NICS user that additional information is available for review.

- SOC

The FBI does not have the statutory authority to make the SOC field in the NICS Indices mandatory. If available and allowable by state law, the SOC is helpful in the accurate identification of a potential buyer to a NICS Indices entry. Some state's laws prohibit the SOC to be shared to the NICS Indices in its entirety, therefore, some states only provide the last four digits of the SOC to the MIS field. Whether a complete SOC is included in the SOC field or the last four digits are provided in the MIS field, this addition can assist in determining if an individual is a match with a NICS Indices hit once manually examined further.

For data fields in the NICS Indices that are currently not mandatory, a state can implement their own procedure to require those data fields be populated prior to NICS Indices submission. This would be at the discretion of the state but could improve some of the current identification issues encountered during the research of a NICS Indices hit.

## **RECOMMENDATIONS**

The Subcommittee is requested to discuss and approve one from each of the following options:

### Option 1: SID

- a) Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices.
- b) Rescind the 2012 decision by the APB to create an optional field to capture the SID. Contributors will continue to be encouraged to enter SID information if available, in the MIS field.

### Option 2: Henry Fingerprint Classification

- a) Uphold the 2012 decision by the APB to create an optional field in the NICS Indices to capture the Henry Fingerprint Classification.
- b) Rescind the 2012 decision by the APB to create an optional field for the Henry Fingerprint Classification. Contributors will be advised that they may continue to enter this information into the MIS field.

### Option 3: Eye Color/Hair Color

- a) Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.
- b) Rescind the 2012 decision by the APB and remove the eye color/hair color fields from the NICS Indices format since these person-descriptive traits are easily changed.

### Option 4: Weight

- a) Uphold the 2012 decision by the APB to make no changes to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.
- b) Rescind the 2012 decision by the APB and remove the weight field from the NICS Indices format since this is a person-descriptive trait which can fluctuate over time.

### Option 5: Race

- a) Uphold the 2012 decision by the APB to make race a mandatory field when submitting entries into the NICS Indices.
- b) Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.



#### Option 6: DOB

- a) Uphold the 2012 decision by the APB to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC).
- b) Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

#### Option 7: MIS

- a) Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.
- b) Rescind the 2012 decision by the APB and maintain the maximum limit allowed in the MIS field at 1,000 characters.

#### Option 8: Middle Name

- a) The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.
- b) No change, the middle name field will remain an optional field, with no additional requirements if the information is available within the source documentation.

#### Option 9: Additional Information Available Checkbox

- a) Add an optional checkbox to the NICS Indices format that allows contributors to indicate if additional information is available. The addition of this box would not preclude a contributor from also adding comments or data to the MIS field.
- b) No change, the indication of additional information will continue to be notated in the MIS field.

Approved options will be required no sooner than two years from the date of final approval.

## **FALL 2017 WORKING GROUP ACTIONS:**

### **FEDERAL WORKING GROUP ACTION:**

#### **Option 1: SID**

**Motion:** To accept Option “a” for Option 1.

- a) Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices.

**Action:** Motion carried.

#### **Option 2: Henry Fingerprint Classification**

**Motion:** To accept Option “a” for Option 2.

- a) Uphold the 2012 decision by the APB to create an optional field in the NICS Indices to capture the Henry Fingerprint Classification.

**Action:** Motion carried.

#### **Option 3: Eye Color/Hair Color AND Option 4: Weight**

**Motion:** To accept Option “a” for Options 3 and 4.

##### **Option 3: Eye Color/Hair Color**

- a) Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

##### **Option 4: Weight**

- a) Uphold the 2012 decision by the APB to make no changes to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

#### **Option 5: Race**

**Motion:** To accept Option “b” for Option 5.

- b) Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

**Action:** Motion carried.

#### **Option 6: DOB**

**Motion:** To accept Option “b” for Option 6.

- b) Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 7: MIS**

**Motion:** To accept Option “a” for Option 7.

- a) Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

**Action:** Motion carried.

**Option 8: Middle Name**

**Motion:** To accept Option “a” with modified language for clarifying purposes for Option 8.

- a) If the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry. This policy will be considered with a day forward approach following final approval.

If there is no middle name, you can leave the middle name field blank.

**Action:** Motion carried.

**Option 9: Additional Information Available Checkbox**

**Motion:** To accept Option “a” for Option 9.

- a) Add an optional checkbox to the NICS Indices format that allows contributors to indicate if additional information is available. The addition of this box would not preclude a contributor from also adding comments or data to the MIS field.

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Motion 1:** To accept Option A on Option 1.

**Option A:** Uphold the 2012 decision by the APB to allow the SID as an optional field in the NICS Indices.

**Action:** Motion carried.

**Motion 2:** To accept Option B on Option 2.

**Option B:** No change, but advise contributors the Henry Fingerprint Classification information can be entered in the MIS field.

**Action:** Motion carried.

**Motion 3:** To accept Option A on Option 3 and Option 4.

**Option 3 Option A:** Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and allow them as an optional field when entering a NICS Indices record.

**Option 4 Option A:** Uphold the 2012 decision by the APB to make no changes to the weight field, and allow it to continue as an optional field when entering a NICS Indices record

**Action:** Motion carried.

**Motion 4:** To accept Option B on Option 5.  
**Option B:** No change, the Race field will remain an optional field since it is no longer part of the search algorithm.

**Action:** Motion carried.

**Motion 5:** To accept Option B on Option 6.  
**Option B:** The DOB would become a mandatory field for a NICS Indices submission. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Index entry.

**Action:** Motion carried.

**Motion 6:** To accept Option B on Option 7.  
**Option B:** No change, the maximum amount of characters allowed will remain at 1,000.

**Action:** Motion carried.

**Motion 7:** To accept Option A on Option 8.  
**Option A:** The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Motion 8:** To accept Option B on Option 9.  
**Option B:** No change, the indication of additional information will continue to be notated in the MIS field.

**Action:** Motion carried.

#### **NORTHEASTERN WORKING GROUP ACTION:**

##### **Option 1: SID**

**Motion:** To adopt Option 1a: Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices

**Action:** Motion carried.

##### **Option 2: Henry Fingerprint Classification**

**Motion:** To adopt Option 2a: Uphold the 2012 decision by the APB to create an optional field in the NICS Indices to capture the Henry Fingerprint Classification.

**Action:** Motion carried.

**Option 3: Eye Color/Hair Color**

**Motion:** To adopt Option 3a: Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

**Option 4: Weight**

**Motion:** To adopt Option 4a: Uphold the 2012 decision by the APB to make no changes to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

**Option 5: Race**

**Motion:** To adopt Option 5a: Uphold the 2012 decision by the APB to make race a mandatory field when submitting entries into the NICS Indices.

**Action:** Motion carried.

**Option 6: DOB**

**Motion:** To adopt Option 6b: Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 7: MIS**

**Motion:** To adopt Option 7a: Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

**Action:** Motion carried.

**Option 8: Middle name**

**Motion:** To adopt Option 8a: The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 9: Additional Information Available Checkbox**

**Motion:** To adopt Option 9a: Add an optional checkbox to the NICS Indices format that allows contributors to indicate if additional information is available. The addition

of this box would not preclude a contributor from also adding comments or data to the MIS field.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion 1:** To adopt Option 1a: Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices.

**Action:** Motion carried.

**Motion 2:** To adopt Option 2b: Rescind the 2012 decision by the APB to create an optional field for the Henry Fingerprint Classification. Contributors will be advised that they may continue to enter this information into the MIS field.

**Action:** Motion carried.

**Motion 3:** To adopt Option 3a: Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

**Motion 4:** To adopt Option 4a: Uphold the 2012 decision by the APB to make no changes to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

**Motion 5:** To adopt Option 5b: Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

**Action:** Motion carried.

**Motion 6:** To adopt Option 6b: Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Motion 7:** To adopt Option 7a: Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

**Action:** Motion carried.

**Motion 8:** To adopt Option 8a: The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Motion 9:** To adopt Option 9a: Add an optional checkbox to the NICS Indices format that allows contributors to indicate if additional information is available. The addition of this box would not preclude a contributor from also adding comments or data to the MIS field.

**Action:** Motion carried.

### **WESTERN WORKING GROUP ACTION:**

#### **Option 1: SID**

**Motion:** To adopt Option 1a: Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices.

**Action:** Motion carried

#### **Option 2: Henry Fingerprint Classification**

**Motion:** To adopt Option 2b: Rescind the 2012 decision by the APB to create an option field for the Henry Fingerprint Classification. Contributors will be advised that they may continue to enter this information in the MIS field.

**Action:** Motion carried.

#### **Option 3: Eye Color/Hair Color**

**Motion:** To adopt Option 3a: Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

#### **Option 4: Weight**

**Motion:** To adopt Option 4a: Uphold the 2012 decision by the APB to make no changes to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

#### **Option 5: Race**

**Motion:** To adopt Option 5b: Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

**Action:** Motion carried.

**Option 6: DOB**

**Motion:** To adopt Option 6b: Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 7: MIS**

**Motion:** To adopt Option 7a: Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

**Action:** Motion carried.

**Option 8: Middle Name**

**Motion:** To adopt Option 8a: The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 9: Additional Information Available Checkbox**

**Motion:** To adopt Option 9b: No change, the indication of additional information will continue to be notated in the MIS field.

**Action:** Motion carried.

**FALL 2017 NICS SUBCOMMITTEE ACTIONS:**

**Option 1: SID**

**Motion:** To accept Option 1a: Uphold the 2012 decision by the APB to create an optional field to capture the SID in the NICS Indices.

**Action:** Motion carried.

**Option 2: Henry Fingerprint Classification**

**Motion:** To accept Option 2b: Rescind the 2012 decision by the APB to create an option field for the Henry Fingerprint Classification. Contributors will be advised that they may continue to enter this information in the MIS field.

**Action:** Motion carried.

**Option 3: Eye Color/Hair Color**

**Motion:** To accept Option 3a: Uphold the 2012 decision by the APB to make no changes to the eye color/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.



**Option 4: Weight**

**Motion:** To accept Option 4a: Uphold the 2012 decision by the APB to make no changes to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

**Action:** Motion carried.

**Option 5: Race**

**Motion:** To accept Option 5b: Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

**Action:** Motion carried.

**Option 6: DOB**

**Motion:** To accept Option 6b: Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 7: MIS**

**Motion:** To accept Option 7a: Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

**Action:** Motion carried.

**Option 8: Middle Name**

**Motion:** To accept Option 8a: The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information by policy is required to be included in the NICS Indices entry.

**Action:** Motion carried.

**Option 9: Additional Information Available Checkbox**

**Motion:** To accept Option 9b: No change, the indication of additional information will continue to be notated in the MIS field.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL INSTANT CRIMINAL BACKGROUND  
CHECK SYSTEM (NICS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**NICS ISSUE #7**

The Impact of Pseudo-Pointers on State Outreach in the Next Generation Identification (NGI) System

**PURPOSE**

To provide information on how pseudo-pointer records are created in the NGI System with scenarios, the impact on state outreach, and how to reconcile the pseudo-pointer records.

**POINT OF CONTACT**

Biometric Services Section (BSS), Criminal History Information and Policy Unit

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**BACKGROUND**

When an arrest fingerprint submission is forwarded to the FBI CJIS Division for processing, the fingerprints are searched against the NGI System.<sup>1</sup> The submission either identifies to an existing record and the criminal history record information (CHRI) is added or the submission does not identify to an existing record in the NGI System and establishes a new record. The arrest fingerprint submission may or may not have a unique identifier from the state, referred to as a state identification number (SID). This unique identifier, entered into the pointer data field in the NGI System, drives the state outreach mechanism and indicates the source of the most complete CHRI.

The NGI System relies on a decentralized exchange of the CHRI. In addition to the CHRI, the NGI System uses “pointers” contained within the system to direct queries to records maintained by state agencies. Each arrest event housed within the NGI System contains either a pseudo-pointer, or a SID, also known as an active state pointer. These “pointers” indicate whether a

---

<sup>1</sup> For the purposes of this document, the term arrest fingerprint submission refers to any **RETAIN** criminal arrest fingerprint submission, including Criminal Tenprint Submission (Answer Required) (CAR), Criminal Tenprint Submission (No Answer Necessary) (CNA), Criminal Fingerprint Direct Route (CPDR) submission, or Criminal Fingerprint Processing Non-Urgent (CPNU) submission.

state or the FBI is responsible for the maintenance and dissemination of the various portions of the record. For example, when a fingerprint submission sent to the FBI identifies an identity with a state- maintained record, an active state pointer, and the state’s policy supports

disseminating information for the purpose for which the fingerprints were submitted (e.g., licensing), the NGI System follows the pointer and automatically sends a message to the state that holds the record and appends the state record to the FBI's NGI System response. The state information stored within the NGI System identified with the pointer is dropped from the response to reduce the risk of duplication. Therefore, although arrests or dispositions may be missing from the CHRI on the FBI record, the additional arrests or dispositions may be available on the state-appended CHRI. In the majority of cases, adjudicators are provided CHRI with a greater volume of information than resides solely on the FBI record.

The percentage of state records with active state pointers has increased in the last ten years from 74 percent in March 2007 to 81 percent in March 2017. Although efforts are underway to decrease the number of pseudo-pointer records, new pseudo-pointer records are created monthly by Interstate Identification Index (III) states. For instance from July 2016 to March 2017, 13 III states submitted 12,199 arrest fingerprint submissions with missing or invalid SIDs.

### **How are active state pointers created?**

There are two ways active state pointers, often referred to as SIDs, are created: 1) an arrest fingerprint submission containing a valid SID, or 2) a III maintenance message, known as the modify record SID (MRS).

**Fingerprint Submission:** When the FBI processes a III state's first arrest fingerprint submission which includes a valid SID, a date of arrest (DOA) after the state DOA cutoff date, and is not identified with an existing record, the FBI will establish a new record.<sup>2</sup> A new FBI Universal Control Number (UCN) is assigned with the SID as the active state pointer. To notify the state of the record's establishment, the NGI System returns a Submission Results-Electronic (SRE) with a non-identification decision, and the III generates a \$.A.NPR (No Prior Record-III Record Established) message.

If the same submission results in an identification to an existing record that contains no data for the state, the arrest is added with a new active state pointer. The NGI System returns a SRE with an identification decision and the III generates a \$.A.PIR (Prior Record-SID Number Entered in III Record) message.

---

<sup>2</sup> The DOA cutoff is a date established by the state and used to determine how the NGI System processes transactions. The DOA cutoff determines when unsolicited messages are sent in response to III transactions. This functionality assisted states in transitioning to the III and NFF Programs by limiting the number of unsolicited messages they would receive. The DOA cutoff is contained within a table in the NGI System.

**III Maintenance Message:** When a SID is not indexed, the NGI System creates a pseudo-pointer. Authorized III states may submit a III MRS maintenance message to successfully modify the pseudo-pointer to a SID and assume responsibility for the record. It is important to note that even if subsequent arrest fingerprint submissions with a valid SID are received, the pseudo-pointer will not change. The NGI State Outreach would not be triggered since the pseudo-pointer would not change. Instead the SID is added to the corresponding event associated with the arrest fingerprint submission on the CHRI and returned in the NGI System SRE with an identification decision. Once a record is created with a pseudo-pointer, regardless of why or how the pseudo-pointer was created, the only way to change the pseudo-pointer to an active state pointer is the III MRS maintenance message.

### **How are pseudo-pointers created?**

There are several ways pseudo-pointers are created by a III state's first retain arrest fingerprint submission: 1) a missing SID, 2) an invalid SID, or 3) a DOA prior to the DOA cutoff date stored in the NGI System table.

**Missing SID:** When the FBI processes a III state's first arrest fingerprint submission and the SID is missing and the submission is not identified with an existing record, a new record is established. A new FBI UCN is established with a pseudo-pointer. The submitting agency is not notified the SID is missing by the NGI System. An SRE with a non-identification decision is sent. In addition if the DOA is after the DOA cutoff date, a \$.A.RNP (SID Rejected—No Prior III Record) message is generated by the III to notify the state of the record's establishment.

If the same submission results in an identification to an existing record that contains no data for the state, the arrest is added to the existing record with a pseudo-pointer. The NGI System returns an SRE with an identification decision. If the DOA is after the DOA cutoff date, the III also generates a \$.A.RPR (SID Rejected-Prior III Record) unsolicited message.

If a National Fingerprint File (NFF) state's submission does not include a SID, the NGI System front end transaction manager immediately rejects the submission. A reject message is generated by the NGI System and no subsequent III message is sent to notify the state of the missing SID. Therefore, a new record with a pseudo-pointer cannot be created for NFF participants.

**Invalid SID:** The SID should consist of the standard two character state abbreviation followed by numbers totaling three to ten characters long, with some exceptions. If an arrest fingerprint submission includes a SID in the incorrect format, the NGI System front end transaction manager will remove the SID and continue to process the fingerprint submission as if no SID was provided.

For example, if a III state submits an arrest fingerprint submission with an invalid SID XX122334568, the NGI System front end transaction manager will remove the invalid SID and process the submission as if no SID was provided. If the submission is not identified with an existing record with data from that state, a new pseudo-pointer is established. The NGI System would return an SRE with either an identification or non-identification decision. The III would also generate either a \$.A.RNP or \$.A.RPR unsolicited message if the DOA was after the DOA

cutoff date.

An NFF state whose submission contains an invalid SID would immediately be rejected by the NGI System front end transaction manager, which prevents a record being created with a pseudo-pointer. A reject message is generated by the NGI System, and no subsequent III message is sent to notify the state of the missing SID.

**DOA Cutoff:** The DOA cutoff is a date established by the state and used to determine how the NGI System processes transactions. This functionality assists states in transitioning to the III and NFF Programs by limiting the number of unsolicited messages they receive. Although the DOA cutoff assists states, it is having an adverse effect on setting the state pointers in the records. If a state submits a first arrest fingerprint submission to the NGI System with a valid SID, but the DOA is prior to the DOA cutoff date, the NGI System will ignore the SID and create a pseudo-pointer record. However, if an arrest fingerprint submission with a DOA prior to the DOA cutoff is identified to a FBI UCN with an active state pointer from that state, the active state pointer is not modified to a pseudo-pointer. Instead, the arrest fingerprint submission is added to the CHRI as an event.

It should be noted that this effects not only III participating states, but also NFF states. This is the only way a NFF state can continue to create new pseudo-pointer records. If an NFF state whose submission contains a valid SID, but the DOA is prior to the DOA cutoff date, the NGI System will ignore the SID and create a pseudo-pointer record. The submission would not be rejected.

A state's DOA cutoff can be modified or removed from the NGI System at any time by contacting the FBI CJIS Division BSS Information Quality and Solutions Team (IQST) at (304) 625-3652 or e-mail <[FBI-III@leo.gov](mailto:FBI-III@leo.gov)> for assistance.

For example, a III state is automating their hard-copy arrest fingerprint cards and their DOA cutoff is 01/01/2001. A retain arrest fingerprint submission is sent to the NGI System with a valid SID with a DOA of 03/06/1992. If the submission is not identified with an existing record with data from that state, a new a pseudo-pointer is established. The NGI System will not index the SID for this record in the pointer field because the DOA is prior to the DOA cutoff date. The NGI System returns an SRE with either an identification or non-identification decision.

### **What is the impact of pseudo-pointer records?**

The number of pseudo-pointer records negatively impacts the NGI System state outreach, thus impacting the quality of information disseminated and used for making decisions (adjudicators) regarding qualifications for employment, licensing, adoption, healthcare workers for the elderly,

volunteers with children, immigration background checks, etc. In addition, incomplete records hinder criminal investigations and court sentencing decisions, as well as the services provided by the National Instant Criminal Background Check System, and the NGI Rap Back service. Specifically in March 2017, the NGI processed over 1.3 million criminal fingerprint submissions and over 3.2 million civil fingerprint submissions which could have been negatively impacted by the number of pseudo-pointer records.

## **How to reconcile the pseudo-pointer and active state pointer records?**

There are several ways pseudo-pointers and active state pointers can be reconciled: 1) \$.A. unsolicited messages, 2) III audit synchronizations, or 3) correlation requests.

**\$.A. Unsolicited Messages:** When the NGI System successfully processes an agency's initial retain arrest fingerprint submission with a DOA after the DOA cutoff date, it returns an SRE with either an identification or non-identification decision. The III also generates one of the four III \$.A. unsolicited messages, a \$.A. NPR, \$.A.RNP, \$.A.PIR, or \$.A.RPR. Upon receipt of a \$.A.NPR or \$.A.PIR unsolicited message, the state system automatically compares the SID and at least one other identifier (e.g., the name and/or the date of birth of the subject) to the record in its state file before adding the FBI UCN and setting the status flag to indicate single-source or multi-source record. Upon receipt of the \$.A.RNP or \$.A.RPR unsolicited message, the state personnel should review the message. The discrepancy should be identified and the SID corrected using the III MRS maintenance message. If state agencies are actively researching and resolving the \$.A.RNP or \$.A.RPR unsolicited messages, pseudo-pointer records erroneously being created can be immediately corrected. This will also result in fewer discrepancies identified in the III audit synchronizations.

**III Audit Synchronizations:** To comply with the minimum standards for III/NFF Program participation, states are required to conduct bi-annual synchronizations with the option of two additional quarterly synchronizations. Each III/NFF participating state makes a copy of its criminal history records indexed in the III at a designated time frame. The information included consists of biographical information, pointer information, and status flags. The FBI generates a copy of each state's records during the same time frame and provides a copy to the state. The state compares its data against the FBI data. Discrepancies between the two sets of information are researched and corrected, as necessary, in the state criminal history file and/or in the III.

For instance, a discrepancy may be identified in the pointer information when researching the III audit synchronization file. The state shows an active state pointer and the FBI file indicates a pseudo-pointer. The pseudo-pointer could be a result of any of the scenarios previously mentioned. After verifying the state record contains at least as much information as the FBI record, the state can submit a III MRS maintenance message to change the pseudo-pointer to an active state pointer.

**Correlation Requests:** The correlation provides states, upon request, an opportunity to review records which the FBI supports (pseudo pointer records) and take ownership (set the pointer) in these records. Records with the pointer set (SID) are supported by the state via the III. The correlation data is provided in record segments, including the identification segment, the supplemental identifiers segment, the arrest segment, the judicial segment, and the custody-supervision segment. The states compare the data in each record segment to identify records in which the state record reflects essentially the same arrest, court, and custody data as contained in the FBI record. These are records that the state can support and may send the III message to set the active state pointer. As of July 2017, six states have requested correlations, resulting in approximately 1.6 million pseudo-pointer records being sent to the states for comparison and potential setting of the active pointer.

For additional information regarding pseudo-pointer records, please contact the FBI CJIS Division BSS IQST at (304) 625-3652 or e-mail <[FBI-III@leo.gov](mailto:FBI-III@leo.gov)> for assistance.

**FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

This topic was accepted as information only by the Identification Services and NICS Subcommittees.

**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL INSTANT CRIMINAL BACKGROUND  
CHECK SYSTEM (NICS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**NICS ISSUE #8**

Criminal History Update

**PURPOSE**

To provide an update for all criminal history information projects which includes updates on dispositions, Automated Disposition and Processing Technology (ADAPT), non-serious offenses (NSOs), and updating of pseudo-pointer records.

**POINT OF CONTACT**

Biometric Services Section, Criminal History Information and Policy Unit (CHIPU)

Questions regarding this topic should be directed to <agmu@leo.gov>.

**BACKGROUND**

The CHIPU supports the criminal justice and the noncriminal justice (civil) 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 all criminal history information projects, which includes dispositions, ADAPT, NSOs, and updating of pseudo-pointer records.

**Dispositions within the Next Generation Identification (NGI) System**

**FBI Field Office Arrests:** 88 percent of all FBI Field Office arrests have dispositions. The remaining 12 percent are arrests missing dispositions, including arrests which have not been adjudicated.

**Federal Arrests:** 60 percent of all federal arrests have dispositions. The remaining 40 percent are arrests missing dispositions, including arrests which have not been adjudicated.

Multiple efforts are underway to identify federal dispositions (including dispositions for FBI Field Office arrests).

- The U.S. Courts are submitting dispositions for all individuals under federal supervision.



- Discussion is ongoing with the U.S. Attorney’s Office regarding cases which were not referred for prosecution.
- Multiple federal agencies have been provided details of arrests missing dispositions.
- The FBI contractors, Ruchman Associates Incorporated, are researching dispositions.

**State Pseudo-Pointer Arrests<sup>1</sup>:** 44 percent of all state pseudo-pointer arrests have dispositions. The remaining 56 percent are arrests missing dispositions, including arrests which have not been adjudicated. The priority is to establish state identification numbers (SIDs) within the pseudo-pointer arrest events. Multiple efforts are underway to support states establishing SIDs for pseudo-pointer arrests and/or to identify dispositions.

- Biometric, biographic, and arrest information for pseudo-pointer records have been supplied to multiple states.
- Correlation information has been provided to multiple states
- Microfilm records were provided upon request.
- The Interstate Identification Index (III) Disposition Message Key (DSP) has been modified to include the submission of dispositions for pseudo-pointer records by all states.
- The FBI will research dispositions, with the concurrence of the individual state.

**State Arrests:** As background, the NGI System relies on a decentralized exchange of criminal history record information (CHRI).<sup>2</sup> In addition to the CHRI, the NGI System uses “pointers” contained within the system to direct searches to records maintained by state agencies. These pointers also indicate whether a state or other federal agency, or the FBI, is responsible for the maintenance and dissemination of the various portions of the record.

For example, when a fingerprint submission sent to the FBI matches a state-maintained record, and the state’s policy supports disseminating information for the purpose for which the fingerprints were submitted (e.g., licensing), the NGI System follows the pointer and automatically sends a message to the state that holds the record and appends the state record to the FBI’s NGI System response. The state information stored within the NGI System identified with the pointer is dropped from the response to reduce the risk of duplication. Therefore, although a disposition may be missing from the CHRI on the FBI record, the disposition may be available on the state-appended CHRI. In the majority of cases, adjudicators are provided CHRI

---

<sup>1</sup> The CHRs are indexed in the NGI System by either a state-active pointer, indicated by a SID or an FBI pseudo-pointer in the pointer data field. The III pointer identifies the state and federal agencies that contribute information to an individual’s record. An FBI pseudo-pointer record is established in the NGI System when either a fingerprint submission is received from a federal agency, a non-III participating state, or when the SID is not present or was previously assigned to a different individual. In this case, the FBI CJIS Division is responsible for the dissemination of the CHRI for that record subject.

<sup>2</sup> The CJIS Advisory Policy Board proposed a decentralized CHR system in April 1978. The proposal called for the FBI to receive and store CHRI from federal agencies. The states were to maintain full responsibility and control regarding the collection, collation, maintenance, and dissemination of state, county, and local CHRI.

with a greater volume of information from the state's response than what resides solely on the FBI record.

Twenty states participate in the National Fingerprint File (NFF) Program and provide CHRs for authorized uses, including criminal justice and noncriminal purposes. An NFF state submits fingerprint images for each offender's first arrest to the FBI to identify or establish the identity of the offender at the national level, but the CHRI is only maintained at the state level. As such, it is not necessary for the NFF states to submit final disposition reports and expungement orders to the FBI for records they maintain. States that participate in the NFF Program greatly increase the information available to adjudicators by providing their records for all authorized uses.

It would be inaccurate to calculate missing dispositions available to users without including the state information available to be appended to responses. The state statistical information is not available for all states, at this time.

Sixty percent of all state arrests, housed within the NGI System, were submitted from states that do not support all purpose codes. Forty-nine percent of these arrests have missing dispositions, including arrests which have not been adjudicated. All states, which do not support all purpose codes, submit dispositions electronically or are testing to do so. Teleconferences are being held to identify challenges and possible solutions to the submission of dispositions.

**Tribal Arrests:** 48 percent of all tribal arrests have dispositions. The remaining 52 percent are arrests missing dispositions, including arrests which have not been adjudicated. Dashboards were created for tribes displaying the percentage and volume of missing dispositions. Tribal agencies utilizing the Department of Justice's Tribal Access Program have the opportunity to submit dispositions via the III DSP. Discussions are underway regarding submission of missing legacy dispositions.

## **ADAPT**

The ADAPT has been designed to address concerns received from multiple external partners regarding disposition submission. The service leverages existing disposition submission methods and web-based platforms to provide enhanced methods for electronically submitting dispositions.

One of the concerns surrounded the protection of personally identifiable information (PII) during the mailing of Machine Readable Data (MRD) Computer Discs to the CJIS Division. The ADAPT service provides a method to upload bulk dispositions in the MRD format by leveraging the Law Enforcement Enterprise Portal (LEEP) Enterprise File Transfer Service (EFTS). The key technological advancement is that the MRD file is uploaded by an authorized LEEP user to their state folder within the EFTS, and the NGI System automatically retrieves and processes the file. Results are returned in a WinZip file to the state's folder on the LEEP EFTS. As of April 2017, two states piloted the method, and the CJIS Division plans to roll this out to current MRD customers in 2017. This process is called the ADAPT Bulk File Processing via the LEEP EFTS, which will protect the PII while eliminating the mailing costs.

The next phase of the ADAPT service will be the development of a web-based interface, which provides an automated ability for an agency to submit single disposition information using an online form. This service is currently in the requirement development phase and the CJIS Division plans to have more information regarding this functionality late in 2017.

### **State Pseudo-Pointer Records**

In an effort to decrease the number of pseudo-pointer records and increase state active pointers, correlations and electronic fingerprint files (also known as certification files) are being provided to a number of states for processing.

The sole purpose of a correlation is for states to identify the records in the III that the FBI supports (pseudo-pointer records) and take ownership (set the pointer) of the records that can be supported by the state. The correlation data is provided in record segments, including the identification segment, the supplemental identifiers segment, the arrest segment, the judicial segment, and the custody-supervision segment. The states compare the data in each record segment to identify records in which the state has as much or more information as the FBI. These are records that the state can support and may send the III message to set the active state pointer. As of April 2017, six states have requested correlations, resulting in approximately 1.6 million pseudo-pointer records being sent to the states for comparison and potential setting of the active pointer.

In addition, a process has been identified to provide the certification files (cert. files) for pseudo-pointer record arrests not currently on file at the state level. Guidelines and procedures were developed to provide the cert. files through the use of the LEEP EFTS, the same application currently used for the ADAPT. The cert. files are automatically uploaded from the NGI System to the state folder within the EFTS as WinZip files. The state agencies then download the files using the EFTS Upload/Download Wizard. Seven states have requested their cert. files, resulting in approximately 7 million cert. files being sent to the states. Three other states are waiting to complete their correlation before requesting their cert. files, and two additional states have received information on the process. Ultimately, these efforts positively impact the NGI System state outreach and the quality of CHRI shared for employment and licensing adjudications, firearm background checks, Rap Back services, criminal investigations and sentencing decisions.

### **NSO Vetting**

The DOJ will consider the publishing of a Notice of Proposed Rulemaking in the *Federal Register* to allow for the storage of NSOs within the NGI System when the federal or state contributor requests the retention of the fingerprint and arrest data. Title 28, Code of Federal Regulations, Section 20.32 requires the FBI to vet and remove the submitted information, if the arrest is an NSO (regardless of the contributor's retention request). Although a perception exists that NSO retention may negatively impact reentry, the removal of NSOs would also negatively affect identification in the intelligence, criminal, latent, and cold case processing. Analysis is being performed to determine the impact of the change.

**FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

Accepted as information only by the Identification Services Subcommittee.

Accepted as information only by the NICS Subcommittee.



**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL INSTANT CRIMINAL BACKGROUND  
CHECK SYSTEM (NICS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 17, 2017**

**STAFF PAPER**

**NICS ISSUE #9**

Submission of an Originating Case Number during a NICS Disposition of Firearms Background Check

**PURPOSE**

To re-evaluate the requirement previously set forth by the FBI Criminal Justice Information Services (CJIS) Division's National Instant Criminal Background Check System (NICS) Section which directs criminal justice agencies to include an Originating Case Number (OCA) on all Disposition of Firearms (DOF) background checks conducted through the NICS.

**POINT OF CONTACT**

NICS Section, NICS Business Unit

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to evaluate the uses of the OCA and select an option that is least burdensome on the states while still meeting NICS and CJIS audit requirements.

**BACKGROUND**

In January 2006, the FBI requested a regulation change to amend Title 28, Code of Federal Regulations (C.F.R), Section 25.6(j) to allow access to the NICS by criminal justice agencies for the purpose of conducting NICS background checks when disposing of (returning) firearms in their possession. Upon review and approval, the Final Rule was published by the Department of Justice's Office of Legal Policy on November 20, 2014, and access to the NICS for DOF background checks by criminal justice agencies was authorized. Conducting DOF background checks through the NICS is not federally mandated. Access to the NICS for this purpose requires authorization from the state CJIS Systems Officer (CSO).

The methods of access to the NICS for the DOF varies depending on each state's status as a Point of Contact (POC). In full-POC states, criminal justice agencies can contact their state-designated POC agencies to conduct DOF background checks. Criminal justice agencies in partial-POC states can contact their state-designated POC agencies or the state's CSO can

facilitate direct access to the NICS for the criminal justice agencies attempting to dispose of firearms. For states that do not serve in a POC capacity, the NICS Section processes the NICS background checks as mandated by the Brady Handgun Violence Prevention Act of 1993; therefore, the checks for the purpose of returning firearms in the possession of criminal justice agencies may also be conducted through the NICS Section via the NICS E-Check service. However, CSOs may choose to allow criminal justice agencies within their state to conduct DOF background checks directly through the National Crime Information Center (NCIC) via a Query NICS All Protection Orders (QNP). The QNP queries the three databases searched by the NICS: the Interstate Identification Index (III), the NCIC, and the NICS Indices, formerly known as the NICS Index.

Information required to initiate a DOF background check includes the appropriate purpose identification code, the transferee's first and last name, sex, race, date of birth, and state of residence. Additionally, the NICS E-Check also requires the data entry of the potential transferee's place of birth and country of citizenship.

The NICS Section originally advised the CJIS APB that the OCA would be a required field when conducting DOF background checks through the NICS. At that time, the OCA was necessary for auditing purposes to ensure the NICS is only accessed for Brady-authorized uses. Enforcement of the entry of an OCA for DOF background checks submitted to the NICS was delayed until January 2017 to allow states time to make the necessary system changes.

Currently, the NICS is programmed to accept NICS queries both with and without the OCA on DOF background checks. Although not presently required systematically, the NICS Section has encouraged criminal justice agencies to include the OCA when submitting DOF background checks to the NICS. Accordingly, for non-POC states utilizing the NICS Section, criminal justice agencies have been instructed to submit an OCA when utilizing the NICS E-Check.

In 2014, the APB was advised that the CJIS Audit Unit (CAU) and the NICS Section will conduct audits on DOF background checks to ensure compliance with federal regulations governing the NICS. At that time, the NICS Section indicated audits would be performed electronically by conducting a system check utilizing the NICS Transaction Number (NTN) and the OCA.

## **DISCUSSION AND ANALYSIS**

The NICS Section has learned several obstacles, such as lack of funding, exist that may hinder enforcement of a mandatory OCA on DOF background checks. Based on this information, the NICS Section thought it prudent to delay the OCA requirement until further evaluation could be conducted to determine if the OCA remains a beneficial data point to the CJIS Division, the NICS Section, and external customers utilizing the NICS.

In reviewing the practicality of requiring an OCA, the NICS Section extends the following information for consideration:

- *Audit Process*

The CAU and the NICS Section conduct audits to ensure compliance with federal regulations governing the NICS. Discussions with the CAU indicate the OCA may not be as crucial at this point as originally determined. The OCA was originally required to assist agencies when referencing DOF cases during the audit process. Many agencies have since

developed their own forms that are utilized only when returning firearms. All required documentation must be in place to accurately ensure NICS is being utilized appropriately. The use of these forms and the availability of the NTN assists CAU in ensuring the NICS is only accessed for authorized purposes. If the OCA becomes a mandatory field, then agencies will be held accountable for accurately maintaining this information.

- *Availability of an OCA*

Criminal justice agencies utilize the NICS for DOF purposes under various situations. The CJIS Division's Criminal Justice Information Law Unit previously advised that the plain language of 28 C.F.R. §25.9(j) (3) supports that any time a firearm is properly in the possession of a law enforcement or criminal justice agency, a NICS check may be conducted prior to the return or other transfer of that firearm to the individual with apparent ownership interest therein. Most often during a DOF background check conducted via the NICS, a law enforcement officer is returning a confiscated firearm to the original owner due to a court order. In these instances, the availability of an OCA should not present a problem.

However, not all situations are as simple in circumstance. Nothing in the balance of the U.S. Attorney General's published justification for 28 C.F.R. §25.9(j)(3) detracts from the usability of the NICS Indices by police officers who lawfully have seized weapons under any circumstances. Therefore, if an officer employed by a law enforcement or criminal justice agency has properly, under the law of the controlling jurisdiction, seized a firearm during (for example) a routine traffic stop, he/she would be able to initiate a NICS background check before returning the firearms to the subject. An OCA may not be readily available during this situation; therefore, if the OCA is required, the officer may not be able to conduct a DOF background check via the NICS. The law enforcement officer would have the ability to conduct a check of the NCIC and the III but would no longer have access to over 16 million records (e.g., mental health, indictments, state prohibitions) located within the NICS Indices.

- *Access to the NICS Indices*

As of May 1, 2017, 37 states, 26 federal agencies, and 6 tribal entities utilize the NICS to conduct background checks prior to returning seized or confiscated firearms. While several states have completed the necessary programming for inclusion of an OCA when processing DOF background checks, some continue to lack the funding and/or staffing to meet this requirement. If the OCA was currently deemed a required field on all DOF background checks, numerous criminal justice agencies across the country would lose

access to the NICS due to the lack of programming necessary to submit this information. Eliminating access to the NICS for these criminal justice agencies would result in these agencies no longer having access to over 16 million records located within the NICS Indices. Information maintained in the NICS Indices pertains to persons who are prohibited the transfer of and/or possession of firearms (and/or the issuance of firearm-related permits) pursuant to state and/or federal law. The information in the NICS Indices is typically not available in the III or the NCIC.



**RECOMMENDATIONS:**

**The Subcommittee is requested to consider the proposed options and/or make further recommendations:**

Option 1: Require an Originating Case Number on all DOF background checks conducted via the NICS within two years.

Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**The NICS Section recommends approval of Option 2. Based on the analysis conducted to determine the practicality of requiring an OCA, the benefits associated with having the OCA available no longer substantiate the programming changes necessary at the local, state and federal level.**

**FALL 2017 WORKING GROUP ACTIONS:**

**FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To accept Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**Action:** Motion carried.

**NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**Action:** Motion carried.

**FALL 2017 NICS SUBCOMMITTEE ACTION:**

**Motion:** To accept Option 2: The Originating Case Number remains an optional field on all disposition of firearms background checks conducted via the NICS.

**Action:** Motion carried.

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)  
ADVISORY POLICY BOARD (APB)  
DECEMBER 6-7, 2017  
OKLAHOMA CITY, OK**

**STAFF PAPER**

**APB ITEM #8**

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

**IS ISSUE #1\***

Identification Services Coordination Group Update

**IS ISSUE #2**

Impact of Pseudo-Pointers on State Outreach in the Next Generation Identification (NGI) System

**IS ISSUE #3**

A Solicitation to the User Community Regarding their Experiences with Face Recognition Searches of the FBI's NGI Interstate Photo System (IPS) and the Utility of the Responses Received

**IS ISSUE #4**

Proposal to Require Training for Those Conducting Face Recognition Searches of the NGI/IPS

**IS ISSUE #5**

Final Seven of Ten Solution Update and Future Concepts

**IS ISSUE #6**

Criminal History Update

**IS ISSUE #7**

Rapid DNA Update

**IS ISSUE #8\***

Disposition Task Force Update

**IS ISSUE #9**

Update on Fusion Center Access to CJIS Division Systems

**IS ISSUE #10**

NGI Facial Recognition Candidate List Accuracy

**IS ISSUE #11\***

Mobile Identification Search of the Full Criminal Master File for the Repository for Individuals of Special Concern

\*No staff paper

**IS ISSUE #12\***

Miscellaneous Action Items Update

**IS ISSUE #13\***

Adhoc Items

**IS ISSUE #14\***

Legislative Update

\*No staff paper

**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #2**

The Impact of Pseudo-Pointers on State Outreach in the Next Generation Identification (NGI) System

**PURPOSE**

To provide information on how pseudo-pointer records are created in the NGI System with scenarios, the impact on state outreach, and how to reconcile the pseudo-pointer records.

**POINT OF CONTACT**

Biometric Services Section (BSS), Criminal History Information and Policy Unit

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**BACKGROUND**

When an arrest fingerprint submission is forwarded to the FBI CJIS Division for processing, the fingerprints are searched against the NGI System.<sup>1</sup> The submission either identifies to an existing record and the criminal history record information (CHRI) is added or the submission does not identify to an existing record in the NGI System and establishes a new record. The arrest fingerprint submission may or may not have a unique identifier from the state, referred to as a state identification number (SID). This unique identifier, entered into the pointer data field in the NGI System, drives the state outreach mechanism and indicates the source of the most complete CHRI.

The NGI System relies on a decentralized exchange of the CHRI. In addition to the CHRI, the NGI System uses “pointers” contained within the system to direct queries to records maintained by state agencies. Each arrest event housed within the NGI System contains either a pseudo-pointer, or a SID, also known as an active state pointer. These “pointers” indicate whether a

---

<sup>1</sup> For the purposes of this document, the term arrest fingerprint submission refers to any **RETAIN** criminal arrest fingerprint submission, including Criminal Tenprint Submission (Answer Required) (CAR), Criminal Tenprint Submission (No Answer Necessary) (CNA), Criminal Fingerprint Direct Route (CPDR) submission, or Criminal Fingerprint Processing Non-Urgent (CPNU) submission.

state or the FBI is responsible for the maintenance and dissemination of the various portions of the record.

For example, when a fingerprint submission sent to the FBI identifies an identity with a state-maintained record, an active state pointer, and the state's policy supports disseminating information for the purpose for which the fingerprints were submitted (e.g., licensing), the NGI System follows the pointer and automatically sends a message to the state that holds the record and appends the state record to the FBI's NGI System response. The state information stored within the NGI System identified with the pointer is dropped from the response to reduce the risk of duplication. Therefore, although arrests or dispositions may be missing from the CHRI on the FBI record, the additional arrests or dispositions may be available on the state-appended CHRI. In the majority of cases, adjudicators are provided CHRI with a greater volume of information than resides solely on the FBI record.

The percentage of state records with active state pointers has increased in the last ten years from 74 percent in March 2007 to 81 percent in March 2017. Although efforts are underway to decrease the number of pseudo-pointer records, new pseudo-pointer records are created monthly by Interstate Identification Index (III) states. For instance from July 2016 to March 2017, 13 III states submitted 12,199 arrest fingerprint submissions with missing or invalid SIDs.

### **How are active state pointers created?**

There are two ways active state pointers, often referred to as SIDs, are created: 1) an arrest fingerprint submission containing a valid SID, or 2) a III maintenance message, known as the modify record SID (MRS).

**Fingerprint Submission:** When the FBI processes a III state's first arrest fingerprint submission which includes a valid SID, a date of arrest (DOA) after the state DOA cutoff date, and is not identified with an existing record, the FBI will establish a new record.<sup>2</sup> A new FBI Universal Control Number (UCN) is assigned with the SID as the active state pointer. To notify the state of the record's establishment, the NGI System returns a Submission Results-Electronic (SRE) with a non-identification decision, and the III generates a \$.A.NPR (No Prior Record-III Record Established) message.

If the same submission results in an identification to an existing record that contains no data for the state, the arrest is added with a new active state pointer. The NGI System returns a SRE with an identification decision and the III generates a \$.A.PIR (Prior Record-SID Number Entered in III Record) message.

---

<sup>2</sup> The DOA cutoff is a date established by the state and used to determine how the NGI System processes transactions. The DOA cutoff determines when unsolicited messages are sent in response to III transactions. This functionality assisted states in transitioning to the III and NFF Programs by limiting the number of unsolicited messages they would receive. The DOA cutoff is contained within a table in the NGI System.

**III Maintenance Message:** When a SID is not indexed, the NGI System creates a pseudo-pointer. Authorized III states may submit a III MRS maintenance message to successfully modify the pseudo-pointer to a SID and assume responsibility for the record. It is important to note that even if subsequent arrest fingerprint submissions with a valid SID are received, the pseudo-pointer will not change. The NGI State Outreach would not be triggered since the pseudo-pointer would not change. Instead the SID is added to the corresponding event associated with the arrest fingerprint submission on the CHRI and returned in the NGI System SRE with an identification decision. Once a record is created with a pseudo-pointer, regardless of why or how the pseudo-pointer was created, the only way to change the pseudo-pointer to an active state pointer is the III MRS maintenance message.

### **How are pseudo-pointers created?**

There are several ways pseudo-pointers are created by a III state's first retain arrest fingerprint submission: 1) a missing SID, 2) an invalid SID, or 3) a DOA prior to the DOA cutoff date stored in the NGI System table.

**Missing SID:** When the FBI processes a III state's first arrest fingerprint submission and the SID is missing and the submission is not identified with an existing record, a new record is established. A new FBI UCN is established with a pseudo-pointer. The submitting agency is not notified the SID is missing by the NGI System. An SRE with a non-identification decision is sent. In addition if the DOA is after the DOA cutoff date, a \$.A.RNP (SID Rejected—No Prior III Record) message is generated by the III to notify the state of the record's establishment.

If the same submission results in an identification to an existing record that contains no data for the state, the arrest is added to the existing record with a pseudo-pointer. The NGI System returns an SRE with an identification decision. If the DOA is after the DOA cutoff date, the III also generates a \$.A.RPR (SID Rejected-Prior III Record) unsolicited message.

If a National Fingerprint File (NFF) state's submission does not include a SID, the NGI System front end transaction manager immediately rejects the submission. A reject message is generated by the NGI System and no subsequent III message is sent to notify the state of the missing SID. Therefore, a new record with a pseudo-pointer cannot be created for NFF participants.

**Invalid SID:** The SID should consist of the standard two character state abbreviation followed by numbers totaling three to ten characters long, with some exceptions. If an arrest fingerprint submission includes a SID in the incorrect format, the NGI System front end transaction manager will remove the SID and continue to process the fingerprint submission as if no SID was provided.

For example, if a III state submits an arrest fingerprint submission with an invalid SID XX122334568, the NGI System front end transaction manager will remove the invalid SID and process the submission as if no SID was provided. If the submission is not identified with an

existing record with data from that state, a new pseudo-pointer is established. The NGI System would return an SRE with either an identification or non-identification decision. The III would also generate either a \$.A.RNP or \$.A.RPR unsolicited message if the DOA was after the DOA cutoff date.

An NFF state whose submission contains an invalid SID would immediately be rejected by the NGI System front end transaction manager, which prevents a record being created with a pseudo-pointer. A reject message is generated by the NGI System, and no subsequent III message is sent to notify the state of the missing SID.

**DOA Cutoff:** The DOA cutoff is a date established by the state and used to determine how the NGI System processes transactions. This functionality assists states in transitioning to the III and NFF Programs by limiting the number of unsolicited messages they receive. Although the DOA cutoff assists states, it is having an adverse effect on setting the state pointers in the records. If a state submits a first arrest fingerprint submission to the NGI System with a valid SID, but the DOA is prior to the DOA cutoff date, the NGI System will ignore the SID and create a pseudo-pointer record. However, if an arrest fingerprint submission with a DOA prior to the DOA cutoff is identified to a FBI UCN with an active state pointer from that state, the active state pointer is not modified to a pseudo-pointer. Instead, the arrest fingerprint submission is added to the CHRI as an event.

It should be noted that this effects not only III participating states, but also NFF states. This is the only way a NFF state can continue to create new pseudo-pointer records. If an NFF state whose submission contains a valid SID, but the DOA is prior to the DOA cutoff date, the NGI System will ignore the SID and create a pseudo-pointer record. The submission would not be rejected.

A state's DOA cutoff can be modified or removed from the NGI System at any time by contacting the FBI CJIS Division BSS Information Quality and Solutions Team (IQST) at (304) 625-3652 or e-mail <[FBI-III@leo.gov](mailto:FBI-III@leo.gov)> for assistance.

For example, a III state is automating their hard-copy arrest fingerprint cards and their DOA cutoff is 01/01/2001. A retain arrest fingerprint submission is sent to the NGI System with a valid SID with a DOA of 03/06/1992. If the submission is not identified with an existing record with data from that state, a new a pseudo-pointer is established. The NGI System will not index the SID for this record in the pointer field because the DOA is prior to the DOA cutoff date. The NGI System returns an SRE with either an identification or non-identification decision.

### **What is the impact of pseudo-pointer records?**

The number of pseudo-pointer records negatively impacts the NGI System state outreach, thus impacting the quality of information disseminated and used for making decisions (adjudicators) regarding qualifications for employment, licensing, adoption, healthcare workers for the elderly,

volunteers with children, immigration background checks, etc. In addition, incomplete records hinder criminal investigations and court sentencing decisions, as well as the services provided by the National Instant Criminal Background Check System, and the NGI Rap Back service. Specifically in March 2017, the NGI processed over 1.3 million criminal fingerprint submissions and over 3.2 million civil fingerprint submissions which could have been negatively impacted by the number of pseudo-pointer records.

### **How to reconcile the pseudo-pointer and active state pointer records?**

There are several ways pseudo-pointers and active state pointers can be reconciled: 1) \$.A. unsolicited messages, 2) III audit synchronizations, or 3) correlation requests.

**\$.A. Unsolicited Messages:** When the NGI System successfully processes an agency's initial retain arrest fingerprint submission with a DOA after the DOA cutoff date, it returns an SRE with either an identification or non-identification decision. The III also generates one of the four III \$.A. unsolicited messages, a \$.A. NPR, \$.A.RNP, \$.A.PIR, or \$.A.RPR. Upon receipt of a \$.A.NPR or \$.A.PIR unsolicited message, the state system automatically compares the SID and at least one other identifier (e.g., the name and/or the date of birth of the subject) to the record in its state file before adding the FBI UCN and setting the status flag to indicate single-source or multi-source record. Upon receipt of the \$.A.RNP or \$.A.RPR unsolicited message, the state personnel should review the message. The discrepancy should be identified and the SID corrected using the III MRS maintenance message. If state agencies are actively researching and resolving the \$.A.RNP or \$.A.RPR unsolicited messages, pseudo-pointer records erroneously being created can be immediately corrected. This will also result in fewer discrepancies identified in the III audit synchronizations.

**III Audit Synchronizations:** To comply with the minimum standards for III/NFF Program participation, states are required to conduct bi-annual synchronizations with the option of two additional quarterly synchronizations. Each III/NFF participating state makes a copy of its criminal history records indexed in the III at a designated time frame. The information included consists of biographical information, pointer information, and status flags. The FBI generates a copy of each state's records during the same time frame and provides a copy to the state. The state compares its data against the FBI data. Discrepancies between the two sets of information are researched and corrected, as necessary, in the state criminal history file and/or in the III.

For instance, a discrepancy may be identified in the pointer information when researching the III audit synchronization file. The state shows an active state pointer and the FBI file indicates a pseudo-pointer. The pseudo-pointer could be a result of any of the scenarios previously mentioned. After verifying the state record contains at least as much information as the FBI record, the state can submit a III MRS maintenance message to change the pseudo-pointer to an active state pointer.



**Correlation Requests:** The correlation provides states, upon request, an opportunity to review records which the FBI supports (pseudo pointer records) and take ownership (set the pointer) in these records. Records with the pointer set (SID) are supported by the state via the III. The correlation data is provided in record segments, including the identification segment, the supplemental identifiers segment, the arrest segment, the judicial segment, and the custody-supervision segment. The states compare the data in each record segment to identify records in which the state record reflects essentially the same arrest, court, and custody data as contained in the FBI record. These are records that the state can support and may send the III message to set the active state pointer. As of July 2017, six states have requested correlations, resulting in approximately 1.6 million pseudo-pointer records being sent to the states for comparison and potential setting of the active pointer.

For additional information regarding pseudo-pointer records, please contact the FBI CJIS Division BSS IQST at (304) 625-3652 or e-mail <[FBI-III@leo.gov](mailto:FBI-III@leo.gov)> for assistance.

#### **FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

#### **FALL 2017 SUBCOMMITTEE ACTIONS:**

This topic was accepted as information only by the IS and National Instant Criminal Background Check System Subcommittees.

**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #3**

A Solicitation to the User Community Regarding Their Experiences with Face Recognition Searches of the Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) - Interstate Photo System (IPS) and the Utility of the Responses Received

**PURPOSE**

To acquire feedback from the User Community regarding their experience with conducting face recognition searches of the FBI's NGI-IPS.

**POINT OF CONTACT**

Biometric Services Section, Facial Analysis, Comparison, and Evaluation (FACE) Services Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the information included in this paper and provide appropriate comments, suggestions as requested.

**BACKGROUND**

The Government Accountability Office (GAO) visited the FBI Criminal Justice Information Services (CJIS) Division in April 2015 to learn about its use of face recognition. The FBI's NGI-IPS, which includes an investigative Facial Recognition Search component, became operational in April 2015. During the GAO visit, the FBI CJIS Division's Biometric Images Specialists provided a face recognition demonstration and FACE Services Unit staff provided various briefings. Additionally, the FBI responded to many document requests from the GAO, and participated in several teleconferences to answer questions over a 12-month period.

**DISCUSSION AND ANALYSIS**

In May 2016, the GAO published its findings of an audit conducted of the FBI's use of facial recognition technology. As a result, the GAO recommended that the Director of the FBI conduct an operational review of the NGI-IPS at least annually that includes an assessment of the face

recognition searches to determine if it is meeting federal, state, and local law enforcement needs and take actions, as necessary, to improve the system.

In response to this recommendation, the FBI has notified the GAO that it plans to solicit user feedback through the Advisory Policy Board (APB) Process regarding whether the NGI-IPS face recognition searches are meeting their needs. As of April 2017, there are 11 states that are connected to the NGI-IPS. The FBI's FACE Services Unit is requesting APB and associated user feedback in utilizing the NGI-IPS as it relates to items such as, but not limited to: ease of use of the system, the value of the information received, success stories, and recommendations for improvement. This action should address the intent of the GAO recommendation and demonstrate reasonable assurance that the NGI-IPS is meeting federal, state, and local law enforcement needs. Comments may be forwarded to the FACE Services Unit at the following email: <fr\_ips@leo.gov>.

**FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

**FALL 2017 IS SUBCOMMITTEE ACTION:**

Accepted as information only.

**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #4**

Proposal to Require Training for Those Conducting Face Recognition Searches of the Next Generation Identification (NGI) / Interstate Photo System (IPS)

**PURPOSE**

To present a proposal to require training in order to search the NGI/IPS.

**POINT OF CONTACT**

Biometric Services Section, Facial Analysis, Comparison, and Evaluation Services Unit

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the information included in this paper and provide recommendations regarding the proposal to require training for all NGI/IPS users.

**BACKGROUND**

The FBI's NGI System deployed an enhanced IPS in September 2014. As part of the enhanced photo search capability, the IPS provides an investigative Face Recognition Search (FRS) component. An FRS consists of an automated comparison of features from a probe photo against face photos associated with a criminal identity within the IPS repository.

Pursuant to the *NGI IPS Policy and Implementation Guide*, only sworn law enforcement officers may perform face recognition searches of the IPS for authorized law enforcement purposes. The photos available for searching by federal, state, and local law enforcement officers are limited to criminal mugshot photos associated with tenprint fingerprints.

Authorized law enforcement agencies may upload a probe photo collected pursuant to a lawful criminal investigation to be searched against the IPS. Agencies accessing the IPS must protect the Constitutional rights of all persons and cannot search photos against the IPS that have been obtained in violation of an individual's First and Fourth Amendment rights. The FBI protects Constitutional and other statutory rights when its FACE Services Unit searches the IPS in support of FBI agents. In order to search against the NGI/IPS, the probe photos must be obtained pursuant to open investigations and assessments that meet the legal standards of the

Attorney General Guidelines for FBI Domestic Operations. These Guidelines require compliance with the Privacy Act and prohibit the collection of information based solely on the exercise of First Amendment or other Constitutional rights.

The automated searching of the IPS benefits authorized law enforcement users by producing a list of possible candidates to be considered for further investigation. The NGI face recognition technology does not provide a positive identification in the search results; the list of possible candidates provided is strictly intended to serve as an investigative lead.

For FBI cases supported by the FACE Services Unit, the list of possible candidates returned by the IPS is examined by a trained FBI Biometric Images Specialist. These trained specialists analyze, compare, and evaluate the list of possible candidates to determine if a likely match to the probe photo exists. After trained specialists perform three levels of manual review, the final investigative result is returned to the FBI agent. The FBI agent receives a caveat that the final result is an investigative lead only and may not be relied upon to pursue legal action.

This two-part process (i.e. the automated software comparison and the review by a trained human examiner) aligns with both the National Institute of Standards and Technology recommendations and industry standards for FRS performed in a one-to-many, investigation-mode environment. However, when IPS candidate lists are returned to the FBI's law enforcement partners, there is no guarantee that the candidates will be reviewed by a trained specialist or by anyone who has received face recognition training.

The NGI/IPS and face recognition technology are relatively new enhancements that have come under extensive scrutiny by the public, media, and members of Congress. The accuracy of the technology and the need for a human review of candidate lists have been frequent areas of concern. In May 2016, the United States Government Accountability Office (GAO), issued a report after concluding a year-long review of the FBI's use of face recognition technology. During FBI testimony before the House Oversight and Government Reform Committee in March 2017, the GAO report was discussed extensively and questions ensued regarding privacy, accuracy and training. In addition, numerous privacy and advocacy groups, academia, and non-profit organizations have challenged the use of the FBI's face recognition technology. *Required* face recognition training for users of the NGI/IPS may address some concerns raised by these entities, as well as comporting with industry best practices.

## **DISCUSSION AND ANALYSIS**

The current IPS Policy and Implementation Guide, Version 1.3 (dated April 23, 2015), describes policy, operational, and technical considerations for authorized users of the IPS. The IPS Policy and Implementation Guide addresses the subject of training as follows:

### Appendix A: ADDITIONAL SUPPORT FOR FR A.1 Training

The CJIS Division *encourages* the user community to obtain FR training prior to utilizing any FR System. The CJIS Division's Biometric Training Team (BTT) offers Face

Comparison and Identification training to external law enforcement and national security agency personnel. If interested, contact the BTT at (304) 625-5279 or <biometric\_training@leo.gov>. A complete list of course offerings is available online at <[www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/fingerprint-criminal-history-record-training](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/fingerprint-criminal-history-record-training)>.

The above language does not specifically address the use of the NGI/IPS, nor does it require training for access to the NGI/IPS. Eleven states, the District of Columbia Metropolitan Police Department and the FBI's FACE Unit, have conducted face recognition searches of the FBI'S NGI/IPS since April 2015. The majority of those have received face recognition training through a variety of sources including private industry, state trainers, the FBI CJIS Division, and other government agencies. Please note that current users of the system that have not received training would have a grace period of approximately eight months to receive the training before the requirement is made official by the FBI Director.

Agencies/states who utilize other CJIS Systems are required to obtain training. Examples include users of the National Crime Information Center and the National Law Enforcement Data Exchange systems. The FBI CJIS Division's Biometric Training Team, offers Face Comparison Identification Training (FCIT) to external law enforcement and national security agency personnel. FCIT is twenty four hours of classroom training designed for individuals with limited experience in face comparison and identification, yet have a current or upcoming operational need. The three day training covers the following topics: Basic Face Comparison, image conditions and processing, and hands on exercises.

Required training for those conducting face recognition searches of the NGI/IPS would be patterned after the Facial Identification Scientific Working Group (FISWG) "Guidelines and Recommendations for Facial Comparison Training to Competency," Version 1.1, dated 11/18/2010 (attached as a separate document to this paper). The mission of the FISWG is to develop consensus standards, guidelines and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities to advance the state of the science in this field.

The purpose of the FISWG "Guidelines and Recommendations for Facial Comparison Training to Competency" document, Version 1.1, is "to provide guidance on the relevant subject matter to the individual so that upon the completion of training they will be able to conduct comparisons at the basic level or at the advanced level." Completion of the FBI's FCIT training would ensure that the trainee has received the proper training to meet the FISWG guidelines and recommendations.

## **OPTIONS**

The Subcommittee is asked to discuss this proposal and approve one of the following options:

**Option 1:** Require training for agencies/states prior to conducting face recognition searches of the NGI/IPS. Required training is identified as completion of the FBI's Facial Comparison and

Identification Training (FCIT) class which meets the “Guidelines and Recommendations for Facial Comparison Training to Competency,” as outlined by the Facial Identification Scientific Working Group.

If approved the verbiage under Option 1 would be added to the IPS Policy and Implementation Guide, as follows:

Appendix A: ADDITIONAL SUPPORT FOR FR  
A.2 Required Training

The FBI CJIS Division requires training for agencies/states prior to conducting face recognition searches of the NGI/IPS. Required training is identified as completion of the FBI’s Facial Comparison and Identification Training (FCIT) class which meets the “Guidelines and Recommendations for Facial Comparison Training to Competency,” as outlined by the Facial Identification Scientific Working Group.

**Option 2:** Make no change.

**RECOMMENDATION:** The FBI CJIS recommends Option 1.

**FALL 2017 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 with 22 Yay/1 Nay

**NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper.

**Action:** Motion carried with one opposed.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1, as amended (additions in *red, bold italics*): Require training for agencies/states prior to conducting face recognition searches of the NGI/IPS. Required training is identified as completion of the FBI’s Facial Comparison and Identification Training to Competency,” as outlined by the Facial Identification Scientific Working Group. *The FBI CJIS is tasked with exploring options that would establish competency and report those options to the working groups at the Spring 2018 meetings.*

If approved the verbiage under Option 1 would be added to the IPS Policy and Implementation Guide, as follows:

Appendix A: ADDITIONAL SUPPORT FOR FR  
A.2 Required Training

The FBI CJIS Division requires training for agencies/states prior to conducting face recognition searches of the NGI/IPS. Required training is identified as completion of the FBI's Facial Comparison and Identification Training (FCIT) class which meets the "Guidelines and Recommendations for Facial Comparison Training to Competency," as outlined by the Facial Identification Scientific Working Group.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper.

**Action:** Motion carried.

**FALL 2017 IS SUBCOMMITTEE ACTION:**

**Motion:** For the following: Require CJIS Systems Agency/State Identification Bureau approved training for individuals of agencies/states prior to conducting face recognition searches of the NGI/IPS. Training must be consistent with the "Guidelines and Recommendations for Facial Comparison Training to Competency," as outlined by the FISWG.

**Action:** Motion carried.





**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #5**

Final Seven of Ten Solution Update and Future Concepts

**PURPOSE**

To provide a final six month update and to discuss future concepts regarding the NGI (Next Generation Identification) System Seven of Ten Solution.

**POINT OF CONTACT**

Biometric Services Section, Latent Forensic Support Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the information included in this paper and discuss the different concepts suggested concerning swapping of fingerprint images.

**BACKGROUND**

This topic paper is in response to several discussions and requests made by both the National Crime Prevention and Privacy Compact (Compact) Council's (Council) National Fingerprint Qualification Requirements Focus Group and the CJIS Advisory Policy Board (APB) concerning the reduction of rejects based on quality.

**DISCUSSION AND ANALYSIS**

The Compact Council requested CJIS Division to address recommendations for possible NGI System and Electronic Biometric Transmission Specification (EBTS) modifications aimed at reducing fingerprint image quality rejects. To address this request, the "Seven of Ten Solution" NGI System enhancement (referred to as Seven of Ten Processing) was implemented on November 10, 2016.

During the discussion of the Seven of Ten Processing at the October 2016 Identification Services Subcommittee (ISS) meeting, the CJIS APB requested the FBI CJIS Division to look at the

possibility of swapping the better quality plain images with the poor quality rolled images that were removed by the NGI System during the Seven of Ten Processing. They also mentioned the possibility of replacing the removed images with the distals from palm prints if they were included in the submission.

The following information is provided as a refresher on how the NGI System views and processes transactions in reference to the quality of the images supplied in the submission. Fingerprint image quality is commonly defined as a measure of the clarity and extractability of the minutiae used in recognition for fingerprint matcher algorithms. The NGI System assigns a quality metric to fingerprint submissions; each individual finger image is given an image quality score, and is averaged to an overall quality score. This score is based on the clarity, completeness, and extractability of the fingerprint minutiae provided. Tenprint submissions must meet or exceed the overall quality score requirements to result in a high confidence response from the NGI System. Before Seven of Ten Processing, the tenprint submission retained the quality scoring assigned by the NGI System with no adjustment, and returned an L0008 Reject Message (“the quality of characteristics is too low to be used”), if the image quality score did not meet the minimum requirements. With the implementation of Seven of Ten Processing, up to three low scoring images are now eliminated if scoring does not meet quality scoring requirements. When the NGI System removes a low scoring image, the average score increases. This adjustment can result in a quality score increase to a level in which a high confidence response can be returned to the contributor. While Seven of Ten Processing can elevate the overall image quality score average and prevent L0008 rejects when high quality fingerprint images are available, the elimination of up to three prints results in an incomplete tenprint image. Those fingerprint images are only visible for the FBI Fingerprint Examiner for fingerprint image comparison. The UP stamped fingerprint images are no longer visible on the master composite record for this event or searchable for future submissions. However, the NGI System does retain rolled and plain images; therefore, swapping the rolled image for the plain image is only duplicating an image already retained within the NGI System.

The ISS members and the FBI staff agreed this topic would be discussed after review of six months of statistical data after the Seven of Ten Processing implementation and ample time for Information Technology (IT) staff review of the suggested system enhancements. The first six months reflected at least 44.79% reduction in L0008 rejects with approximately 81% of those being civil submissions and 19% being criminal submissions. The full statistical data averages for the first six months of Seven of Ten Processing is as follows:

- 55.82% Right little finger stamped UP
- 71.37% Left little finger stamped UP
- 12.86% Right ring finger stamped UP
- 21.58% Left ring finger stamped UP
- 4.48% Right middle finger stamped UP

6.31%	Left middle finger stamped UP
4.79%	Right index finger stamped UP
6.51%	Left index finger stamped UP
1.24%	Right thumb finger stamped UP
1.70%	Left thumb finger stamped UP
0.49%	Both index fingers stamped UP

This topic paper is to initiate open discussions concerning the different methods of swapping of fingerprint images, the advantages and disadvantages of doing so, and what next steps are suggested by the user community with this type of system change.

**FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

**FALL 2017 IS SUBCOMMITTEE ACTION:**

Accepted as information only.



**Disclaimer:**

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available), and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: [FISWG@yahoogroups.com](mailto:FISWG@yahoogroups.com).

**Redistribution Policy:**

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.



## Section 3

### *Guidelines and Recommendations for Facial Comparison Training to Competency*

#### Introduction

With growing use of one-to-one facial examinations and automated facial recognition systems, the need for trained individuals to perform facial comparisons is increasing. In addition, the recommendations provided in the National Academy of Sciences' report, *Strengthening Forensic Science in the United States: A Path Forward*<sup>1</sup>, include the need for sufficient training. The purpose of this document is to provide the recommended elements of training to achieve competency in facial comparisons. Future FISWG documents will address the elements described in this document in greater detail. The level of training necessary to conduct facial comparison is dependent upon the quality of images that are being analyzed and the purpose of the analysis.

The task of facial review in an investigative capacity includes, but is not limited to, the use of a facial recognition system to review one-to-many galleries. For example, an officer at a booking station will conduct a one-to-many search of a controlled image against a database of controlled images. This task may also include applications involving high volume throughput. These reviewers require a basic level of training to acquire general knowledge and comprehension of the technology and major elements of the facial comparison discipline.

The task of facial examination includes, but is not limited to, a rigorous one-to-one analysis, comparison, and evaluation of controlled and uncontrolled images for the purpose of effecting a conclusion. Examiners in this situation have to draw on a larger foundation of knowledge, skill, and ability to accurately reach their conclusions. Additionally, the articulation of the scientific and legal basis for the expression of conclusions for many forensic, intelligence, or law enforcement purposes requires an even more advanced level of training to include an expanded set of knowledge, skills, and abilities above the level of basic concepts.

The purpose of this document is to provide guidance on the relevant subject matter to the individual so that upon the completion of training they will be able to conduct comparisons at the basic level or at the advanced level.

#### Training for Facial Review

##### *Basic Level*

General Knowledge:

The trainee should be familiar with the history of facial comparisons in forensic science to include past methods, such as the Bertillion method, and their shortcomings. In addition, they should also understand the perception of facial recognition in the legal community.

Both the principles of individuality and the principles of permanence should be examined. The trainee must be able to distinguish between class and individual characteristics, as well as transient and stable characteristics.

The trainee must understand common terminology and the definitions used within the relevant community, such as the distinction between human facial recognition, automated facial recognition, and facial identification.

An understanding of the principles of comparison should be demonstrated. These principles include:

- Assessment of facial image quality to determine the value for examination

<sup>1</sup> *Strengthening Forensic Science in the United States: A Path Forward* ([http://www.nap.edu/catalog.php?record\\_id=12589#toc](http://www.nap.edu/catalog.php?record_id=12589#toc))

- Process of Analysis, Comparison, Evaluation and Verification (ACE-V)
- Methods of comparisons (see One-to-One Facial Examination Overview)
- Levels of conclusion
- Ability to render proper conclusions
- Overview and effects of cognitive bias, to include confirmation bias
- Understanding of the benefits of verification by a second qualified reviewer/examiner

The trainee should have a general knowledge of automated biometric systems. This includes, but is not limited to, user input and operation, system operation and output, and the limitations of the technology, such as the ability of the technology to distinguish between twins and the impact of disguises and image quality.

The basics of image science are a critical component for the trainee to demonstrate an understanding of, to include:

- Vision
  - Color
  - Illumination
- Photography
  - General principles
  - Hardware and settings
- Perspective
  - Camera to subject distance
  - Angle of view
- Digital images and compression

When applicable, the trainee should be skilled in proper handling of media, write protection of that media, and generating working copies.

Facial Knowledge:

The trainee should be familiar with the bones that comprise the skull and the overlying musculature. An awareness of the varying features of the skin, hair, and hairlines, and their level of permanence, should be obtained. Additionally, anthropometric landmarks, general nomenclature of the facial shapes, and the properties of the ear should be reviewed.

Due to the variable nature of the human face over time, the results of aging must be understood. The trainee should also be aware of other alterations of the face, both temporary and permanent. Examples of temporary changes are: cosmetics, weight changes, hair color changes, wounds, and abrasions. Permanent changes may include: scars, surgical alterations, dental changes, tattoos, and piercings.

Legal/Justice Issues (for examiners who may testify):

Individuals testifying to facial review must be aware of the implications of the relevant judicial decisions that govern admittance of scientific evidence in court. Additionally, attention must be paid to issues such as proper chain of custody, documentation and notes, reporting of results, and technical review.

The trainee should be aware of common misconceptions created by popular media to include fictional television shows, novels, and movies, cumulatively known as 'The CSI Effect'.

## **Training for Facial Examination**

### ***Advanced level***

General Knowledge:

The trainee must be able to summarize the history of facial comparisons in forensic science to include past methods, such as the Bertillion method, and their shortcomings. In addition, they should be able to demonstrate knowledge of the perception of facial recognition in the legal community. Likewise, the trainee must be able to summarize the history of forensic photographic comparisons.

The trainee must be able to define the principles of individuality and the principles of permanence. The differences between class and individual, as well as transient and stable characteristics, must also be compared and contrasted.

The trainee must be able to apply common terminology and the definitions used within the relevant community, to include the distinction between human facial recognition, automated facial recognition, and facial identification.

A comprehensive working knowledge of the principles of comparison must be demonstrated. These principles include:

- Assessment of facial image quality to determine the value for examination
- Process of Analysis, Comparison, Evaluation and Verification (ACE-V)
- Methods of comparisons (see One-to-One Facial Examination Overview)
- Models of Evaluation and Interpretation
- Levels of conclusion
- Ability to render proper conclusions
- Overview and effects of cognitive bias, to include confirmation bias
- Understanding of the benefits and limitations of review by a second qualified reviewer/examiner

The trainee must have an in-depth knowledge of automated biometric systems. If the agency does not utilize an automated biometrics system, the trainee should have a general knowledge of these systems. This knowledge includes user input and operation, system operation and output, and the factors that affect the performance of the technology, such as the ability to distinguish between twins and the impact of disguises and image quality. Additionally, general biometric matching algorithms should be understood.

The trainee must demonstrate and understand the principles of image science to assist in predicting the effects of photographic processes. This includes:

- Vision
  - Color
  - Illumination
  - Perception
- Photography
  - General principles and theory
  - Hardware and settings
  - Lens properties and potential distortions
  - Illumination of scene and subject
  - Human factors, such as pose and expression
- Perspective
  - Camera to subject distance
  - Angle of view
- Components of digital images and compression
  - Knowledge of sensors, pixels, and resolution
- Methods for the detection of manipulation within images
- Properties of video

The trainee must be skilled in proper handling of media, write protection of that media, and generation of working copies.

Tasks involving image processing may be necessary in facial examination. Therefore, the trainee must demonstrate competency in performance of a range of processing tasks to include, but not limited to, the following:

- Brightness and contrast adjustments
- Rotations and cropping
- Sharpening and blurring
- Scaling and overlays
- Color channel separation
- Effects of image adjustments and enhancements

Facial Knowledge:

The trainee must be able to locate the bones that comprise the skull. Similarly, the knowledge of the overlying musculature and anatomical function must be articulated. The trainee must demonstrate a thorough understanding of the varying features of the skin, hair, and hairlines, and their level of permanence. Additionally, general nomenclature of the facial shapes must be demonstrated. The trainee should be aware of available and relevant statistics regarding facial shapes and relative frequency of occurrence within the general population and subpopulations (e.g., ethnic groups).

Knowledge of the history of ear comparisons, to include the distinction between analysis of ear prints and ear imagery,



must be described. An ability to identify the features of the ear and knowledge of the general nomenclature must be demonstrated.

Due to the variable nature of the human face over time, the results of aging must be understood to include, but not be limited to, predicting the common locations of wrinkles. The trainee must also be aware of other alterations of the face, both temporary and permanent. Examples of temporary changes are: cosmetics, weight changes, hair color changes, wounds, and abrasions. Permanent changes may include: scars, surgical alterations, dental changes, tattoos, and piercings.

Legal/Justice Issues (for examiners who may testify):

Individuals testifying to facial examinations must know the implications of the relevant judicial decisions that govern admittance of scientific evidence in court. Additionally, attention must be paid to issues such as proper chain of custody, documentation and notes, reporting of results, and technical review. The history of photographic comparisons in court and relevant case law should be understood.

The trainee must be competent in explaining the process of facial examinations to the jury, the limits of the relevant science and technology, and the creation of visual aids. This competency should be demonstrated through the process of moot courts and/or mock trials.

Lastly, the trainee should be aware of common misconceptions created by popular media to include fictional television shows, novels, and movies, cumulatively known as 'The CSI Effect'.

## Reference List

FISWG documents can be found at:  
[www.FISWG.org](http://www.FISWG.org)

<b>Section</b>	<b>Title</b>
Section 1	Glossary
Section 2	Facial Comparison Overview
Section 3	Guidelines and Recommendations for Facial Comparison Training to Competency
Section 4	Guidelines for Specifications, Procurement, Deployment, and Operations of Facial Recognition Systems
Section 5	
Section 6	
Section 7	
Section 8	
Section 9	
Section 10	



**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #6**

Criminal History Update

**PURPOSE**

To provide an update for all criminal history information projects which includes updates on dispositions, Automated Disposition and Processing Technology (ADAPT), non-serious offenses (NSOs), and updating of pseudo-pointer records.

**POINT OF CONTACT**

Biometric Services Section, Criminal History Information and Policy Unit (CHIPU)

Questions regarding this topic should be directed to <agmu@leo.gov>.

**BACKGROUND**

The CHIPU supports the criminal justice and the noncriminal justice (civil) 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 all criminal history information projects, which includes dispositions, ADAPT, NSOs, and updating of pseudo-pointer records.

**Dispositions within the Next Generation Identification (NGI) System**

**FBI Field Office Arrests:** 88 percent of all FBI Field Office arrests have dispositions. The remaining 12 percent are arrests missing dispositions, including arrests which have not been adjudicated.

**Federal Arrests:** 60 percent of all federal arrests have dispositions. The remaining 40 percent are arrests missing dispositions, including arrests which have not been adjudicated.

Multiple efforts are underway to identify federal dispositions (including dispositions for FBI Field Office arrests).

- The U.S. Courts are submitting dispositions for all individuals under federal supervision.

- Discussion is ongoing with the U.S. Attorney’s Office regarding cases which were not referred for prosecution.
- Multiple federal agencies have been provided details of arrests missing dispositions.
- The FBI contractors, Ruchman Associates Incorporated, are researching dispositions.

**State Pseudo-Pointer Arrests<sup>1</sup>:** 44 percent of all state pseudo-pointer arrests have dispositions. The remaining 56 percent are arrests missing dispositions, including arrests which have not been adjudicated. The priority is to establish state identification numbers (SIDs) within the pseudo-pointer arrest events. Multiple efforts are underway to support states establishing SIDs for pseudo-pointer arrests and/or to identify dispositions.

- Biometric, biographic, and arrest information for pseudo-pointer records have been supplied to multiple states.
- Correlation information has been provided to multiple states
- Microfilm records were provided upon request.
- The Interstate Identification Index (III) Disposition Message Key (DSP) has been modified to include the submission of dispositions for pseudo-pointer records by all states.
- The FBI will research dispositions, with the concurrence of the individual state.

**State Arrests:** As background, the NGI System relies on a decentralized exchange of criminal history record information (CHRI).<sup>2</sup> In addition to the CHRI, the NGI System uses “pointers” contained within the system to direct searches to records maintained by state agencies. These pointers also indicate whether a state or other federal agency, or the FBI, is responsible for the maintenance and dissemination of the various portions of the record.

For example, when a fingerprint submission sent to the FBI matches a state-maintained record, and the state’s policy supports disseminating information for the purpose for which the fingerprints were submitted (e.g., licensing), the NGI System follows the pointer and automatically sends a message to the state that holds the record and appends the state record to the FBI’s NGI System response. The state information stored within the NGI System identified with the pointer is dropped from the response to reduce the risk of duplication. Therefore, although a disposition may be missing from the CHRI on the FBI record, the disposition may be available on the state-appended CHRI. In the majority of cases, adjudicators are provided CHRI

<sup>1</sup> The CHRs are indexed in the NGI System by either a state-active pointer, indicated by a SID or an FBI pseudo-pointer in the pointer data field. The III pointer identifies the state and federal agencies that contribute information to an individual’s record. An FBI pseudo-pointer record is established in the NGI System when either a fingerprint submission is received from a federal agency, a non-III participating state, or when the SID is not present or was previously assigned to a different individual. In this case, the FBI CJIS Division is responsible for the dissemination of the CHRI for that record subject.

<sup>2</sup> The CJIS Advisory Policy Board proposed a decentralized CHR system in April 1978. The proposal called for the FBI to receive and store CHRI from federal agencies. The states were to maintain full responsibility and control regarding the collection, collation, maintenance, and dissemination of state, county, and local CHRI.

with a greater volume of information from the state's response than what resides solely on the FBI record.

Twenty states participate in the National Fingerprint File (NFF) Program and provide CHRs for authorized uses, including criminal justice and noncriminal purposes. An NFF state submits fingerprint images for each offender's first arrest to the FBI to identify or establish the identity of the offender at the national level, but the CHRI is only maintained at the state level. As such, it is not necessary for the NFF states to submit final disposition reports and expungement orders to the FBI for records they maintain. States that participate in the NFF Program greatly increase the information available to adjudicators by providing their records for all authorized uses.

It would be inaccurate to calculate missing dispositions available to users without including the state information available to be appended to responses. The state statistical information is not available for all states, at this time.

Sixty percent of all state arrests, housed within the NGI System, were submitted from states that do not support all purpose codes. Forty-nine percent of these arrests have missing dispositions, including arrests which have not been adjudicated. All states, which do not support all purpose codes, submit dispositions electronically or are testing to do so. Teleconferences are being held to identify challenges and possible solutions to the submission of dispositions.

**Tribal Arrests:** 48 percent of all tribal arrests have dispositions. The remaining 52 percent are arrests missing dispositions, including arrests which have not been adjudicated. Dashboards were created for tribes displaying the percentage and volume of missing dispositions. Tribal agencies utilizing the Department of Justice's Tribal Access Program have the opportunity to submit dispositions via the III DSP. Discussions are underway regarding submission of missing legacy dispositions.

## **ADAPT**

The ADAPT has been designed to address concerns received from multiple external partners regarding disposition submission. The service leverages existing disposition submission methods and web-based platforms to provide enhanced methods for electronically submitting dispositions.

One of the concerns surrounded the protection of personally identifiable information (PII) during the mailing of Machine Readable Data (MRD) Computer Discs to the CJIS Division. The ADAPT service provides a method to upload bulk dispositions in the MRD format by leveraging the Law Enforcement Enterprise Portal (LEEP) Enterprise File Transfer Service (EFTS). The key technological advancement is that the MRD file is uploaded by an authorized LEEP user to their state folder within the EFTS, and the NGI System automatically retrieves and processes the file. Results are returned in a WinZip file to the state's folder on the LEEP EFTS. As of April 2017, two states piloted the method, and the CJIS Division plans to roll this out to current MRD customers in 2017. This process is called the ADAPT Bulk File Processing via the LEEP EFTS, which will protect the PII while eliminating the mailing costs.

The next phase of the ADAPT service will be the development of a web-based interface, which provides an automated ability for an agency to submit single disposition information using an online form. This service is currently in the requirement development phase and the CJIS Division plans to have more information regarding this functionality late in 2017.

### **State Pseudo-Pointer Records**

In an effort to decrease the number of pseudo-pointer records and increase state active pointers, correlations and electronic fingerprint files (also known as certification files) are being provided to a number of states for processing.

The sole purpose of a correlation is for states to identify the records in the III that the FBI supports (pseudo-pointer records) and take ownership (set the pointer) of the records that can be supported by the state. The correlation data is provided in record segments, including the identification segment, the supplemental identifiers segment, the arrest segment, the judicial segment, and the custody-supervision segment. The states compare the data in each record segment to identify records in which the state has as much or more information as the FBI. These are records that the state can support and may send the III message to set the active state pointer. As of April 2017, six states have requested correlations, resulting in approximately 1.6 million pseudo-pointer records being sent to the states for comparison and potential setting of the active pointer.

In addition, a process has been identified to provide the certification files (cert. files) for pseudo-pointer record arrests not currently on file at the state level. Guidelines and procedures were developed to provide the cert. files through the use of the LEEP EFTS, the same application currently used for the ADAPT. The cert. files are automatically uploaded from the NGI System to the state folder within the EFTS as WinZip files. The state agencies then download the files using the EFTS Upload/Download Wizard. Seven states have requested their cert. files, resulting in approximately 7 million cert. files being sent to the states. Three other states are waiting to complete their correlation before requesting their cert. files, and two additional states have received information on the process. Ultimately, these efforts positively impact the NGI System state outreach and the quality of CHRI shared for employment and licensing adjudications, firearm background checks, Rap Back services, criminal investigations and sentencing decisions.

### **NSO Vetting**

The DOJ will consider the publishing of a Notice of Proposed Rulemaking in the *Federal Register* to allow for the storage of NSOs within the NGI System when the federal or state contributor requests the retention of the fingerprint and arrest data. Title 28, Code of Federal Regulations, Section 20.32 requires the FBI to vet and remove the submitted information, if the arrest is an NSO (regardless of the contributor's retention request). Although a perception exists that NSO retention may negatively impact reentry, the removal of NSOs would also negatively affect identification in the intelligence, criminal, latent, and cold case processing. Analysis is being performed to determine the impact of the change.

**FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

Accepted as information only by the IS Subcommittee.

Accepted as information only by the National Instant Criminal Background Check System Subcommittee.





**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #7**

Rapid Deoxyribonucleic Acid (DNA) Update

**PURPOSE**

To provide an update on the FBI Booking Station Rapid DNA Initiative

**POINTS OF CONTACT**

FBI Laboratory (Lab) Division/Information Technology Management Section, Biometrics  
Technology Support Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

**BACKGROUND**

The Rapid DNA Task Force has been planning for Rapid DNA Analysis in the booking environment since April 2010 – identifying business requirements and processes, recognizing policy concerns and issues, and outlining technical enhancement and/or changes necessary for law enforcement participation. Specifically, the FBI Lab and CJIS Divisions have finalized a checklist entitled “Requirements for Rapid DNA in the Booking Environment”, as well as the “Arrestee Enrollment Format Interface Specification Document” (AEF ISD), that have been included with previous ABP Topic Papers.

These documents were developed to help guide Law Enforcement Agencies (LEAs) and Combined DNA Index System (CODIS) Labs planning for Rapid DNA integration following federal law authorizing Rapid DNA Enrollment – the submission of CODIS DNA profiles developed utilizing FBI-approved Rapid DNA systems from outside of an accredited laboratory. Both of the documents, as well as an “Executive Summary” will be posted on the FBI’s Rapid DNA webpage at: [www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna-analysis](http://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna-analysis) following a change in Federal Law authorizing booking station Rapid DNA analysis for CODIS.

During “National Police Week” (May 14-12, 2017), the House of Representatives and the Senate took action on legislation that would authorize the FBI to approve Rapid DNA instruments for

use outside of accredited laboratories (in booking stations). As of June, slight differences between the House and Senate versions of the *Rapid DNA Act of 2017* need to be addressed. In anticipation of implementation of the *Rapid DNA Act of 2017*, this topic paper highlights some of the key concepts regarding Rapid DNA Analysis that are being worked by the FBI.

### CODIS Enhancements

The CODIS 8.0 development effort by the FBI Lab Division is the largest software release of CODIS since the initial release and is planned to be implemented in January of 2018. One of its major enhancements is the CODIS Rapid Enrollment (CRE) Application (Rapid App) that will validate the DNA import or Common Message Format (CMF) file created from the AEF information required by CODIS to support the Rapid DNA enrollment and searching.

### CJIS Message Manager

When a Rapid DNA profile is submitted from the booking station and “hits” to a forensic unknown during the initial search, an Unsolicited DNA Notification (UDN) will need to be sent to all LEA’s involved. The arresting and booking agency (if different) and the investigating agency with the forensic unknown CODIS DNA profile will each receive information necessary to enable real-time contact.

To do this, the CJIS Message Manager (CMM) will manage Rapid Hit Notifications from CODIS and will send the UDN messages to the specified LEAs utilizing existing messaging capabilities similar to “Wants and Warrants” to communicate Rapid DNA hit notifications. To do this, the CMM will utilize the Electronic Fingerprint Conversion (EFCON) International Justice and Public Safety Network (Nlets) Adapter. This adapter manages all Nlets-related messaging as SOAP-based Web Services, separate and outside of biometric transaction processing within the Next Generation Identification (NGI) system. The FBI Lab and CJIS Divisions anticipate being ready to test messaging between the CMM and CODIS in August of 2017.

### Rapid DNA Video

In addition to the documents to be made available online, the FBI Rapid DNA Program Office plans to provide additional outreach information about Rapid DNA Analysis to the Law Enforcement and CODIS communities. Specifically, a “Rapid DNA in the Booking Station” video scripted by the APB’s Rapid DNA Task Force to outline the integration of Rapid DNA within the booking process will be finalized and made available following a change in Federal Law. The video will demonstrate best practices for the booking station collection of DNA samples when an Arrestee is processed. Scenarios for Rapid DNA processes involving Enrollment and Hit Notification will also be included in the video. The “Rapid DNA in the Booking Station” video will also be posted on the FBI’s webpage once finalized and approved – [www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna-analysis](http://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna-analysis).

### Booking Station Rapid DNA Policy, Procedure and Standard Considerations

Introduction of Rapid DNA and CODIS access to Booking Stations has necessitated consideration of authority with regard to a number of FBI responsibilities such as: User access; governance; DNA collection procedures; DNA analysis standards; and, quality assurance audits and corrective actions. The CJIS APB's Rapid DNA Task Force has concluded the FBI Lab Division and its CODIS Unit should be responsible for coordinating the applicable policy agreements (e.g. Authority to Operate [ATO], Booking Station Collection Procedures, DNA Analysis Standards, MOU or other User Agreements). The FBI CJIS Division will provide SME input regarding booking and auditing procedures in addition to ATO, MOU, and User Agreement examples. In fact, a meeting discussion between the Lab's CODIS Unit and the CJIS Audit Unit was held on October 3, 2016.

### Rapid DNA Pilot

Initially, participation by (LEAs in booking station Rapid DNA Pilots will be restricted and monitored. The FBI CODIS Unit will work with State DNA Index System Agencies in States with DNA arrestee laws for initial pilot studies. The Rapid DNA Program Office is considering plans for pilots involving Federal Arrestees and one or more States that could participate within six months of a change in federal law. A series of Rapid DNA Pilots will provide monitored participation for test and evaluation of Booking Station DNA analysis enrollment software, IT connectivity and booking station procedures needed for efficient Rapid DNA integration into Arrestee States across the country.

### Vendor Day

Additionally, a "Rapid DNA Business Day" similar to the one held in November 2014 at the CJIS Division, has been proposed to bring representatives together from both the CODIS, Law Enforcement, Rapid DNA and Live-Scan communities. Specifically, the event would be for LEAs and the private sector to discuss pilot implementation, education/outreach, policy, procedure and standard development, along with other issues and concerns. This meeting will occur within two months following a change in Federal Law authorizing booking station Rapid DNA analysis for CODIS.

### **NEXT STEPS**

The FBI Lab and CJIS Divisions will continue to coordinate follow-up, Rapid DNA planning discussions with the APB Rapid DNA Task Force. The next Task Force meeting is planned for August 23-24, 2017 at the CJIS Division.

## **FALL 2017 WORKING GROUP ACTIONS:**

### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Action:** Motion carried.

### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Action:** Motion carried

### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Action:** Motion carried.

### **SOUTHERN WORKING GROUP ACTION:**

**Motion:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA profiles to CODIS.

**Action:** Motion carried.

### **WESTERN WORKING GROUP ACTION:**

**Motion:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Action:** Motion carried.

### **FALL 2017 IS SUBCOMMITTEE ACTION**

**Motion:** To accept option two as recommended by the Task Force, “The FBI shall issue guidance on the limited use of Rapid DNA devices, including the specific prohibition against enrolling and searching of crime scene evidence developed from Rapid DNA devices in CODIS.”

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #9**

Update on Fusion Center Access to Criminal Justice Information Services (CJIS)  
Division Systems

**PURPOSE**

To provide an update regarding the CJIS Division's efforts to fulfill the CJIS Advisory Policy Board's (APB's) recommendations regarding fusion center access to CJIS Division systems.

**POINT OF CONTACT**

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**

The Subcommittee is requested to review the information presented in this paper, and provide comments and recommendations to the APB.

**BACKGROUND**

There are currently 78 fusion centers recognized by the Department of Homeland Security (DHS) operating within the United States and its territories. The National Fusion Center Association (NFCA) reports a small number (less than nine) of these fusion centers lack direct access to the systems managed by the Federal Bureau of Investigation's (FBI's) CJIS Division. This lack of direct access, as reported, creates difficulties from an information-sharing standpoint. The vast majority of fusion centers are either established directly within a criminal justice agency (CJA), and that CJA controls the terminal access within the fusion center, or the fusion centers leverage a partnering CJA's access. As research indicates, other partnering CJAs, (e.g., police departments, sheriff's offices, etc.) working within a fusion center also establish their own terminal access within that fusion center to support their criminal investigation needs.

Access to CJIS Division systems is governed by Title 28, Code of Federal Regulations (C.F.R.), Part 20, which stipulates the types of agencies and the functions those agencies must perform to qualify for access. To qualify for access to CJIS Division systems, an agency must be a CJA or a subunit of a noncriminal justice agency, performing the administration of criminal justice as a primary function (interpreted by the Department of Justice (DOJ) to mean more than 50 percent of the agency's annual budget supports criminal justice functions). The functions which are considered the administration of criminal justice are specified in 28 C.F.R. §20.3(b), and include detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

The primary function of these fusion centers is to compile and share information to support the detection of criminal and terrorist activity. The term "detection" as it relates to the administration of criminal justice must be predicated on an "articulable suspicion" to justify a query of CJIS Division systems. Under the CJIS Division's review, the functions of the fusion centers lacking access did not conclusively meet the threshold requirements in 28 C.F.R. §20.3(b) to be considered the administration of criminal justice.

The compilation, analysis, and sharing of generalized or nonspecific threat information is not considered the administration of criminal justice. The fusion centers lacking direct access which have directly engaged the CJIS Division have been unable to provide documentation to support their primary function is the detection of articulable or specified criminal or terrorist activity. In some cases, the CJIS Systems Agencies (CSAs), for the states of the fusion centers in question, do not support granting direct access to those fusion centers and recommend for a CJA to control the access. For information, CSAs control access to CJIS Division systems for all agencies within their state or territory.

## **DISCUSSION AND ANALYSIS**

A topic was presented at the Spring 2016 Advisory Process meetings. The APB recommended for the CJIS Division and FBI's Office of General Counsel (OGC) to identify a long-term solution to fusion centers lacking direct access to CJIS Division systems and bring the solution(s) back through the Advisory Process for consideration. The APB also moved, pending the outcome of the FBI's review of a long-term solution, to grant fusion centers interim access through the use of management control agreements. This would facilitate access to CJIS Division systems through the management control of a CJA. The CJIS Division is aware of at least one state where this interim solution is currently being implemented.

Throughout this process, the CJIS Division has been engaged with the criminal justice community, the NFCA, the DHS, and the International Association of Chiefs of Police. In addition, the CJIS Division's Assistant Director served on the DOJ Criminal Intelligence Coordinating Council and provided substantial input on the topic of fusion center access.

To fulfill the APB’s recommendation, the CJIS Division and the OGC have collaborated to propose the option to formalize the interim solution stated above by clarifying the existing language in the regulation. The regulation changes will clarify language to definitively authorize a criminal justice agency to enter into a management control agreement with a noncriminal justice governmental agency to perform criminal justice functions on its behalf. A modification to the definition of a CJA under 28 C.F.R. §20.3(g) to include fusion centers was originally discussed during the Spring 2016 Advisory Process discussions, but the APB requested further exploration before making a final recommendation. After consideration of the discussion during the Advisory Process meeting and other engagement with the user community, the CJIS Division and the OGC determined a clarification of the language within 28 C.F.R. §20.33 (a)(6) may be a better option to accomplish this goal. Currently, 28 C.F.R. §20.33 (a)(6) reads, “To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies.” The proposed changes to 28 C.F.R. §20 will memorialize the ability for noncriminal justice governmental agencies, such as the small number of fusion centers lacking direct access, to enter into agreements with CJAs to perform the administration of criminal justice functions on behalf of the CJA. Should this proposed regulation change be endorsed, it should be noted it is a lengthy administrative process that could take many years to accomplish.

Another point to consider is the current administration’s Executive Order 13771 to limit new regulations. On January 30, 2017, the President signed Executive Order 13771, which states “that for every one new regulation issued, at least two prior regulations be identified for elimination . . . .” This Order affects not only the Department of Justice, but all Federal Executive Agencies, and it has brought the federal regulatory amendment process to a near halt. The APB can be assured that if the proposed language under Option 1 is accepted, the FBI will perform due diligence to move the proposed language change forward.

The Subcommittee is requested to provide input on the information provided in this paper and provide recommendations regarding the following options.

## **OPTIONS**

### **Option 1**

Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*



## **Option 2**

No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

## **Option 3**

Discontinue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

### **RECOMMENDATION**

The NCIC Operations and Policy Unit recommends Option 1.

### **FALL 2017 WORKING GROUP ACTIONS:**

#### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

#### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA. FBI Action: FBI should continue to research various scenarios which may result from any proposed regulatory change. Continue with the interim solution.

**Action:** Motion carried with 11 Yay/11 Nay, Chair broke the tie with a Yay vote

#### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2. No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1. Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

**IS SUBCOMMITTEE ACTION:**

**Motion:** To accept a revised Option 1: "Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a) (6) as the long term solution to facilitate access to CJIS Division systems, which would grant criminal justice agencies the same authority to contract with noncriminal justice governmental agencies as they currently have to contract with private entities. Accept the language as proposed below:

*6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency."*

**Action:** Motion carried.

**N-DEx SUBCOMMITTEE ACTION:**

Accepted as information only.

**NCIC SUBCOMMITTEE ACTION:**

**Motion:** Recommendation to the Identification Services Subcommittee for Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as

private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**SA SUBCOMMITTEE ACTION:**

**Motion:** To recommend Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**IS ISSUE #10**

Next Generation Identification (NGI) Face Recognition Candidate List Accuracy

**PURPOSE**

To provide a summary of recent testing performed to validate NGI face recognition accuracy performance for candidate lists of various lengths.

**POINT OF CONTACT**

Global Operations Section, Programs Research and Standards Unit (*formerly the Biometric Center of Excellence Unit*)

Questions regarding this topic should be directed to <agmu@leo.gov>.

**BACKGROUND**

The goal of NGI's automated face recognition technology was to expand the Interstate Photo System (IPS) capability and enhance existing photo investigation services. Established performance criteria required the NGI IPS face recognition technology to return the correct subject a minimum of 85% of the time within the top 50 candidates when a mate exists in the photo repository. Performance criteria were chosen based on (1) benchmark information available for vendors within the face recognition industry, (2) feedback from the NGI user canvass, and (3) consultation with face recognition subject matter experts and the Face Identification Scientific Working Group (FISWG). The automated face recognition algorithm chosen for implementation within NGI IPS was tested<sup>1</sup> and proved compliant with the performance criteria.

On March 22, 2017 the FBI's Criminal Justice Information Services (CJIS) Division testified before the House Committee on Government Reform and Oversight on the FBI's use of automated face recognition technology. In the wake of that hearing, the Chairman and Ranking Member of the Committee sent a letter dated May 17, 2017 to Acting FBI Director McCabe requesting the FBI begin accuracy testing of the NGI IPS face recognition technology for all allowable candidate list sizes (which are 2-50). Accuracy testing has been completed as requested.

---

<sup>1</sup> NIST Multiple Biometric Evaluation (MBE), Report on the Evaluation of 2D Still-Image Face Recognition Algorithms, 2010

The ability of the NGI IPS facial recognition technology to return the correct subject for the given candidate list size is detailed in Table 1. Results are based on 50,076 searches of a photo repository of 6,173,009 images<sup>2</sup>. This testing was performed leveraging current NGI IPS operational settings for the MorphoTrust Automated Biometric Identification System (ABIS)

7.2.4 product. (Note: The referenced 2010 MBE leveraged a photo repository of 1,600,000 images.)

Candidate List Size	Accuracy (%)
2	88.200
5	89.039
10	89.646
20	90.257
30	90.640
40	90.892
50	91.078
100	91.715
200	92.388

Table 1: NGI IPS face recognition technology accuracy statistics per candidate list

Accuracy is defined as the ability of the NGI IPS face recognition technology to automatically return the correct subject in the candidate list of a given size when a mate exists in the photo repository. Results shown in Table 1 demonstrate the current FBI face recognition technology exceeds performance criteria for all allowable candidate lists.

The minimum NGI IPS provided candidate list size of two subjects continues to meet the established NGI requirements. Therefore, no recommendation will be made to adjust the minimum allowable candidate list size at this time. As noted in Table 1, slight accuracy improvements can be gained by extending candidate lists beyond 50 subjects. The FBI is consulting with the National Institute of Standards and Technology to benchmark and report on accuracy of current face recognition technology. The FBI will continue these efforts to ensure the most advanced technologies are available to law enforcement.

**FALL 2017 IS SUBCOMMITTEE ACTION:**

Accepted as information only.

---

<sup>2</sup> NGI Criminal Face Repository = 28,578,837 face images; as per the April 2017 NGI Monthly Fact Sheet

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)  
ADVISORY POLICY BOARD (APB)  
OKLAHOMA CITY, OK  
DECEMBER 6-7, 2017**

**STAFF PAPER**

**APB ITEM #10**

**Chairman's Report on the National Crime Information Center (NCIC) Subcommittee**

**NCIC ISSUE #1\***

Fugitive from Justice Discussion

**NCIC ISSUE #2**

Update on Fusion Center Access to CJIS Division Systems

**NCIC ISSUE #3**

Florida Department of Law Enforcement National Sex Offender Registry Pilot

**NCIC ISSUE #4**

Proposal to Add the Date of Expiration Field in the Wanted Person File

**NCIC ISSUE #5\*\***

CJIS Division National Crime Information Center Status

**NCIC ISSUE #6\***

N3G Task Force Status Update

**NCIC ISSUE #7**

NCIC Third Generation Project

- Concept 13 – Alternative Access;
- Concept 4 – Name Search Algorithm;
- Concept 8 – Enhanced Testing Environment;
- Concept 2 – Tailored Functionality

**\* No staff paper.**

**\*\* Issue 5 was delivered with Subcommittee Information Only staff papers as topic letter J.**



**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**NCIC ISSUE #2**

Update on Fusion Center Access to Criminal Justice Information Services (CJIS)  
Division Systems

**PURPOSE**

To provide an update regarding the CJIS Division's efforts to fulfill the APB's recommendations regarding fusion center access to CJIS Division systems.

**POINT OF CONTACT**

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**

The Subcommittee is requested to review the information presented in this paper, and provide comments and recommendations to the APB.

**BACKGROUND**

There are currently 78 fusion centers recognized by the Department of Homeland Security (DHS) operating within the United States and its territories. The National Fusion Center Association (NFCA) reports a small number (less than nine) of these fusion centers lack direct access to the systems managed by the Federal Bureau of Investigation's (FBI's) CJIS Division. This lack of direct access, as reported, creates difficulties from an information-sharing standpoint. The vast majority of fusion centers are either established directly within a criminal justice agency (CJA), and that CJA controls the terminal access within the fusion center, or the fusion centers leverage a partnering CJA's access. As research indicates, other partnering CJAs, (e.g., police departments, sheriff's offices, etc.) working within a fusion center also establish their own terminal access within that fusion center to support their criminal investigation needs.



Access to CJIS Division systems is governed by Title 28, Code of Federal Regulations (C.F.R.), Part 20, which stipulates the types of agencies and the functions those agencies must perform to qualify for access. To qualify for access to CJIS Division systems, an agency must be a CJA or a subunit of a noncriminal justice agency, performing the administration of criminal justice as a primary function (interpreted by the Department of Justice (DOJ) to mean more than 50 percent of the agency's annual budget supports criminal justice functions). The functions which are considered the administration of criminal justice are specified in 28 C.F.R. §20.3(b), and include detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

The primary function of these fusion centers is to compile and share information to support the detection of criminal and terrorist activity. The term "detection" as it relates to the administration of criminal justice must be predicated on an "articulable suspicion" to justify a query of CJIS Division systems. Under the CJIS Division's review, the functions of the fusion centers lacking access did not conclusively meet the threshold requirements in 28 C.F.R. §20.3(b) to be considered the administration of criminal justice.

The compilation, analysis, and sharing of generalized or nonspecific threat information is not considered the administration of criminal justice. The fusion centers lacking direct access which have directly engaged the CJIS Division have been unable to provide documentation to support their primary function is the detection of articulable or specified criminal or terrorist activity. In some cases, the CJIS Systems Agencies (CSAs), for the states of the fusion centers in question, do not support granting direct access to those fusion centers and recommend for a CJA to control the access. For information, CSAs control access to CJIS Division systems for all agencies within their state or territory.

## **DISCUSSION AND ANALYSIS**

A topic was presented at the Spring 2016 Advisory Process meetings. The APB recommended for the CJIS Division and FBI's Office of General Counsel (OGC) to identify a long-term solution to fusion centers lacking direct access to CJIS Division systems and bring the solution(s) back through the Advisory Process for consideration. The APB also moved, pending the outcome of the FBI's review of a long-term solution, to grant fusion centers interim access through the use of management control agreements. This would facilitate access to CJIS Division systems through the management control of a CJA. The CJIS Division is aware of at least one state where this interim solution is currently being implemented.

Throughout this process, the CJIS Division has been engaged with the criminal justice community, the NFCA, the DHS, and the International Association of Chiefs of Police. In addition, the CJIS Division's Assistant Director served on the DOJ Criminal Intelligence Coordinating Council and provided substantial input on the topic of fusion center access.

To fulfill the APB’s recommendation, the CJIS Division and the OGC have collaborated to propose the option to formalize the interim solution stated above by clarifying the existing language in the regulation. The regulation changes will clarify language to definitively authorize a criminal justice agency to enter into a management control agreement with a noncriminal justice governmental agency to perform criminal justice functions on its behalf. A modification to the definition of a CJA under 28 C.F.R. §20.3(g) to include fusion centers was originally discussed during the Spring 2016 Advisory Process discussions, but the APB requested further exploration before making a final recommendation. After consideration of the discussion during the Advisory Process meeting and other engagement with the user community, the CJIS Division and the OGC determined a clarification of the language within 28 C.F.R. §20.33 (a)(6) may be a better option to accomplish this goal. Currently, 28 C.F.R. §20.33 (a)(6) reads, “To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies.” The proposed changes to 28 C.F.R. §20 will memorialize the ability for noncriminal justice governmental agencies, such as the small number of fusion centers lacking direct access, to enter into agreements with CJAs to perform the administration of criminal justice functions on behalf of the CJA. Should this proposed regulation change be endorsed, it should be noted it is a lengthy administrative process that could take many years to accomplish.

Another point to consider is the current administration’s Executive Order 13771 to limit new regulations. On January 30, 2017, the President signed Executive Order 13771, which states “that for every one new regulation issued, at least two prior regulations be identified for elimination . . . .” This Order affects not only the Department of Justice, but all Federal Executive Agencies, and it has brought the federal regulatory amendment process to a near halt. The APB can be assured that if the proposed language under Option 1 is accepted, the FBI will perform due diligence to move the proposed language change forward.

The Subcommittee is requested to provide input on the information provided in this paper and provide recommendations regarding the following options.

## **OPTIONS**

### **Option 1**

Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

## **Option 2**

No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

## **Option 3**

Discontinue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

## **RECOMMENDATION**

The NCIC Operations and Policy Unit recommends Option 1.

## **FALL 2017 WORKING GROUP ACTIONS:**

### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA. FBI Action: FBI should continue to research various scenarios which may result from any proposed regulatory change. Continue with the interim solution.

**Action:** Motion carried with 11 Yay/11 Nay, Chair broke the tie with a Yay vote

### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2. No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1. Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

**IS SUBCOMMITTEE ACTION:**

**Motion:** To accept a revised Option 1: "Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a) (6) as the long term solution to facilitate access to CJIS Division systems, which would grant criminal justice agencies the same authority to contract with noncriminal justice governmental agencies as they currently have to contract with private entities. Accept the language as proposed below:

*6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency."*

**Action:** Motion carried.

**N-DEx SUBCOMMITTEE ACTION:**

Accepted as information only.

**NCIC SUBCOMMITTEE ACTION:**

**Motion:** Recommendation to the Identification Services Subcommittee for Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as

private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**SA SUBCOMMITTEE ACTION:**

**Motion:** To recommend Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**NCIC ISSUE #3**

The Florida Department of Law Enforcement (FDLE) National Sex Offender Registry (NSOR) Pilot

**PURPOSE**

To seek approval to continue the FDLE NSOR Pilot

**POINT OF CONTACT**

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**

The Subcommittee is requested to review the information provided in this paper and provide appropriate comments, suggestions or recommendations to the APB.

**BACKGROUND**

In 2007, the Florida Department of Law Enforcement (FDLE) was provided an extract of all records within the NCIC's National Sex Offender Registry (NSOR) to assist with the location efforts of registered sex offenders from the state of Louisiana which may have fled to Florida due to Hurricane Katrina. The information exchange between the Criminal Justice Information Services (CJIS) Division and the FDLE became known as Operation Locator.

Due to the project's success, in May 2015 the FDLE received support from the Advisory Policy Board's (APB's) Executive Committee for the FBI to allow the FDLE to conduct a 2 year NSOR Pilot. In November 2015, Operation Locator II was launched to compare data from the NCIC's NSOR against data from the Florida Department of Highway Safety and Motor Vehicles (DHSMV). Florida statutes require a sexual offender to identify himself or herself as such to the Florida DHSMV upon securing a Florida driver license, renewing a Florida driver license, or securing an identification card, regardless of the jurisdiction in which they are required to register. The goal of Operation Locator II is to identify potential subjects living in Florida who have failed to properly register as sexual offenders which can result in criminal penalty.

Below is a brief timeline indicating the Operation’s major milestones:

Time Line:

- May 2015 – APB’s Executive Committee support for a 2 year FDLE NSOR Pilot
- October 5, 2015 – Memorandum of Understanding signed between the CJIS Division and FDLE
- November 18, 2015 – FDLE receives the NSOR Extract from CJIS
- November 20, 2015 – Initial Load from DHSMV
- December 2016 – FDLE provided a status update to the APB’s Executive Committee
- February 2, 2017 – FDLE receives an updated NSOR Extract from CJIS

**DISCUSSION AND ANALYSIS**

The Operation had three parts; first an Initial Run of records (approximately 24 million) from the DHSMV database of Florida issued driver’s licenses and any subjects who had registered a vehicle in Florida against the NSOR data file. The second part establishes a Nightly File transfer of records from DHSMV to FDLE for comparison. Finally, a Make Up file was created, containing licenses issued between the initial pull of data and establishing the nightly process, to ensure no records were missed in the interim.

For the Initial Run a scoring system was defined by the FDLE to help prioritize hits. Potential hits were identified by scoring matches based on Name, Date of Birth (DOB), and Social Security number (SOC). The higher the score the more likely a Florida DHSMV record correlated to a sex offender in the NSOR data file.

In late 2015, the first part of the project was completed. The initial comparison identified approximately 6,000 potential hits, with a Name, DOB, and SOC match, which resulted in 19 offenders being arrested/prosecuted and 14 offenders being brought into compliance. Due to the large number of potential hits, only those with a Name, DOB, and SOC match have been investigated, and work on the initial list continues today.

<b>Initial Run</b>		<b>Case Outcomes</b>	
Number of Cases	5,885	Subject Arrested	19
Confirmed Match	548	Brought into Compliance	14
Subject already registered in Florida or in another state	492	Pending Arrest	8
Viable Cases	56	Left the state of Florida	11
		Under Research	11

\*\* Results as of 04/01/2017

The following case stories display a few examples of the Operation Locator II's success.

### **DHSMV/FBI Match Case Stories**

#### **Arrest of Subject A**

Subject A was an absconded sexual offender from New Jersey. In March 2016, the FDLE located him in Florida via the DHSMV/FBI comparison file. Subject A had been previously convicted of Aggravated Sexual Assault against a 14 year old girl in New Jersey and posed a direct threat to public safety. The FDLE brought the United States Marshal Service (USMS) into the investigation. A federal arrest warrant was issued by the USMS on 04/22/2016. He was arrested in New Jersey on 04/23/2016. Subject A had traveled from Florida back to New Jersey in an effort to elude law enforcement. He was extradited back to FL to face charges for failure to register as a sex offender.

#### **Arrest of Subject B**

Subject B was an absconded sexual offender from New York. He was located in Florida via the DHSMV/FBI comparison file. Subject B was previously convicted of Dissemination of Indecent Material to a Minor and posed a direct threat to public safety. Through additional research by the FDLE, it was discovered that he was residing in Panama City, Florida unregistered. The FDLE brought the USMS and the Bay County Sheriff's Office into the investigation and Subject B was arrested in Panama City on 2/15/16.

#### **Arrest of Subject C**

Subject C is a sexual offender from Maryland. He was located in Florida by the FDLE via the DHSMV/FBI comparison file. Subject C was previously convicted of Aggravated Criminal Sexual Abuse and posed a direct threat to public safety. According to the Maryland Sex Offender Registry and the Baltimore Police Department, he was compliant and currently residing in Baltimore. Through additional research by the FDLE, it was discovered that Subject C had actually been residing in Lehigh Acres, Florida for nearly 3 months unregistered. The FDLE brought the USMS and the Lee County Sheriff's Office into the investigation and he was arrested for failure to register on 3/28/2017.

#### **Arrest of Subject D**

Subject D is a sexual offender from Michigan. He was located in Florida by the FDLE via the DHSMV/FBI comparison file. Subject D was previously convicted in Michigan on two separate cases of 2<sup>nd</sup> Degree Criminal Sexual Conduct, one case on a 6 year old and the other a 7 year old child and posed a direct threat to public safety. Through additional research by the FDLE, it was discovered that he was residing as a transient in Port Charlotte, Florida unregistered. The FDLE brought the USMS and the Charlotte County Sheriff's Office into the investigation and Subject D was arrested for failure to register on 4/4/2017.

#### **Arrest of Subject E**

Subject E was an absconded sexual offender from Iowa. He was located in Florida by the FDLE via the DHSMV/FBI comparison file. Subject E was previously convicted in Iowa of assault with intent to commit sexual abuse and posed a direct threat to public safety. Through additional research by the FDLE, it was discovered that he was collecting wages in Reddick, Florida



unregistered. The FDLE brought the USMS and the Marion County Sheriff's Office into the investigation and Subject E was arrested for failure to register on 4/28/2017.

The success stories display the value to public safety and the investigative benefit to law enforcement to track sex offenders who have absconded to Florida and/or are not properly registered within their jurisdiction. If this proposal is approved, the FDLE NSOR Project will continue. In addition, other CJIS Systems Agencies (CSAs) with the appropriate statutory authority which imposes a criminal penalty on noncompliant sex offenders could explore utilizing the NSOR data for similar purposes.

The Subcommittee is requested to review the information in this paper and provide feedback on the following options:

### **RECOMMENDATIONS**

Option 1: Allow the FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

Option 2: Discontinue the FDLE NSOR Pilot.

### **FALL 2017 WORKING GROUP ACTIONS:**

#### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Allow the FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

**Action:** Motion carried.

#### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Allow the FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

**Action:** Motion carried

#### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1: Allow the FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1: Allow the FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1: Allow the FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

**Action:** Motion carried.

**FALL 2017 NCIC SUBCOMMITTEE ACTION:**

**Motion:** To accept Option 1: Allow FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.

**Action:** Motion carried.



**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**NCIC ISSUE #4**

Proposal to Add the Date of Expiration (EXP) Field in the Wanted Person File

**PURPOSE**

To present a proposal to add the EXP Field as optional in the Wanted Person File

**POINT OF CONTACT**

Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the information provided in this paper and provide appropriate comments, suggestions or recommendations to the APB. Also, provide comments and recommendations as to what priority should be assigned to any approved recommendation.

**BACKGROUND**

Currently, the EXP Field is available in the NCIC's Protection Order File (POF). The EXP is the date the protection order (final, temporary, or emergency) expires. If the protection order does not have an expiration date, non-expiring (NONEXP) should be entered.

Specifically, the *NCIC Operating Manual* provides the following guidelines for record retention in the POF Chapter:

**1.4 RECORD RETENTION PERIOD**

1. A POF record (EPO or ETO) will remain active until it is canceled or cleared by the entering agency or until the order expires. Five days prior to an order's expiration date, an unsolicited \$.P. administrative message will be sent to the ORI of record. This message will serve to notify the agency of the order's impending expiration date (EXP). It also serves to remind the agency that the record will have to be modified if the EXP is changed by the court.

2. If no action is taken by the entering agency to modify the EXP, the record will expire after the fifth day. Inactive records (cleared or expired) will be maintained on-line for the remainder of the year plus 5 years. At the end of that time, NCIC will not notify the ORI of record. Records that are in inactive status cannot be modified or cleared; however, inactive records can be canceled.

3. Nonexpiring Records:

Records for protection orders that have no expiration are referred to as nonexpiring records (NONEXP). These records will remain active until cleared or canceled by the entering agency.

4. Inactive Records:

Inactive records (expired or cleared) will be accessible, via the QPO message, for the remainder of the year in which the record was cleared or expired plus 5 years.

## **DISCUSSION AND ANALYSIS**

The Columbia County Sheriff's Office (CCSO) in Appling, Georgia is requesting the EXP Field be added to the Wanted Person File. Since the EXP Field is not available, the agencies do not have a way to enter an expiration date on a warrant if one exists. A possible solution is to add an Optional EXP Field to the Wanted Person File for the warrants which have a date of expiration. If a warrant does have a date of expiration listed, or is subjected to a statute of limitations, then the entering agency would have the option to enter that date. The CCSO suggests five days prior to the expiration date, an administrative \$.P. message could be generated to the entering agency to further explore the warrant's date of expiration.

Also, the CCSO believes the EXP Field could assist in eliminating invalid warrants in NCIC. Currently, the only way to track a warrant's expiration date is manually. If the warrant expires between validation cycles, then the entering agency would have to track and manually remove the record from NCIC on the date of expiration. NCIC validation policy requires Wanted Person records to be validated annually. To minimize this gap, states can require more stringent reviews of their records to ensure expired warrants are removed. If the EXP Field is added to the Wanted Person File, entering agencies will be able to manage expiration dates electronically and the NCIC system would auto-purge these records on their date of expiration.

If this proposal is approved, agencies will have the capability to enter a specific warrant expiration date and be notified when the warrant is about to expire. An additional consideration is whether the expired warrants should go into an inactive status and be retrievable in an offline search or by a direct query? This is similar to the functionality for the POF. If by direct query, then an additional message key (MKE) and programming will need to be added.

If the EXP Field is created, each state would be responsible for programming the new field and the Subcommittee is requested to select if the Field should be designated as critical for the completeness review during an Federal Bureau of Investigation NCIC Audit.

NCIC has mandatory and optional fields in NCIC record entries. The *NCIC Operating Manual* uses the terms in a technical meaning. Mandatory fields are required to programmatically enter the record. Whereas optional fields are not necessary to meet the criteria for entry and to place the record into NCIC. Critical information is defined as data fields that will increase the likelihood of a positive hit on the subject or property and will aid in the identification of a subject or property.

The Subcommittee is requested to review the information in this paper and provide feedback on the following options:

### **RECOMMENDATIONS**

Option 1: Add the optional EXP Field to the Wanted Person File. Depending on technical feasibility, this enhancement may be implemented in the current environment, during the development of NCIC 3<sup>rd</sup> Generation (N3G), or post N3G initial operating capability.

If Option 1 is chosen, then:

Option 1A: Allow expired warrants to go into an inactive status and be retrievable by a direct inquiry. A direct inquiry would cause an additional MKE and programming.

Option 1B: Do not allow expired warrants to be retrievable by a direct inquiry.

Option 2: No Change.

### **FALL 2017 WORKING GROUP ACTIONS:**

#### **FEDERAL WORKING GROUP ACTION:**

**Motion 1:** To accept Option 1: Add the optional EXP Field to the Wanted Person File. Depending on technical feasibility, this enhancement may be implemented in the current environment, during the development of NCIC 3<sup>rd</sup> Generation (N3G), or post N3G initial operating capability.

**Action:** Motion carried.

**Motion 2:** To accept Option 1B: Do not allow expired warrants to be retrievable by a direct inquiry.

**Action:** Motion carried.

**Motion 3:** To make the field non-critical for audit purposes.

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1 and Option 1A

**Option 1:** Add the optional EXP Field to the Wanted Person File. Depending on technical feasibility, this enhancement may be implemented in the current environment, during the development of NCIC 3<sup>rd</sup> Generation (N3G), or post N3G initial operating capability.

**Option 1A:** Allow expired warrants to go into an inactive status and be retrievable by a direct inquiry. A direct inquiry would cause an additional MKE and programming.

Non-Critical for audit purposes.

**Action:** Motion carried with 21 Yay/2 Nay

**NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: No change.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion 1:** To adopt Option 1: Add the optional EXP Field to the Wanted Person File. Depending on technical feasibility, this enhancement may be implemented in the current environment, during the development of NCIC 3<sup>rd</sup> Generation (N3G), or post N3G initial operating capability.

**Action:** Motion carried.

**Motion 2:** To adopt Option 1B: Do not allow expired warrants to be retrievable by a direct inquiry.

**Action:** Motion carried. Priority level 3M. Non-critical for audit purposes.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt a new Option 3: The N3G Task Force should explore the addition of the optional EXP Field to the Wanted Person File, including if it should be returned in all Wanted Person hit responses.

**Action:** Motion carried.

**FALL 2017 NCIC SUBCOMMITTEE ACTION:**

**Motion:** To accept the following: The N3G Task Force will further explore the addition of the expiration field in NCIC files, including whether or not the records will be retrievable by direct inquiry.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
NATIONAL CRIME INFORMATION CENTER (NCIC) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 18, 2017**

**STAFF PAPER**

**NCIC ISSUE #7**

National Crime Information Center (NCIC) Third Generation (N3G) Project

**PURPOSE**

To request approval of the N3G requirements recommended by the N3G Task Force

**POINT OF CONTACT**

Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the information provided in this paper and provide appropriate comments, suggestions, or recommendations to the APB.

**BACKGROUND**

The purpose of the N3G Project is to identify requirements that 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 APB approved, for further exploration, 14 high-level concepts as representation of more than 5,500 user requests. Since further exploration of all concepts has been approved, each of the underlying element or “sub-concepts” will undergo a more comprehensive review, with the findings being brought to the Criminal Justice Information Services (CJIS) Advisory Process for further consideration and disposition.

The 14 high-level concepts are listed for your reference with the specific concepts discussed in this paper depicted with **bold** font.

Concept 1: Flexible Data Format – Director Approved

**Concept 2: Tailored Functionality**

Concept 3: Access Data Repositories – Pending Director Approval



#### **Concept 4: Name Search Algorithm**

Concept 5: Enhanced Data Search – Pending Director Approval

Concept 6: System Search – Spring 2018

Concept 7: Enhanced Training Resources – Fall 2018

#### **Concept 8: Enhanced Testing Environment**

Concept 9: Record Content – Spring 2018

Concept 10: Enhanced Multimedia – Pending Director Approval

Concept 11: Improved Data Management – Fall 2018

Concept 12: Alternative Outbound Communications – Fall 2018

#### **Concept 13: Alternative Access**

Concept 14: Improved Outbound Communications – Spring 2018

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 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 before introducing the functional requirements into the CJIS Advisory Process. The inaugural N3G Task Force meeting was held on August 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, the functional requirements for each concept are currently being drafted. Concept 1 was approved by the December 2016 APB. Task Force approved functional requirements for Concepts 3, 10 and 5 were approved by the CJIS APB in June 2017.

Throughout the system development process, several assumptions have been identified as necessities to the NCIC System stakeholders. These “guiding principles” will be taken into consideration as the user concepts are further analyzed and developed. One such principle is to ensure current system performance and response times are not degraded. Another is continued support of legacy functionality. Since CJIS Systems Agency (CSA) 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, to 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.

**It is important to note that as these concepts and sub-topic functional requirements are approved, legal and technical reviews will be ongoing. The CJIS Advisory Process will continue to be apprised when any approved concepts require further refinement or elimination from the N3G Project development effort.**

This paper outlines four specific Concepts with corresponding functional requirements that have been discussed and approved by the N3G Task Force. Each Concept should be reviewed independently and recommendations are requested for each separate issue within the specific sub-topic. The Concepts included in this paper are: Name Search Algorithm, Enhanced Testing Environment, Tailored Functionality, and Alternative Access.

### **N3G Project – Concept #13 – Alternative Access**

Currently, the NCIC System communicates with end users primarily through the CSA switch. Alternative access would allow users to communicate directly to the NCIC System bypassing the CSA. During the user canvass, users indicated that direct connections to the NCIC System would be beneficial only in exigent circumstances. Other NCIC System access in this Concept include web services capabilities and alternative disaster recovery site connectivity. Functional requirements for Alternative Access were vetted through the N3G Task Force. Members concluded that the only circumstance that should be considered would be for disaster recovery purposes, which the NCIC System already supports. The N3G Task Force determined that alternative access methods for disaster recovery purposes should not be confined to a set of functional requirements for the next generation of the NCIC System. Rather, these decisions should remain at the discretion of the CJIS Division and the affected CSA. After substantial discussion, it was determined that all of the functional requirements for this concept be excluded. As such, no recommendations are forwarded through the Advisory Process for consideration related to Concept 13 as it has been excluded in its entirety.

### **N3G Project – Concept #4 – Name Search Algorithm**

#### **Current Functionality**

During the N3G Project canvass, the importance of improving the name search algorithm used in the NCIC System echoed throughout. The NCIC System currently uses the New York State Identification and Intelligence System (NYSIIS) algorithm for name searches. The NYSIIS is an open source algorithm that phonetically converts names to searchable values. Users have indicated that the current algorithm produces an excessive amount of false positive hits, especially with Arabic and Hispanic origin names.

The CJIS Division is initiating a study to develop a data profile that accurately describes or characterizes the biographic data contained in the NCIC System. This data profile will aid in the development and selection of a search algorithm that will ultimately produce the most effective results. This study is scheduled to commence in fiscal year 18 and will strive to incorporate the functional requirements that are approved through the CJIS Advisory Process.

Two issues were reviewed during the name search discussion: Expanded Name Search and Improved Algorithm. Each issue will be described with the correlating functional requirements that were approved by the N3G Task Force for further exploration.

### **Issue #1: Expanded Name Search**

The Expanded Name Search included functional requirements to improve and expand the types of name searches conducted by the system. This would include the ability to automatically transpose or rearrange names provided in the inquiry to produce the best match. It also included the flexibility to search on partial names and variations of common versions of names.

The N3G Task Force endorsed the following functional requirements related to name search algorithm for further consideration:

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

### **Issue #2: Improved Algorithm**

The second issue discussed is an Improved Algorithm and includes the functional requirements to improve the function of the algorithm used for NCIC System searches. The focus of the functional requirements ranged from generically improving the name search algorithm to making the name search algorithm available to the users. Users also mentioned the need for conducting searches independent of accent marks. As mentioned, focus was also based on users indicating that the current algorithm takes into account the common American English pronunciation and returns an excessive amount of false positive for names of foreign origin.

The N3G Task Force recommended the following functional requirements related to name search algorithm for further consideration:

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

## **RECOMMENDATIONS**

### **Issue #1 – Expanded Name Search**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

Option 2: Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

Option 3: Approve further exploration of the following functional requirements:

### **Issue #2 – Improved Algorithm**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

Option 2: Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

Option 3: Approve further exploration of the following functional requirements:

## **N3G Project – Concept #8 – Enhanced Testing Environment**

### **Current Functionality**

The NCIC System maintains tiered environments with diverse capabilities tailored to intended users. The current structure can be subcategorized into four distinct environments: Development (DEV), Successive Level Integration Test System (SLI), First Level Integration Test System (FLI), and Operational Environment (OE).

The DEV environment is comprised of multiple regions. The regions are used solely by the CJIS Division's Information Technology Management Section (ITMS) developers as new capabilities and enhancements are coded for integration to the operational system. Upon completion of testing in the DEV environment, the ITMS testing team utilizes multiple SLI regions to

determine any deficiencies in system integrity and operation. The coded enhancements are vetted under controlled conditions until the internal testing team determines evaluation criteria have been met with no remaining negative impact in system performance.

The NCIC System changes are then implemented in the FLI testing environment. The FLI is the nonoperational environment (NOE) that resides on the same mainframe as the OE. The FLI is accessible to the CSAs, 24/7, to test NCIC enhancements and make any necessary programming adjustments prior to implementation of OE updates. Although the FLI retains many of the same capabilities of the OE, some limitations exist, such as batch processing and special request (SPRQ) transactions are not available transaction types in the current FLI environment. For example, test records entered into the FLI mirror the retention of OE records; however, the validation and purge notifications are not generated. Additionally, certain NCIC files, such as the Known or Suspected Terrorist (KST) file, cannot be entered by the CSAs and NCIC System users due to specific Originating Agency Identifiers (ORIs) being designated as the only authorized record owner(s). As such, the restriction may inhibit the ability to program accordingly for inquiry and record display those files.

As part of the NCIC 2000 project, an additional testing header was implemented in the OE and required for NCIC 2000 compliance. The Operational Test header, TN01, allows NCIC users to test in the OE when using the TN01 header rather than the normal header 1N01. A transaction can occur in the production environment against a separate dataset from routine transactions. Test notifications are not generated in the OE due to the possibility of an agency mistaking a notification as authentic. For example, the \$.8. Child Abduction Notification is sent to the National Center for Missing and Exploited Children (NCMEC) and the FBI when a missing person entry contains a value of CA for Child Abduction in the Missing Person (MNP) Field. If notifications were generated when a state tested the ability to enter codes in the MNP field, then NCMEC and the FBI would be alerted to the test record entry under the CA scenario.

### **Issue #1: Improved Test Environment**

The NCIC user community described the NCIC operational and testing environments as functionally different. From a testing perspective, these differences prove challenging at times for CSAs to effectively program NCIC System changes. Furthermore, users requested the development and delivery of a more robust test region with expanded testing capabilities. By providing a more comprehensive testing environment, users will be able to transition efficiently to enhancements approved in N3G as well as future system updates.

The N3G Task Force endorsed the following functional requirements related to an enhanced testing environment for further consideration:

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

## **Issue #2: Test Records**

It was determined that the lack of test records available negatively impacts the ability to test effectively. CSAs often contact CJIS Division staff to provide test records for specific files.

Users proposed a standardized set of test record entries created and maintained in the NCIC System, but accessible to CSAs. The universal database could contain record entries in all 21 NCIC files and be a realistic juxtaposition to the operational dataset. Furthermore, if a specific dataset of test records existed CSAs would retrieve expected results while testing enhancements.

The N3G Task Force endorsed the following functional requirements related to an enhanced training environment for further consideration:

1. Provide test records.

## **RECOMMENDATIONS**

### **Issue #1 – Improved Test Environment**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

Option 2: Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

Option 3: Approve further exploration of the following functional requirements:

### **Issue #2 – Test Records**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide test records

Option 2: Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

Option 3: Approve further exploration of the following functional requirements:

## **N3G Project – Concept #2 – Tailored Functionality**

The NCIC System was deployed in 1967 with the creation of the Wanted Person, Article, Gun, License Plate, and Vehicle Files. Over the following decades, additional files were added. The

mission of the NCIC System from inception was to identify fugitives, locate stolen property, and protect tactical law enforcement officers and the public through a national network. Since then, NCIC has evolved to support more investigative functions through the establishment of files such as the Gang and KST Files. Despite a changing law enforcement landscape with a more investigative pivot, the NCIC System continues to support its key mission of providing officer and public safety with almost instantaneous results.

As NCIC policy and validation requirements have become more defined and the need for statistics within each state or territory has become more necessary, administrative use cases for the NCIC System have emerged. However, it is critical that the primary mission of immediate public safety not be diminished as the uses for the NCIC System continue to evolve to serve more investigative and administrative functions. Hence, most of the investigative and administrative functionality supported by the NCIC System today is conducted in an offline environment.

During the N3G user canvass, it was identified that there was a need for different types of NCIC information to be made available in the online environment based on the function that a user was performing at the time. Originally, the concept brought forth through the canvass was to allow CSA's to identify access to certain functionality based on the role of the user; possibly through specific logon information. Understanding that officers change roles regularly, the N3G Task Force concluded that an NCIC System that tailors its responses based on the need of the user would best serve the NCIC user community at the transaction level. Based on this guidance, the concept evolved to propose that access to NCIC information be based on the situation or circumstance of the user. Responses will be returned as a result of an inquiry based on the function the user is performing at the time of the inquiry. The three possible functions could be either Tactical, Investigative, or Administrative.

The functional requirements for this concept approved by the N3G Task Force were:

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

### ***Tactical***

NCIC Tactical users would be defined as the "boots on the ground" law enforcement officers performing encounter based inquiries that require immediate responses. The information returned serves an immediate response to assist the officer or agent in adequately and accurately identifying the encountered individual or property in the performance of their mission.

The current average response time for tactical queries is less than .02 seconds (which would be an online query in the existing operational environment). This average response time is well under the established time requirement set forth by the NCIC System policy guidelines. One of the most commonly used inquiries utilized by NCIC users is a Person Query. The Person Query searches the Wanted Person File as well as other person and property files. This transaction is most useful to the officer on the street for tactical purposes as the information returned greatly

protects the officer and the public by providing relevant information and warnings with a near immediate response time.

During the N3G user canvass, the desire to select the content of data returned from a search in a tactical environment was expressed. However, a central theme brought up by stakeholders was that users become inundated with irrelevant responses. The number of false hits can also prolong the response time back to the user which is detrimental to the officer on the street. Since many of the concepts derived from the user canvass could potentially slow down the response time, they should be considered more investigative in nature. For example, the key word search option identified in N3G Concept 5 (Enhanced Data Search) would potentially inundate tactical officers with responses.

### ***Investigative***

As previously mentioned, law enforcement has expressed interest in a need for more investigative functionality in the NCIC System. Currently, data in the offline environment may satisfy a portion of this need. An offline search is a special technique used to extract information from the NCIC System which cannot be obtained through an online query. Offline searches are typically more investigative in nature than online searches. As a result, response times back to the requesting agency may be much longer. CSAs maintain the ability to perform limited offline searches but the majority are conducted by CJIS Division staff. NCIC policy requires that the search is criminally investigative in nature and the requesting agency possesses a law enforcement Originating Agency Identifier. The originating agency can submit its request via an International Justice and Public Safety Network (Nlets) administrative message or through email.

Unlike online inquiries that require a quick tactical response, offline searches are valuable to law enforcement in instances that aren't as immediate or require a more in-depth level of information returned. Offline searches can retrieve historical records back to 1990. To name a few, offline searches may provide an investigator with information to:

- Determine if an agency entered an NCIC record or conducted an inquiry on a particular individual or item of property.
- Substantiate or discredit an alibi.
- Identify previous encounters individuals have had with law enforcement.

As stated previously, many NCIC investigative functions occur within the offline environment and are limited to CJIS Division staff and CSAs. As part of N3G, it was requested that Investigative functions be expanded to all users that have access to the NCIC System and participate in investigative activities. Investigative functions would be used for purposes in which the user desires to receive as much information as possible regarding a person or property to analyze data and determine relevance to their investigation.

Users could also potentially choose the data necessary for investigation by selecting which databases to be searched while performing an NCIC System inquiry. N3G Concept 3 (Access Data Repositories) aims to provide NCIC users with data from other databases. If approved, users would have the ability to select which databases to search that may be pertinent to their



investigation and deselect certain searchable databases that may return information that is either unnecessary or irrelevant to the scope of their current operational requirement.

Since tactical response times cannot be degraded, the Investigative functions may have to reside in a separate environment. This change may require programming for additional messages. Bandwidth concerns need to be addressed, especially with large data files and returns to the users of Investigative functions. Additionally, CSAs may have to establish organizational controls for use of the Investigative functions.

### ***Administrative***

Administrative functions would be similar to those available today in the current NCIC System offline environment. Administrative functions in an online environment would be expanded to support personnel performing searches for data pertinent to their administrative function. Similar to Investigative functions, response times have the potential to be slower than that of Tactical functions as Administrative queries may also produce a large data set. It is essential that Administrative queries will primarily be for in-house research (e.g., an agency inquiring about their own NCIC records, an agency searching transactions, and logs for statistical reporting purposes). Users have requested that the NCIC System offline search capabilities be expanded to the online operational environment for statistical purposes to allow for easier access and use.

CSAs currently have the ability to conduct limited administrative offline or special request searches to gain access to retired record information. It has been requested through the N3G Project that other off-line data (such as transaction logs) be made accessible as well. NCIC System policy and programming requirements may need to change if that ability is expanded to the local level with the proposed delineation of functional environments. If expanded, the presumed massive increase of special request type searches may negatively impact CSAs or the NCIC System by causing a potential overload of information. Therefore, certain CSA controls may need to be considered to limit the number of searches conducted and/or the amount of data returned.

### ***Summary***

It is currently unknown how tailored functionality will be accomplished. One option would be the creation of new and separate Message Keys. New transaction headers could also be added. In the event that environments are separated to account for different types of NCIC data, headers could be the trigger for routing transactions to the respective desired NCIC System environment. However, these changes would require programming efforts for both the CJIS Division as well as the user community. Regardless of the technical solution, certain information that is being requested as part of the tailored functionality concept may lend itself to necessary policy changes. For example, providing access to transaction log histories and retired record information to all users will most likely make it necessary to implement additional oversight to account for the potential misuse or overuse of the system.

If the Subcommittee is in support of the tailored functionality concept moving forward, a more detailed implementation strategy will be provided once future analysis is conducted during the requirements building and early development stages of the N3G Project.

## **RECOMMENDATIONS**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

Option 2: Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

Option 3: Approve further exploration of the following functional requirement:

## **FALL 2017 WORKING GROUP ACTIONS:**

### ***CONCEPT 2: TAILORED FUNCTIONALITY***

#### **FEDERAL WORKING GROUP ACTION:**

##### **Concept 2: Tailored Functionality**

**Motion:** To accept Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Action:** Motion carried.

#### **NORTH CENTRAL WORKING GROUP ACTION:**

##### **Concept 2: Tailored Functionality**

**Motion:** To accept Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Action:** Motion carried.

#### **NORTHEASTERN WORKING GROUP ACTION:**

##### **Concept 2: Tailored Functionality**

**Motion:** To adopt Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.

2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Concept #2 – Tailored Functionality**

**Motion:** To adopt Option 1. Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Concept #2 – Tailored Functionality**

**Motion:** To adopt Option 1. Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Action:** Motion carried.

**FALL 2017 NCIC SUBCOMMITTEE ACTION:**

**Concept #2 – Tailored Functionality**

**Motion:** To accept Option 1 for Issues 1 and 2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Action:** Motion carried.

---

***CONCEPT #4 – NAME SEARCH ALGORITHM***

**FEDERAL WORKING GROUP ACTION:**

**Concept 4 - Name Search Algorithm Issues 1 and 2**

**Motion:** To accept Option 1 for both Issues 1 and 2.

**Issue #1 – Expanded Name Search**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.

4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

**Issue #2 – Improved Algorithm**

Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Concept 4 - Name Search Algorithm**

**Issue #1 – Expanded Name Search**

**Motion:** To adopt Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

**Action:** Motion carried.

**Issue #2 – Improved Algorithm**

**Motion:** To adopt Option 1: Approve further exploration of the N3G Task Force recommended functional requirements.

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Action:** Motion carried.

## **NORTHEASTERN WORKING GROUP ACTION:**

### **Concept 4 - Name Search Algorithm**

**Motion:** To adopt Option 1 for both Issue #1 and Issue #2.

#### **Issue #1: Expanded Name Search**

Option #1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

#### **Issue #2: Improved Algorithm**

Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Action:** Motion carried.

## **SOUTHERN WORKING GROUP ACTION:**

### **Concept 4 – Name Search Algorithm**

#### **Issue #1 – Expanded Name Search**

**Motion:** To adopt Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

**Action:** Motion carried.

#### **Issue #2 – Improved Algorithm**

**Motion:** To adopt Option 1: Approve further exploration of the N3G Task Force recommended functional requirements.

1. Improve the name search algorithm.

2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Concept 4 – Name Search Algorithm**

**Issue #1 – Expanded Name Search**

**Motion:** To adopt Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

**Action:** Motion carried.

**Issue #2 – Improved Algorithm**

**Motion:** To adopt Option 1: Approve further exploration of the N3G Task Force recommended functional requirements.

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Action:** Motion carried.

**FALL 2017 NCIC SUBCOMMITTEE ACTION:**

**Concept 4**

**Motion:** To accept Option 1 for Issues 1 and 2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

Issue 1 – Expanded Name Search

1. Ability to search on partial names.
2. Transpose the first, middle and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.

9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

Issue 2 – Improved Algorithm

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm.
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Action:** Motion carried.

---

***CONCEPT 8 - ENHANCED TESTING ENVIRONMENT***

**FEDERAL WORKING GROUP ACTION:**

**Concept 8 - Enhanced Testing Environment**

**Issue #1 – Improved Test Environment**

**Motion:** To accept Option 1 for Issue #1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

**Action:** Motion carried.

**Issue #2 – Test Records**

**Motion:** To accept Option 1 for Issue #2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide test records

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Concept 8 - Enhanced Testing Environment**

**Issue #1 – Improved Test Environment**

**Motion:** To accept Option 1 for Issue #1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

**Action:** Motion carried.

**Issue #2 – Test Records**

**Motion:** To accept Option 1 for Issue #2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide test records

**Action:** Motion carried.

**NORTHEASTERN WORKING GROUP ACTION:**

**Concept 8 - Enhanced Testing Environment**

**Motion:** To adopt Option 1 for both Issue #1 and Issue #2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

**Issue #1 – Improved Test Environment**

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

**Issue #2 – Test Records**

1. Provide test records

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Concept 8 – Enhanced Testing Environment**

**Issue #1 – Improved Test Environment**

**Motion:** To adopt Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

**Issue #2 – Test Records**

**Motion:** To adopt Option 1: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

1. Provide test records

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Concept 8 - Enhanced Testing Environment**

**Motion:** To adopt Option 1 for both Issue #1 and Issue #2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

**Issue #1 – Improved Test Environment**

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

**Issue #2 – Test Records**

1. Provide test records

**Action:** Motion carried.

**FALL 2017 NCIC SUBCOMMITTEE ACTION:**

**Concept 8**

**Motion:** To accept Option 1 for Issues 1 and 2: Approve further exploration of all functional requirements as recommended by the N3G Task Force.

**Issue #1 – Improved Test Environment**

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.



**Issue #2 – Test Records**

**Action:** 1. Provide test records  
Motion carried.

---

***CONCEPT 13 - ALTERNATIVE ACCESS***

Accepted as information only by all five working groups.

Accepted as information only by the NCIC Subcommittee.

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)  
ADVISORY POLICY BOARD (APB)  
DECEMBER 6-7, 2017  
OKLAHOMA CITY, OK**

**STAFF PAPER**

**APB ITEM #14**

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

**UCR ISSUE #1**

UCR Status Report

- Demonstration of the Crime Data Explorer
- Demonstration of the Use of Force

**UCR ISSUE #2**

Modification of the Application of the Current Embargo Policy for the Release of UCR Program Data

**UCR ISSUE #3**

Addition of UCR Offenses for Federal Crime Reporting to the National Incident-Based Reporting System (NIBRS)

**UCR ISSUE #4**

The Use of the Judicial District for Federal Agencies to Report a NIBRS Incident to the UCR Program

**UCR ISSUE #5**

Expansion of the UCR Program Police Employee Collection

**UCR ISSUE #6**

Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

**UCR ISSUE #7\***

The Federal Bureau of Investigation's UCR Quality Assurance Review to Resume Operations in Accordance with the CJIS Division, CJIS Audit Unit's Triennial Audit Schedule

**AdHoc Discussion\*\***

Nomenclature of the NIBRS Sex Offenses for Publications, Technical Manuals, and Other Documents as Applicable

\* Delivered with the information only staff papers

\*\* No staff paper



**CJIS ADVISORY POLICY BOARD (APB)  
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**UCR ISSUE #1**

UCR Status Report

**PURPOSE**

The purpose of this paper is to provide a status report on the Crime Statistics Management Unit (CSMU) UCR Program.

**POINT OF CONTACT**

Law Enforcement Support Section (LESS), CSMU

Questions regarding this topic should be directed to <agmu@leo.gov>.

**BACKGROUND**

The UCR Program was conceived in 1929, by the International Association of Chiefs of Police (IACP) to meet a need for reliable uniform crime statistics for the nation. In 1930, the Federal Bureau of Investigation (FBI) was tasked, by the Department of Justice (DOJ), with collecting, publishing, and archiving those statistics. The FBI's LESS, CSMU is responsible for the development, implementation, and dissemination of all guidelines and procedural matters associated with reporting crime statistics. Today, several annual statistical publications, such as the *Crime in the United States*, *Hate Crime Statistics*, *National Incident-Based Reporting System* (NIBRS) and *Law Enforcement Officers Killed and Assaulted* (LEOKA) are produced from data provided by over 17,000 law enforcement agencies across the United States.

In 2015, the FBI CJIS Division was tasked with a Director's Priority Initiative (DPI) to improve the nation's UCR statistics for reliability, accuracy, accessibility, and timeliness, and expand the depth and breadth of data collected. The Crime Data Modernization (CDM) Initiative is one of seven DPIs currently being managed.

The mission of the CDM is to improve the nation's UCR crime statistics reporting standard for local, state, tribal, and federal law enforcement agencies (LEAs) and to provide richer data to inform, educate, and strengthen communities. This effort will be achieved through the completion of a five prong approach. Prong one is to transition local, state, and tribal LEAs from the Summary Reporting System (SRS) to the NIBRS. Prong two 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. Prong three and Prong four both include federal LEA compliance with the Uniform Federal Crime Reporting Act (UFCRA) of 1988 which

mandates all federal agencies report their crime statistics to the National UCR Program. Strategically planned, Prong three specifically addresses FBI participation in the UCR Program. Prong four facilitates participation from the remaining DOJ entities, as well as all other federal agencies, and Prong five relates to technical efforts to create the Crime Data Explorer (CDE), which is designed to ensure crime data is timely and accessible.

## **DISCUSSION AND ANALYSIS**

### **NIBRS Transition (Prong 1)**

The FBI currently employs two crime data collection systems known as the SRS and the NIBRS. The SRS only requires aggregate crime totals, whereas the NIBRS requires detail-specific data elements regarding each crime, thus providing richer and more accurate data; however, only 31.2% of LEAs are currently covered by the NIBRS.

The transition of local, state, and tribal LEAs from the SRS to the NIBRS is gaining momentum throughout the nation. In early 2015, the FBI received a public resolution from the major law enforcement organizations supporting a five-year retirement of the SRS and transitioning the UCR Program to a NIBRS only. Additionally, on December 2, 2015, the CJIS Advisory Policy Board (APB) approved the recommendation to sunset the SRS and replace it with the NIBRS as the national standard for crime reporting by January 1, 2021. This recommendation was signed by the Director of the FBI on February 9, 2016.

During this time, the FBI began a NIBRS Modernization Study, in which current business practices and policies employed by local, state, tribal, and federal LEAs are being assessed, and how they compare with the requirements to transition these LEAs from the SRS to the NIBRS for purposes of collecting crime statistics. Moreover, the NIBRS is being assessed to determine if it meets current policing needs in its present state or also requires modernization. Policing policies and strategies have evolved over the last 30 years. Law enforcement has acknowledged NIBRS is the pathway to more accurate crime data; however, we must ensure the policy evolves to guarantee the best data. The NIBRS Modernization Study is anticipated to be complete September, 2017.

In efforts to initiate the NIBRS transition, the FBI has partnered with the Bureau of Justice Statistics (BJS) to implement the National Crime Statistics Exchange (NCS-X), in which the goal is to transition select state UCR programs and 400 local law enforcement agencies from the SRS to the NIBRS. The NCS-X initiative is a strategic expansion of the number of law enforcement agencies contributing data to the NIBRS in order to produce nationally-representative estimates of crime using the NIBRS dataset. Currently, there are too few law enforcement agencies reporting to the NIBRS to make inferences about crime occurring at the national level. A valid statistical sample of 400 agencies was selected as part of the NCS-X initiative. When NIBRS data from these sampled agencies is added to data from current participating NIBRS agencies, national estimates of crime can accurately be produced.

One of the largest barriers to the NIBRS transition is the financial burden LEAs will experience regarding both the planning and implementation to replace the SRS. The FBI is financially

assisting with the transition of the 400 agencies and state UCR programs not fully NIBRS compliant, through cooperative agreements the BJS is administering.

Fiscal Year (FY) 2017 solicitations for 27 large agencies, three state UCR programs, and one state agency were released in May 2017, and closed on June 30, 2017. The states of Alaska, Arizona, New Mexico and Mississippi were eligible to apply for funding. The large agencies were: Arizona (Tucson), California (Alameda County, Kern County, City of Fresno, Riverside County, Sacramento County, San Bernardino County, City of San Francisco, City of San Jose, Santa Clara County), the District of Columbia, Georgia (City of Atlanta, DeKalb County Police Department), City of Indianapolis, Indiana, Louisiana (East Baton Rouge Parrish, Jefferson Parrish, City of New Orleans), Maryland (City of Baltimore, Baltimore County Police Department), City of St. Louis, Missouri, New York (Nassau County Police Department, New York City Police Department, Suffolk County Police Department), City of Pittsburgh, Pennsylvania, and Texas (Harris County, City of Houston, Travis County). To date, 22 states have received funding. Seven states have received planning grants: California, Florida, Illinois, Maryland, Nevada, Wisconsin, and Wyoming, and 15 states have received implementation grants: Alabama, Hawaii, Kansas, Louisiana, Maine, Minnesota, Missouri, Nebraska, New Jersey, New York, Pennsylvania, Oklahoma, Utah, Washington, and North Carolina, which received BJS Pilot funds but not as part of a direct competitive award.

Furthermore, the following state programs have provided respective transition dates:

- North Carolina – 2018 (full state solution)
- Indiana - 2020 (full state solution)
- Georgia - 2019 (full state solution)
- Texas - 2019 (full state transition)
- Minnesota - 2021 (full state transition)

The addition of these states and their law enforcement agencies will greatly increase the percent of population covered by NIBRS.

The FBI is educating audiences via clear and concise messages in order to raise awareness and educate individuals on more accurate and comprehensive views of crime in the United States, as well as more transparency and uniformity through detailed reporting. This effort involves creating a means to routinely inform stakeholders, via a website, of the status of the NIBRS transition, and provide data and resources for audiences to use within their respective communities. The website also includes Frequently Asked Questions (FAQs), “Ask an Expert”, basic information and lessons learned, and access to other resources for support and information. This NIBRS website is available to the general public at: <<https://ucr.fbi.gov/nibrs-overview>>. The NIBRS video may be viewed from this website.

Finally, the FBI CJIS Division has hosted regional NIBRS Training Sessions in Fiscal Year (FY) 2017. These training sessions are designed to help agencies participating in the BJS NCS-X initiative gain a better understanding of the NIBRS to assist them in a successful implementation by January 1, 2021. NIBRS subject matter experts from across the FBI, and representatives from the BJS NCS-X initiative, are in attendance. These experts are addressing “Why the NIBRS, Why Now?” as well as guidelines for implementation planning including a Concept of

Operations regarding development and cost estimation to assist transitioning agencies. The training sessions occurred as follows:

- February 14-16, 2017 (Orlando, Florida)
- April 4-6, 2017 (Tulsa, Oklahoma)
- June 27-29, 2017 (Baltimore, Maryland)
- August 1-3, 2017 (Phoenix, Arizona)
- September 19-21, 2017 (St. Louis, Missouri)

### **National Use-of-Force (UOF) Data Collection (Prong 2)**

The FBI has a long-standing tradition of providing crime statistics on Law Enforcement Officers Killed or Assaulted (LEOKA) and justifiable homicides which facilitate transparency and accountability. To improve the data currently available, the FBI will collect use-of-force data. The CJIS APB approved the recommendation to develop this collection in their December 3, 2015 meeting, and the Director of the FBI signed this recommendation on February 9, 2016.

The definition of the collection of use of force is:

“The collection and reporting of use of force by a law enforcement officer {as defined by Law Enforcement Officers Killed and Assaulted (LEOKA)} to the FBI. The collection and reporting would include use of force that results in the death or serious bodily injury of a person, as well as when a law enforcement officer discharges a firearm at or in the direction of a person.”

The definition of serious bodily injury is based in part upon 18 United States Code Section 2246 (4):

“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 CJIS APB approved a minimum set of data elements to be used for a high-level national collection on law enforcement use of force. The data elements include information relating to the incident, the subjects of the use of force, and any officers involved. Additionally, the FBI assembled a UOF Task Force in January 2016, whose mission was to further define the scope of data elements to be collected, initiate a marketing campaign for participation, and define the publication process. This Task Force met on January 27, 2016; March 17, 2016; May 4-5, 2016; August 3, 2016; and September 7, 2017. The following data elements were identified for inclusion and measurement in the National UOF Data Collection by the UOF Task Force:

#### **Incident Information**

- Date and time of the incident.
- Total number of officers who applied actual force during time of incident.
- Number of officers from your agency who applied actual force during time of incident.
- Location of the incident.
- Location type of the incident.
- Did the officer(s) approach the subject(s)?

- Was a supervisor or a senior officer acting in a supervisory capacity present or consulted at any point during the incident?
- Was this an ambush incident?
- Reason for initial contact between subject and officer.
- If incident involved multiple law enforcement agencies, case numbers for the local “use-of-force reports” at the other agencies.

#### Subject Information

- Age, sex, race, ethnicity, height, and weight of the subject(s).
- Injury/Death of subject(s).
- Type(s) of force used connected to serious bodily injury or death.
- Whether the subject(s) resisted.
- Was the threat by the subject(s) perceived to be directed to the officer or to another party?
- Type(s) of subject resistance/weapon involvement.
- Apparent or known impairment/physical conditions of subject?
- At any time during the incident, was the subject(s) armed or believed to be armed with a weapon (other than hands, fist, or feet)?

#### Officer Information

- Age, sex, race, ethnicity, height, and weight of the officer(s).
- Officer’s years of service as a law enforcement officer (total tenure).
- Full-time?
- Was the officer readily identifiable by clothing or insignia at the time of the incident?
- Was the officer on duty at the time of the incident?
- Did the officer discharge a firearm?
- Officer(s) injured.
- Officer injury type.

Furthermore, the CJIS APB made a recommendation regarding the collection mechanism to be used:

“The APB recommends the creation of a separate collection mechanism under the FBI CJIS for the reporting of use of force data. The new data collection will be maintained separately by the national UCR Program and apart from the criminal incident and offense information. CJIS Systems Officers, in consultation with UCR Program Managers, will determine if agencies within their jurisdiction may submit directly to the FBI. UCR Programs will have timely and on-going access to all data submitted directly to the FBI.”

The FBI is leveraging the Law Enforcement Enterprise Portal (LEEP) for this collection. A data collection tool has been developed and is accessible from LEEP. The FBI began a pilot study on July 1, 2017, and will continue until December 31, 2017. The goals of the pilot study is to work with a set of targeted LEAs to assess data quality and data completeness before an anticipated nationwide effort to collect data in early 2018. As of August 16, 2017, 71 local have enrolled to participate in the pilot study. The FBI continues to receive requests from LEAs to participate in the pilot study.



To market the National UOF Data Collection, the FBI developed the following webpage which LEAs and the general public may use to obtain answers to FAQs and access resources and support information: <<http://www.fbi.gov/use-of-force>>. Additionally, the UOF has created a series of “how to” videos ranging in length from one to three minutes which were produced to demonstrate how to successfully complete specific tasks within the National UOF web portal, such as “How to Create and Incident Report,” “How to Create and Submit a Zero Report,” “How to Review an Incident Report,” etc. These videos can be used in conjunction with a User Manual to supplement training components regarding the use of the National UOF web portal. These resources will be housed on the National UOF Data Collection Special Interest Group (SIG).

### **FBI Reporting (Prong 3) and DOJ and Other Federal Agency Reporting (Prong 4)**

The traditional concept of “*offenses known*” by law enforcement was adopted in 1929 by the IACP as the data collected in the National UCR Program. The aim in creating UCR was to get a true sense of crime in the nation. Implementation of the UFCRA of 1988 posed unique opportunities for the National UCR Program data collection. The UCR Program was designed to be an innate step for local and state agencies to report the crimes most common and most likely to come to the attention of law enforcement. However, because of the types of crimes federal agencies investigate, investigation processes and procedures, and building the case, is often fundamentally different than local and state agencies. Federal agencies found it difficult to fit into the UCR model. The FBI led three conferences among affected federal agencies in 1989 and 1990 and published guidance for their participation in September, 1990. However, no federal agency was able to fully implement the statutory requirements, and only six agencies in two departments provide any data at all.

The first priority within the federal reporting effort concentrated on FBI participation. Designated as a DPI the intent of the federal reporting effort is to improve the nation’s crime statistics, and ensure these statistics include data from all applicable federal law enforcement agencies. The National UCR Program reported FBI arrest data by field office for Human Trafficking, Hate Crime, and Criminal Cyber Intrusion in the 2014 *Crime in the United States (CIUS)*. The FBI then worked to expand the types of offenses reported for 2015, adding Bank Robbery, Child Exploitation, Health Care Fraud, and Securities Fraud. Additional offenses applicable to FBI reporting are currently being identified. The FBI has taken steps to develop the capability within Sentinel to capture and report incident data. These changes are nearing completion and rollout is anticipated to begin in October 2017. The *CIUS Federal Crime Data, 2015* also included data submitted from the National Institutes of Health (NIH) and several agencies within the U.S. Department of the Interior (DOI), as well as, selected offenses from the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF).

The federal initiative continues to encourage DOJ participation. Along with established FBI crime data, and reporting of the DOI and NIH, the ATF; and the US Marshals Service (USMS) have reported data for the upcoming *CIUS Federal Crime Data 2016* which should be released in September, 2017. The FBI has identified other federal agencies which should be reporting to the UCR Program and is actively seeking commitments for participation from the identified DOJ and other federal agencies. Once commitments are received from these agencies, readiness assessments are conducted to determine reporting capabilities and timeliness.

Currently, the following federal agencies are working toward compliance of the UFCRA of 1988: the Drug Enforcement Agency (DEA), the Department of Homeland Security (DHS), the DOI, the Department of State, the Federal Protective Service (FPS), the USMS, the United States Department of Veteran’s Administration (VA), and the United States Postal Service. Furthermore, the ATF, DOI, FPS, and VA are actively working toward incident-based reporting. The FBI is assisting these agencies with planning and implementation, where necessary, to bridge existing technical gaps.

Without the inclusion of federal crime data, any picture of crime in the United States is incomplete. The FBI is committed to providing a complete picture and will endeavor to partner with the other federal law enforcement agencies to determine how to make this happen. While there have been obstacles to overcome, the FBI will continue to develop reporting standards which take into account the differences between federal agencies’ data and state and local agencies’ data without compromising the quality and consistency of the data.

### **Crime Data Explorer (CDE) (Prong 5)**

Technical efforts to improve accessibility, and timeliness of crime data reported to the National UCR program is Prong 5. The FBI CJIS Division has built the CDE which moves toward this vision. The CDE supports the FBI’s broader effort to modernize and improve accessibility to reported crime data. It will replace the National UCR Program’s online Data Tool maintained by the BJS, however it will not impact the reporting, collection, and processing of UCR data at the national program level.

Crime Data Explorer (CDE) went live on June 30, 2017. This cloud-based system includes a user-friendly interface, the ability to search, and visualize SRS and NIBRS data, and the ability to compare state and national crime trends. CDE provides rich, dynamic views of the data, bulk data downloads and exploration of data by location and crime type.

CDE will enable a user to query, view, and make available for download crime reporting data submitted to the National UCR Program to include:

- NIBRS
- Historical aggregate SRS
  - Although SRS will be phased out of data submission and collection by January 1, 2021, it will still be necessary for historical SRS data to be made available on the CDE until a full transition to the NIBRS reporting system is complete and the historical data is preserved for data comparison and trending computations.
- Granularity of the data will reflect:
  - National
  - State
  - Agency

CDE changes UCR data offerings from solely static publication tables to ad hoc user-driven requests which enable interaction with national data crime data in an intuitive and easy manner. CDE is the first service of its kind for the National UCR Program to anyone with internet access.

CDE is designed for a spectrum of stakeholders, novice to expert, to include:

- General public
- Students
- Legislative staff
- Criminal justice advocates
- Journalists
- Open data experts/civic technicians
- Researchers
- CJIS and Law Enforcement

The FBI will continue gathering requirements for additional development of CDE. The FBI will explore the addition of new features, capabilities, and data, improving CDE's value to the general public, law enforcement and other stakeholders. CDE will also be leveraged to enhance our traditional annual crime publications, improving their utility and broadening their appeal to the public.

## **OPERATIONS**

### ***Publication***

CSMU is planning to disseminate all UCR related publications as planned for 2017. In addition, CSMU has implemented a Publication Modernization Team to plan for the future of crime data publications post CDE deployment. Understanding the initial capability CDE will provide, the Publications Modernization Initiative is designed to engage stakeholders and determine what UCR Publications will be needed in the future, working toward the goal of a timelier release of submitted crime data. The team will be reaching out to gather input regarding publication look and feel, timeliness, and other attributes to inform a viable strategy.

The 2017 publication schedule for 2016 crime data reported to the National UCR Program is:

*Crime in the United States* – September 25, 2017

*Law Enforcement Officers Killed or Assaulted* – October 30, 2017

*Hate Crime* – November 27, 2017

*National Incident-Based Reporting System* – December 18, 2017 Semi-Annual Publication – January 29, 2018

## **LEOKA**

More than two decades ago, the LEOKA Program adopted an integrative approach for collecting data on incidents in which a law enforcement officer was killed or seriously injured while performing his or her assigned duty. This approach involves the in-depth examination of the law enforcement officer, the offender, and the circumstances of the incident. The LEOKA

Program and the Critical Incident Response Group, Behavioral Research and Instruction Unit (BRIU) personnel have partnered during those decades to conduct special research projects regarding the felonious deaths and assaults of our nation's law enforcement officers. Those projects resulted in three publications entitled *Killed in the Line of Duty* (1992), *In the Line of Fire: Violence against Law Enforcement* (1997), and *Violent Encounters* (2006) which in-turn the Officer Safety Awareness Training (OSAT) was developed and implemented across the nation.

### ***Ambush Study***

The LEOKA Program and West Virginia University (WVU) personnel are now embarking on their fourth special research project. This study is focusing on felonious deaths and assaults of law enforcement officers during ambush and unprovoked attack situations. The LEOKA Program categorizes ambush incidents as those which involve "entrapment and premeditation." These are situations where an unsuspecting officer was targeted or lured into danger as the result of conscious consideration and planning by the offender. Unprovoked attacks on officers are those not prompted by official contact at the time of the incident between the officer and the offender. The LEOKA/WVU Team identified approximately 80 cases involving both categories to be used for the research project. Victim officers and offenders were contacted regarding their participation in the study and team members conducted interviews of those individuals to gain insight into these incidents. The findings from this study will be published under the title of *Ambushes and Unprovoked Attacks; Assaults on our Nation's Law Enforcement Officers* and will be made available to all law enforcement executives, officers, and trainers.

### ***LEOKA Points of Interest***

The LEOKA Program continuously strives to fulfill the mission of reducing the number of officer deaths and assaults. Some of those efforts are as follows:

- The LEOKA Program develops and publishes officer safety articles which are posted on the Law Enforcement Enterprise Portal "Highlights" page at <[www.CJIS.gov](http://www.CJIS.gov)>. Articles have been published with titles such as, *Accidental Deaths, Speed & Seatbelts, Officer Perceptions, Offender Perceptions, The Benefits of Training and Turning Data into Training*, just to name a few. All topics are relevant, examining everyday issues law enforcement officers face as part of their profession. Selected articles are also published in a dedicated "Officer Survival Spotlight" section of the FBI Law Enforcement Bulletin <[www.leb.fbi.gov](http://www.leb.fbi.gov)>, as well as the FBI National Academy Association bi-monthly magazine (The Associate). With these three mediums for publications, the LEOKA Program now has an outreach to over 3 million viewers both nationally and internationally. Publications are archived and continually available on the Law Enforcement Enterprise Portal <[www.CJIS.gov](http://www.CJIS.gov)> in the LEOKA Special Interest Group.
- The LEOKA Officer Safety Awareness Training (OSAT) course was developed to provide valuable officer safety training with an eye toward reducing line of duty deaths and assaults. Since 2009, the LEOKA OSAT course has been attended by more than 77,800 law enforcement professionals from over 24,700 national and international law enforcement

agencies. This comprehensive training is offered free of charge to all law enforcement agencies. To request an OSAT course, send e-mail to: <LEOKA.Training@ic.fbi.gov> or call 304-625-2939.

- The LEOKA Program is developing a paperless mode of collection to replace the current 701 and 701a paper forms for when an officer is killed or seriously assaulted by firearm or knife/other cutting instrument. This electronic format is being developed in an effort to reduce the burden on agencies who encounter these tragic events.

## **Program Development Group**

### ***Hate Crime Statistics***

The mission of the FBI UCR Hate Crime Data Collection is to provide a national, representative picture of hate crime in our nation in order to inform, educate, and strengthen the communities providing hate crime data to the UCR Program. The UCR hate crime personnel continue to liaison with various federal agencies, law enforcement, and advocacy groups stress the importance of reporting hate crime incidents to law enforcement and the UCR Program. Personnel are also developing a strategic plan for increasing participation in this data collection.

### ***Human Trafficking***

To comply with the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, the National UCR Program began publishing Human Trafficking incident data in 2013. The human trafficking initiative serves not only as a means to evaluate current efforts but is an important tool to help our law enforcement partners facilitate the potential development of new policies and programs aimed to target traffickers and provide services to victims/survivors. Although collection of this initiative is relatively new, the program continues to see a marked increase in state participation and incident reporting of human trafficking crimes each year. This early success assures training and marketing will continue to attract more contributors.

### ***Animal Cruelty***

Since January 2016, the FBI's UCR program has been collecting Animal Cruelty offenses leveraging the following definition:

*Cruelty to Animals: Intentionally, knowingly, or recklessly taking an action that mistreats or kills any animal without just cause, such as torturing, tormenting, mutilation, maiming, poisoning, or abandonment. Included are instances of duty to provide care, e.g., shelter, food, water, care if sick or injured; transporting or confining an animal in a manner likely to cause injury or death; causing an animal to fight with another; inflicting excessive or repeated unnecessary pain or suffering, e.g., uses objects to beat or injure an animal. This definition does not include proper maintenance of animals for show or sport; use of animals for food, lawful hunting, fishing or trapping.*

The collection is then broken down utilizing the following data values to help define the exact nature of the criminal offense:

- Simple/Gross Neglect
- Intentional Abuse and Torture
- Organized Abuse (Dog Fighting and Cock Fighting)
- Animal Sexual Abuse

### ***Cyberspace***

Cyberspace was implemented in January 2016, as a new NIBRS location code (#58) and is defined as:

- A virtual or internet-based network of two or more computers in separate locations, which communicate either through wireless or wire connections”.

The intent of the cyberspace location is to properly capture offenses which could not have occurred had the internet not been available. While not an offense itself, Cyberspace as a location is being implemented at the same time as two additional Group A fraud offenses. The two new offenses are:

- Identity Theft (26F): Wrongfully obtaining and using another person’s personal data (e.g., name, date of birth, Social Security number, driver’s license number, credit card number)
- Hacking/Computer Invasion (26G): Wrongfully gaining access to another person’s or institution’s computer software, hardware, or networks without authorized permissions or security clearances.

Not all 26F and 26G fraud offenses will be directly associated with the 58 location code Cyberspace. Cyberspace is to be utilized to identify those offenses known to law enforcement which had the internet not been accessible/available, then the crime identified could not have been committed.

### ***Cargo Theft***

Although participation in the UCR Program is voluntary, and states or agencies may choose not to participate, the National UCR Program is continuing efforts to collect and report accurate and complete Cargo Theft data. In 2013, seven states participated in the first release of Cargo Theft data from the National UCR Program. In 2014, a total of 29 states and the Bureau of Indian Affairs submitted Cargo Theft data to the National UCR Program. In 2015, a total of 31 states and the Bureau of Indian Affairs participated in submitting data to the UCR Program, although only 19 states were able to verify data submitted as publishable.

Participation in the Cargo Theft Initiative has gradually increased; however, several factors have been identified having a direct impact on this important data collection:

- States may not have the resources required to make the necessary technical changes or to align their local and state statutes with federal requirements.
- States may not have the necessary resources to conduct data quality checks on reported

incidents associated with cargo theft, which could result in inaccurate data reported.

- States may not have adequate resources to train participants on how to recognize and properly record cargo theft incidents.
- States may not perceive cargo theft as a priority or a significant problem within their states and make decisions based on their immediate needs regarding resources allocation.

Quality data concerning cargo theft can help us better understand this crime and the threats associated with it. As more agencies choose to report their incidents, the FBI's UCR Program will be able to provide more information about cargo theft on a national scale.

### **APB Topic Update (December 2016)**

1. **APB Item #13 UCR Issue #1:** Modification of the UCR Program Data Collection to Include 26F = Identity Theft and 26G = Hacking/Computer Invasion for the Cargo Theft Data Collection.

**APB Motion:** The APB moved to accept Option 2: Add the offense codes of 26F = Identity Theft and 26G = Hacking/Computer Invasion as cargo theft related offenses for the reporting of Cargo Theft data in the National Incident-Based Reporting System (NIBRS). Priority Level 3M

**National UCR Program Status:** Appropriate Office of Management and Budget documentation has been submitted. In addition, staff is working to update appropriate user manual and technical specifications.

2. **APB Item #13 UCR Issue #2:** Development of a State Profile for Each UCR Program.

**APB Motion:** The APB moved to accept Option 2: Accept the state profile with the following changes:

- Under state UCR personnel add a category for "other."
- Under the agency reporting status, if mandatory, add state statute.
- Create a new bullet item for describing the state NIBRS certification process, and
- Remove the "additional data information" section.

**National UCR Program Status:** All state profiles have been sent for verification to each respective State Program Manager.

3. **APB Item #13 UCR Issue #3:** Expansion of the UCR Program Police Employee Collection.

**APB Motion:** The APB moved to accept Option 1.1: In consultation with CJIS Systems Officers (CSOs) and UCR State Program Managers, add the ability to capture the following information to the current Police Employee collection:

- Part-time (to include officers and civilian staff working on average less than 35 hours per week)
- Reserve/Auxiliary/Other (to include other staff and volunteers serving as a law enforcement officer at the request of a law enforcement agency whose officers meet the current Law Enforcement Officers Killed and Assaulted (LEOKA)

definition).

**National UCR Program Status:** In development.

**APB Motion: II.** Addition of Race and Ethnicity to Police Employee Counts

The APB moved to accept Option 2.1: In consultation with CSOs and UCR State Program Managers, add the ability to capture the following race and ethnicity categories to the Police Employee collection:

- Hispanic or Latino, of any race
- American Indian or Alaska Native, not Hispanic or Latino
- Asian, not Hispanic or Latino
- Black or African-American, not Hispanic or Latino
- Native Hawaiian or Other Pacific Islander, not Hispanic or Latino
- White, not Hispanic or Latino
- Two or more races, not Hispanic or Latino

**National UCR Program Status:** In development.

**APB Motion: III.** Addition of Recorded Contacts with Citizens to the Annual Police Employee Collection.

The APB moved that the UCR Program Office (PO) in consultation with, at a minimum, the CJIS Systems Officers (CSO) and UCR State Program Managers shall establish a common definition for “police contact” with citizens for collection in the annual Police Employee data collection. The UCR PO will notify the APB of the common definition. Any changes to the common definition established by the UCR PO shall go through the advisory process.

**National UCR Program Status:** Topic paper with the proposed definition will be presented at the 2017 Fall Working Groups.

4. **APB Item #13 UCR Issue #4:** Proposal to Allow Vehicular/Vessel Negligent Manslaughter and Vehicular/Vessel Negligent Assault Data to be submitted to the National UCR Program’s NIBRS.

APB Motion: Regarding Collecting the V/VNM (Impaired and/or Distracted Operator) offenses under Negligent Manslaughter. This change would require modifying the definition of Negligent Manslaughter to include Driving Under the Influence (DUI) and other offenses (see below), modify Data Element (DE) 8 (Offender Suspected of Using) to include ‘handheld devices’ with Computer Equipment, modify DE 13 (Type Weapon/Force Involved) to include ‘Vessel’ with Motor Vehicle, and modify the paragraph referring to Negligent Manslaughter in DE 31 (Aggravated Assault/Homicide Circumstances) to allow for collecting traffic fatalities using the identified offenses.

- Negligent Manslaughter – The killing of another person through negligence.



- This offense includes killings from hunting accidents, gun cleaning, children playing with guns, and arrests associated with DUI, distracted driving (using a cell/smartphone), and reckless driving traffic fatalities.
- It does not include deaths of persons due to their own negligence and accidental deaths not resulting from gross negligence, and accidental traffic fatalities.
- Note: The Vehicular Manslaughter Task Force supports the addition of arrests associated with distracted driving (using a cell/smartphone) and reckless driving traffic fatalities as a result of law enforcement's investigative findings.

**APB Motion:** Regarding creating a new V/VNA (Impaired and/or Distracted Operator) offense: The APB moved to make no change.

**National UCR Program Status:** The documentation has been submitted to OMB. Upon approval documentation will be forwarded to OMB. Collection will begin January 1, 2019.

#### 5. **APB Item #13 UCR Issue #5:** NIBRS User Manual Changes

**APB Motion:** The APB moved to request the UCR Program Office update the NIBRS User Manual to incorporate the administrative revisions identified by FBI CJIS and forward the document to the Association of State Uniform Crime Reporting Programs (ASUCRP) for review and comment.

**National UCR Program Status:** User Manual was submitted to ASUCRP for comment and document is currently being reviewed by CSMU staff to ensure synchronization with the User Manual and NIBRS Technical Specification document Version 3.2.

#### **FALL 2017 WORKING GROUP ACTIONS:**

Accepted as information only by all five working groups.

#### **FALL 2017 UCR SUBCOMMITTEE ACTION:**

Accepted as information only.

**CJIS ADVISORY POLICY BOARD (APB)  
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**UCR ISSUE #2**

Modification of the Application of the Current Embargo Policy for the Release of UCR Program Data

**PURPOSE**

To propose a modification of the current data embargo policy that would allow for the UCR Program to update data in the Crime Data Explorer on a more frequent basis.

**POINT OF CONTACT**

Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to decide on whether to implement the proposed change to the application of the UCR data embargo policy.

**BACKGROUND**

On June 30, 2017, the UCR Program launched its Crime Data Explorer (CDE), which provides users a more interactive and visual interface with UCR data. The CDE is one of five parts of the Crime Data Modernization Director's Priority Initiative. The goal of the Crime Data Modernization initiative is "to improve the nation's Uniform Crime Reporting (UCR) crime statistics for reliability, accuracy, accessibility, and timeliness, and to expand depth and breadth of data collected."

Specifically, the CDE seeks to increase the accessibility and timeliness of crime data releases by creating a site that is more easily updated as newer data is available for publication. While not one of the official publications of the UCR Program, it does change the general approach to releasing data in both easily-consumable visualizations as well as provides new Application Programming Interfaces (commonly referred to as APIs) to release raw data. The technical framework of the CDE allows for the UCR Program to push new data to the site on a more frequent basis than annually.

## **DISCUSSION AND ANALYSIS**

### *Current Embargo Policy*

The UCR embargo policy states that “[c]ontributing law enforcement agencies are deemed to own their respective data until the FBI formally publishes them. Therefore, until the time of official release, the data are restricted from any entity besides the owning agency requesting them. Once published, UCR data (as a whole) falls into the public domain and is accessible to anyone upon request.<sup>1</sup>” The embargo policy does not prevent the UCR Program from releasing data as frequently as it publishes it. However, the embargo has always been enforced until the annual release of crime data, even though the data may be published more frequently. For example, Part I offenses are published with six-months of data in the Preliminary Semi-annual Release and with twelve-months of data in the annual publication, *Crime in the United States*. The data files are not released to requestors until the publication of *Crime in the United States*.

### *Impact of Embargo Policy on Contributing Agencies and the FBI UCR Program*

The FBI acknowledges that the benefits derived from enforcing the embargo on an annual basis primarily address concerns regarding the frequency of reporting for data quality reviews and resources associated with those reviews. The annual embargo is useful to encourage more frequent periodic data submissions from state and domain UCR programs and directly-contributing agencies with the assurance that data will not be prematurely released. This allows for FBI UCR Program staff to use the extra time to review the data submission and correspond with the state and domain UCR programs regarding questions about the data. Many state and domain UCR programs only publish their own data on an annual basis due to limited resources to handle the compilation of data and requests for information from the media and other entities.

As a collateral benefit, the FBI cites the data embargo for delaying the fulfillment of pre-publication requests for data regardless of whether they have been received directly to the FBI UCR Program or through the Freedom of Information Act process.

### *Positioning the FBI UCR Program for More Frequent Publications*

It has been noted that there is a need to increase the frequency of publications to provide more timely views of crime data. The launch of the CDE provides a platform for the FBI UCR Program to release data sooner after its submission by contributing agencies. By discontinuing the application of the existing data embargo policy, the FBI UCR Program will be in a better position to take advantage of the technological improvements with data ingest and data dissemination and release data as soon as it is deemed appropriate.

---

<sup>1</sup> “Uniform Crime Reporting Policy Implementation Guide,” Federal Bureau of Investigation, Criminal Justice Information Services Division, November 23, 2010.

## **RECOMMENDATION**

In order to fully take advantage of new upcoming improvements to its data collection/ingest system and the CDE, the FBI UCR Program recommends that the current application of the embargo policy cease. Instead, the FBI UCR Program looks to refresh the data in the CDE at appropriate intervals.

## **OPTIONS**

Option 1:

The UCR Program should cease its application of the data embargo policy allowing for more frequent updates to the CDE.

Option 2:

No change

## **FALL 2017 WORKING GROUP ACTIONS:**

### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: The UCR Program should cease its application of the data embargo policy allowing for more frequent updates to the CDE.

**Action:** Motion carried.

### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** The UCR Program should cease its application of the data embargo policy allowing for more frequent updates to the CDE with appropriate caveats indicating the data may be incomplete or partial from some contributors.

**Action:** Motion carried.

### **NORTHEASTERN WORKING GROUP ACTION**☺

**Motion:** Refer the question back to the UCR Subcommittee for recommendations on frequency of submission, frequency of release, what data elements are to be collected and released, and what caveats concerning the data that is released.

**Action:** Motion carried.

### **SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1: The UCR Program should cease its application of the data embargo policy allowing for more frequent updates to the CDE.

**Action:** Motion carried.

### **WESTERN WORKING GROUP ACTION:**

**Motion:** The Western Working Group supports the concept of eliminating the data embargo. It directs CJIS to further explore the concept and bring back their findings to the Working Groups prior to implementation.

**Action:** Motion carried.

**FALL 2017 UCR SUBCOMMITTEE ACTIONS:**

**Motion 1:** To accept Option 1: The UCR Program should cease its application of the data embargo policy allowing for more frequent updates to the CDE.

**Action:** Motion carried.

**Motion 2:** Prior to the 2017 and later data being published in the CDE, the FBI (in cooperation with local, state, federal, tribal, and academic representatives) will develop the necessary standards on frequency of submission, frequency of release, what data elements are to be collected and released, and what caveats concerning the data that is released. The work of the FBI will be concluded by May 2018.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**UCR ISSUE #3**

Addition of UCR Offenses for Federal Crime Reporting to the National Incident-Based Reporting System (NIBRS)

**PURPOSE**

The purpose of this paper is to present the recommendation of additional UCR offenses for federal agencies to report crime data to the NIBRS.

**POINT OF CONTACT**

Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the recommendations and changes presented in this paper and recommend options for federal reporting to the UCR Program.

**BACKGROUND**

The FBI's Criminal Justice Information Service (CJIS) Division's Crime Data Modernization (CDM) Team has been working with federal agencies to assist them in complying with the Uniform Federal Crime Reporting Act (UFCRA) of 1988, which states, "The Attorney General shall acquire, collect, classify, and preserve data on Federal Criminal offenses as part of the Uniform Crime Reports. All departments and agencies within the federal government (including the Department of Defense) which routinely investigate complaints of criminal activity, shall report details about crime within their respective jurisdiction to the Attorney General in uniform manner and on a form prescribed by the Attorney General. The reporting required by this subsection shall be limited to the reporting of those crimes comprising the Uniform Crime Reports." During the process of working with federal agencies, the CDM Team learned federal agencies are unique in the types of crimes they investigate and how investigations are managed. In addition, differences exist at the federal level regarding the length of the case investigations and the location of the crimes nationwide. These differences must be taken into account to allow

federal data to be displayed clearly without impacting the data submitted by local, state, and tribal agencies.

In order to resolve the issues facing federal agencies, the CDM Team organized a Federal Task Force consisting of representatives from the Department of Homeland Security (DHS), the United States (U.S.) Marshals Service (USMS), the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Environmental Protection Service (EPA), the Department of the Interior (DOI), and the Drug Enforcement Administration (DEA). During the discussion, the task force addressed the need to expand the Group A and B offenses to be added in order to capture details of crime for federal reporting.<sup>1</sup>

## **DISCUSSION AND ANALYSIS**

The majority of federal agencies capture crime information within their Records Management Systems based on U.S. Statutes. In mapping these statutes to the NIBRS UCR offense codes, many offenses investigated by federal law enforcement would map to a ‘90Z All Other Offenses’ category, reducing transparency in crime reporting.

The current mapping of these offenses when compiled for statistical comparison would be misleading because the true crime (i.e., immigration violations, perjury, treason, etc.) would not be explicitly stated. For example, in Calendar Year 2016, 13 percent (2,992) of FBI arrests, 7 percent (588) of ATF arrests, and 25 percent (34,455) of USMS arrests were classified as ‘90Z All Other Offenses’. It is anticipated the number of offenses mapped to the 90Z category will increase significantly as additional federal agencies begin reporting.

In order to provide a valuable data set of federal crime, a change in the NIBRS reporting should be considered for federal law enforcement agencies. The Federal Task Force recommends adding the following National Crime Information Center derived offense codes to the NIBRS Group A offenses:

- 26H – Money Laundering (Crime Against Society)
  - The process of transforming the profits of a crime into a legitimate asset.
- 36C – Failure to Register as a Sex Offender (Crime Against Society)
  - The failure to register or update a registration as required as a sex offender.
- 101 – Treason (Crime Against Society)
  - The crime of betraying one’s country, especially by attempting to kill the sovereign or over throw the government.
  -

---

<sup>1</sup> Law enforcement must report both incidents and arrests for Group A offenses, which are based on the seriousness or significance of an offense, the frequency, and the prevalence. A full description of Group A and Group B classification criteria can be found on page 12 of the Criminal Justice Information Services (CJIS) Division UCR Program NIBRS User Manual, Version 1.0, dated 01/17/2013, <<https://ucr.fbi.gov/nibrs/nibrs-user-manual>>.

- 103 – Espionage (Crime Against Society)
  - The practice of spying or using spies, typically by governments to obtain political and military information.
- 301 – Illegal Entry to the U.S. (Crime Against Society)
  - To attempt to enter the U.S. at any time or place other than as designated; or eludes examination/inspection by immigration officers.
- 302 – False Citizenship (Crime Against Society)
  - Whoever falsely and willfully represents themselves to be a citizen of the U.S.
- 303 – Smuggling Aliens (Crime Against Society)
  - When a person knowingly encouraged, induced, assisted, abetted, or aided another person to enter, or try to enter, the U.S.
- 304 – Re-entry After Deportation (Crime Against Society)
  - Individual who enters, attempts to enter, or has been found in the U.S. after being removed, excluded, deported, or has departed the U.S. while an order of removal exclusion or deportation is outstanding.
- 399 – Other Immigration Violations (Crime Against Society)
  - All other immigration violations.
- 490 – Fugitive (Harboring Escapee/Concealing from Arrest) (Crime Against Society)
  - Harboring or concealing any person for whose arrest a warrant or process has been issued under the provision of any law of the U.S. to prevent his/her discovery and arrest. This includes any prisoner after his/her escape from the custody of the Attorney General, or from a federal penal or correctional institution.
- 499A – Fugitive (Flight to Avoid Prosecution) (Crime Against Society)
  - Moving or traveling in interstate or foreign commerce with intent to avoid prosecution, custody, confinement, or to avoid giving testimony in any criminal proceedings.
- 499B – Fugitive (Flight to Avoid Deportation) (Crime Against Society)
  - Moving or traveling in interstate or foreign commerce with intent to avoid deportation.
- 500 – Perjury (Crime Against Society)
  - The offense of willfully telling an untruth in a court after having taken an oath of affirmation.
- 580 – Import Violations (Crime Against Property)
  - Any individual who knowingly or willfully, with intent to defraud the U.S., smuggles, imports, or clandestinely introduces, or attempts to smuggle, import, or clandestinely introduce, merchandise that should have been invoiced, received, bought, sold, or facilitates the transportation, the concealment, or sale of such merchandise after importation.
- 581 – Export Violations (Crime Against Property)
  - Any individual who knowingly or willfully, with intent to defraud the U.S., smuggles, exports, or clandestinely distributes, or attempts to smuggle, export, or clandestinely distribute, merchandise that should have been invoiced, received,



bought, sold, or facilitates the transportation, the concealment, or sale of such merchandise after exportation.

- 610A – Federal Liquor Offenses (Crime Against Society)
  - The shipment or transportation of any intoxicating liquor of any kind, from one State, Territory, or District of the United States, into any other State, Territory, or District of the United States, which fails to comply with legislation.
- 610B – Federal Tobacco Offenses (Crime Against Society)
  - The sell, transfer, shipment, or transportation of cigarettes or smokeless tobacco for profit into a State, locality, or Indian country of an Indian tribe which fails to comply with legislation.
- 620 – Wildlife Trafficking (Crime Against Society)
  - Violations of the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), which regulates exports, imports, and re-exports of wildlife.

The Federal Task Force recommends the following Group B additions:

- 90K – Bond Default/Failure to Appear (Crime Against Society)
  - The failure to appear in court without a satisfactory excuse, after bond has been set.
- 90L – Federal Resource Violations (Crime Against Society)
  - Crimes related to the damage or destruction of the nation’s natural resources including land, mineral, air, or water such as the violation of any Act regarding national parks, national monuments, or any natural resource covered by the jurisdiction of federal agencies such as The Lacey Act, Antiquities Act, Wilderness Act, National Historic Preservation Act, etc.

At this time, these offenses would only be reported by federal agencies. In the future, these additional offense types could be made available for reporting by local and state law enforcement agencies if recommended. The UCR Program is anticipating these changes will be made to the NIBRS in Fiscal Year 2018.

## **OPTIONS**

Option 1—Accept all recommended NIBRS UCR offense codes for federal reporting.

Option 2—Accept all recommended NIBRS UCR offense codes for federal reporting. In addition, accept the following further offense codes (please list):

## **RECOMMENDATION**

The UCR Program recommends accepting all recommended offenses as new options for federal reporting.

## **FALL 2017 WORKING GROUP ACTIONS:**

### **FEDERAL WORKING GROUP ACTION:**

**Motion:** Moved to accept Option 1: Accept all recommended NIBRS UCR offense codes for federal reporting.

**Action:** Motion carried.

### **NORTH CENTRAL WORKING GROUP ACTION:**

This topic was accepted for information only.

### **NORTHEASTERN WORKING GROUP ACTION:**

This topic was accepted for information only.

### **SOUTHERN WORKING GROUP ACTION:**

This topic was accepted for information only.

### **WESTERN WORKING GROUP ACTION:**

**ACTION ITEM:** To explore expanding beyond federal agencies to states and local agencies, and to bring back through Working Groups in the spring.

## **FALL 2017 UCR SUBCOMMITTEE ACTION:**

**Motion:** To accept Option 2: Accept all recommended NIBRS UCR offense codes for federal and tribal reporting. In addition, accept the following further offense codes and additional changes:

- 520A – Firearm (violation of the National Firearm Act of 1934)
  - The violation of federal laws prohibiting the manufacture, importation, sale, purchase, transfer, possession or interstate transportation of unregistered (non-tax paid) weapons including machineguns, firearm mufflers or silencers, short barreled rifles, short barreled shotguns, destructive devices, and any other weapons as defined at 26 USC § 5845 - Definitions.
- 520B – Weapons of Mass Destruction
  - The violation of federal laws prohibiting the unlawful use, attempted use, conspiracy to use, or use of interstate travel or facilities in furtherance of the use of a weapon of mass destruction as defined at 18 U.S. Code § 2332a - Use of weapons of mass destruction
- 526 – Explosives
  - The violation of federal laws prohibiting the manufacture, importation, sale, purchase, transfer, possession, unlawful use, interstate transportation, or improper storage of explosives as defined at 18 USC § 841 (c).

**Additionally, the definitions of the below offenses are amended as follows:**

- Federal Liquor Offense
  - The violation of federal laws prohibiting the production, importation, distribution, transportation, sale, purchase, or possession of non-tax paid distilled spirits, wine, or beer, and the equipment or devices utilized in their preparation.
- Federal Tobacco Offense
  - The violation of federal laws prohibiting the production, importation, distribution, transportation, sale, purchase, or possession of non-tax paid tobacco products.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**UCR ISSUE #4**

The Use of the Judicial District (JD) for Federal Agencies to Report a National Incident-Based Reporting System (NIBRS) Incident to the UCR Program

**PURPOSE**

The purpose of this paper is to present the recommendation for federal agencies to report the location of a NIBRS incident to the UCR Program by JD.

**POINT OF CONTACT**

Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the recommendations and changes presented in this paper and recommend options for federal reporting to UCR.

**BACKGROUND**

The FBI's Criminal Justice Information Service (CJIS) Division's Crime Data Modernization (CDM) Team has been working with federal agencies to assist them in complying with the Uniform Federal Crime Reporting Act (UFCRA) of 1988, which states, "The Attorney General shall acquire, collect, classify, and preserve data on Federal Criminal offenses as part of the Uniform Crime Reports. All departments and agencies within the federal government (including the Department of Defense) which routinely investigate complaints of criminal activity, shall report details about crime within their respective jurisdiction to the Attorney General in uniform manner and on a form prescribed by the Attorney General. The reporting required by this subsection shall be limited to the reporting of those crimes comprising the Uniform Crime Reports." During the process of working with federal agencies, the CDM Team learned federal agencies are unique in the types of crimes they investigate and how investigations are managed. In addition, differences exist at the federal level regarding the length of the case investigations and the location of the crimes nationwide. These differences must be taken into account to allow

federal data to be displayed clearly without impacting the data submitted by local, state, and tribal agencies.

In order to resolve the issues facing federal agencies, the CDM Team organized a Federal Task Force consisting of representatives from the Department of Homeland Security (DHS), the United States (U.S.) Marshals Service (USMS), the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Environmental Protection Service (EPA), the Department of the Interior (DOI), and the Drug Enforcement Administration (DEA). During the discussion, the task force addressed how federal agencies would report the location where an incident occurred to the UCR Program.

## **DISCUSSION AND ANALYSIS**

For local, state, and tribal law enforcement agencies, the location of a crime is linked to the submitting agency's Originating Agency Identifier (ORI). Federal agencies have jurisdiction in most, if not all, of the United States mainland and territories. Federal agencies submitting UCR data utilizing the ORIs assigned to each field office provide the arresting agency details, but the ORI does not designate the area where the crime occurred. The Area of Responsibility (AOR) of a field office may span multiple states and federal agents may work well outside their home field office AORs. Some federal agency field offices are geographically aligned, whereas others are aligned with federal court jurisdictions.

The Federal Task Force recommends using the JD to identify the location of the incident. A JD does not cross state boundaries or split a county. By using JD as the location, all federal UCR data will be reported in the same manner, resulting in a standardized dataset. To accomplish this for federal submissions, a new Data Element (DE), Judicial District Code, would be created to capture a three-digit numerical code associated with the JD for reporting to the NIBRS. For example, the Southern Alabama JD encompasses the counties of Baldwin, Choctaw, Clarke, Conecuh, Dallas, Escambia, Hale, Marengo, Mobile, Monroe, Perry, Washing, and Wilcox. The Southern Alabama JD identification number is '3'. When any federal agency investigates an incident in that locale, the new DE would capture this as '003' to represent the location of the incident, and not the location of prosecution. Currently, there are 95 JDs in the U.S. and territories. The Federal Task Force recommends that the DE be three characters to accommodate possible changes in the number of JDs. This would minimize the necessity of modifications to the NIBRS.

Federal agencies are concerned with the granularity of the incident location. Many undercover agents (UA) and confidential informants (CI) operate within federal investigations. There is concern that if the location is too granular, criminals could utilize the UCR data to determine knowledge of agency cases or, a worst case scenario, the details would lead to a degradation in case integrity and affect judicial proceedings. This could be possible though there is no personally identifiable information to identify a UA or CI. The members of the Federal Task Force believe using the JD is a good compromise between granularity and obscurity. Because

the JDs have county and state boundaries, comparisons of federal data to local and state data can be analyzed to a reasonable degree.

Without the addition of the JD, the UCR Program would lose the ability to map a large portion of the federal data to a geographic region. Data submitted by federal agencies, in many cases, would come from one location and the accompanying ORI. For example, ORI DCATF0000 is for ATF Headquarters. Using this ORI, all ATF NIBRS submissions would have the incident location as Washington D.C. Using the Judicial District, a NIBRS submission would come in for ATF (DCATF0000) with a DE value of '003'. This submission would show that the incident is being reported by the ATF and it occurred in the Southern Alabama JD verses showing the incident occurred in D.C.

The UCR Program understands there are federal agencies currently working toward compliance with the UFCRA using the current NIBRS Technical Specification<sup>1</sup>. This change will directly impact those federal agencies. However, all of the agencies currently developing technical solutions are aware of the recommended change. While this change will have an affect on those agencies, the feedback has been positive, as it is recognized as a necessary change in order to have a standard reporting location for all federal agencies. This change will have no impact to local, state, and tribal agencies. The UCR Program is anticipating these changes will be made to the NIBRS in Fiscal Year 2018.

### **OPTIONS**

Option 1—Create a new DE that exists in the Administrative Segment that captures the JD code for federal agencies to report the location of a NIBRS incident to the UCR Program.

Option 2—No Change.

### **RECOMMENDATION**

The UCR Program recommends creating a new DE that exists in the Administrative Segment that captures the JD code.

### **FALL 2017 WORKING GROUP ACTIONS:**

#### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Create a new DE that exists in the Administrative Segment that captures the JD code for federal agencies to report the location of a NIBRS incident to the UCR Program.

**Action:** Motion carried.

---

<sup>1</sup> The current NIBRS Technical Specification is Version 3.1 dated 02/01/2017, CJIS Document Number – UCRRP-DOC-04521-3.1.

**NORTH CENTRAL WORKING GROUP ACTION:**

This topic was accepted for information only.

**NORTHEASTERN WORKING GROUP ACTION:**

This topic was accepted for information only.

**SOUTHERN WORKING GROUP ACTION:**

This topic was accepted for information only.

**WESTERN WORKING GROUP ACTION:**

This topic was accepted for information only.

**FALL 2017 UCR SUBCOMMITTEE ACTION:**

**Motion:** To accept Option 1: Create a new DE that exists in the Administrative Segment that captures the JD code for federal agencies to report the location of a NIBRS incident to the UCR Program.

**Action:** Motion carried.

**CJIS ADVISORY POLICY BOARD (APB)  
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**UCR ISSUE #5**

Expansion of the UCR Program Police Employee Collection

**PURPOSE**

To propose a definition for measuring the number of police contacts with the public in order to relate them to incidents of use of force and assaults against law enforcement officers.

**POINT OF CONTACT**

Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review the definition for measuring police-public interactions and either approve or approve with modifications.

**BACKGROUND**

In December 2015, the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) approved a series of recommendations that created a new UCR Program data collection on law enforcement use of force. Part of the process of identifying the scope and content of the new data collection is the input from a Task Force comprised of law enforcement representatives and representatives from the major law enforcement organizations. A key theme to the discussions from both the CJIS APB and the Task Force is the need to provide sufficient context around the data collected on use of force in order for the general public to understand the reported figures. As a result, the Task Force recommended at its May 4, 2016, meeting that the UCR Program pursue the additional information on agency activities to the UCR Program Police Employee collection.

The Police Employee collection is an annual collection that includes details on the sworn or civilian status and gender of the law enforcement agency staff as of October 31 of the collection year. The information was originally included on an early version of the Law Enforcement Officers Killed and Assaulted (LEOKA) form when both collections were annual. However, by the mid-1970s, the two collections separated as the LEOKA data changed to a monthly report, while the Police Employee collection remains an annual one. While the collection could be considered a part of the Summary Reporting System, the information is not specifically addressed in the technical



specifications of the National Incident-Based Reporting System (NIBRS). In the future, these specifications will either be included in those for the NIBRS or in a separate specification. A key component to interpreting the information that is collected in the LEOKA Program, as well as the proposed data collection on law enforcement use of force, is the volume of police contacts with the public. There is no national measure available that would provide a standardized estimate for the number of times a law enforcement officer interacts with members of his or her community. As the UCR Program looks to add a data collection on law enforcement use of force, it is critical to contextualize these data within the broader idea of the volume of interactions that occur over the course of a year. The UCR Program is proposing that some basic counts of these interactions be collected on an annual basis and that the Police Employee collection is the best means to achieve that goal.

The concept of adding measures of police-public interaction to the existing Police Employee collection was taken through the CJIS APB process in the fall of 2016. The purpose of the initial proposal was to gauge general support for the concept and elicit feedback on the viability of the proposed collection. During discussion at the Working Groups and the UCR Subcommittee meetings, there was concern that some early examples were biased towards the types of interactions that take place between municipal police departments and the public. Members who represent sheriffs' offices and federal agencies voiced a need to add interactions that do not necessarily fall neatly into a "call for service" paradigm. These same concerns were echoed in the discussion with the CJIS APB in December 2016. During the discussion of the motion, the membership stated a desire for the categories to be reviewed by representatives from the law enforcement community and that the Use of Force Task Force would be well-suited to provide that input. The final approved motion from the CJIS APB reads:

APB Recommendation #14: III. Addition of Recorded Contacts with Citizens to the Annual Police Employee Collection

"The APB moved that the UCR Program Office (PO) in consultation with, at a minimum, the CSOs and UCR State Program Managers shall establish a common definition for "police contact" with citizens for collection in the annual Police Employee data collection. The UCR PO will notify the APB of the common definition. Any changes to the common definition established by the UCR PO shall go through the advisory process."

## **DISCUSSION AND ANALYSIS**

The UCR Program will focus on the types of information that are typically captured in the computer-aided dispatch (CAD) system or some similar system used to record officer contacts with the public such as calls for service and officer-initiated activity. Because both systems and policies regarding the recording of information may vary from agency-to-agency, the UCR Program will request some additional subcategories that will allow for the proper interpretation of these volumes and enhance the analytical value of the data. In addition to the utility of this data within the LEOKA and the law enforcement use of force data collections, these counts will also allow for the UCR Program to fine-tune its current methodology used to produce national, regional, and state estimates of crime volumes that account for agencies that have not provided complete crime data

within a reporting year. The total number of recorded calls/requests can be used as an additional measure to categorize agencies with similar agencies.

*Description of the Data Collection on Police-Public Interactions*

The description for the new data to be collected on the police and public interactions was built around the LEOKA-Feloniously Killed data collection and the National Use-of-Force Data Collection. Both data collections have questions that capture information on the law enforcement activities that were occurring at or near the time of the event. By using broad categories that can be closely aligned with the two existing data collections, the UCR Program will assist law enforcement agencies in two important ways. First, the additional detail will provide law enforcement agencies with guidance on how certain activities or interactions should be coded. The categories in existence within the LEOKA-Feloniously Killed data collection and the National Use-of-Force Data Collection have either worked or will be working (i.e., the pilot study of the National Use-of-Force Data Collection) with agencies to clarify the meaning behind each collection’s categories. Second, the coordination of the proposed categories with the two existing data collections also ensures that the data derived from the collection can provide analytical value. The Table 1 below provides a “crosswalk” between the proposed categories for police-public interactions and the two existing data collections—LEOKA-Feloniously Killed data collection and the National Use-of-Force Data Collection. In addition, a third category of law enforcement activities that may not be specifically captured in the existing data collections is also provided.

The proposed description was presented to the Use of Force Task Force for discussion and comment. The feedback from the Task Force was centered on the idea of limiting the number of categories in order to minimize the burden of participating in the data collection by law enforcement agencies. After reviewing an early draft that proposed as many as twelve categories, the consensus of the group was that many activities could be classified as either calls for service or unit/officer-initiated activities. Additional categories were also recommended for law enforcement activities that are more commonly associated with crowd control or group events. The final recommended set of categories are the following five categories: citizen calls for service; unit/officer-initiated contacts; protests/mass demonstrations/other security detail; court/bailiff activities; and community outreach.

*Table 1. Crosswalk between the proposed categories for police-public encounters and the existing data collections in the Uniform Crime Reporting Program*

<b>Police-Public encounters</b>	<b>LEOKA (Feloniously Killed)</b>	<b>National Use-of Force Data Collection</b>	<b>Other Activities</b>
Citizen calls for service	<ul style="list-style-type: none"> <li>• Citizen complaint (all)</li> <li>• Respond to a crime in progress (all)</li> <li>• Respond to a report of a crime (all)</li> <li>• Disturbance call</li> <li>• Domestic disturbance</li> <li>• Domestic violence</li> </ul>	<ul style="list-style-type: none"> <li>• Response to unlawful or suspicious activity</li> <li>• Medical, mental health, or welfare assistance</li> <li>• Warrant service</li> <li>• Service of a court order</li> </ul>	

<b>Police-Public encounters</b>	<b>LEOKA (Feloniously Killed)</b>	<b>National Use-of Force Data Collection</b>	<b>Other Activities</b>
	<ul style="list-style-type: none"> <li>• Handling persons with mental illness</li> <li>• Arrest situation</li> <li>• Encounter or assist an</li> </ul>		
	<p>emotionally disturbed person</p> <ul style="list-style-type: none"> <li>• Tactical situation-serving/attempted to serve arrest warrant</li> <li>• Tactical situation-Serving/Attempting to serve search warrant</li> </ul>		
Unit/officer-initiated contacts	<ul style="list-style-type: none"> <li>• Investigative activity</li> <li>• Investigate suspicious persons or circumstances</li> <li>• Investigate possible DUI/DWI suspect</li> <li>• Investigate motor vehicle crash</li> <li>• Wanted person</li> <li>• Tactical situation-Active shooter</li> <li>• Tactical situation-barricaded/hostage situation</li> <li>• Tactical situation-other tactical situation</li> <li>• Undercover situation</li> <li>• Drug-related matter</li> <li>• Felony traffic stop</li> <li>• Traffic violation stop</li> <li>• Assist another law enforcement officer (all)</li> <li>• Respond to an alarm (all)</li> <li>• Pursuit (all)</li> <li>• Traffic control</li> <li>• Assist motorist</li> <li>• Prisoner transport</li> <li>• Other administrative assignment</li> </ul>	<ul style="list-style-type: none"> <li>• Routine patrol other than traffic stop</li> <li>• Follow up investigation</li> <li>• Traffic stop</li> </ul>	<ul style="list-style-type: none"> <li>• Interviews with witnesses, subjects of investigations, other persons of interest (e.g., FBI FD-302s; DEA Form 6s, etc.)</li> </ul>
Protests/Mass demonstration/Other security detail	<ul style="list-style-type: none"> <li>• Civil disorder</li> </ul>	<ul style="list-style-type: none"> <li>• Mass demonstration</li> </ul>	<ul style="list-style-type: none"> <li>• Parades</li> <li>• Motorcade</li> </ul>
Court/Bailiff activities	<ul style="list-style-type: none"> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Other</li> </ul>	
Community outreach	<ul style="list-style-type: none"> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Other</li> </ul>	

*Measures*

In order to minimize the burden and avoid required record-keeping changes for contributing law enforcement agencies, the new collection will have a minimal number of measures. For law enforcement encounters that are often recorded at the call or request-level, a basic count will be requested for two of the proposed five categories. The Use of Force Task Force recommended that the count descriptions clearly indicate that it is not a person count, rather a count of the number of calls, requests, or reports. For the three law enforcement encounters and activities that are typically associated with large groups or crowds, the number of attendees is requested. Law enforcement agencies can specify, for any of these five categories, that the counts are based upon an estimate or not available.

The impact on state UCR programs and contributing agencies includes modification to current systems and reports that are used to provide police-employee counts as part of their regular UCR submission. The benefit to law enforcement is better contextual data that can be used to facilitate the proper interpretation of data collected by the LEOKA Program and on law enforcement use of force.

**RECOMMENDATION**

FBI CJIS recommends that the APB accept Option 1 as specified below.

**OPTIONS**

**Option 1:**

In consultation with CJIS Systems Officers and UCR State Program Managers, add the ability to capture the information on recorded police contacts with the public *to the annual Police Employee data collection*. Included in this collection should be the ability to discern the most common types of calls for service or officer-initiated actions that are recorded by the agency in a CAD system or other similar record-keeping system. (See the sample collection shown below.)

Please provide a count of the following types of recorded police contacts with the public by officers employed by your agency. All counts should include contacts from January 1 to December 31 of the calendar year.

<b>Category</b>	<b>Call/Request Count</b>
Citizen calls for service	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Unit/officer-initiated contacts	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
	<b>Attendee Count</b>
Protests/Mass demonstration/Other security detail	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Court/Bailiff activities	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Community outreach	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available

**Option 2:**

Approve the description in Option 1 with modifications

**Option 3:**

No change.

**FALL 2017 WORKING GROUP ACTIONS:**

**FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 2: The modification to Option 1 was that the topic be referred to the Federal Crime Data Reporting Task Force for review and the topic be brought back through the process with categories that pertain to Federal agencies.

**Option 2:** Approve the description in Option 1 with modifications.

Option 1: In consultation with CJIS Systems Officers and UCR State Program Managers, add the ability to capture the information on recorded police contacts with the public *to the annual Police Employee data collection*. Included in this collection should be the ability to discern the most common types of calls for service or officer-initiated actions that are recorded by the agency in a CAD system or other similar record-keeping system. (See the sample collection shown below.)

Please provide a count of the following types of recorded police contacts with the public by officers employed by your agency. All counts should include contacts from January 1 to December 31 of the calendar year.

<b>Category</b>	<b>Call/Request Count</b>
Citizen calls for service	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Unit/officer-initiated contacts	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
	<b>Attendee Count</b>
Protests/Mass demonstration/Other security detail	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Court/Bailiff activities	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Community outreach	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available

The Federal Working Group would refer this to the Federal Crime Data Reporting Task Force to provide recommendations for federal categories.

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To accept Option 3: No Change.

**Action:** Motion carried with 22 Yay/1 Nay

**NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper.

**Action:** Motion carried with 9 opposed.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** The UCR Subcommittee should review and bring back to the Working Groups recommended reporting that is in a contextual, consistent, and fair manner.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt a new Option 4. The Western Working Group supports this in concept. However, the data collection would not be implemented prior to a formal definition for police contact approved by the CSOs and state UCR Program managers.

**Action:** Motion carried

**FALL 2017 UCR SUBCOMMITTEE ACTIONS:**

**Motion:** Add the ability to capture the information on recorded police contacts with the public on an annual basis and revise the table as provided below.

Please provide a count of the following types of recorded police contacts with the public by officers employed by your agency. All counts should include contacts from January 1 to December 31 of the calendar year.

Category	Call/Request/Individuals on the Docket Count
Citizen calls for service	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable
Unit/officer-initiated contacts	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable
Court/Bailiff Activities	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable

**Action:** Motion carried.



**CJIS ADVISORY POLICY BOARD (APB)  
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**UCR ISSUE #6**

Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

**PURPOSE**

Present for discussion the current UCR Program definition of a law enforcement officer and the Law Enforcement Officers Killed and Assaulted (LEOKA) Program's data collection criteria in regard to law enforcement officers who are paid from government funds set aside specifically for payment of sworn law enforcement representatives.

**POINT OF CONTACT**

Law Enforcement Support Section, Crime Statistics Management Unit.

Questions regarding this topic should be directed to <[agmu@leo.gov](mailto:agmu@leo.gov)>.

**REQUEST OF THE SUBCOMMITTEE**

The Subcommittee is requested to review and approve the changes to the FBI UCR Program definition of a law enforcement officer and the LEOKA criteria and exclusions.

**BACKGROUND**

During the APB meeting on December 7, 2016, the FBI UCR Program was asked to review the definition of a law enforcement officer as it relates to the paid or unpaid status of a law enforcement officer and be a member of a public governmental law enforcement agency to ensure the terms do not contradict the current criteria for reporting LEOKA and provide a recommendation to the APB for consideration.

**DISCUSSION AND ANALYSIS**

During the 2014 Spring UCR Subcommittee meeting, it was suggested the UCR Program explore the removal of the "are paid from government funds set aside specifically for payment of sworn law enforcement representatives" item from the LEOKA criteria.



The 2014 fall meetings of the Working Groups, UCR Subcommittee and the APB resulted in the addition of an exception to the traditional LEOKA criteria. The LEOKA data collection includes victim officers who meet all of the following criteria:

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- Were members of a public governmental law enforcement agency
- Were paid from government funds set aside specifically for payment of sworn law enforcement representatives
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

#### Exclusions from the LEOKA Program's Data Collection

Deaths resulting from the following are not included in the LEOKA Program's statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program's statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers

The following is a portion of the LEOKA Policy which addresses the "paid from government funds set aside specifically for payment of sworn law enforcement representatives" item of the criteria:

#### Line of duty means:

Any action which an officer 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. The officer is compensated by the public law enforcement agency which he or she serves.

Any action the officer is so obligated or authorized to perform in the course of performing his or her functions as described above.

#### Elements of Law Enforcement Officer Status

All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective governmental authorities to uphold the law and to safeguard the rights, lives and property of American citizens. **They must have full arrest powers and be members of a public governmental law enforcement agency, paid from government funds set aside specifically for payment to sworn police law enforcement** organized for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

#### A public governmental law enforcement agency means:

Any agency, organized and governmental authorized to enforce criminal law, arrest violators and keep public order of the United States, any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands of the United States, Guam, American Samoa, the Trust Territories of the Pacific Islands, the Commonwealth of the Northern Mariana Islands, and any territory or possession of the United States, or any unit of local investigation government, department, agency, or instrumentality of any of the foregoing.

Officers not having full arrest powers are not included in the LEOKA Program. This refers to a portion of the UCR Program policy (UCR, Policy Implementation Guide, 0343PG). This policy pursuant to the intentions of the UCR founding fathers (International Association of Chiefs of Police) attempts to define a “law enforcement officer” or “law enforcement agency” as it relates to the UCR Program.

The term “law enforcement” or “law enforcement agency” describes the police officer, sheriff or federal officer who performs police duties of enforcing laws, investigating crimes for those crimes (particularly for UCR purposes) which might be solved by immediate follow-up investigation or are likely to have suspects close to the crime scene. As his primary duty, this law enforcement officer would respond to routine calls for police service/emergencies, crime scenes, perform routine patrol, render emergency services, enforce criminal laws and traffic regulations, and investigate violations of criminal laws and traffic accidents. Finally, the law enforcement officer is one who ordinarily wears a badge, carries a gun, has full arrest powers, and is paid from government funds set aside specifically for payment to sworn police law enforcement representatives.

Therefore, for example, after serious consideration and reflection on the term “law enforcement officers” as it relates to the UCR Program, individuals such as Federal judges, U.S. and Assistant U.S. Attorneys, Probation Officers, Bureau of Prison Officers, and Correctional/Corrections Officers are not incorporated in the program.

The intention of the founding fathers of the UCR Program was to create a data collection (LEOKA) to capture information in regard to crimes that are committed against our nation’s law enforcement officers who are working the streets of our cities and communities. Under their direction, the data has and continues to be used to supply law enforcement agencies with the information needed in order to provide the necessary resources to do the job, as safely as possible. In addition, for more than 40 years, the information has also been used to conduct research in regard to the life-threatening incidents law enforcement officers face on a daily basis. As a result of these studies, the LEOKA Program and many other agencies conduct officer safety training to attempt to reduce the number of lives lost each year.

Throughout the history of the LEOKA Program, the data collection criteria have remained the same and very strict in regard to whom could be included in the collection. However, as times have changed, so have the types of personnel who are involved in life-threatening law enforcement incidents. The LEOKA Program recognizes this, but cautions against diluting the true intention of the collection as it should remain consistent and most beneficial to our stakeholders. Two examples of these changes are the evolution of campus security officers to sworn police officers and the increase of reserve officers with full arrest powers,

If the terms “public governmental law enforcement agency”, and “paid from government funds” are eliminated, the LEOKA Program recommends the following changes, which are in bold text, to the law enforcement officer definition and the LEOKA criteria and exclusions:

Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of American citizens. They must have **statutory** arrest powers and **be members of a law enforcement agency, paid from funds set aside specifically for payment to sworn law enforcement** organized for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

#### LEOKA Criteria

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**

- **Were paid from funds set aside specifically for payment of sworn law enforcement**
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

#### Exclusions from the LEOKA Program’s Data Collection

Deaths resulting from the following are not included in the LEOKA Program’s statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program’s statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

#### OPTIONS

Option 1 – Accept and approve the changes to the UCR Program’s definition of a law enforcement officer and the LEOKA collection criteria as identified below with the following changes, which are in bold text, to the law enforcement officer definition and the LEOKA criteria and exclusions:

Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of American citizens. They must have **statutory** arrest powers and **be members of a law enforcement agency, paid from funds set aside specifically for payment to sworn law enforcement** organized for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

### LEOKA Criteria

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**
- **Were paid from funds set aside specifically for payment of sworn law enforcement**
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

### Exclusions from the LEOKA Program's Data Collection

Deaths resulting from the following are not included in the LEOKA Program's statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program's statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

Option 2 – No change.

### **RECOMMENDATION**

The FBI UCR and LEOKA Programs recommend the approval of the changes to the definition of a law enforcement officer and the LEOKA criteria and exclusions.

**FALL 2017 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 adopt Option 1 with revisions to the language as follows – Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of ~~American citizens~~ individuals. They must have **statutory** arrest powers and **be members of a law enforcement agency, paid from funds set aside specifically for payment to sworn law enforcement** organized for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1, as amended, (additions in *red italics*, deletions in **bold strikethrough**): Accept and approve the changes to the UCR Program’s definition of a law enforcement officer and the LEOKA collection criteria as identified below with the following changes, which are in bold text, to the law enforcement officer definition and the LEOKA criteria and | exclusions:

Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of American citizens. They must have **statutory** arrest powers and **be members of a law enforcement agency, paid from funds set aside specifically for payment to sworn law enforcement** organized for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

LEOKA Criteria

- Wore/carried a badge (ordinarily)

- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**
- ~~Were paid from funds set aside specifically for payment of sworn law enforcement~~
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

Exclusions from the LEOKA Program’s Data Collection

Deaths resulting from the following are not included in the LEOKA Program’s statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program’s statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs (*non-sworn*)
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper.

**Action:** Motion carried.

**FALL 2017 UCR SUBCOMMITTEE ACTIONS:**

**Motion:** To accept Option 1 with modifications.  
 Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal

law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of ~~American citizens~~ **individuals**. They must have **statutory** arrest powers and **be members of a law enforcement agency** ~~paid from funds set aside specifically for payment to sworn law enforcement~~ **organized and funded** for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

#### LEOKA Criteria

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**
- ~~Were paid from funds set aside specifically for payment of sworn law enforcement~~
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

#### Exclusions from the LEOKA Program's Data Collection

Deaths resulting from the following are not included in the LEOKA Program's statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program's statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

**Action:** Motion carried.





**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)  
ADVISORY POLICY BOARD (APB)  
OKLAHOMA CITY, OK  
DECEMBER 6-7, 2017**

**STAFF PAPER**

**APB ITEM #17**

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

**SA ISSUE #1**

*CJIS Security Policy Language Changes in Section 5.12*

**SA ISSUE #2**

*CJIS Security Policy Restriction for Criminal Justice Information Stored in Offshore Cloud Computing Facilities*

**~~SA ISSUE #3 (cancelled)~~**

~~*Vetting of Non-U.S. Citizen Contractors/Vendors for Access to State Criminal Justice Information Systems*~~

**SA ISSUE #4\***

*Task Force Updates (Cloud, Mobile, Courts)*

**SA ISSUE #5 (*For SA Information Only*)**

*Update on Fusion Center Access to CJIS Division Systems*

**SA ISSUE #6\***

*Information Security Officer Symposium Review*

**Ad Hoc Issues\***

1. Use of the Regional Information Sharing System (RISS) and other Identity Data Providers
2. FDLE Cloud Provider Audit Briefing
3. Tentative - FirstNet Discussion
4. 5.1.1.4 Interagency and Management Control Agreements

\*No staff paper



**CJIS ADVISORY POLICY BOARD (APB)  
SECURITY AND ACCESS (SA) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**SA ISSUE #1**

*CJIS Security Policy* Language Changes in Section 5.12

**PURPOSE**

Propose modifications to *CJIS Security Policy* Section 5.12

**POINT OF CONTACT**

Information Technology Management Section, CJIS Information Assurance Unit,  
Information Security Officer Program

Questions regarding this topic should be directed to <agmu@leo.gov>.

**REQUEST OF THE SUBCOMMITTEE**

Approve one of the recommendations presented in this topic paper

**BACKGROUND**

The FBI CJIS APB Designated Federal Officer (DFO) received an external topic paper submission (attachment #1) requesting *CJIS Security Policy* Sections 5.12.1.1 and 5.12.1.2 be merged into a single policy section to cover all personnel with unescorted access to unencrypted CJI. Additionally, the topic paper submission requested modifications be made to Section 5.12.2 Personnel Termination.

The CJIS ISO Program presented this topic as an ad-hoc agenda item at the Spring 2017 Security and Access (SA) Subcommittee for discussion. The SA Subcommittee discussed the topic and voiced general agreement and support with the topic paper request. One question was asked to clarify whether or not these changes will have any impact to advanced authentication (AA) determination. While the determination was made there is no impact to AA, the SA Subcommittee did caution changes made to Section 5.12 have the potential to impact the noncriminal justice agency (NCJA) community. The CJIS ISO Program will also be brief the Compact Council to ensure an opportunity to review and offer guidance with respect to this topic.

## **DISCUSSION AND ANALYSIS**

It is stated in the opening paragraph of CJIS Security Policy Section 5.12 that the requirements in this section apply to all personnel who have access to unencrypted CJI including those individuals with only physical and logical access to devices that store, process, or transmit unencrypted CJI. It details a requirement pertaining to all individuals who require access to CJI. Yet, there has been confusion as evidenced by questions received by the CJIS ISO Program about when and to whom the requirements in this section apply.

The CJIS ISO Program recently began reviewing this section to devise a way to add clarifying language to ensure the detailed requirements are clearly understood. Ironically, an external topic paper was received which detailed changes to this Policy section, such as merging Sections 5.12.1.1 and 5.12.1.2. The topic requestor believes the proposed changes would provide consistent, easy-to-understand policy regarding record check requirements for all personnel with access to CJI.

One concern identified in the topic paper request is how an agency employee and a private contractor employee are “vetted” differently. Section 5.12.1.1 details the minimum screening requirements for individuals requiring access to CJI and how any records found during the screening process are to be reviewed. This section pertains specifically to agency employees. Section 5.12.1.2 provides the personnel screening requirements for contractor and vendors.

The topic requestor believes the inconsistencies between the two sections can be problematic and should be aligned. For example, an agency employee can have access up to 30 days before the fingerprint record check must be done, but a contractor must be “cleared” prior to access. The topic requestor does not agree the contractor should be held to a higher standard. It is conceivable that CJI would be subject to higher risk with agency personnel having access for a full 30 days before finding out the person has a disqualifying felony offense. The risk of damage from an insider threat attack is greatly increased. There does not seem to be any justification in the mind of the topic requestor for the delay. The topic requestor believes all “vetting” for agency employees and contractors should be done prior to CJI access.

The topic requestor would also like to address another inconsistency regarding review of felony offenses. Under 5.12.1.1(3), the CSO may grant a variance following review of a felony offense for an agency employee. However, 5.12.1.2(4) does not allow such a review and will not allow for a variance for a contractor.

Finally, the topic requestor identified what he believes is a misconception with Section 5.12. Section 5.12.1.1(1) currently states the following:

*“To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel*

*who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.”*

This statement implies that background checks ONLY apply if the individual has “direct access to CJI...” While it is true that direct access to CJI requires a background check, the converse (indirect access to CJI) may also require a background check. This is because access to (unencrypted) CJI must always be within a physically secure location or within controlled areas during times of processing. CJI must be encrypted (or securely stored in locked containers/file cabinets if hard copy) whenever stored, transmitted, or processed outside a physically secure location or controlled area. As detailed in 5.12.1.1(9), personnel need access to the physically secure location (or controlled area) to have access to the data. To have unescorted access to these areas, a background check is required; thus creating a paradox.

Both the topic requestor and CJIS ISO Program are confident the changes proposed in this topic paper will remove the inconsistencies in Section 5.12 between agency employees and contractors and clear any misconception about when a background check is required for the criminal justice community.

## **OPTIONS**

Approve one of the below recommendations:

1. Accept the following recommended changes within CJIS Security Policy Section 5.12 (item A) and Appendix J (B) as shown below (additions in ***red, bold italics***, deletions in **~~bold strikethrough~~**).

### **A. Proposed CJIS Security Policy Section 5.12 Language Changes:**

#### **5.12 Policy Area 12: Personnel Security**

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section’s security terms and requirements apply to all personnel who have ***unescorted*** access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

#### **5.12.1 Personnel *Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI* Security Policy and Procedures**

##### **~~5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:~~**

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted **~~within 30 days of assignment~~ *prior to granting access to CJI*** for all personnel who

have ~~direct~~ *unescorted* access to *unencrypted CJI and or unescorted access to physically secure locations or controlled areas (during times of CJI processing)*. ~~those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.~~ However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a Nlets CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

- (i) 5 CFR 731.106; and/or
- (ii) Office of Personnel Management policy, regulations, and guidance; and/or
- (iii) agency policy, regulations, and guidance.

~~(See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.)~~ Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

*See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.*

- 2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
- ~~3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.~~
- 3. ~~4.~~ If a record of any ~~other~~ kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
  - a) If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.*
  - b) Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant*

*disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.*

*c) If a record of any kind is found on a Contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.*

4. ~~5.~~ If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.

~~6. If the person is employed by a NCJA, the CSO or his/her designee shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.~~

5. ~~7.~~ If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.

6. ~~8.~~ If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.

~~9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.~~

*7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.*

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

#### ~~5.12.1.2 Personnel Screening for Contractors and Vendors~~

~~In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:~~

~~1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However,~~



~~if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.~~

- ~~2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.~~
- ~~3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.~~
- ~~4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.~~
- ~~5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.~~
- ~~6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.~~

~~Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.~~

#### 5.12.2 Personnel Termination

~~The agency, upon termination of individual employment, shall immediately terminate access to CJI. *Upon termination of personnel employed by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.*~~

#### B. Proposed CJIS Security Policy Appendix J Noncriminal Justice Agency Supplemental Guidance:

## APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

---

...

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have *unescorted* access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring *unescorted* access to *unencrypted* CJI. ~~–listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.2.~~

...

2. Make no changes to the *CJIS Security Policy*

If Option 1 is approved, the requirement(s) should be assigned a priority tier of:

\_\_\_\_\_ (enter 1 or 2) 5.12.1(1) – To verify identification, a state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(1) – However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(1) – When appropriate, the screening shall be consistent with (i) 5 CFR 731.106; and/or (ii) Office of Personnel Management policy, regulations, and guidance; and/or (iii) agency policy, regulations, and guidance.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(2) – All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(2) – All CSO designees shall be from an authorized criminal justice agency.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(3) – If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(3)(a) – If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(3)(c) – If a record of any kind is found on a Contractor, the CGA shall be formally notified...

\_\_\_\_\_ (enter 1 or 2) 5.12.1(3)(c) – ...and system access shall be delayed pending review of the criminal history record information.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(3)(c) – The CGA shall in turn notify the Contractor-appointed Security Officer.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(4) – If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(5) – If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(6) – If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied...

\_\_\_\_\_ (enter 1 or 2) 5.12.1(6) – ...and the person's appointing authority shall be notified in writing of the access denial.

\_\_\_\_\_ (enter 1 or 2) 5.12.1(7) – The granting agency shall maintain a list of personnel who have been authorized access to CJI

\_\_\_\_\_ (enter 1 or 2) 5.12.1(7) – ...and shall, upon request, provide a current copy of the access list to the CSO.

\_\_\_\_\_ (enter 1 or 2) 5.12.2 – Upon termination of personnel employed by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI.

\_\_\_\_\_ (enter 1 or 2) 5.12.2 – Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems are also terminated.

\_\_\_\_\_ (enter 1 or 2) 5.12.2 – If the employee is an employee of an NCJA or a Contractor the employer shall notify all Interface Agencies that may be affected by the personnel change.

## **RECOMMENDATION**

The CJIS ISO Program recommends option 1 (A and B) and a priority tier assignments of 1 for all requirements. Currently, all requirements in the impacted Policy sections have been assigned a tier 1 status.

Attachments:

1 – Topic Request Form, Don Cathey, Kansas ISO

2 – Proposed *CJIS Security Policy* Sections 5.12.1 and 5.12.2 (clean version)

**FALL 2017 WORKING GROUP ACTIONS:**

**FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1 as presented in the topic paper.  
**Action:** Motion carried.

**Motion:** To assign a priority of TIER 1 to all requirements in Option 1 and the proposed changes to 5.12.  
**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1 as presented in the topic paper.  
**Action:** Motion carried with 20 Yay/3 Nay

**Motion:** To assign a Tier 1 priority to all requirements.  
**Action:** Motion carried.

**NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper. Priority of Tier 1.  
**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper. Tier one assignments for all requirements.  
**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper. Priority of Tier 1.  
**Action:** Motion carried with three opposed.

**FALL 2017 SA SUBCOMMITTEE ACTION:**

**Motion:** To accept Option 1 as presented in the topic paper.  
**Action:** Motion carried.

**Motion:** To assign a priority tier of 1 for all requirements.  
**Action:** Motion carried.

## **FBI CJIS ADVISORY PROCESS REQUEST FOR TOPIC**

Please provide the following information when submitting a request for a policy review.

### **1. Clear statement of request**

Review FBI CSP Policy Area 5.12.1.1 and 5.12.1.2 for possible merging of the two into a single policy to cover all personnel with access to CJI.

### **2. How this is handled now (or description of problem being solved)**

Currently, a governmental employee (of a CJA or NCJA) are “vetted” per 5.12.1.1., while a private contractor employee (P.C.) doing the exact same job must be vetted per 5.12.1.2. There are some differences between the two that seem to be inconsistent. For instance:

A) A government employee can have access up to 30 days before the fingerprint record check must be done, but a P.C. must be checked prior to access.

B) Under 5.12.1.1. (1) A CJA employee with *indirect access* might not be required to undergo a fingerprint record check, while 5.12.1.2 (1) requires a P.C. with any kind of access to be checked. This is problematic when the CJA employee is going to be available locally, but a P.C. may be considerable distance away causing a logistical problem.

**3. Suggested solution:** Suggested changes attached. Review 5.12.1.1. And 5.12.1.2 for possibility of combining into a single policy for all personnel requiring any access to CJI.

1) Remove the 30 day “grace period” and the **direct** access conditional from 5.12.1.1 for employees to be consistent with the P.C. requirement so that checks occur PRIOR to ANY access to CJI for everyone.

2) Allowing the CSO to review ALL felony and other CHRI for possible variances allowed under current 5.12.1.1(3) to be consistent for all personnel requesting access to CJI.

### **4. Scenario/example**

One scenario could arise where a CJA employee was granted a variance for a previous felony under 5.12.1.1. (3). That CJA employee separates from the CJA, then wants to work for a Private Contractor doing the same tasks they did as a CJA employee. However, current policy 5.12.1.2 (4) will not allow it – even though they had previously been allowed a variance as an employee.

Under current policy, another is a LEO who only receives hard copy reports (Indirect) is not required to undergo a fingerprint record check, while the dispatcher who performed the transaction to produce the printout must be fingerprinted.

### **5. Benefit to the criminal justice community**

Provide a single consistent policy regarding record checks requirements for all personnel with access to CJI.

### **6. Impact on state system users, if known. (Time and resources)**

A single procedure can be documented to follow to conduct and adjudicate all potential personnel needing access to CJI.

### **7. Importance/criticality** \_\_\_\_\_

### **8. Contact Person**

Don Cathey, Kansas Highway Patrol, KS CJIS ISO (785)-368-6518 don.cathey@ks.gov

## **Proposed CJIS Security Policy Sections 5.12.1 and 5.12.2 (clean version)**

### **5.12 Policy Area 12: Personnel Security**

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

#### **5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI**

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a Nlets CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
  - (i) 5 CFR 731.106; and/or
  - (ii) Office of Personnel Management policy, regulations, and guidance; and/or
  - (iii) agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
  - a) If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
  - b) Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
  - c) If a record of any kind is found on a Contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

#### **5.12.2 Personnel Termination**

Upon termination of personnel employed by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

**CJIS ADVISORY POLICY BOARD (APB)  
SECURITY AND ACCESS (SA) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**SA ISSUE #2**

*CJIS Security Policy* Restriction for Criminal Justice Information (CJI) Stored in Offshore Cloud Computing Facilities

**PURPOSE**

Propose language changes to *CJIS Security Policy* Section 5.10.1.5 to restrict where criminal justice information (CJI) can be stored in cloud computing facilities

**POINT OF CONTACT**

Information Technology Management Section, CJIS Information Assurance Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

**REQUEST OF THE SUBCOMMITTEE**

Approve one of the recommendations presented in this topic paper

**BACKGROUND**

The FBI CJIS APB Designated Federal Officer (DFO) received an external topic paper submission (attachment #1) requesting the examination of potential security risks to CJIS data stored in “off-shore” cloud facilities and explore the possibility of restricting off-shore cloud storage of CJI in the *CJIS Security Policy*.

The CJIS ISO Program intended to present this topic as an ad-hoc agenda item at the Spring 2016 Security and Access (SA) Subcommittee for discussion. However, prior to this presentation, the SA Subcommittee motioned to establish the Cloud Task Force. It was agreed upon by the Subcommittee that all cloud-related topics, both current and future, would be deliberated by the task force prior to moving forward through the Advisory Board process. Blaine Koops, SA member and topic paper submitter, agreed to have the topic sent to the Cloud Task Force where it would undergo a due diligence process. The Cloud Task Force agreed to create and provide a recommendation to the Fall 2016 SA Subcommittee.

The Cloud Task Force discussed this topic in great length and collectively developed a recommendation which was presented to the 2016 Fall SA Subcommittee as an ad-hoc



topic. The SA Subcommittee unanimously endorsed the recommendation and requested the CJIS ISO Program take forth a topic paper through the 2017 Spring Advisory Policy Board (APB) process.

This topic was presented to the Working Groups during the Spring 2017 APB cycle. Although the SA Subcommittee endorsed the proposed language during the ad hoc discussion at the Fall 2016 Subcommittee meeting, the ISO Program's recommendation to the Working Groups was for "no change" pending development of policy language which would not exclude APB member countries, i.e. Canada. Three Working Groups voted for "no change." Two Working Groups motioned for the SA Subcommittee to have the Cloud Task Force draft new language giving consideration to the APB partner country, Canada, and other treaties and exchange agreements. This topic was then presented to the SA Subcommittee. After much discussion, a recommendation was made for "no change" with the understanding this issue would be taken back to the Cloud Task Force to craft new language. The APB subsequently approved the motion recommended by the SA Subcommittee to draft new language and bring the modified topic back to the Fall 2017 Working Groups.

## **DISCUSSION AND ANALYSIS**

The essential premise of the *CJIS Security Policy* is to provide the minimum controls to protect the full lifecycle of CJI. The Policy is also designed to be somewhat malleable to enable the use of new and emerging technologies, such as cloud computing. As the concept and acceptance of cloud computing grows within the law enforcement community, concern is raised about protecting CJI stored within environments which are outside the direct control of the agency. This concern sparked the submission of a topic paper request (attached) asking for a risk assessment and possible restriction of permitting CJI storage inside datacenters outside of the United States and U.S. territories.

The SA Subcommittee, upon creation of the Cloud Task Force, asked the group to review and discuss this topic. Over the course of the many discussions, one primary concern continually raised revolves around the difficulty in restricting access to unencrypted CJI to foreign nationals on foreign soil where international laws differ from those in the United States. Encryption is the most common method used to provide data confidentiality. Encryption can also provide a means of access control to data via key management. For example, a person with access to the encryption/decryption key has access to unencrypted data. However, the *CJIS Security Policy* does not require encryption when CJI is stored within physically secure locations. There is also no restriction on storing CJI in foreign-based areas that would be established as physically secure locations, such as cloud service provider's datacenters. Additionally, many cloud products or services may be severely restricted if the cloud service provider cannot have access to the data in an unencrypted form.

During presentation at the 2017 Spring SA Subcommittee meetings there was discussion regarding support from foreign governments for assistance in cases of misuse of data. The reason for the proposed restriction is the concern that adequate support and recourse

is unclear and/or insufficient. The SA Subcommittee clarified this issue pertains to a criminal justice agency storing CJI in a commercial cloud service provider's facility located in another country versus an authorized agency (e.g., the Royal Canadian Mounted Police (RCMP)) storing data in their own facility. The CJIS ISO Program explained the Policy restriction presented in the topic paper would render RCMP out of compliance even when stored in their own datacenters as they would be located in Canada and not in the US or US territories.

The CJIS ISO Program facilitated discussions to rework language with the Cloud Task Force to develop another option that allows for the storage of CJI in cloud environments in a foreign country if it can be assured the management control of CJI protection remains with a APB member country. The SA Subcommittee agreed to send the issue back to the Cloud Task Force to craft new language. The CJIS ISO Program would then bring a modified topic paper back to the Fall 2017 Working Groups.

The Cloud Task Force discussed the challenges with the lack of ability to prevent access to unauthorized foreign nationals when CJI data is stored within a datacenter of another country. This concern exists even when CJI is encrypted. Because the data can be replicated, unauthorized personnel would have unlimited time to perform off-line attacks on the encryption with the expectation of defeating the algorithm. The Cloud Task Force stressed they cannot blindly trust a foreign nation's privacy laws and cannot expect a small law enforcement agency to have the knowledge or ability to know how to fight an international legal battle should the need arise. After much discussion, the Cloud Task Force collectively developed a recommendation to modify the Policy language in Section 5.10.1.5.

## **OPTIONS**

Approve one of the below recommendations:

1. Accept the following recommended changes to CJIS Security Policy Section 5.10.1.5 and Appendix B as shown below (additions in ***red, bold italics***, deletions in **~~bold strikethrough~~**).

- ***The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).***

***Note: This restriction does not apply to exchanges of CJI with foreign criminal justice agencies under international exchange arrangements (i.e., the Preventing and Combatting Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).***

- **Proposed Additions to CJIS Security Policy Appendix B: Acronyms:**

Acronym	Term
<b><i>RCMP</i></b>	<b><i>Royal Canadian Mounted Police</i></b>

2. Make no changes to the *CJIS Security Policy*

If this recommendation is approved, the requirement(s) should be assigned a priority tier of:

**(enter 1 or 2)** The storage of CJI, regardless of encryption status, **shall** only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

### **RECOMMENDATION**

The CJIS ISO Program Office recommends option 1 and a priority tier assignment of 1 for the requirement.

Attachments:

- 1 – Topic Request Form, Sheriff Blaine Koops, Allegan County, Michigan

**FALL 2017 WORKING GROUP ACTIONS:**

**FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1.

**Action:** Motion carried.

**Motion:** To reconsider the first vote for Option 1 and vote down the first motion.

**Action:** Motion carried.

**Motion:** To accept Option 1 with amended language to replace "...foreign criminal justice agencies..." with "...foreign government agencies..." as shown below.

1. Accept the following recommended changes to CJIS Security Policy Section 5.10.1.5 and Appendix B as shown below (additions in *red, bold italics*, deletions in ~~bold strikethrough~~).

- *The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of an APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and under the legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).*

*Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange arrangements (i.e., the Preventing and Combatting Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).*

- **Proposed Additions to CJIS Security Policy Appendix B:**

**Acronyms:**

Acronym	Term
<i>RCMP</i>	<i>Royal Canadian Mounted Police</i>

**Action:** Motion carried.

**NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1 and Tier 1 as presented in the topic paper.

**Action:** Motion carried.

**NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper. Priority of Tier 1.  
**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper.  
**Action:** Motion carried. Tier one assigned to the requirement.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1 as presented in the topic paper. Priority of Tier 1.  
**Action:** Motion carried.

**FALL 2017 SA SUBCOMMITTEE ACTION:**

**Motion:** To accept Option 1 with amended language to replace “foreign criminal justice agencies” with “foreign government agencies”.

1. Accept the following recommended changes to CJIS Security Policy Section 5.10.1.5 and Appendix B as shown below (additions in *red, bold italics*, deletions in ~~bold strikethrough~~).

- *The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).*

*Note: This restriction does not apply to exchanges of CJI with foreign ~~criminal justice~~ government agencies under international exchange arrangements (i.e., the Preventing and Combatting Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).*

- **Proposed Additions to CJIS Security Policy Appendix B: Acronyms:**

Acronym	Term
<i>RCMP</i>	<i>Royal Canadian Mounted Police</i>

**Action:** Motion carried.

**Motion:** To assign the requirement a priority tier of 1.

**Action:** Motion carried.

**FBI CJIS ADVISORY PROCESS REQUEST FOR TOPIC**

Please provide the following information when submitting a request for a topic paper.

**1. Clear statement of request:**

Examine the security risk to CJIS data stored in “off-shore” cloud facilities and develop draft policy, if necessary, for working group and subcommittee consideration.

**2. How this is handled now (or description of problem being solved):**

Currently, the topic is considered a business decision by each CJIS entity, rather than a system-wide policy issue.

**3. Suggested solution:**

Explore the possibility of restricting off-shore cloud CJIS data storage through the CJIS Security Policy.

**4. Scenario/example:**

A state CJIS agency procures the services of a cloud computing and data storage vendor. Unknown to the state CJIS agency, the cloud data is stored in an unsecured facility in a foreign country.

**5. Benefits to the criminal justice community:**

Greater security for individual FBI CJIS partners and overall greater security for the entire national CJIS system.

**6. Impact on state system users, if known. (Time and resources):**

Unknown

**7. Importance/criticality:**

High Importance

**8. Suggested Topic Name:**

Security of CJIS data stored in off-shore cloud computing facilities and the ramifications to CJIS security.

**9. Contact person:**

Sheriff Blaine Koops, Allegan County, MI and/or Ms. Dawn Brinningstaull, CSO, Michigan

**Please provide any additional information that may be helpful to understand the topic.**

Co-Requestors:

Mr. Michael Lesko, CSO, Texas CJIS

Mr. Joseph Dominic, CSO, California CJIS

Mr. Bradley Truitt, CSO, Tennessee CJIS

Mr. Charles Schaeffer, CSO, Florida CJIS



**CJIS ADVISORY POLICY BOARD (APB)  
SECURITY AND ACCESS (SA) SUBCOMMITTEE  
ORLANDO, FLORIDA  
OCTOBER 19, 2017**

**STAFF PAPER**

**SA ISSUE #5**

Update on Fusion Center Access to Criminal Justice Information Services (CJIS)  
Division Systems

**PURPOSE**

To provide an update regarding the CJIS Division's efforts to fulfill the CJIS Advisory Policy Board's (APB's) recommendations regarding fusion center access to CJIS Division systems.

**POINT OF CONTACT**

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**

The Subcommittee is requested to review the information presented in this paper, and provide comments and recommendations to the APB.

**BACKGROUND**

There are currently 78 fusion centers recognized by the Department of Homeland Security (DHS) operating within the United States and its territories. The National Fusion Center Association (NFCA) reports a small number (less than nine) of these fusion centers lack direct access to the systems managed by the Federal Bureau of Investigation's (FBI's) CJIS Division. This lack of direct access, as reported, creates difficulties from an information-sharing standpoint. The vast majority of fusion centers are either established directly within a criminal justice agency (CJA), and that CJA controls the terminal access within the fusion center, or the fusion centers leverage a partnering CJA's access. As research indicates, other partnering CJAs, (e.g., police departments, sheriff's offices, etc.) working within a fusion center also establish their own terminal access within that fusion center to support their criminal investigation needs.



Access to CJIS Division systems is governed by Title 28, Code of Federal Regulations (C.F.R.), Part 20, which stipulates the types of agencies and the functions those agencies must perform to qualify for access. To qualify for access to CJIS Division systems, an agency must be a CJA or a subunit of a noncriminal justice agency, performing the administration of criminal justice as a primary function (interpreted by the Department of Justice (DOJ) to mean more than 50 percent of the agency's annual budget supports criminal justice functions). The functions which are considered the administration of criminal justice are specified in 28 C.F.R. §20.3(b), and include detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

The primary function of these fusion centers is to compile and share information to support the detection of criminal and terrorist activity. The term "detection" as it relates to the administration of criminal justice must be predicated on an "articulable suspicion" to justify a query of CJIS Division systems. Under the CJIS Division's review, the functions of the fusion centers lacking access did not conclusively meet the threshold requirements in 28 C.F.R. §20.3(b) to be considered the administration of criminal justice.

The compilation, analysis, and sharing of generalized or nonspecific threat information is not considered the administration of criminal justice. The fusion centers lacking direct access which have directly engaged the CJIS Division have been unable to provide documentation to support their primary function is the detection of articulable or specified criminal or terrorist activity. In some cases, the CJIS Systems Agencies (CSAs), for the states of the fusion centers in question, do not support granting direct access to those fusion centers and recommend for a CJA to control the access. For information, CSAs control access to CJIS Division systems for all agencies within their state or territory.

## **DISCUSSION AND ANALYSIS**

A topic was presented at the Spring 2016 Advisory Process meetings. The APB recommended for the CJIS Division and FBI's Office of General Counsel (OGC) to identify a long-term solution to fusion centers lacking direct access to CJIS Division systems and bring the solution(s) back through the Advisory Process for consideration. The APB also moved, pending the outcome of the FBI's review of a long-term solution, to grant fusion centers interim access through the use of management control agreements. This would facilitate access to CJIS Division systems through the management control of a CJA. The CJIS Division is aware of at least one state where this interim solution is currently being implemented.

Throughout this process, the CJIS Division has been engaged with the criminal justice community, the NFCA, the DHS, and the International Association of Chiefs of Police. In addition, the CJIS Division's Assistant Director served on the DOJ Criminal Intelligence Coordinating Council and provided substantial input on the topic of fusion center access.

To fulfill the APB’s recommendation, the CJIS Division and the OGC have collaborated to propose the option to formalize the interim solution stated above by clarifying the existing language in the regulation. The regulation changes will clarify language to definitively authorize a criminal justice agency to enter into a management control agreement with a noncriminal justice governmental agency to perform criminal justice functions on its behalf. A modification to the definition of a CJA under 28 C.F.R. §20.3(g) to include fusion centers was originally discussed during the Spring 2016 Advisory Process discussions, but the APB requested further exploration before making a final recommendation. After consideration of the discussion during the Advisory Process meeting and other engagement with the user community, the CJIS Division and the OGC determined a clarification of the language within 28 C.F.R. §20.33 (a)(6) may be a better option to accomplish this goal. Currently, 28 C.F.R. §20.33 (a)(6) reads, “To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies.” The proposed changes to 28 C.F.R. §20 will memorialize the ability for noncriminal justice governmental agencies, such as the small number of fusion centers lacking direct access, to enter into agreements with CJAs to perform the administration of criminal justice functions on behalf of the CJA. Should this proposed regulation change be endorsed, it should be noted it is a lengthy administrative process that could take many years to accomplish.

Another point to consider is the current administration’s Executive Order 13771 to limit new regulations. On January 30, 2017, the President signed Executive Order 13771, which states “that for every one new regulation issued, at least two prior regulations be identified for elimination . . . .” This Order affects not only the Department of Justice, but all Federal Executive Agencies, and it has brought the federal regulatory amendment process to a near halt. The APB can be assured that if the proposed language under Option 1 is accepted, the FBI will perform due diligence to move the proposed language change forward.

The Subcommittee is requested to provide input on the information provided in this paper and provide recommendations regarding the following options.

## **OPTIONS**

### **Option 1**

Endorse the CJIS Division’s and FBI OGC’s recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

## **Option 2**

No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

## **Option 3**

Discontinue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

### **RECOMMENDATION**

The NCIC Operations and Policy Unit recommends Option 1.

### **FALL 2017 WORKING GROUP ACTIONS:**

#### **FEDERAL WORKING GROUP ACTION:**

**Motion:** To accept Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

#### **NORTH CENTRAL WORKING GROUP ACTION:**

**Motion:** No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA. **FBI Action:** FBI should continue to research various scenarios which may result from any proposed regulatory change. Continue with the interim solution.

**Action:** Motion carried with 11 Yay/11 Nay, Chair broke the tie with a Yay vote

#### **NORTHEASTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2. No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**SOUTHERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

**WESTERN WORKING GROUP ACTION:**

**Motion:** To adopt Option 1. Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**FALL 2017 SUBCOMMITTEE ACTIONS:**

**IS SUBCOMMITTEE ACTION:**

**Motion:** To accept a revised Option 1: "Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a) (6) as the long term solution to facilitate access to CJIS Division systems, which would grant criminal justice agencies the same authority to contract with noncriminal justice governmental agencies as they currently have to contract with private entities. Accept the language as proposed below:

*6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency."*

**Action:** Motion carried.

**N-DEx SUBCOMMITTEE ACTION:**

Accepted as information only.

**NCIC SUBCOMMITTEE ACTION:**

**Motion:** Recommendation to the Identification Services Subcommittee for Option 1: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long

term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Action:** Motion carried.

**SA SUBCOMMITTEE ACTION:**

**Motion:** To recommend Option 2: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Action:** Motion carried.

# Science and Technology Branch Priorities & Initiatives Federal Bureau of Investigation



CJIS Advisory Policy Board  
December 6, 2017

## Current Issues

Science and Technology Branch



- **Identity Resolution:** Biographic information can be manipulated
  - Biometric identifiers can provide validation, authentication, and positive identification
  - Use of biometric identifiers can be a valuable contributor to officer safety

2

Unclassified//For Official Use Only

## Current Issues

Science and Technology Branch

- **Data Collection and Management:** Advances in wireless communication technology, along with the broad emergence of smartphone video capabilities, have drastically increased video collection needs
  - In FY2016, the FBI managed approximately three petabytes of video recordings, which equates to almost 1.3 million hours of video (or 638,298 DVD movies)

3

Unclassified//For Official Use Only


## Branch Areas of Focus

Science and Technology Branch


- **Biometrics:** Building an updated, integrated, sustainable FBI biometric identification approach
  - Upgrading the law enforcement community's ability to collect, store, process, analyze, retrieve, and share biometric data for accurate and timely matching of identities

4

Unclassified//For Official Use Only



## Branch Areas of Focus

Science and Technology Branch 

- **Video Analytics:** Developing analytics to extract and exploit intelligence and leads from video data/evidence
  - Improving the law enforcement community's capability to collect and manage video data/evidence

5

Unclassified//For Official Use Only



## Branch Areas of Focus

Science and Technology Branch 

- **Information Technology Integration:** Advancing the use of automation and system integration to enhance performance, productivity, and organizational effectiveness

6

Unclassified//For Official Use Only



## Biometrics

Science and Technology Branch

- **Rapid DNA:** In August 2017, the President signed the Rapid DNA Act, which allows DNA profiles to be generated outside of an accredited laboratory and searched against the FBI Laboratory's national DNA database
  - Technology has significant potential to aid law enforcement
  - FBI has initiated preparations for implementation of Rapid DNA in booking stations, for use with reference samples

7

Unclassified//For Official Use Only

## Biometrics

Science and Technology Branch

- **Iris Pilot:** CJIS has established a pilot study to explore criminal justice applications of iris scanning and matching technology
  - Pilot study scheduled to conclude at the end of FY2018
  - At the end of FY2017, the database held almost 750,000 records, an increase of approximately 25% since FY2016
  - Pilot resulted in the identification of 372 wanted persons in FY2017

8

Unclassified//For Official Use Only

## Video Analytics

Science and Technology Branch

- **Integration of Video Enterprise Architecture:**
  - There is a video analytics element to almost every case
  - The Operational Technology Division's improvements in collection, storage, exploitation, analysis, and presentation of video data are resulting in significant increases in the FBI's capacity to process and analyze video evidence

9

Unclassified//For Official Use Only

## Video Analytics

Science and Technology Branch

- **Facial Recognition:**
  - CJIS and the Operational Technology Division are working collaboratively to update the FBI's facial recognition matching tools and improve ability to draw facial recognition from video products
    - Efforts also driving improvements in still photo facial matching

10

Unclassified//For Official Use Only



## Information Technology Integration

Science and Technology Branch 


- **The FBI remains committed to Crime Data Modernization and the NIBRS transition**
  - Full support of FBI Leadership
  - Maintained as a Director's Priority Initiative
  - 2021 implementation remains the FBI's goal

11

Unclassified//For Official Use Only



## Information Technology Integration

Science and Technology Branch 

- **The FBI continues to invest in Crime Data Modernization**
  - Allocated \$70 million to assist with NIBRS transition
  - FBI systems of record are being modernized for NIBRS compatibility
  - Awarded more than \$34 million in grant money to date
    - Four more opportunities to apply in FY2018

12

Unclassified//For Official Use Only



## Information Technology Integration

Science and Technology Branch

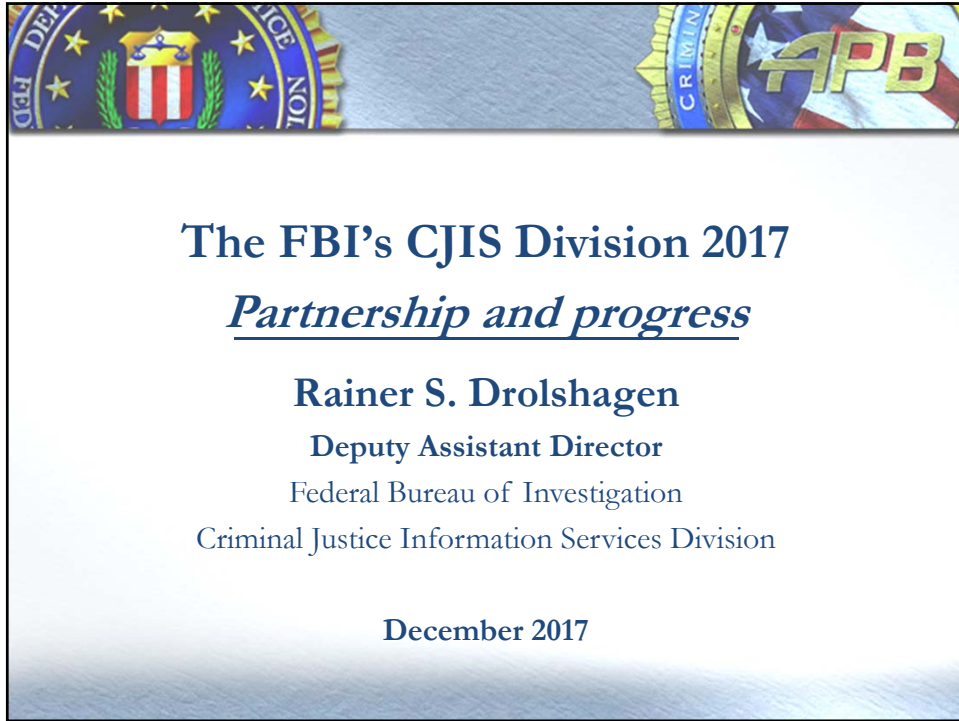


- **The FBI continues to invest in Crime Data Modernization**
  - Use of Force Data Collection Pilot concludes in December
    - More than 100 agencies currently participating
  - Developed and deployed Crime Data Explorer

13

Unclassified//For Official Use Only





**Crime Data Modernization**


- Continue toward NIBRS-only reporting by January 1, 2021
- Use of Force Data Collection pilot
- Crime Data Explorer

**Improving access to crime data**

The Crime Data Explorer makes nationwide crime data accessible in a wide range of ways. You can explore detailed data by state, and across the Crime Data API for reported crime at the national, state, and agency levels.


**Explore by location and type of crime**

Location:  All violent crime  View results





**Use our data in your project**

<p><b>Estimated crime data</b></p> <p>Crime trends at the state and national level for violent crime and property crime since 1992.</p>	<p><b>NIBRS data</b></p> <p>Incident-based data for crimes known to law enforcement for crime reporting NIBRS.</p>	<p><b>Other datasets</b></p> <p>More crime, available on law enforcement, justice programs, data, agency performance, organ theft, and human trafficking.</p>
---	--	---




## NCIC 3<sup>rd</sup> Generation

- Vetting of 14 high level concepts completed
- Capability to test NCIC using NIEM XML
- Statement of Objectives draft released through Request for Information



## National Instant Criminal Background Check System

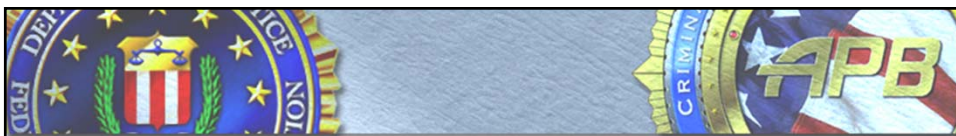
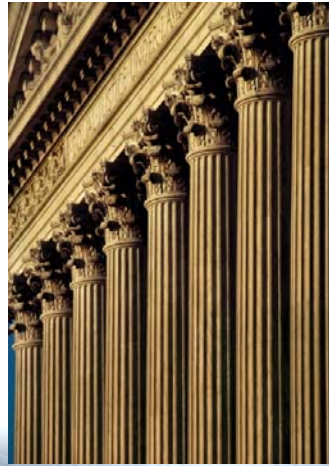
- New highest day record!  
Nov. 24, 2017 (Black Friday)
- Division and FBI-wide support of NICS Section





## Missing dispositions update

- 7 million federal arrests missing dispositions
- 65.1 million state/local agency arrests missing dispositions
- FBI down to 10 percent missing dispositions



## Improved handling of requests for Identity History Summaries (Departmental Orders)

- New system will allow the public to submit requests and receive their Identity History Summaries online
- Developing a pilot with the USPS to submit fingerprints





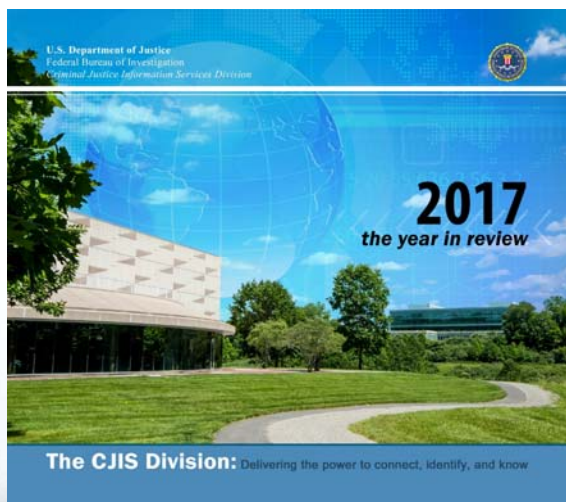
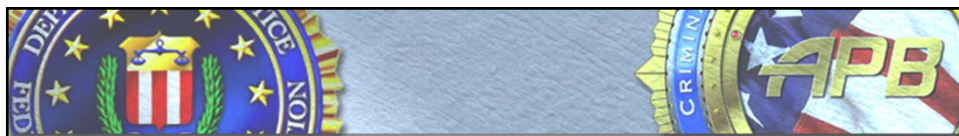


## Public Access Line

- Serving all 56 FBI field offices

In FY 2017, PAL:

- Answered 745,511 calls
- Processed 733,589 E-tips
- Forwarded 20,446 tips to investigators
- Activated 43 Major Case Contact Center cases (1-800-CALL-FBI)



- Highlights from FY 2017
- Program updates
- Statistics
- Perspectives from APB members



# Advisory Policy Board (APB) Board Item #3 National Data Exchange (N-DEx) Subcommittee Chairwoman's Report

Ms. Carol A. Gibbs,  
Illinois State Police

UNCLASSIFIED



## N-DEx Issue # 1 N-DEx Program Status



The N-DEx Program Office presented an update on the N-DEx Program activities.

- N-DEx System Participation Snapshot
- Stakeholder Outreach and Customer Support
- Outstanding action items (to include Criminal Intel Project)
- Nlets Pilot
- Success Story Awards Program
- N-DEx System Technical Enhancements

### ***Subcommittee Action:***

This issue was accepted for information only.

UNCLASSIFIED

2



## N-DEx Issue # 2



Creation of a N-DEx System Use Code for Federal Security Clearances, Suitability, and Fitness for Federal Employment, Credentialing and Related Federal Matters.

---

In response to Executive Order 13764, the N-DEx Program Office will implement a new use code to support the backgrounding of individuals seeking such federal clearances.

- The Program Office is working with FBI OGC to create specific policy language for the *N-DEx Policy and Operating Manual*.

UNCLASSIFIED

3



## N-DEx Issue # 2



Creation of a N-DEx System Use Code for Federal Security Clearances, Suitability, and Fitness for Federal Employment, Credentialing and Related Federal Matters.

- 
- Record-owning agencies will be contacted to determine if they will allow their data to be used for this purpose.

***Subcommittee Action:***

This issue was accepted for information only.

4



## N-DEx Issue # 3

### N-DEx Institutional and Community Corrections (ICC) Update

---



- Nine state Departments of Corrections directly contribute data to N-DEx.
- Receiving ICC data from contributors in four additional states.
- Significant growth in batch search use by corrections/probation/parole.
- Received endorsement from the National Institute of Corrections (NIC) in September 2017.

***Subcommittee Action:***

This issue was accepted for information only.

UNCLASSIFIED

5



## N-DEx Issue #4

### Update on Fusion Center Access to Criminal Justice Information Services (CJIS) Division Systems

---



The subcommittee was provided an update by the NCIC Operations and Policy Unit about fusion center access to Criminal Justice Information Services (CJIS) Division Systems.

***Subcommittee Action:***

This issue was accepted for information only.

UNCLASSIFIED

6



## N-DEX Issue #5

### NICS Searching N-DEX Update



- Technical implementation is on schedule.
- Training to be conducted during testing phase later in 2018.
- Outreach on applying sharing rules expected to be completed by end of summer 2018.

#### ***Subcommittee Action:***

This issue was accepted for information only.



## N-DEX Ad-Hoc Discussion Items



The N-DEX Program Office presented two ad-hoc items to the subcommittee.

- “Yellow” Record Results
- The CJIS Division's Bioterrorism Risk Assessment Group (BRAG) Request Access to Query N-DEX for Security Risk Assessments

#### ***Subcommittee Action:***

These issues were accepted for information only.



## NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) SUBCOMMITTEE

Lynn Rolin  
Chair, NICS Subcommittee



## MEMBERSHIP



- Lynn Rolin, Chair, South Carolina
- Ross Loder, Vice-Chair, Iowa
- Julie Butler, Nevada
- Dalene Drum, Maryland
- Alphonso Hughes, Bureau of Alcohol, Tobacco, Firearms and Explosives
- Charles W. Klebe, Kansas
- Robin Sparkman, Florida
- Lawrence "Lance" Tyler, Utah
- Melanie Veilleux, Arizona
- Sheriff Kathy Witt, Kentucky

2



## NICS ISSUES #1 AND #3 INFORMATIONAL

---



### NICS Operational Status Update and Fugitive From Justice Update

Annual Statistical Data

NICS Looking Ahead

Fugitive From Justice

UNCLASSIFIED/FOUO

3



## NICS ISSUES #2 AND #4 INFORMATIONAL

---



### NICS Enhancement Status

Update to Items Approved by the APB

### National Data Exchange Program (N-Dex) Status

Collaborative Efforts

UNCLASSIFIED/FOUO

4



## NICS ISSUE #5 ACTION TOPIC

---



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

Re-evaluating Mandatory and Optional Fields within the NICS Indices

UNCLASSIFIED/FOUO

5



## NICS ISSUE #5 ACTION TOPIC

---



### Option 1: State Identification Number (SID)

- a) Uphold the 2012 decision by the Advisory Policy Board (APB) to create an optional field to capture the SID in the NICS Indices.
- b) Rescind the 2012 decision by the APB to create an optional field to capture the SID.

UNCLASSIFIED/FOUO

6





## NICS ISSUE #5 ACTION—NICS Subcommittee Vote

---



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 1a—Uphold the 2012 decision by the Advisory Policy Board (APB) to create an optional field to capture the SID in the NICS Indices.

UNCLASSIFIED/FOUO

7



## NICS ISSUE #5 ACTION TOPIC

---



### Option 2: Henry Fingerprint Classification

- a) Uphold the 2012 decision by the APB to create an optional field in the NICS Indices to capture the Henry Fingerprint Classification.
- b) Rescind the 2012 decision by the APB to create an optional field in the NICS Indices to capture the Henry Fingerprint Classification.

UNCLASSIFIED/FOUO

8



## NICS ISSUE #5 ACTION—NICS Subcommittee Vote

---



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 2b—Rescind the 2012 decision by the APB to create an optional field in the NICS Indices to capture the Henry Fingerprint Classification

UNCLASSIFIED//FOUO

9



## NICS ISSUE #5 ACTION TOPIC

---



### Option 3: Eye Color/Hair Color

- a) Uphold the 2012 decision by the APB to make no changes to the eye/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.
- b) Rescind the 2012 decision by the APB and remove the eye/hair fields from the NICS Indices format since these person-descriptive traits are easily changed.

UNCLASSIFIED//FOUO

10



## NICS ISSUE #5

### ACTION—NICS Subcommittee Vote

---



#### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 3a—Uphold the 2012 decision by the APB to make no changes to the eye/hair color fields and to continue to allow them as an optional field when creating a NICS Indices entry.

UNCLASSIFIED//FOUO

11



## NICS ISSUE #5

### ACTION TOPIC

---



#### Option 4: Weight

- a) Uphold the 2012 decision by the APB to make no change to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.
- b) Rescind the 2012 decision by the APB and remove the weight field from the NICS Indices format since this is a person-descriptive trait which can fluctuate over time.

UNCLASSIFIED//FOUO

12



## NICS ISSUE #5

### ACTION—NICS Subcommittee Vote

---



#### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 4a—Uphold the 2012 decision by the APB to make no change to the weight field and to continue to allow it to be entered as an optional field when creating a NICS Indices entry.

UNCLASSIFIED/FOUO

13



## NICS ISSUE #5

### ACTION TOPIC

---



#### Option 5: Race

- a) Uphold the 2012 decision by the APB to make race a mandatory field when submitting entries into the NICS Indices.
- b) Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

UNCLASSIFIED/FOUO

14



## NICS ISSUE #5 ACTION—NICS Subcommittee Vote



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 5b—Rescind the 2012 decision by the APB and allow the race field to remain optional when making an entry into the NICS Indices since it is no longer part of the search algorithm.

UNCLASSIFIED/FOUO

15



## NICS ISSUE #5 ACTION TOPIC



### Option 6: DOB

- a) Uphold the 2012 decisions by the APB to make the DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique personal identifier (MNU or SOC).
- b) Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

UNCLASSIFIED/FOUO

16



## NICS ISSUE #5 ACTION—NICS Subcommittee Vote



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 6b—Uphold the 2012 decision by the APB (with one new addition) to make DOB a mandatory field when submitting entries into the NICS Indices. If a valid DOB is not available, all zeros (0000/00/00) is permissible; however, the entry must include an additional unique identifier (MNU or SOC). However, if the source documentation contains the complete DOB, this information by policy is required to be included in the NICS Indices entry.

UNCLASSIFIED/FOUO

17



## NICS ISSUE #5 ACTION TOPIC



### Option 7: MIS

- a) Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.
- b) Rescind the 2012 decision by the APB and maintain the maximum limit allowed in the MIS field at 1,000 characters.

UNCLASSIFIED/FOUO

18



## NICS ISSUE #5 ACTION—NICS Subcommittee Vote



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 7a—Uphold the 2012 decision by the APB to allow for the expansion of the MIS field to the allowable system limit. The recommendation is to restrict character length to 2,500.

UNCLASSIFIED//FOUO

19



## NICS ISSUE #5 ACTION TOPIC



### Option 8: Middle Name

- a) The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information, by policy, is required to be included in the NICS Indices entry.
- b) No change, the middle name field will remain an optional field, with no additional requirements if the information is available within the source documentation.

UNCLASSIFIED//FOUO

20



## NICS ISSUE #5 ACTION—NICS Subcommittee Vote



### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 8a—The middle name field will remain optional. However, if the source documentation maintained by the contributor contains the middle name or middle initial, this information, by policy, is required to be included in the NICS Indices entry.

UNCLASSIFIED/FOUO

21



## NICS ISSUE #5 ACTION TOPIC



### Option 9: Additional Information Available Checkbox

- a) Add an optional checkbox to the NICS Indices format that allows contributors to indicate if optional information is available. The addition of this box would not preclude a contributor from also adding comments or data to the MIS field.
- b) No change, the indication of additional information will continue to be notated in the MIS field.

UNCLASSIFIED/FOUO

22





## NICS ISSUE #5

### ACTION—NICS Subcommittee Vote

---



#### Re-evaluation of the Expansion of Information Required with the Submission of a Record to the NICS Indices, Formerly Known as the NICS Index, and Potential Fields to be Added

**Motion:** To endorse option 9b—No change, the indication of additional information will continue to be notated in the MIS field. The middle name field will remain optional.

UNCLASSIFIED/FOUO

23



## NICS ISSUE #6

### INFORMATIONAL

---



#### Importance of the Identification for Firearm Sales (IFFS) Program to the NICS User Community

Enhancements in Efficiency

UNCLASSIFIED/FOUO

24



## NICS ISSUES #7 AND #8 INFORMATIONAL



### The Impact of Pseudo-Pointers on State Outreach in the NGI System

### Criminal History Update

UNCLASSIFIED//FOUO

25



## NICS ISSUE #9 ACTION TOPIC



### Submission of an Originating Case Number (OCA) during a NICS Disposition of Firearms (DOF) Background Check

#### Option 1:

Require an OCA on all DOF background checks conducted via the NICS within two years.

#### Option 2:

The OCA remains an optional field on all DOF background checks conducted via the NICS.

UNCLASSIFIED//FOUO

26



## NICS ISSUE #9

### **ACTION—NICS Subcommittee Vote**

---

#### **Submission of an Originating Case Number (OCA) during a NICS Disposition of Firearms (DOF) Background Check**

**Motion:** To endorse option 2—The OCA remains an optional field on all DOF background checks conducted via the NICS.

UNCLASSIFIED/FOUO

27



## NICS ISSUE #10

### **INFORMATIONAL**

---

#### **Update on Outstanding NICS Subcommittee Action Items**

Total Action Items: 52  
Completed Action Items: 25  
Ongoing Action Items: 3  
Open Action Items: 20  
New Action Items Received: 4

UNCLASSIFIED/FOUO

28



## NICS ISSUE #11 ADHOC

---



Discussion on various new topics

- Law Enforcement Enterprise Portal
- Technical Operational Updates vs. Interface Control Document Updates
- NICS Denied Transaction File Responses
- Audit Process

UNCLASSIFIED//FOUO

29



---

Lynn Rolin  
Chair, NICS Subcommittee  
South Carolina Law Enforcement Division  
lrolin@sled.sc.gov  
803-896-7162

UNCLASSIFIED//FOUO

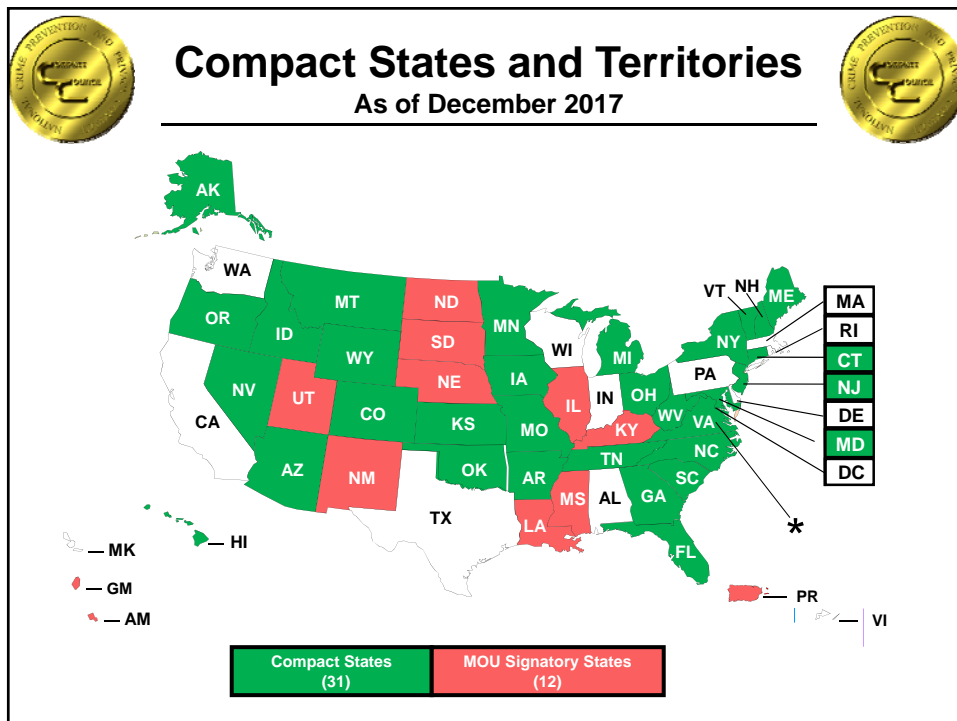
30

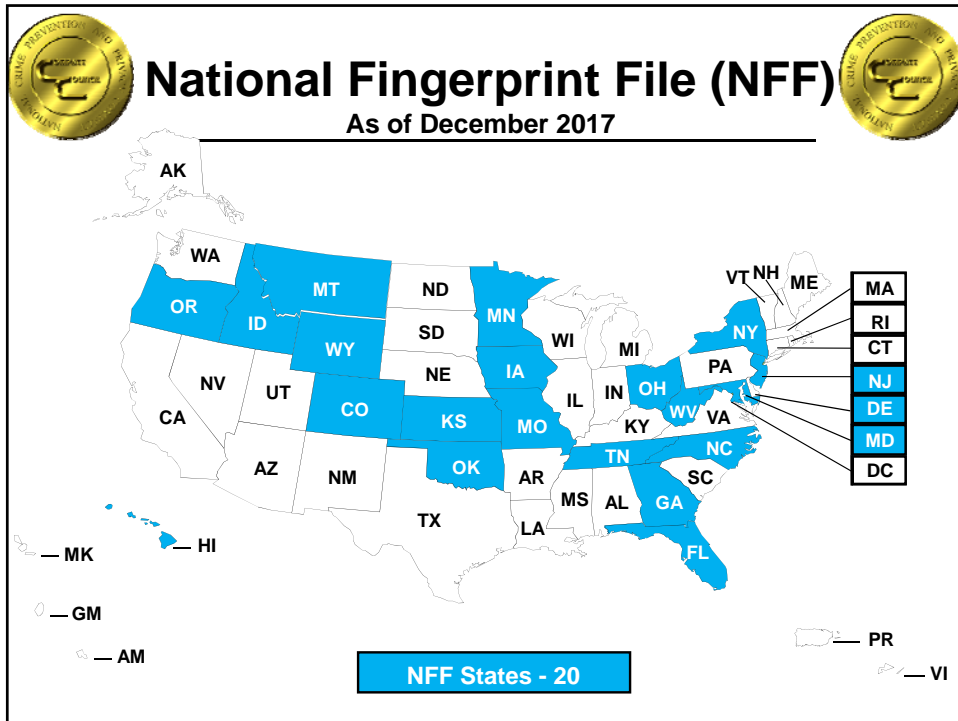


# National Crime Prevention and Privacy Compact Council Update



**Ms. Dawn A. Peck**  
Compact Council Chairman  
(Nov. 2013 – Nov. 2017)





## Fall Council Update

- FBI Compact Officer Report
- Retention of Below Threshold Quality Civil Submissions
- Alternate NFF Program
- Council Member Update



## **FBI Compact Officer Report**

---



- 1 year in review – “Fresh Eyes Observations”
- Four Cornerstones of Success
- Continued support of the states and the Council



## **Retention of Below Threshold Quality Civil Submissions**

---



- “Best 7 of 10” Solution implemented by FBI CJIS Division in November 2016
- Solution aimed to reduce image quality rejects while simultaneously protecting the quality of the national fingerprint repository
- Analysis shows decrease in civil and criminal image quality rejects since implementation





## The Alternate NFF Program

---



- In 2016 Council approved an “alternate” path to NFF participation
- The A-NFF option will continue to place the record maintenance and dissemination on the state
- A-NFF Task Force was established to provide input on technical requirements
- November 2017 Council approved the CJIS Division move forward with development of the A-NFF Program



## Council Member Update

---



### **Council Chairman:**

- Ms. Katie Bower, Michigan

### **Council Vice Chairman:**

- Mr. Wyatt Pettengill, North Carolina

### **Newly Appointed State Compact Officers:**

- Ms. Jennifer Bishop, Hawaii
- Lt. Jeremy Kaplan, Virginia
- Mr. Eric Wiltanger, Wyoming
- Ms. Beverly Wilson, Maryland



## Upcoming Meetings



**Standards and Policy Committee  
Planning and Outreach Committee  
March 21-22, 2018  
Clarksburg, West Virginia**

**Compact Council  
May 16-17, 2018 (tentative)  
Location to be determined**



## Contact Information



**Council Chairman  
Ms. Katie Bower  
(517) 284-3072  
E-mail: [bowerk@michigan.gov](mailto:bowerk@michigan.gov)**

**FBI Compact Officer  
Ms. Chasity S. Anderson  
(304) 625-2803  
E-mail: [csanderson@fbi.gov](mailto:csanderson@fbi.gov)**

**Council Website:  
<http://www.fbi.gov/services/cjis/compact-council>**



# Nlets Update

Frank Minice  
Deputy Executive Director



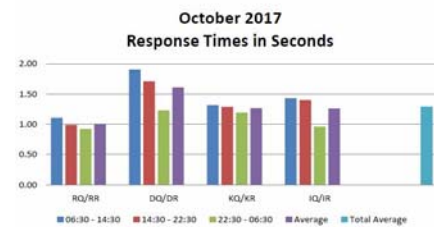
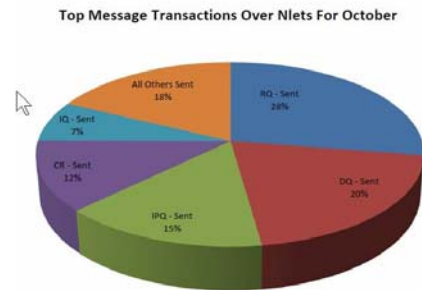
## Nlets Statistics

- *23,000 connected Law Enforcement, Justice and Public Safety, Court and Correction agencies in the United States and Canada.*
- *Over 1 million users.*
- *1,509,508,700 Transactions YTD (through October)*

On pace for over 1.8  
billion transactions in  
2017

# System Statistics

- System Uptime: 99.989%
- Network Uptime: 100%
- Response Time: 76.45ms average



# Nlets Hosting



- Colo Hosting- Rack and stack, Nlets/CJIS compliant datacenters in Phoenix and Louisville (ex: ARJIS, NICB, LoJack, DCI, etc.)
- Backup services available
- NOVA turnkey Nlets Infrastructure as a Service (IaaS) cloud offering
- Direct access capability to the Nlets Network and NJIN system
- CJIS included the NOVA environment in the Nlets 2017 Triannual Audit (passed with no findings)
- Nova disaster recovery offering will be available 1<sup>st</sup> Quarter of 2018.



## NIEF Trust Fabric

- Nlets is a member of the National Identity Exchange Federation
- Project underway to allow access to the Nlets Justice Portal via ICAM with SAML assertions (Kansas, New York, Tennessee.)
- Project underway to exchange Trustmarks to validate users to specific resources (GTRI, EPIC.)

## Multi-State Query Enhancements

- Nlets service enabling users to query all participating states by sending to a single destination of “NL”
- Responses are collated, no hits are suppressed and a summary is provided
- In production for State Warrant Queries (SWQ), Sex Offender Registration Queries (SOQ), Wildlife Licensing Queries (WLQ), CHRI Identity Queries (IQ), Vehicle Registration (RQ), and Drivers License Queries (DQ.)

# Nlets Parsing Service

- Nlets Parsing Services
  - Criminal History (FR and CR messages)
  - Stolen Vehicle Feed
  - Driver License Responses
  - Registration Responses
  - Multi-state Queries (no-hit suppression)

## Common Implementation Pattern

- Parsed messages employ new message keys (P\*R)
- Parsing is implemented for a particular message type for a state or individual ORI
- P\*R schemas mirror standardized formats, but
  - Remove cardinalities
  - Remove enumerations
  - Add QualityCommentText
  - Add OriginalResponseText

## Sunsetting of Nlets Socket Protocol

### *BOD Fall 2014 Motion 8*

Resolved that Nlets will sunset Nlets Socket Protocol by July 2017

## Sunseting of Legacy Text Formats

### *BOD Fall 2014 Motion 7*

Resolve that Nlets will sunset dot delimited text formats by December 2018 at which time all Nlets message traffic will be in standardized XML format.

### *BOD Fall 2015 Motion 20*

Resolve that Nlets extend the deadline to sunset dot-delimited text to December 2019.

## What does this mean?

- All Nlets members must transition from Nlets Socket Protocol to either Web Services or MQ
- All Nlets members must implement **standardized XML** for all message keys that they use
  - Legacy Text wrapped in XML **does not fulfill** this directive
  - Standardized NIEM XML format created and made available in 2015



## New Vin Assist Transaction Available

- Nlets, in cooperation with The National Insurance Crime Bureau, now provides Nlets users with VIN decoding information online. The VIN Assist transaction leverages data provided by the National Highway Transportation Safety Administration Service.
- Nlets created a new message key for this capability (GVQ transaction.)
- By sending an GVQ to the destination code NL, searching on VIN, users will receive specific vehicle details such as vehicle type, vehicle make, vehicle model, model year, color, plant and date of manufacture and much more.

## DHS 5 Eyes Project

- Project to open up access to DHS IDENT for LE via Nlets
- Pilot project includes current DHS components
- Nlets will leverage new message key to call the DHS IDENT service
- NIEM standard
- Nlets will provide stylesheets
- Due to complete late 2017/early 2018 – 100 Users

# DHS LENS Enhancement Project

- The purpose of the Law Enforcement Notification System (LENS) is to transmit informational messages to a state, notifying them that a subject (who meets specific criteria) is being released from ICE custody.
  - Each message is automatically generated by the ICE system of record and sent through NLETS to a state-identified ORI
  - A message will only apply to subjects released who have a conviction documented in ICE's system with specific NCIC charges

## LENS Message

1

\*\*\*\*\***\*ICE CUSTODY RELEASE\***\*\*\*\*\*

FROM NLETS ON 01/13/15 AT 15:58:23  
AM. VTCICE00000  
13:58 04/21/2015  
13:58 04/21/2015 VTCICE0000

2

THE INDIVIDUAL IDENTIFIED BELOW IS EXPECTED TO BE RELEASED FROM THE CUSTODY OF THE U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE) DALLAS FIELD OFFICE TODAY 01/13/2015. FOR FURTHER INFORMATION PLEASE CONTACT THE LESC ON (802) 872-6020 OR VIA NLETS ADMINISTRATIVE MESSAGE (AM) TO VTINS07S0 / VTCICE0900.

SUBJECT INFORMATION:

LNAME: NGUYEN  
CITZ: VIETNAM  
ALIAS: VIN LI  
FBI# A1234567

FNAME: VAN

DOB: 06/05/1971

SID# 123456789

MNAME: XAVIER

A# 123456789

PIN# 123456789

ADDRESS: 123 Main Street, Phoenix, AZ 20009

\*\*\*For your situational awareness only. This is For Official Use Only. Please forward to need-to-know entities as appropriate\*\*\*

## Nlets Approach

- Leverage CHRI parsing project
- Leverage Nlets NJIN routing capability
- Leverage NJP
- Leverage partnerships with SEARCH, Pragmatica, DCI, CPI and other Strategic Partners

## Key Tasks

- LENS Subscription Service Upgrade
- Nlets System Routing Upgrades
- Authoritative State Charge Code Mapping
- Nlets Parsing Service Upgrades
- State Repository Mapping
- Extended Sex Offender Notifications
- Disaster Recovery Replication

# Questions?







# **Identification Services Subcommittee (ISS) Report**

**December 6-7, 2017**

**Mr. Michael Lesko  
Texas Department of Public Safety**

Unclassified

1

## **Information Only Topics**

Unclassified

2

### ***Information Only Topics***

---

- IS Issue #1 Identification Services Coordination Group Update
- IS Issue #2 Impact of Pseudo-Pointers on State Outreach in the NGI System
- IS Issue #3 Solicitation to the User Community Regarding Experiences with Face Recognition Searches of the FBI's NGI Interstate Photo System (IPS) and Utility of the Responses Received
- IS Issue #5 Final Seven of Ten Solution Update and Future Concepts
- IS Issue #6 Criminal History Update
- IS Issue #8 Disposition Task Force Update

Unclassified

3

### ***Information Only Topics***

---

- IS Issue #10 NGI Face Recognition Candidate List Accuracy
- IS Issue #11 Mobile Identification Search of Full Criminal Master File for the Repository for Individuals of Special Concern (RISC)
- IS Issue #12 Miscellaneous Action Items Update
- IS Issue #13 Adhoc Items
- IS Issue #14 Legislative Update

Unclassified

4

**IS Issue #12**  
***Miscellaneous Action Items Update***

---

**Purpose:** Provide updates on miscellaneous action items.

- Consider the effect of 1,000 ppi on current algorithms.
- The FBI will include in the study the analysis of arrest, charge, and disposition in the NSO project and how that could impact National Security and the Brady Act.
- Request the FBI to look at how to make the expungement and modification forms fillable, online forms with electronic submission.
- Advise how disposition notifications (e.g. NFF-related and nonfinal dispositions) will affect the Rap Back responses.

Unclassified

5

**IS Issue #12**  
***Miscellaneous Action Items Update***

---

- The APB passed a motion to support the concept as presented with further study on the impact of using flat fingerprints for criminal justice purposes be performed by NGI in close coordination with the ISS.
- The APB moved to request the CJIS Division staff review, analyze, and report back to the ISCG and the ISS the level of effort and time line necessary to expand RISC searches to additional repositories to include the Criminal Master File.

Unclassified

6



## Action Topics

Unclassified

7

### **IS Issue #4** ***Proposal to Require Training for Those Conducting Face Recognition Searches of the NGI IPS***

---

**Purpose:** Present a proposal to require training for those conducting face recognition searches of the NGI IPS.

- Require Training to Search NGI IPS
- Face Recognition Search
- *NGI IPS Policy and Implementation Guide*

Unclassified

8

**IS Issue #4**  
***Proposal to Require Training for Those  
Conducting Face Recognition Searches of the  
NGI IPS***

---

**Option One:** Require training for agencies/states prior to conducting face recognition searches of the NGI IPS. Required training is identified as completion of the FBI's Facial Comparison and Identification Training class which meets the "Guidelines and Recommendations for *Facial Comparison Training to Competency*" as outlined by the FISWG.

**Option Two:** Make no change.

**Additional Option:** Require training for agencies/states prior to conducting face recognition searches of the NGI/IPS. Required training is identified as completion of the FBI's *Facial Comparison and Identification Training* class or contractor-supplied training which meets the *Guidelines and Recommendations for Facial Comparison Training to Competency* as outlined by the FISWG.

Unclassified

9

**IS Issue #4**  
***Working Group Actions***

---

**Federal:** Accept option one as presented in the topic paper.

**North Central:** Accept option one as presented in the topic paper.

**Northeastern:** Adopt option one as presented in the topic paper.

**Southern:** Adopt option one as amended: Require training for agencies/states prior to conducting face recognition searches of the NGI/IPS. Required training is identified as completion of the FBI's Facial Comparison and Identification Training to Competency" as outlined by the FISWG. The FBI CJIS is tasked with exploring options that would establish competency and report those options to the Working Groups at the Spring 2018 meetings.

**Western:** Adopt option one as presented in the topic paper.

Unclassified

10

## ***IS Motion for APB***

---

**Motion:** Adopt option one as amended: Require CJIS Systems Agency/State Identification Bureau approved training for individuals of agencies/states prior to conducting face recognition searches of the NGI/IPS. Training must be consistent with the “Guidelines and Recommendations for Facial Comparison Training to Competency” as outlined by the FISWG.

Unclassified

11

## **IS Issue #7**

### ***Rapid Deoxyribonucleic Acid (DNA) Update***

---

**Purpose:** Provide an update on the FBI Booking Station Rapid DNA Initiative.

- *Rapid DNA Act of 2017*
- Major Developments
- Rapid DNA Analysis
- Booking Environment
  - Pilots
- Issues Needing Addressed

Unclassified

12

## IS Issue #7

### *Rapid DNA Update*

**Original Recommendation:** Encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for crime scene evidence and the inability to submit those Rapid DNA profiles to CODIS.

**Recommendation One:** The FBI shall issue guidance on the limited use of Rapid DNA Analysis for CODIS, including the prohibition of CODIS entry and searching of crime scene Rapid DNA Profiles

**Recommendation Two:** The FBI shall issue guidance on the limited use of Rapid DNA devices, including the specific prohibition against enrolling and searching of crime scene evidence developed from Rapid DNA devices in CODIS

**Recommendation Three:** The FBI shall issue guidance to Criminal Justice Agencies on the limited use of Rapid DNA machines, including the specific NDIS/CODIS prohibition against enrolling and searching of crime scene profiles developed from Rapid DNA machines

Unclassified

13

## IS Issue #7

### *Working Group Actions*

**Federal:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**North Central:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Northeastern:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Southern:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

**Western:** To encourage the FBI to consider issuing guidance on the use of Rapid DNA Analysis for Crime Scene Evidence, and the inability to submit those Rapid DNA Profiles to CODIS.

Unclassified

14

### ***IS Motion for APB***

---

**Motion:** Accept option two as recommended by the Task Force, “The FBI shall issue guidance on the limited use of Rapid DNA devices, including the specific prohibition against enrolling and searching of crime scene evidence developed from Rapid DNA devices in CODIS.”

.

Unclassified

15

### **IS Issue #9**

#### ***Update on Fusion Center Access to CJIS Division Systems***

---

**Purpose:** Provide an update regarding efforts to fulfill the APB’s recommendations on fusion center access to CJIS Division systems.

- Fusion Center Access to CJIS Division Systems

Unclassified

16

## IS Issue #9

### ***Update on Fusion Center Access to CJIS Division Systems***

**Option One:** Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**Option Two:** No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Option Three:** Discontinue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

Unclassified

17

## IS Issue #9

### ***Working Group Actions***

**Federal:** Accept option one: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency*

**North Central:** No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA. FBI Action: FBI should continue to research various scenarios which may result from any proposed regulatory change. Continue with the interim solution.

**Northeastern:** Adopt option two: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Southern:** Adopt option two: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

**Western:** Adopt option one: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency*

Unclassified

18

## ***IS Issue #9***

### ***Other Subcommittee Actions***

---

**N-DEX:** Accept as information only.

**NCIC:** Option One: Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*

**SA:** To recommend option two: No change to existing regulation and continue the interim solution of granting fusion centers access to CJIS Division systems through a management control agreement with a CJA.

Unclassified

19

## ***IS Motion for APB***

---

**Motion:** Option one as revised, "Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant criminal justice agencies the same authority to contract with noncriminal justice governmental agencies as they currently have to contract with private entities. Accept the language as proposed below: *(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*"

Unclassified

20

# Questions/Comments?

Unclassified

21







U.S. Immigration  
and Customs  
Enforcement

# ICE Programs Update: Biometrics and Advanced Analytics

*FBI CJIS Advisory Policy Board (APB) Meeting*

December 6, 2017



U.S. Immigration  
and Customs  
Enforcement

## EAGLE Directed Identification Environment (EDDIE)

- **EDDIE is a mobile biometric capture device that allows ICE officers to remotely capture and search a subject's fingerprints for immigration and criminal history while in the field**
  - EDDIE runs fingerprints against IDENT or NGI biometric databases (or both) and provides responses to officers within 30 seconds (on average)
  - Significant time and manpower savings; without EDDIE, subjects would have to be taken back to an ICE office to run fingerprint and background checks or are not checked at all
- **Immediate Success**
  - Non-targeted individual encountered during at-large operation
  - Individual provided false name information for a biographic records check, which produced no results
  - Individual was also fingerprinted using EDDIE, which returned an IDENT match with derogatory information indicating an outstanding warrant (for a rape charge; subject is currently serving a 16 year sentence)
- **Current status**
  - FY17 Q4 saw 3,471 biometric captures using EDDIE
  - Currently an average of 240 individual EDDIE users per month

1



- **HFE is an effort to digitize “ink and roll” fingerprint cards into the authoritative DHS repository, IDENT**
  - To date, approximately 400,000 A-files have been reviewed with the purpose of identifying fingerprint hard cards for which there is no digital record and enrolling them into IDENT
  - Efforts have increased match rates on encounters, identified cases of immigration fraud, and added to the availability of information on subjects of national security concern
- **Predictive Data Analytics**
  - ICE has analyzed the volume of files already reviewed to predict which A-files will not have a hard card (deprioritized) and which A-files will have a hard card and are likely matches to fraud (prioritized)
- **ICE is continuing to use predictive data analytics to further refine and prioritize unenrolled A-files to focus on cases with a high likelihood of immigration fraud**
  - Current plan is to complete the review of unenrolled A-files by end of CY2020

2



- **Congress has tasked ICE to enhance and augment current efforts to notify local law enforcement agencies of offender releases from ICE facilities**
  - Existing ICE automated notification system is triggered by NCIC data, which is currently manually inputted by ICE officers
- **ICE is building on its partnership with NLETS to enhance an existing NLETS service that delivers RAP Sheets:**
  - New capability will ensure that **all RAP Sheets** provided by NLETS contain standardized NCIC code data corresponding to the state-specific crime data (if NCIC data is not already included in the RAP Sheet)
- **Potential use to broader Law Enforcement Community**
  - Standardizes criminality data across jurisdictions and allows for the automation of decision support features (e.g., notifications, prioritization)
- **Next Steps**
  - ICE is working to establish a group of stakeholders who value the potential shared benefit and are ready to shape this capability as it is developed

3



**Mr. Philip T. Miller**

*Deputy Executive Associate Director, Enforcement and Removal  
Operations (ERO)*

*U.S. Immigration and Customs Enforcement (ICE)*

**Philip.T.Miller@ice.dhs.gov**





# **National Crime Information Center (NCIC) Subcommittee Report**

**Walt Neverman, Chairman  
December 2017 CJIS APB Meeting  
Oklahoma City, Oklahoma**



**Accepted as Information Only**



**NCIC Issue #5 – NCIC Status Update**

**NCIC Issue #6 – NCIC 3<sup>rd</sup> Generation (N3G)  
Task Force Status Update**

**Ad Hoc Topic – Update on a spring 2017  
NCIC Subcommittee Action Item regarding  
NCIC Code Updates**



## NCIC Issue #1

Fugitive from Justice Discussion



### ***Purpose:***

To obtain recommendations on how to improve processes as a result of a change to the fugitive from justice federal prohibitor



## NCIC Issue #1 Continued



### ***Subcommittee Result:***

FBI Action Item: The NCIC Operations and Policy Unit (NOPU) and the NICS Section shall discuss lessons learned from the changes to the fugitive from justice prohibitor after the initial 12 months. The NOPU will present findings to the N3G Task Force for further review.

FBI Action Item: the NICS Section shall provide additional clarification to assist with establishing each of the three criteria for the fugitive from justice prohibitor and release the information to the CSOs for distribution.



## NCIC Issue #2

Update on Fusion Center Access to  
CJIS Division Systems



### ***Purpose:***

To provide an update regarding the CJIS Division's efforts to fulfill the APB's recommendations regarding fusion center access to CJIS Division systems.



## NCIC Issue #2 Continued



### ***Subcommittee Motion:***

The NCIC Subcommittee made a recommendation to the Identification Services Subcommittee for Option 1:

Endorse the CJIS Division's and FBI OGC's recommendation to sponsor a language change to clarify 28 C.F.R. §20.33(a)(6) as the long term solution to facilitate access to CJIS Division systems, which would grant noncriminal justice governmental agencies the same authority as private entities to contract with CJAs. Accept the language as proposed below:

*(6) To noncriminal justice agencies pursuant to an interagency agreement with a criminal justice agency and for the purpose of performing the administration of criminal justice on behalf of that criminal justice agency.*





## NCIC Issue #3

The Florida Department of Law Enforcement (FDLE)  
National Sex Offender Registry (NSOR) Pilot



### ***Purpose:***

To seek approval to continue the FDLE NSOR Pilot



## NCIC Issue #3 Continued



### **Available Options Considered:**

**Option 1:** Allow FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.  
*(All five Working Groups endorsed option #1)*

**Option 2:** Discontinue the FDLE NSOR Pilot.



## NCIC Issue #3 Continued



### ***Subcommittee Motion:***

The NCIC Subcommittee moved to endorse Option 1:

Allow FDLE NSOR Pilot to become permanent. Additionally, this would allow all CSAs to explore their statutory authority to utilize the NSOR data file for similar operations upon signing an MOU with the FBI.



## NCIC Issue #4

Proposal to Add the Date of Expiration (EXP) Field in  
the Wanted Person File



### ***Purpose:***

To present a proposal to add the EXP Field as optional in the Wanted Person File



## NCIC Issue #4 Continued



### Available Options Considered:

**Option 1:** Add the optional EXP Field to the Wanted Person File. (Three Working Groups endorsed option #1)

**Option 1A:** Allow expired warrants to go into an inactive status and be retrievable by a direct inquiry. A direct inquiry would cause an additional MKE and programming. (One Working Group endorsed option #1A)

**Option 1B:** Do not allow expired warrants to be retrievable by a direct inquiry. (Two Working Groups endorsed option #1B)

**Option 2:** No Change. (One Working Group endorsed option #2)

(One Working Group created a new option: Option 3 – The N3G Task Force should explore the addition of the optional EXP Field to the Wanted Person File, including if it should be returned in all Wanted Person hit responses.)



## NCIC Issue #4 Continued



### ***Subcommittee Motion:***

The NCIC Subcommittee made the following motion:

The N3G Task Force will further explore the addition of the expiration field in NCIC files, including whether or not the records will be retrievable by direct inquiry.



## NCIC Issue #7

NCIC 3<sup>rd</sup> Generation (N3G) Project



### ***Purpose:***

To request approval of the N3G requirements recommended by the N3G Task Force

Concept 13 – Alternative Access  
Concept 4 – Name Search Algorithm  
Concept 8 – Enhanced Testing Environment  
Concept 2 – Tailored Functionality



## NCIC Issue #7 Continued

Concept 13 – Alternative Access



### **Subcommittee Result:**

This concept was accepted for information only.



## NCIC Issue #7 Continued

### Concept 4 – Name Search Algorithm



#### Available Options Considered:

##### Issue 1 – Expanded Name Search

1. Ability to search on partial names.
2. Transpose the first, middle, and last names.
3. Transpose the portion of names separated by hyphens.
4. Transpose the portion of names separated by spaces.
5. Search the phonetic version of ethnic names.
6. Expand the search variations or common versions of names.
7. Provide the ability to conduct an exact name search.
8. Conduct a name search of alias fields.
9. Allow the user to select search options.
10. Provide the ability for a wildcard name search.

**Option 1:** Approve further exploration of all functional requirements as recommended by the N3G Task Force. (5 Working Groups endorsed option #1)



## NCIC Issue #7 Continued

### Concept 4 – Name Search Algorithm



#### Available Options Considered:

**Option 2:** Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

**Option 3:** Approve further exploration of the following functional requirements:



## NCIC Issue #7 Continued

### Concept 4 – Name Search Algorithm



#### Available Options Considered:

##### Issue 2 – Improved Algorithm

1. Improve the name search algorithm.
2. Reduce the number of false positive hits based on the name search algorithm
3. Make the name search algorithm available to users.
4. Conduct searches independent of accent marks.

**Option 1:** Approve further exploration of all functional requirements as recommended by the N3G Task Force.

(5 Working Groups endorsed option #1)

**Option 2:** Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

**Option 3:** Approve further exploration of the following functional requirements:



## NCIC Issue #7 Continued

### Concept 4 – Name Search Algorithm



#### ***Subcommittee Motion:***

##### Concept 4

The NCIC Subcommittee moved to endorse Option 1 for Issues 1-2:

Approve further exploration of all functional requirements as recommended by the N3G Task Force.



## NCIC Issue #7 Continued

### Concept 8 – Enhanced Testing Environment



#### Available Options Considered:

##### Issue 1 – Improved Test Environment

1. Create a more robust test environment.
2. Mirror the functionality between test and operational environments.

**Option 1:** Approve further exploration of all functional requirements as recommended by the N3G Task Force.  
(5 Working Groups endorsed option #1)

**Option 2:** Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

**Option 3:** Approve further exploration of the following functional requirements:



## NCIC Issue #7 Continued

### Concept 8 – Enhanced Testing Environment



#### Available Options Considered:

##### Issue 2 – Test Records

1. Provide test records.

**Option 1:** Approve further exploration of all functional requirements as recommended by the N3G Task Force.  
(5 Working Groups endorsed option #1)

**Option 2:** Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

**Option 3:** Approve further exploration of the following functional requirements:



## NCIC Issue #7 Continued

### Concept 8 – Enhanced Testing Environment



#### ***Subcommittee Motion:***

##### Concept 8

The NCIC Subcommittee moved to endorse Option 1 for Issues 1-2:

Approve further exploration of all functional requirements as recommended by the N3G Task Force.



## NCIC Issue #7 Continued

### Concept 2 – Tailored Functionality



#### **Available Options Considered:**

1. Provide the ability for users to select the content of data returned from a search in the operational environment.
2. Meet or exceed the approved response times, as designated by the APB, for searches designated as tactical, investigative, and administrative.

**Option 1:** Approve further exploration of all functional requirements as recommended by the N3G Task Force.

(5 Working Groups endorsed option #1)

**Option 2:** Do not approve further exploration of any of the N3G Task Force recommended functional requirements.

**Option 3:** Approve further exploration of the following functional requirements:





## NCIC Issue #7 Continued

### Concept 2 – Tailored Functionality



#### ***Subcommittee Motion:***

##### Concept 2

The NCIC Subcommittee moved to endorse Option 1:

Approve further exploration of all functional requirements as recommended by the N3G Task Force.



## N3G Task Force Update

**Wyatt Pettengill, Chairman**  
**December 2017 CJIS APB Meeting**  
**Oklahoma City, Oklahoma**



## ***N3G Task Force Update***



### ***Concepts presented and endorsed at June 2017 APB:***

- Concept 10 – Enhanced Multimedia
- Concept 3 – Access Data Repositories
- Concept 5 – Enhanced Data Search

### ***N3G ongoing review of functional requirements:***

- Monthly teleconferences
- Face-to-face meetings
  - Jacksonville – June 2017
  - Louisville – September 2017

### ***Current status:***

- Reviewed approximately 1,200 functional requirements
- 415 requirements approved for further exploration (36%)
- Completed review of all concepts



## ***N3G Task Force Update***



### ***Next steps:***

Topic papers are being drafted for presentation during the spring 2018 Working Group meetings, to include:

- Approved Functional Requirements for Concepts 6, 9, and 14
- Agile Developmental Approach

Continue to provide the CJIS Division guidance with drafting topic papers for the APB



## Conclusion

---



***Questions or Comments?***



## N3G Task Force Update

Wyatt Pettengill, Chairman  
December 2017 CJIS APB Meeting  
Oklahoma City, Oklahoma

### *N3G Task Force Update*

---

***Concepts presented and endorsed at June 2017 APB:***

- Concept 10 – Enhanced Multimedia
- Concept 3 – Access Data Repositories
- Concept 5 – Enhanced Data Search

***N3G ongoing review of functional requirements:***

- Monthly teleconferences
- Face-to-face meetings
  - Jacksonville – June 2017
  - Louisville – September 2017

***Current status:***

- Reviewed approximately 1,200 functional requirements
- 415 requirements approved for further exploration (36%)
- Completed review of all concepts

## *N3G Task Force Update*

---

### ***Next steps:***

Topic papers are being drafted for presentation during the spring 2018 Working Group meetings, to include:

Approved Functional Requirements for Concepts 6, 9, and 14

Agile Developmental Approach

Continue to provide the CJIS Division guidance with drafting topic papers for the APB

## Conclusion

---

***Questions or Comments?***

•

•



Criminal Justice Information Services  
Advisory Policy Board  
December 6, 2017

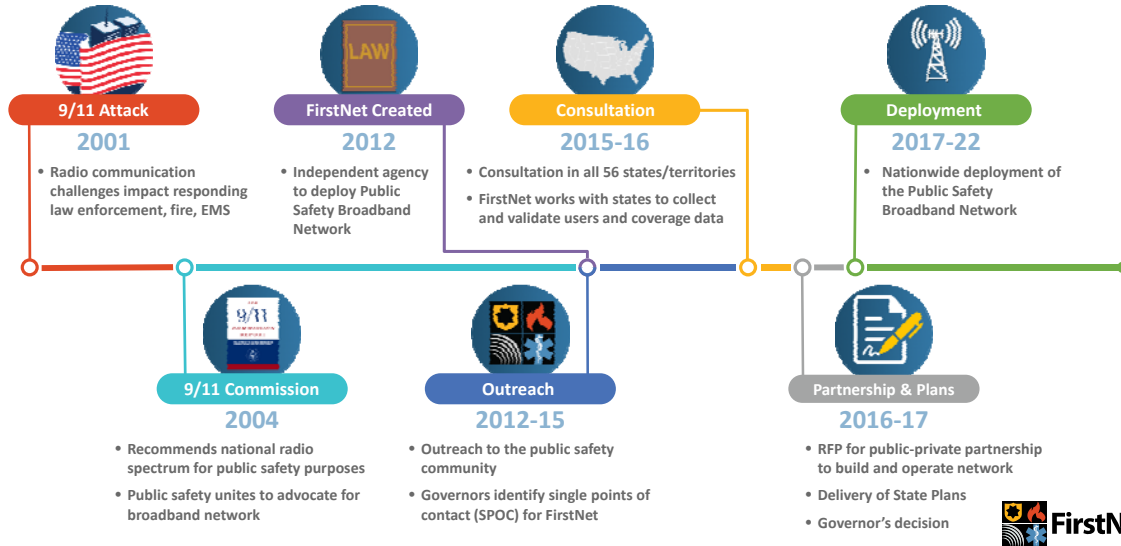
Christopher Algieri  
FirstNet Federal Consultation Lead



## Agenda

- FirstNet Overview
- The Partnership
- Network Deployment and Architecture
- Applications and Devices

# FirstNet's Journey



# Transforming Public Safety Communications



## FirstNet - Dedicated to Excellent Customer Experience (CX)



Prepared under Contract No. D17PC00163. FirstNet retains title to these materials. Public availability to be determined under 47 U.S.C. 1426(d).

# Innovative public-private partnership

**FirstNet**

- Customer experience
- 20MHz Spectrum
- Program management
- Public safety

**AT&T**

- \$180B Infrastructure
- Technology & Innovation
- Secured Network
- Telecom Expertise

Creating an infrastructure dedicated to public safety

## About FirstNet State Plans

States and territories receive a customized, digital State Plan outlining how the FirstNet network will be deployed in the state or territory



Each state's or territory's plan includes key information about FirstNet

<p><b>FirstNet Overview</b></p> <ul style="list-style-type: none"> <li>About FirstNet</li> <li>Value of FirstNet</li> </ul>	<p><b>State Plan Consultation</b></p> <ul style="list-style-type: none"> <li>State/territory consultation</li> <li>Nationwide outreach</li> </ul>	<p><b>Governor's Decision</b></p> <ul style="list-style-type: none"> <li>Executive summary</li> <li>Acceptance and opt-out guides</li> </ul>
<p><b>Coverage</b></p> <ul style="list-style-type: none"> <li>Nationwide coverage</li> <li>Rural providers</li> </ul>	<p><b>Network Architecture</b></p> <ul style="list-style-type: none"> <li>RAN</li> <li>Core network</li> <li>Implementation</li> <li>Security</li> </ul>	<p><b>Products &amp; Services</b></p> <ul style="list-style-type: none"> <li>Features</li> <li>Devices</li> <li>Rate plans</li> <li>Applications</li> </ul>

Based on the State Plan, the state/territory governor can:

**OPT-IN**

FirstNet and AT&T will deploy, maintain and operate the state/territory Radio Access Network (RAN) at no cost to the state for 25 years. Once a state/territory opts in, FirstNet services will be available to public safety agencies and personnel in that state or territory.

To create customized plans, FirstNet consulted with:

**140,000+**  
PUBLIC SAFETY STAKEHOLDERS  
NATIONWIDE

**50**  
STATES  
**5**  
TERRITORIES & DC

**2 MILLION**  
PUBLIC SAFETY PERSONNEL  
THROUGH A **12,000**  
AGENCY DATA COLLECTION EFFORT

**OPT-OUT**

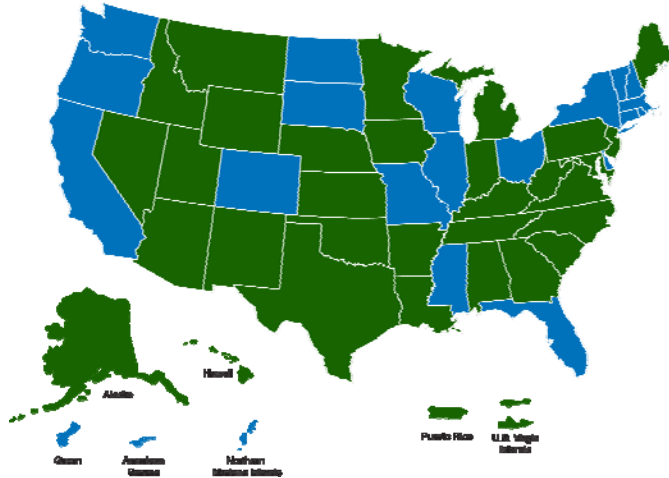
Opt-out means the state/territory is responsible for deployment, operation, maintenance, and improvement of a public safety RAN in that state/territory – including costs and risks.



# 33 “Opt-In” States | Territories



As of Nov. 17, 2017



- Alabama
- Alaska
- Arizona
- Arkansas
- Georgia
- Hawaii
- Idaho
- Iowa
- Indiana
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Michigan
- Minnesota
- Montana
- Nebraska
- Nevada
- New Jersey
- New Mexico
- North Carolina
- Oklahoma
- Pennsylvania
- Puerto Rico
- South Carolina
- Tennessee
- Texas
- U.S. Virgin Islands
- Utah
- Virginia
- West Virginia
- Wyoming



## Radio Access Network – Multi-Band Solution for Public Safety

### Capacity

- Additional bandwidth
- Lower cost/bit as can often deploy more spectrum vs. new sites to add capacity

### Coverage

- More sites & in-building DAS available to Public Safety communications

### Time To Market

- Utilizing an established RAN network with legacy spectrum allows to launch Public Safety services sooner.

### Resiliency

- Wireless interference tends to be band specific & multiple spectrum bands allows for alternative communication paths if one has interference

### Faster Data Speeds

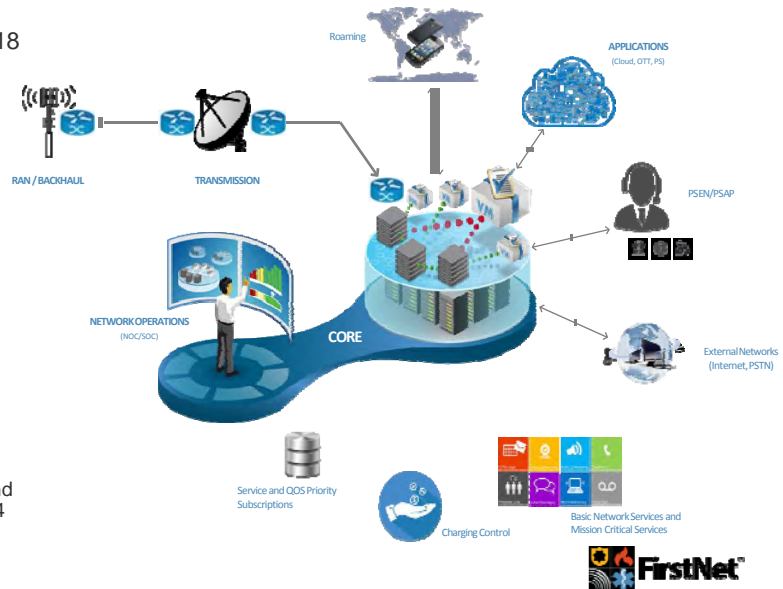
- Combining separate LTE bands (Carrier Aggregation) allows faster data speeds by combining multiple LTE spectrum



34

## Dedicated FirstNet Public Safety Core Network

- FirstNet Core fully implemented March 2018 (IOC-2)
- Based on standardized Evolved Packet Core (EPC) and IP Multimedia Subsystem (IMS)
- Dedicated core for opt-in and opt-out states/territories RANs
- FirstNet Core to provide:
  - Basic network services
  - Mission-critical services (future)
  - Secure access to private/public networks, PSEN/PSAP, enterprise and cloud applications
  - Enables full network sharing among Band 14 and AT&T commercial bands while enabling Band 14 secondary use (MOCN)
    - QoS, priority and preemption across all AT&T LTE bands



## Upcoming: By March 30, 2018

- **Public Safety's own Evolved Packet Core**
- **FirstNet SIM card, network identifier**
- **QoS Management Tool for Administrators**
- **End-to-end Priority, Encryption**
- **"Uplift" capability**
- **Pre-emption**
- **Deployables dedicated to public safety**

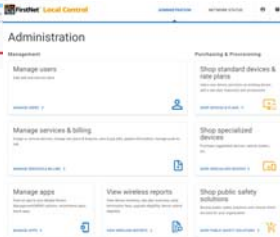
10



# FirstNet Applications Ecosystem V1



Public Safety Home Page



Local Control Administration



Application Store

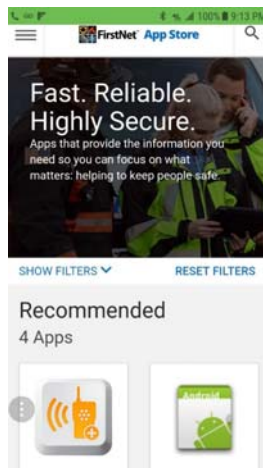
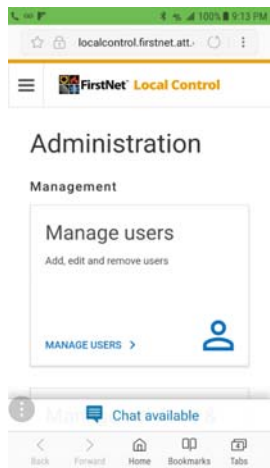


Developer Portal

11



# Local Control and App Store: Mobile Views



## Mobile View

- Mobile Device View of Local Control and App Store

12

These data are submitted with limited rights under Government Contract No. D17PC00163. These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture not disclosed outside the Government. This notice shall be marked on any reproduction of these data, in whole or in part. Pursuant to Clause H.8, Title to Materials, the Contractor transfers to the Government the copyright in written works contained in the materials, subject to the Contractor's rights under FAR 52.27-14, Rights in Data.



# Devices and Ecosystem



## Smartphones



Apple iPhone (iOS)  
Samsung (Android)  
LG (Android)  
Kyocera Duraforce (Android rugged)

## Feature Phone



Sonim XP5 (rugged)  
Kyocera Dura (rugged)  
LG X Venture (rugged)

## Tablets



Apple iPad  
Samsung Galaxy LG G Pad  
Microsoft Surface

## Data Only



Netgear Unite Hotspot (rugged)  
ZTE USB Aircards  
ZTE Hotspot  
AT&T Home Base (router)

## Wearables



Apple Watch  
LG Watch  
Samsung Gear

13

These data are submitted with limited rights under Government Contract No. D379C00163. These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government. This notice shall be marked on any reproduction of these data, in whole or in part. Pursuant to Clause H.8, Title to Materials, the Contractor transfers to the Government the copyright in written works contained in the materials, subject to the Contractor's rights under FAR 52.27-14, Rights in Data.



# FirstNet Application Standards Strategy

## Pillars for Driving Standards

### Technical

- Drive adoption of existing standards, or the creation of new ones
- Drive economies of scale
- Improve user experience
- Minimize interop challenges

### Marketing

- Create strategies to encourage development and use of apps that employ standards
- Lower barriers to entry for new public safety application developers

### Legislative

- Advocate changes to grant programs encouraging (requiring) selection of apps that employ standards

### Stakeholders

- Include PSAC, PS users, agencies, developers, AT&T, academia, associations, and federal partners

14





# Thank You

Christopher Algieri  
Federal Consultation Lead  
First Responder Network Authority

12201 Sunrise Valley Dr. M/S 243  
Reston, VA 20192

[Christopher.algieri@firstnet.gov](mailto:Christopher.algieri@firstnet.gov)  
Office: 571-665-6034  
Mobile: 202-763-6669



# Operational uses of NIBRS



David Bierie, Acting Chief

Business Integration Center  
Investigative Operations Division  
United States Marshals Service  
U.S. Department of Justice

1

## Today's talk



### 1. The U.S. Marshals?

### 2. Applied Science

- Who shoots at police?

### 3. Operational Tools

- NIBRS Profiler (e-Profile)
- Serial Crime Analysis (S.C.An.)
- Community-Connector ( $c^2$ )

### 4. Three bold ideas for NIBRS

❑ The whole is greater than the sum of its parts

❑ NIBRS offers more than annual crime stats or dissertations

❑ Thank You!

2

## Who are the U.S. Marshals?



- Similar to a federal sheriff
- Established in 1789
- 95 districts + FFOs
- 3000 sworn & 2000 support staff
- IOD (Fugitive) Mission:
  - ✓ 60 district fugitive task forces
  - ✓ 7 regional fugitive task forces
  - ✓ ~35,000 federal fugitive cases closed per year
  - ✓ ~75,000 state/local fugitive cases closed per year

Some themes in our history (and NIBRS):  
Justice, Rule of Law, National, Innovation

3

## What is the Business Integration Center?



Science, policy, innovation, integration

Read more at: <http://cebcp.org/wp-content/TCmagazine/TC12-Spring2017>

4



# 1. Science & policy

“Gun violence directed at police officers”

5

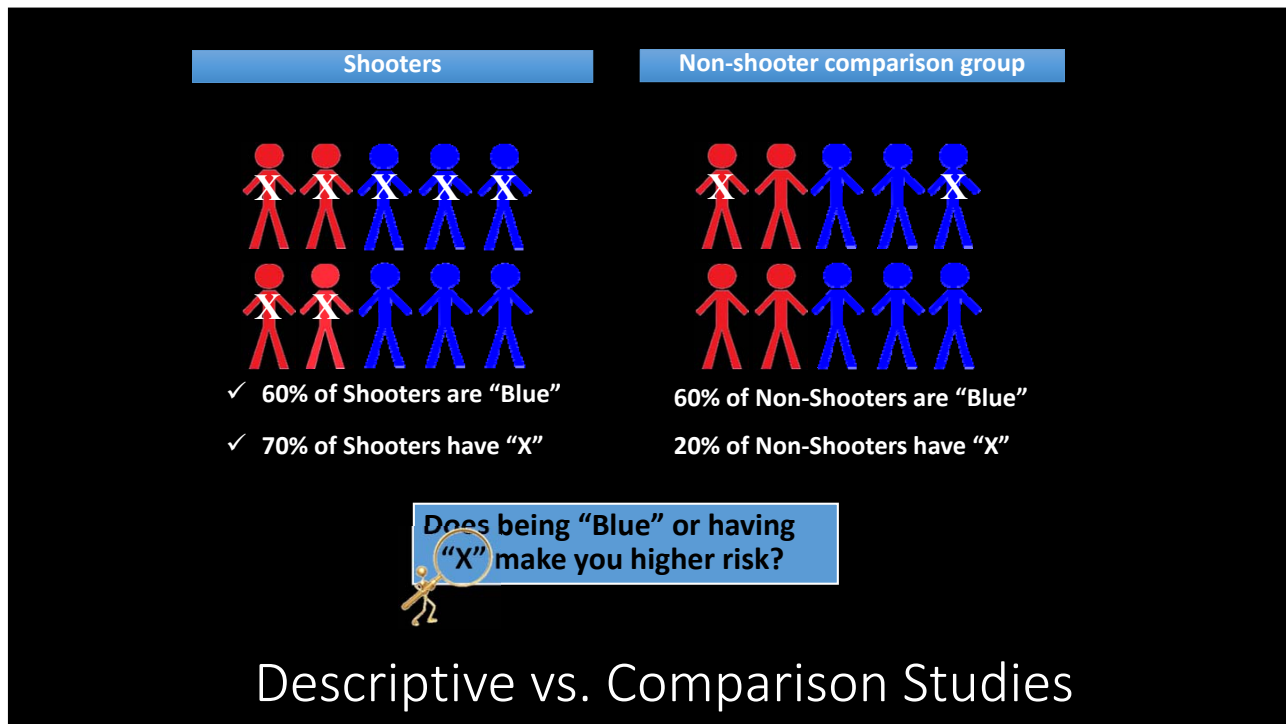
## Why this analysis?

- Officer safety concerns after several LOD deaths in 2010-2011
- We engaged a number of steps to diagnose and mitigate that risk
- One of which was to obtain, read, & learn from every prior study on **risk factors** for firearm violence directed at police.
- That was easy.... there were none.
- Thus, we needed to create scientific facts for our use, and we also wanted to ensure the broader academic, policy, and police community had some facts available to them as well
- *We chose NIBRS because it is the single largest, relevant and useful data set in existence for this question*



6





### Method

✓ **Data:** Compared all incidents with (a) officer-victim of (b) firearm-involved crime (c) at arrests occurring (d) at least one day after incident (n=860) to a random sample of arrests without this type of violence (n=3,000)

✓ **Estimation:** Case control design estimated via a variety of multivariate regression strategies (e.g., skewed, Random Effects)

### RESULTS

- ✓ **Risk factors:** Myriad offender and crime scene predictors, not all of which were mere common sense
- ✓ More specific info at:

➤ <http://journals.sagepub.com/doi/pdf/10.1177/0011128713498330>



## How was this useful?

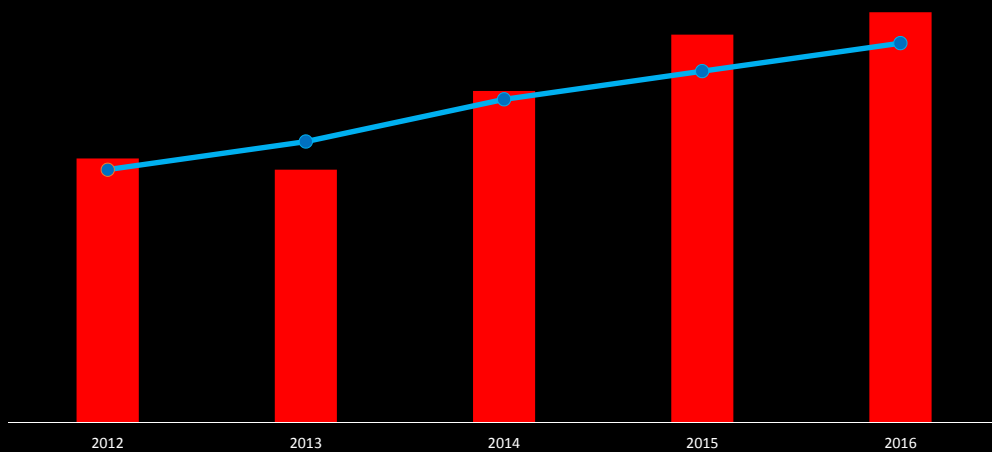
- In conjunction with two other peer-reviewed studies we conducted on violence directed at police, we were able to:
  1. **Training.** Offer some new ideas for our trainers regarding what was risky and how risky, when engaging offenders
  2. **Academia.** Spur additional academic research
  3. **Policy.** Help explain shooting patterns at our agency
    - This was an important step because it provided risk context to patterns at USMS that might have otherwise been perceived differently.



9

## Decomposing shooting trend

Rate of **Firearm Discharges** per 10,000 physical arrests  
Average **Risk** of Fugitive Encountered



10

## But what's the real point?

❑ Analyzing any single county or state would have generated:

1. **Too few cases to analyze rigorously.** We need at least 200 cases (plus 10 per independent variable) to estimate a logistic regression equation.
2. **Too little variance to model.** We need diversity in each of the measures and situations in order to better estimate relationships (i.e., cross state diff).

❑ *Analyzing a rare event like this was only possible because of the size/diversity of the national NIBRS data*

11

## A few more examples

- ❑ Bierie, D. M., & Davis-Siegel, J. C. (2015). Measurement matters: Comparing old and new definitions of rape in federal statistical reporting. *Sexual Abuse*, 27(5), 443-459.
- NIBRS made it possible to assess the impact of this change on total prevalence estimates and trends over time.
- ❑ Bierie, D. M., & Budd, K. M. (2016). Romeo, Juliet, and statutory rape. *Sexual Abuse*, 1079063216658451.
- NIBRS made it possible to test the assumption that police (and the registry) was saturated in unintended sex crimes: 'statutory liaisons' between similarly aged teenager.
- ❑ Bierie et al., "Sexual assaults at parks and playgrounds" (in progress)
- Exclusion laws presume parks/playgrounds are attractive target spaces for those who would target strangers/children. Is this assumption reasonable? NIBRS shows....Yes.
- ❑ Bierie et al., "Do registries improve clearance speed of sex crimes?" (in progress)
- Sex offender registries are intended, in part, to facilitate police investigations of stranger involved sexual offending. Do counties have a faster closure once they enacted a registry? NIBRS shows....Yes

12

## Other applied-science examples from our team

- Williams, K. S., & Bierie, D. M. (2015). An incident-based comparison of female and male sexual offenders. *Sexual Abuse*, 27(3), 235-257.
- Bierie, D. M. (2015). Enhancing the National Incident–Based Reporting System: A Policy Proposal. *International journal of offender therapy and comparative criminology*, 59(10), 1125-1143.
- Bierie, D. M., Detar, P. J., & Craun, S. W. (2016). Firearm violence directed at police. *Crime & Delinquency*, 62(4), 501-524.
- Bierie, D. M. (2015). Assault of police. *Crime & Delinquency*, 0011128715574977.
- Budd, K. M., Bierie, D. M., & Williams, K. (2017). Deconstructing incidents of female perpetrated sex crimes: comparing female sexual offender groupings. *Sexual Abuse*, 29(3), 267-290.
- Budd, K. M., Rocque, M., & Bierie, D. M. (2017). Deconstructing incidents of campus sexual assault: comparing male and female victimizations. *Sexual Abuse*, 1079063217706708.
- Budd, K. M., & Bierie, D. M. (2017). Injury Matters: On Female-Perpetrated Sex Crimes. *Journal of Interpersonal Violence*, 0886260517711178.

❖ You can obtain FREE full-text version of any of these via [www.google.com/scholar](http://www.google.com/scholar)



## 2. Conceptualizing Operational Tools

1. e-profiler
2. Serial Crime Analysis
3. Community Connections

## Behavioral Analysis Unit

- How “profiling” usually works:
  - ❑ Scour the scientific literature for known facts/correlates of case details
  - ❑ Theoretically informed expansions from those empirical facts
- A common goal is:
  - ❑ Prioritize leads in the face of scarce resources
- Problems with profiling:
  - ❑ The weirder the case, the more likely that.....
    1. There are few or no prior studies or examples
    2. The studies that do exist have small sample sizes
      - E.g., Stranger sexual assaults at playgrounds → largest study has N=12!

15

## What is the NIBRS e-Profiler?

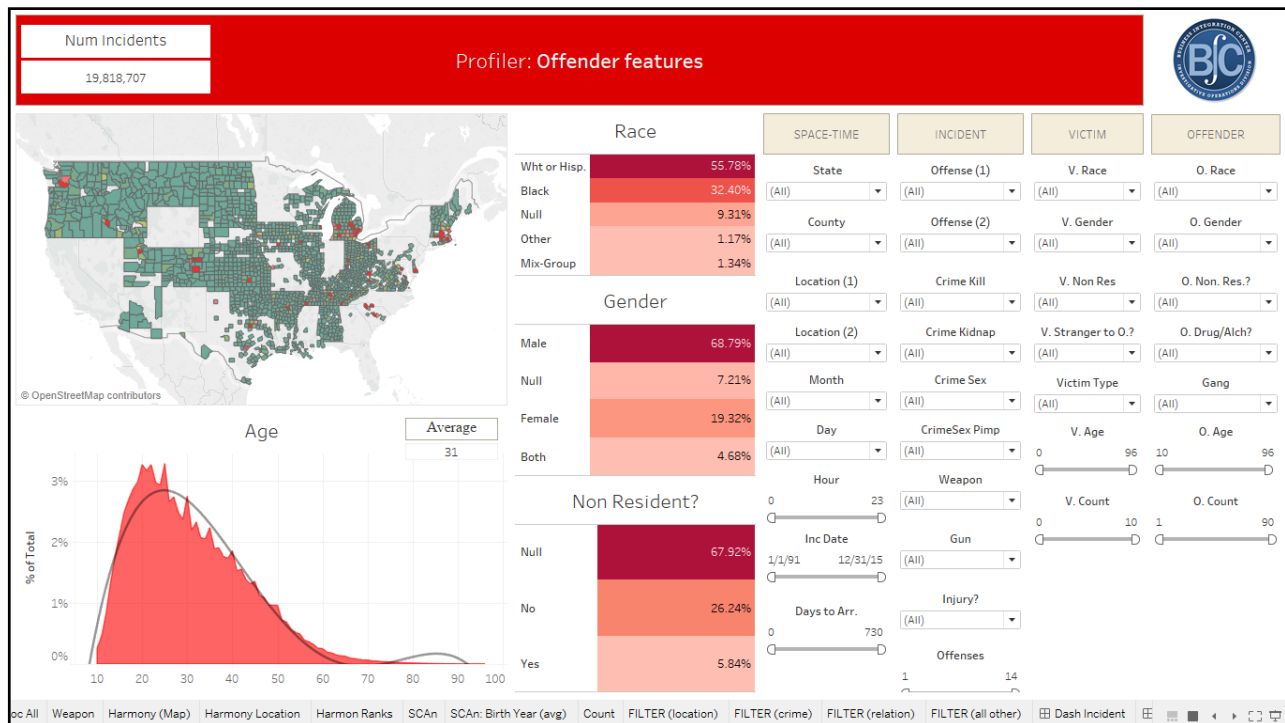
- ✓ **What:**
  - Visual analytic dashboard with all NIBRS data, myriad data elements as filters, and other data merged in as well (county level)
- ✓ **How:**
  - Dynamic use of filter combinations as information arrives (known) shows probabilistic information about ‘unknown’ information (non parametric)
- ✓ **Why?**
  - Focus investigation toward or away from certain basic assumptions
  - Prioritize leads in the face of scarce resources

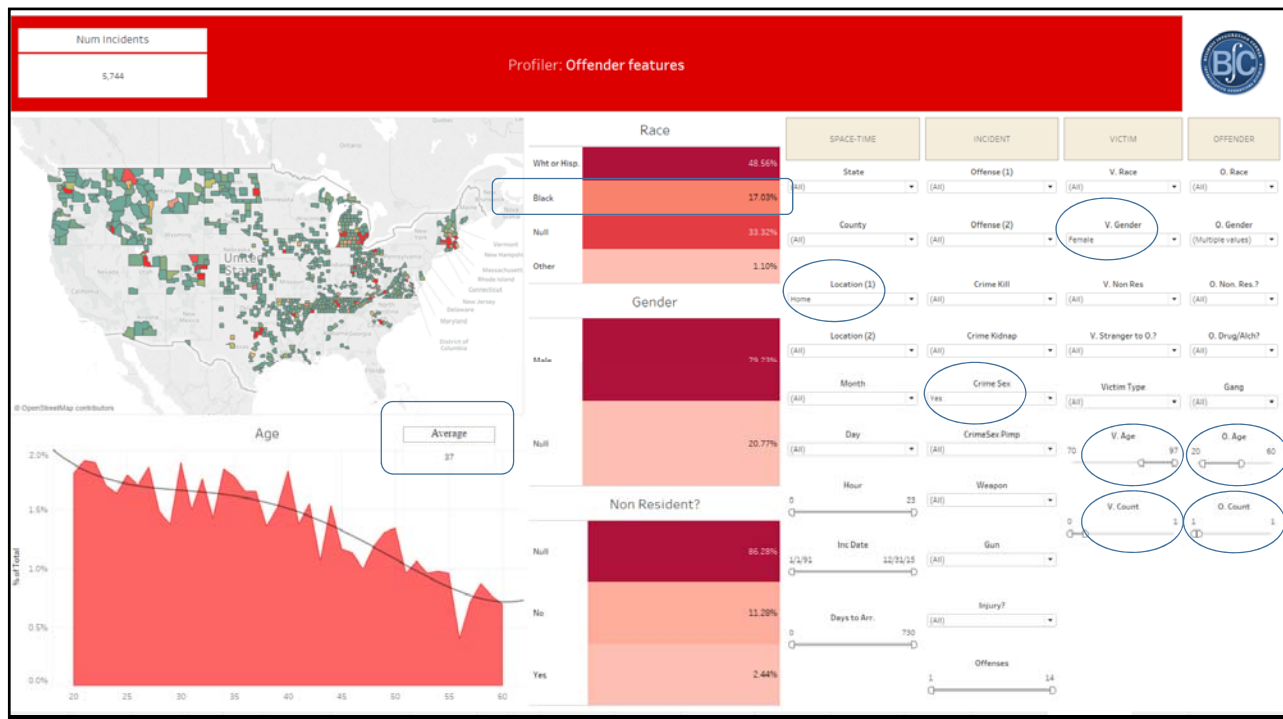
16



# Case example: Serial rapist targeting elderly

17





## Another example: child sexual assault in FL

- ❑ Home surveillance camera captures attack
- ❑ Girl reports black male, approx. 55 years old
- ❑ E-Profiler “given” of:
  - 10 – 12 yo, white, female victim in open area, sexually assaulted by stranger, who was a black, male. (You could also add day of the week and time.)
  - E-profiler said age 23 was the most likely
- ❑ Arrest two days later of 23 year old man who was on leave from the military.



# Serial Crime Analysis (S.C.An.)

21

## What is S.C.An.?

### ✓ What?

- Visual analytic dashboard with all NIBRS data, all data elements as filters, and other data merged in as well (county level) in order to *find crimes that may be linked to the same offender(s)*.

### ✓ How?

- Identify “weird” features of a particular crime or series that are also NIBRS data elements, subset to see other incidents with similar features, and map them to view over time and space.

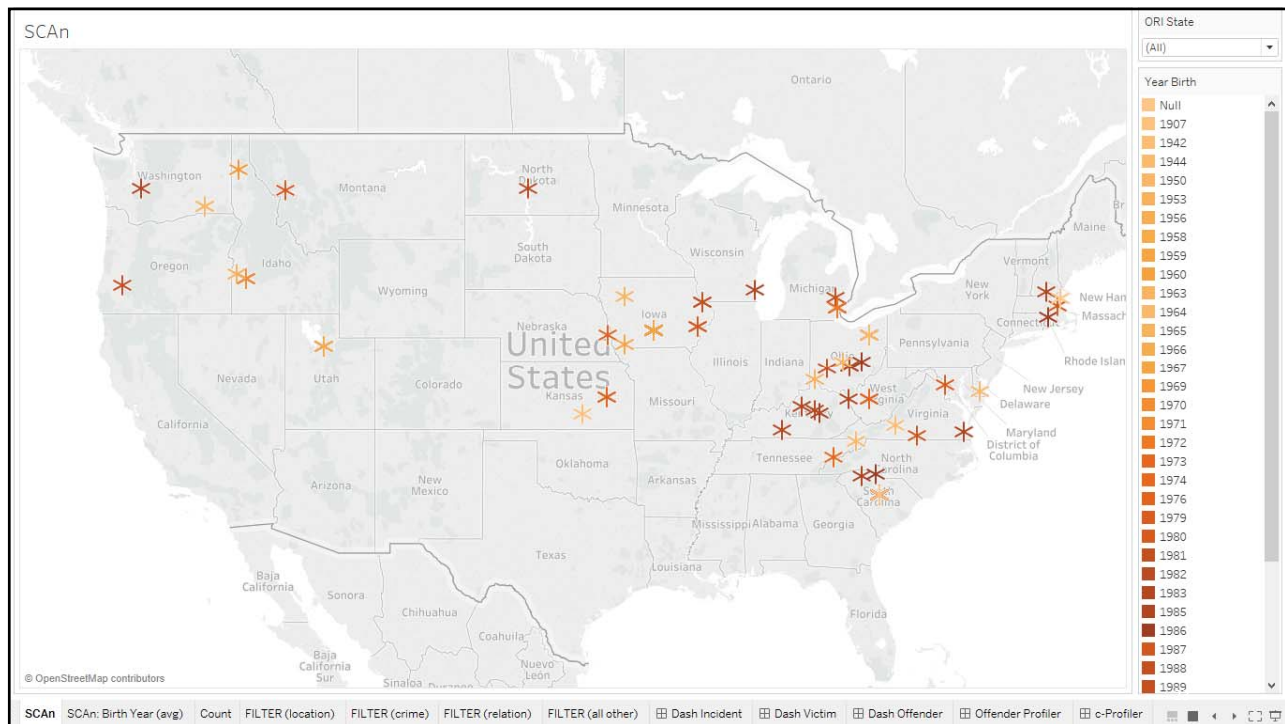
### ✓ Why?

- Finding crimes linked to the same offender(s) could help identify that offender (e.g., combining evidence from different crime scenes).
- NIBRS is a huge pool of cases in which a few weird features can be isolated

□ Example: *Serial abductions in western state by a man and woman in their 20s abducting young girls (10 – 13) into a van, sexually assaulting them, and then dropping them off. A young couple working as a team engaged in forcible abduction/sexual assaults is kind of rare, and in NIBRS. So .....*

22





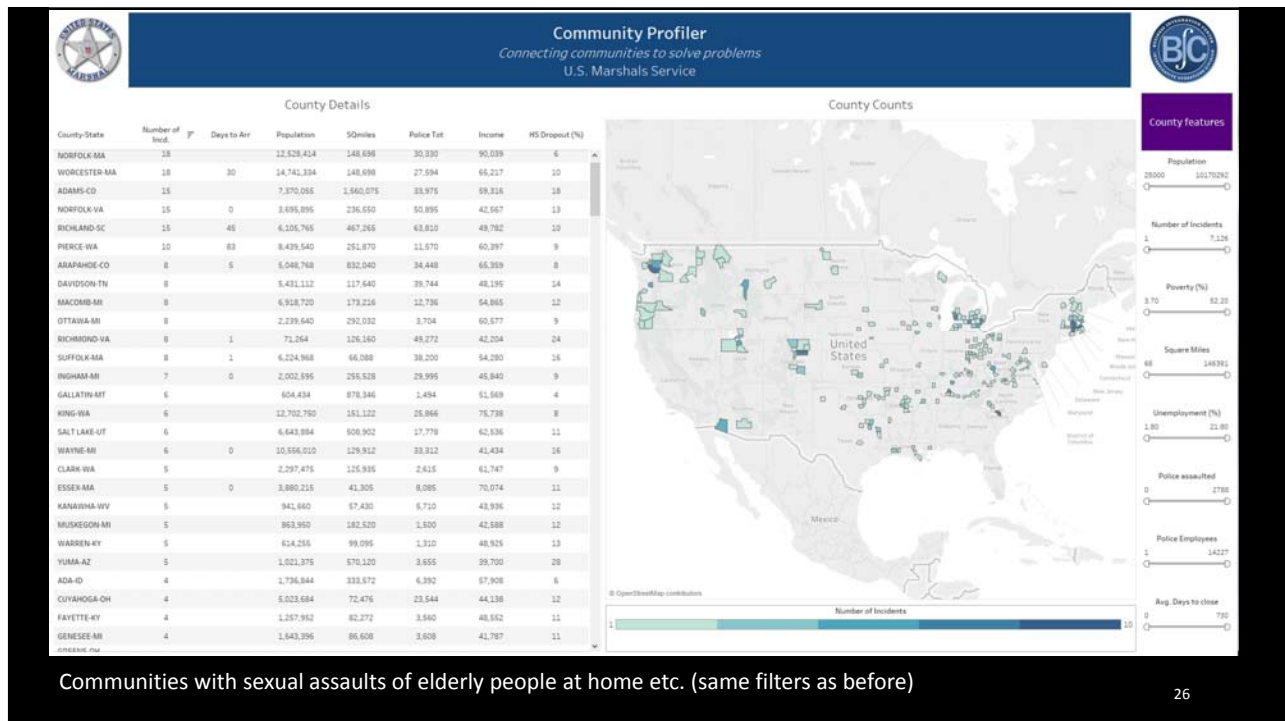
$c^2$  Community Connections

24

# What is Community Connector (c<sup>2</sup>)

- **What?**
  - Visual analytic dashboard with all NIBRS data, all data elements as filters, and other data merged in as well (county level) in order to *find other communities that may have insight to offer*.
- **How?**
  - Articulate a feature of one community in terms of NIBRS elements in order to see other communities:
    - Who else is dealing with similar issues, having dealt with similar issues, or having avoided them.
    - Can I zero in on communities like mine (population, police size, unemployment, etc.) to get even more comparable insights?
- **Why?**
  - To avoid reinventing the wheel, get as many ideas on the table, and ultimately identify a faster and more reliable solution to a local problem.
- **Example:** Who else has experience with forcible rapes of elderly women at their homes—who can we call for help/insight?

25



26



## Now for the ask.....

Two ideas about NIBRS

27

### 1. Record arresting ORI in arrestee table?

#### Effort Level?

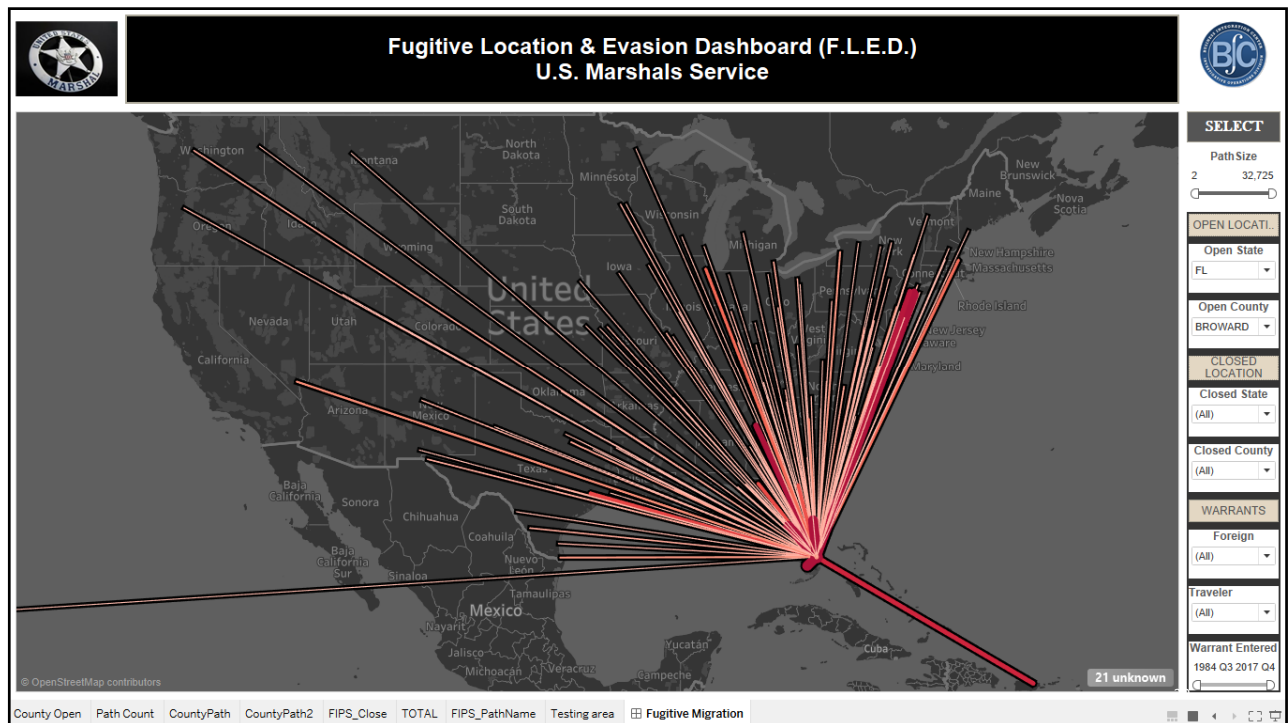
- ✓ We probably all have this in our data systems already and its an easily accepted item for FBI/NIBRS (I assume)?

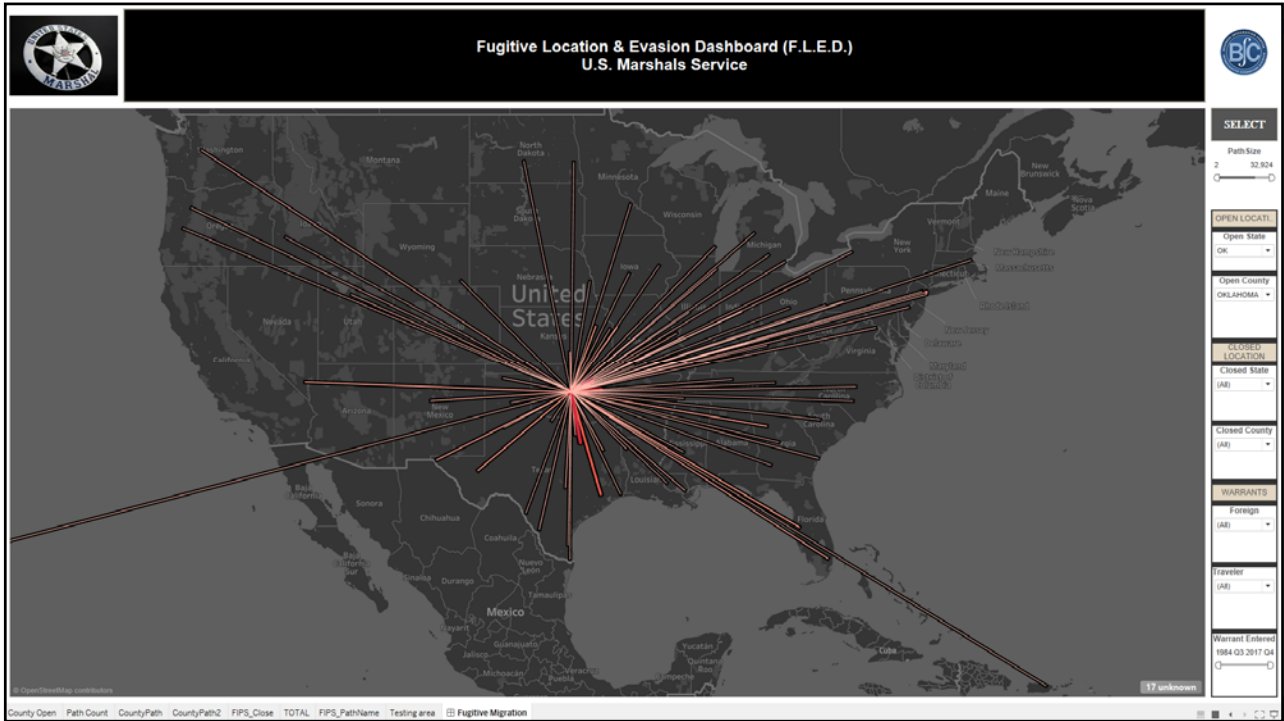
#### Why do it?

- ✓ You need to know how many, what kind, and who's criminals are being arrested in your jurisdiction, and who is likely to flee.
- ✓ We want to create nuanced predictive models of who flees a jurisdiction and where they go.
  - Partly this is so we can justify our mission/budget as the agency that crosses any jurisdiction – we clear 100,000 local cases per year and have no way to show that in NIBRS!
  - Mostly this is so we can create tools to help us catch bad guys faster
  - We think this would help all NIBRS contributors with myriad NIBRS uses

28

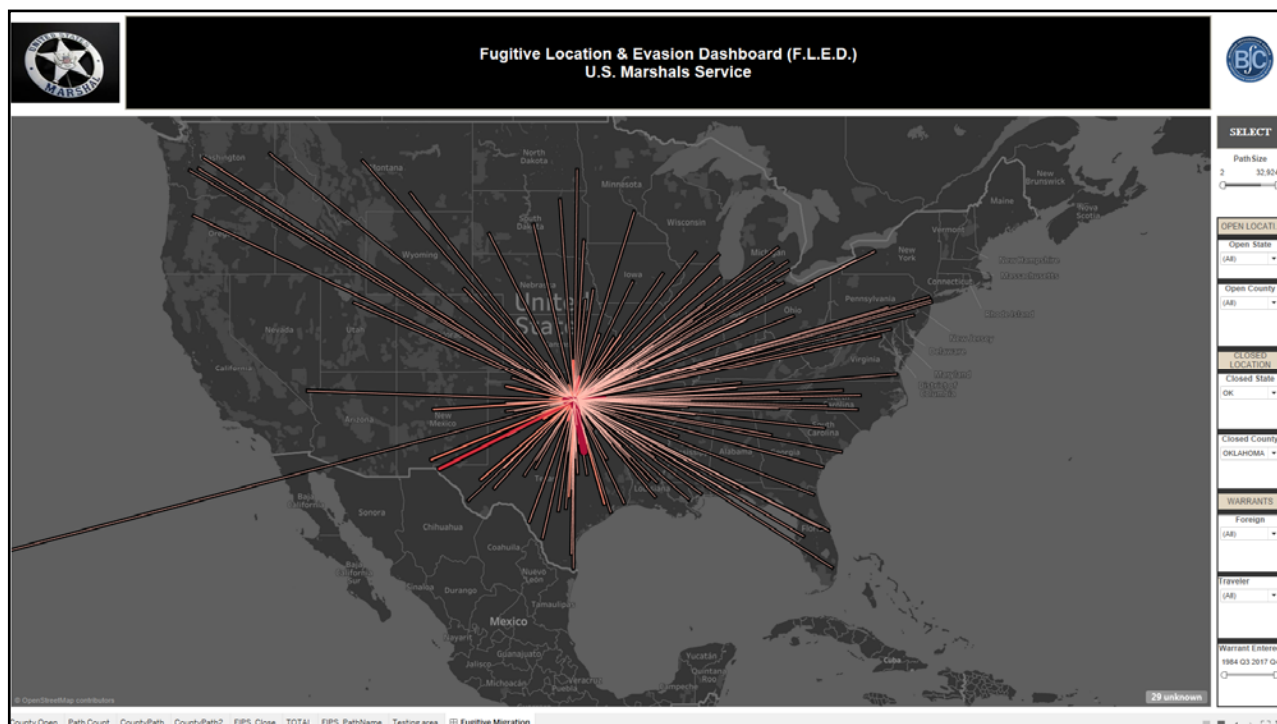
Fleeing from....





Fleeing to....

32



## 2. Can we include the FBI# of arrestees?

### Effort level

- If it exists for that offender, we probably all have it in our systems
- This could be protected / encrypted just as FBI already does for OCA

### Why do it? It would enhance our ability to ....

1. fill in missing data from other NIBRS entries or other federal data systems
2. analyze criminal careers over time and space
3. analyze linked crimes (serial offending)
4. analyze criminal networks (social network analysis/change
5. and correct a HUGE statistical error in many uses of NIBRS data: violation of the independent observations assumption

❖ That is a lot of incidents: ~50% of crime is committed by ~5% of offenders!

34

## Summary

- ❑ NIBRS is also useful for operational applications
  - Applied science & Policy guidance
  - Perhaps Investigative guidance tools
  
- ❑ The national data has value beyond the sum of the parts
  - Especially for rare events
  
- ❑ I bet there is room to discover and increase value of NIBRS
  - In addition to adding new elements to NIBRS, or new contributors,
  - Can we add new *functionality* such as facilitate network, criminal career, or migration capacity?
    - Would that be hard? Yes. Crazy? Maybe. And yet.....



## Thank you

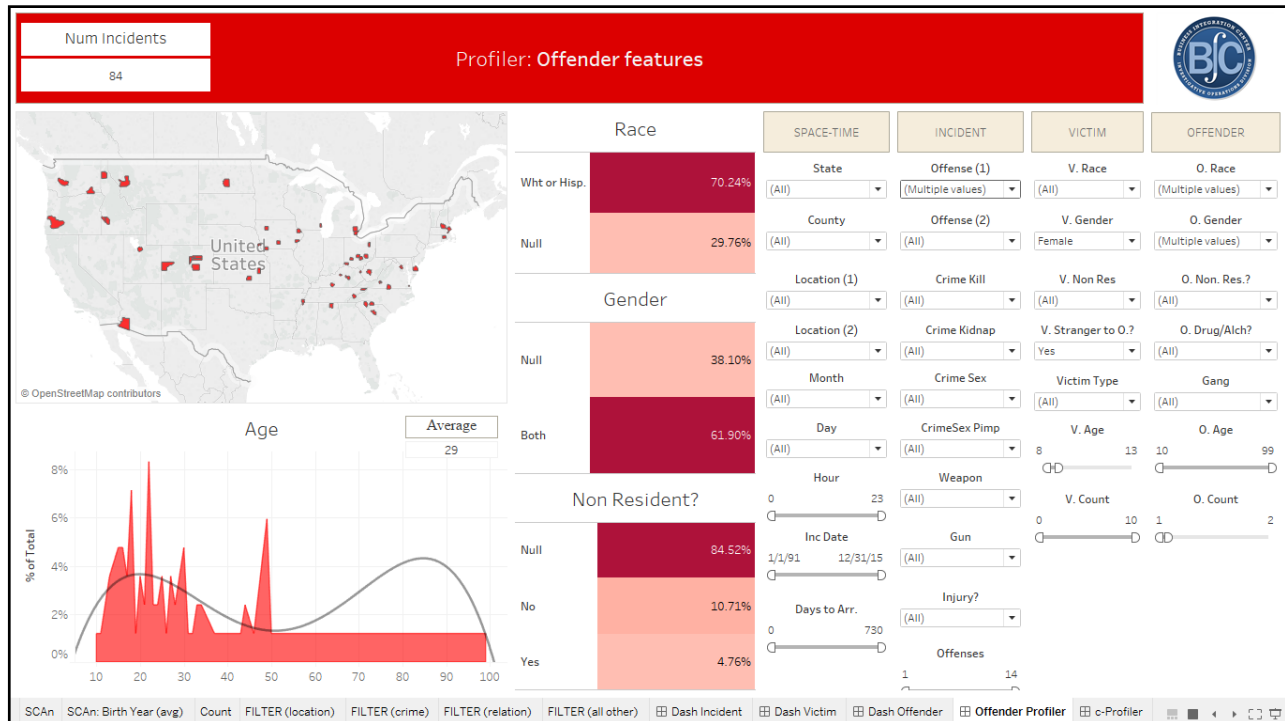
David Bierie

Business Integration Center  
Investigative Operations Division  
U.S. Marshals Service

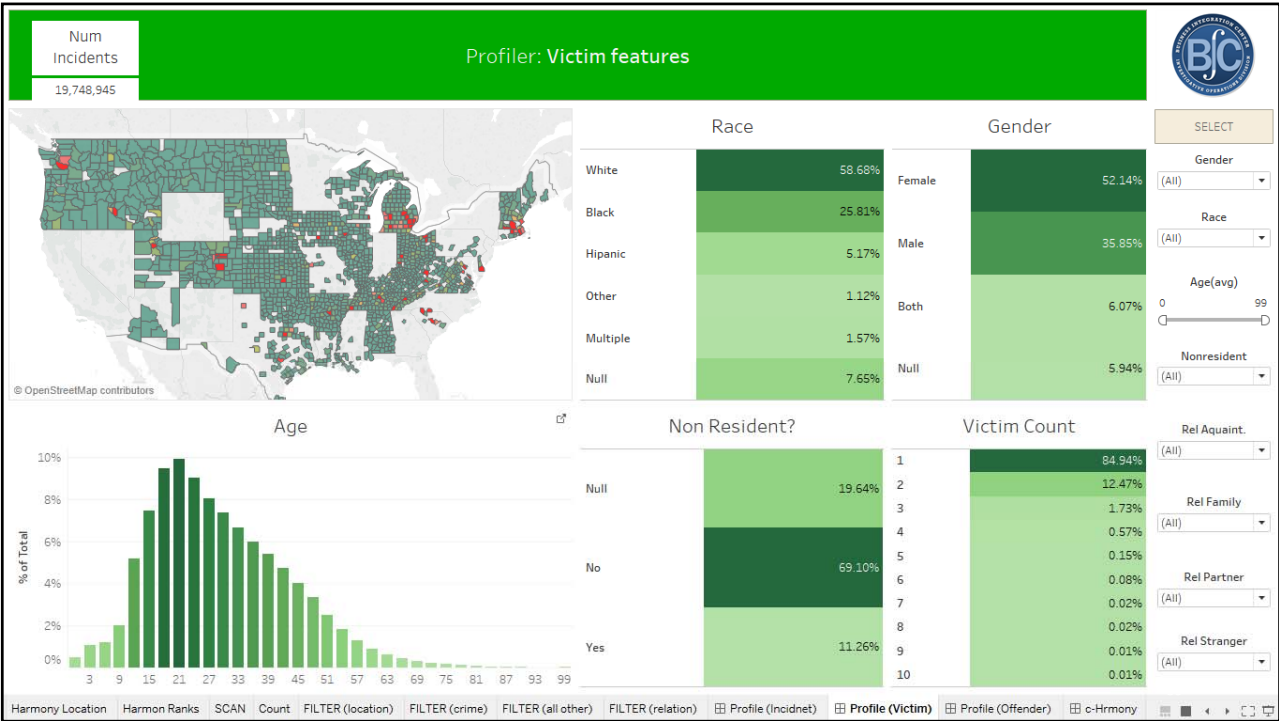
David.Bierie@usdoj.gov



# Extra slides









## **Uniform Crime Reporting (UCR) Subcommittee Report**

**Colonel Douglas A. Middleton  
Criminal Justice Information Services (CJIS)  
Advisory Policy Board (APB) Meeting  
December 2017  
Oklahoma City, Oklahoma**



### **UCR Issue #2**

**Modification of the Application of the Current  
Embargo Policy for the Release of  
UCR Program Data**



#### ***Purpose:***

Propose a modification of the current data embargo policy that would allow for the Federal Bureau of Investigation's (FBI) UCR Program to update data in Crime Data Explorer (CDE) on a more frequent basis.

UNCLASSIFIED

2



**UCR Issue #2, continued**  
**Modification of the Application of the Current  
Embargo Policy for the Release of  
UCR Program Data**



***Subcommittee Options:***

**Option 1:** The UCR Program should cease its application of the data embargo policy allowing for the most frequent possible updates to the CDE.

**Option 2:** No Change

UNCLASSIFIED

3



**UCR Issue #2, continued**  
**Modification of the Application of the Current  
Embargo Policy for the Release of  
UCR Program Data**



***The UCR Subcommittee recommended two motions:***

**Motion 1 - Option 1:** The UCR Program should cease its application of the data embargo policy allowing for the most frequent possible updates to the CDE.

UNCLASSIFIED

4



## UCR Issue #2, continued

### Modification of the Application of the Current Embargo Policy for the Release of UCR Program Data



#### ***The UCR Subcommittee recommended two motions:***

**Motion 2** - Prior to the 2017 and later data being published in the CDE, the FBI (in cooperation with local, state, federal, tribal, and academic representatives) will develop the necessary standards on frequency of submission, frequency of release, what data elements are to be collected and released, and what caveats concerning the data that is released. The work of the FBI will be concluded by May 2018.

UNCLASSIFIED

5



## UCR Issue #3

### Addition of UCR Offenses for Federal Crime Reporting to the NIBRS



#### ***Purpose:***

Present the recommendation of additional UCR offenses for federal agencies to report crime data to the National Incident-Based Reporting System (NIBRS).

UNCLASSIFIED

6



## UCR Issue #3, Continued

Addition of UCR Offenses for Federal Crime Reporting to the NIBRS



### ***Subcommittee Options:***

**Option 1:** Accept all recommended NIBRS UCR offense codes for federal reporting

**Option 2:** Accept all recommended NIBRS UCR offense codes for federal reporting. In addition, accept the following further offense codes (please list):

UNCLASSIFIED

7



## UCR Issue #3, Continued

Addition of UCR Offenses for Federal Crime Reporting to the NIBRS



### ***The UCR Subcommittee recommends the following motion:***

**Option 2:** Accept all recommended NIBRS UCR offense codes for federal and tribal reporting. In addition, accept the following further offense codes and additional changes:

- 520A – Firearm (violation of the National Firearm Act of 1934)
- 520B – Weapons of Mass Destruction
- 526 – Explosives

UNCLASSIFIED

8



### **UCR Issue #3, Continued**

**Addition of UCR Offenses for Federal Crime Reporting to the NIBRS**



***The UCR Subcommittee recommends the following motion continued:***

Additionally, the definitions of the below offenses are amended as follows:

- Federal Liquor Offense - The violation of federal laws prohibiting the production, importation, distribution, transportation, sale, purchase, or possession of non-tax paid distilled spirits, wine, or beer, and the equipment or devices utilized in their preparation.
- Federal Tobacco Offense - The violation of federal laws prohibiting the production, importation, distribution, transportation, sale, purchase, or possession of non-tax paid tobacco products.

UNCLASSIFIED

9



### **UCR Issue #4**

**The Use of the Judicial District (JD) for Federal Agencies to Report a NIBRS Incident to the UCR Program**



***Purpose:***

Present the recommendation for federal agencies to report the location of a NIBRS incident to the FBI UCR Program by JD.

UNCLASSIFIED

10



## UCR Issue #4, Continued

The Use of the Judicial District (JD) for Federal Agencies to Report a NIBRS Incident to the UCR Program



### ***Subcommittee Options:***

**Option 1:** Create a new data element that exists in the Administrative Segment that captures the JD code for federal agencies to report the location of a NIBRS incident to the UCR Program.

**Option 2:** No Change

UNCLASSIFIED

11



## UCR Issue #4, Continued

The Use of the Judicial District (JD) for Federal Agencies to Report a NIBRS Incident to the UCR Program



### ***The UCR Subcommittee recommends the following motion:***

**Option 1:** Create a new data element that exists in the Administrative Segment that captures the JD code for federal agencies to report the location of a NIBRS incident to the UCR Program.

UNCLASSIFIED

12



## UCR Issue #5 Expansion of the UCR Program Police Employee Collection



### ***Purpose:***

Propose a definition for measuring the number of police contacts with the public in order to relate them to incidents of use of force and assaults against law enforcement officers.

UNCLASSIFIED

13



## UCR Issue #5, Continued Expansion of the UCR Program Police Employee Collection



### ***Subcommittee Options:***

**Option 1:** In consultation with CJIS Systems Officers and UCR State Program Managers, add the ability to capture the information on recorded police contacts with the public *to the annual Police Employee data collection*. Included in this collection should be the ability to discern the most common types of calls for service or officer-initiated actions that are recorded by the agency in a CAD system or other similar record-keeping system. (See the sample collection shown on next slide.)

UNCLASSIFIED

14





**UCR Issue #5, Continued  
Expansion of the UCR Program Police  
Employee Collection**



***Subcommittee Options:***

Please provide a count of the following types of recorded police contacts with the public by officers employed by your agency. All counts should include contacts from January 1 to December 31 of the calendar year

Category	Call/Request Count
Citizen calls for service	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Unit/officer-initiated contacts	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
	<b>Attendee Count</b>
Protests/Mass demonstration/Other security detail	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Court/Bailiff activities	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available
Community outreach	<input type="checkbox"/> Estimated <input type="checkbox"/> Not available

UNCLASSIFIED

15



**UCR Issue #5, Continued  
Expansion of the UCR Program Police  
Employee Collection**



***Subcommittee Options:***

**Option 2:** Approve the description in Option 1 with modifications

**Option 3:** No Change

UNCLASSIFIED

16



## UCR Issue #5, Continued Expansion of the UCR Program Police Employee Collection



### The UCR Subcommittee recommends the following motion:

Add the ability to capture the information on recorded police contacts with the public on an annual basis and revise the table as provided.

- Please provide a count of the following types of recorded police contacts with the public by officers employed by your agency. All counts should include contacts from January 1 to December 31 of the calendar year

Category	Call/Request/Individuals on the Docket Count
Citizen calls for service	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable
Unit/officer-initiated contacts	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable
Court/Bailiff activities	<input type="checkbox"/> Actual <input type="checkbox"/> Estimated <input type="checkbox"/> Not available <input type="checkbox"/> Not applicable

UNCLASSIFIED

17



## UCR Issue #6 Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"



### **Purpose:**

Present for discussion the current FBI UCR Program definition of a law enforcement officer and the Law Enforcement Officers Killed and Assaulted (LEOKA) Program's data collection criteria in regard to law enforcement officers who are paid from government funds set aside specifically for payment of sworn law enforcement representatives.

UNCLASSIFIED

18



## UCR Issue #6, Continued



Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

### ***Subcommittee Options:***

**Option 1:** Accept and approve the changes to the UCR Program's definition of a law enforcement officer and the LEOKA collection criteria as identified on the next slides with the following changes, which are in bold text, to the law enforcement officer definition and the LEOKA criteria and exclusions.

**Option 2:** No Change

UNCLASSIFIED

19



## UCR Issue #6, Continued



Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of American citizens. They must have **statutory** arrest powers and **be members of a law enforcement agency, paid from funds set aside specifically for payment to sworn law enforcement** organized for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

UNCLASSIFIED

20



## UCR Issue #6, Continued



### Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

#### LEOKA Criteria

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**
- **Were paid from funds set aside specifically for payment of sworn law enforcement**
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

UNCLASSIFIED

21



## UCR Issue #6, Continued



### Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

#### Exclusions from the LEOKA Program's Data Collection

Deaths resulting from the following are not included in the LEOKA Program's statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program's statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

UNCLASSIFIED

22



## UCR Issue #6, Continued



Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

***The UCR Subcommittee recommends the following motion:***

**Option 1 with modifications**

UNCLASSIFIED

23



## UCR Issue #6, Continued



Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

Law Enforcement Officer - All local, county, state, tribal and federal law enforcement officers (such as municipal, county police officers, constables, state police, highway patrol, sheriffs, their deputies, federal law enforcement officers, marshals, special agents, etc.) who are sworn by their respective **authorities** to uphold the law and to safeguard the rights, lives and property of ~~American citizens~~ **individuals**. They must have **statutory** arrest powers and **be members of a law enforcement agency, paid from funds set aside specifically for payment to sworn law enforcement** organized and **funded** for the purposes of keeping order and for preventing and detecting crimes, and apprehending those responsible.

UNCLASSIFIED

24



## UCR Issue #6, Continued



Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

### LEOKA Criteria

- Wore/carried a badge (ordinarily)
- Carried a firearm (ordinarily)
- Were duly sworn and had full arrest powers
- **Were members of a law enforcement agency**
- ~~Were paid from funds set aside specifically for payment of sworn law enforcement~~
- Were acting in an official capacity, whether on or off duty, at the time of incident
- If killed, the deaths were directly related to the injuries received during the incident

An exception to the above criteria includes individuals who are killed or assaulted while acting in a law enforcement capacity at the request of a law enforcement agency whose officers meet the LEOKA criteria.

UNCLASSIFIED

25



## UCR Issue #6, Continued



Review of the UCR Program's Definition of a Law Enforcement Officer as it Pertains to the Phrases, "Public Governmental Law Enforcement Agency" and "Paid for from Government Funds"

### Exclusions from the LEOKA Program's Data Collection

Deaths resulting from the following are not included in the LEOKA Program's statistics:

- Natural causes such as heart attack, stroke, aneurism, etc.
- On duty, but death is attributed to their own personal situation such as domestic violence, neighbor conflict, etc.
- Suicide

Examples of job positions not typically included in the LEOKA Program's statistics (unless they meet the above exception):

- Corrections/correctional officers
- Bailiffs
- Probation/parole officers
- Federal judges
- U.S. and Assistant U.S. Attorneys
- Bureau of Prisons Officers
- **Private Security Officers**

UNCLASSIFIED

26



## Informational Topics



The UCR Subcommittee accepted the following topics for Information Only:

**UCR Issue #1** – UCR Status Report

- NIBRS Update
- Demonstration of CDE
- Demonstration of the UoF Portal

**UCR Issue #7** – The Federal Bureau of Investigation's UCR Quality Assurance Review to Resume Operations in Accordance with the CJIS Division, CJIS Audit Unit's Triennial Audit

**AdHoc Discussion** – Nomenclature of the NIBRS Sex Offenses for Publications, Technical Manuals, and Other Documents as Applicable

UNCLASSIFIED

27



# Uniform Crime Reporting Program (UCR) National Incident-Based Reporting System (NIBRS) Transition Status Update

**Amy C. Blasher**  
Unit Chief

Crime Statistics Management Unit (CSMU)  
Law Enforcement Support Section

## Crime Data Modernization



- One of eight Director's Priority Initiatives (DPI) to improve the nation's UCR statistics for reliability, accuracy, accessibility, and timeliness
- Achieved through the completion of a five-prong approach



# NIBRS Transition

On December 2, 2015, the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) approved the recommendation to sunset the Summary Reporting System (SRS) and replace it with NIBRS



“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 to develop a transition plan and timeline for conversion.”

3

# NIBRS Transition

- The FBI has partnered with the Bureau of Justice Statistics (BJS) to implement the National Crime Statistics Exchange (NCS-X)
  - The FBI is financially assisting with the transition of 400 agencies and state UCR programs
  - Funding is only available until **December 2018**
  - Fiscal Year 2018 solicitations are tentatively scheduled for:
    - December 2017
    - February 2018
    - April 2018
    - July 2018



4

# NIBRS Transition

- The FBI continues to engage stakeholders and establish initiative champions within stakeholder communities.
  - FBI UCR Program has established a Working Group to refine transition strategies and marketing for NIBRS
    - Refine the CJIS shared management approach using the Use of Force Task Force model
    - First meeting held November 16, 2017
  - FBI Special Agents in Charge (SAC)
    - Engage FBI SACs to promote NIBRS transition goals with local agencies in their areas of responsibility



5

# NIBRS Transition

- NIBRS Regional Training
- NIBRS Webpage  
<<https://ucr.fbi.gov/nibrs-overview>>
  - Features helpful resources including the technical specifications, user manual, and the NIBRS video
  - Provides quick links to the NIBRS publications
- NIBRS Video
  - Describes the UCR Program's history and importance of NIBRS for improving the overall quality of crime data
- Resources and tools to promote NIBRS education and awareness
  - Feature articles and success stories
  - "NIBRS: The Future of U.S. Crime Data," The Police Chief, October 2017
- Data integration specialists provide programmatic assistance regarding development and transition to XML
  - Code reviews
  - XML examples and gap analysis



- Subject matter support by email and phone:  
<[UCR-NIBRS@ic.fbi.gov](mailto:UCR-NIBRS@ic.fbi.gov)> or  
(304) 625-9999 (NIBRS Line)

6



# Questions?

Amy C. Blasher  
Chief

Crime Statistics Management Unit

FBI CJIS Division

Phone: 304-625-4840

E-mail: <[acblasher@fbi.gov](mailto:acblasher@fbi.gov)>



9



## **SEARCH, The National Consortium for Justice Information and Statistics**

**Becki Goggins**

Director, Law and Policy Program

**Criminal Justice Information Services (CJIS)  
Advisory Policy Board (APB)**

December 6-7, 2017



## **Law and Policy Program Update**



## Survey of State Criminal History Information Systems, 2016

- The 2016 survey is the 14<sup>th</sup> survey of criminal history information systems conducted by SEARCH for the Bureau of Justice Statistics (BJS)
- The survey provides a snapshot of **data, trends, improvements, and practices** spanning repository and particularly criminal history operations in each state
- Publication pending BJS approval

U.S. Department of Justice  
Office of Justice Programs

Bureau of Justice Statistics

### Survey of State Criminal History Information Systems

Criminal Justice Information Policy

## Quality Assurance Program (QAP)

- **Revised checklist to reflect the implementation of NGI and new Compact Council policies**
- **Version 2.0**
  - Alaska
  - Hawaii
  - Montana
  - New York\*
  - South Carolina

State Repository Quality Assurance Program  
– Program Guide  
– Program Checklist

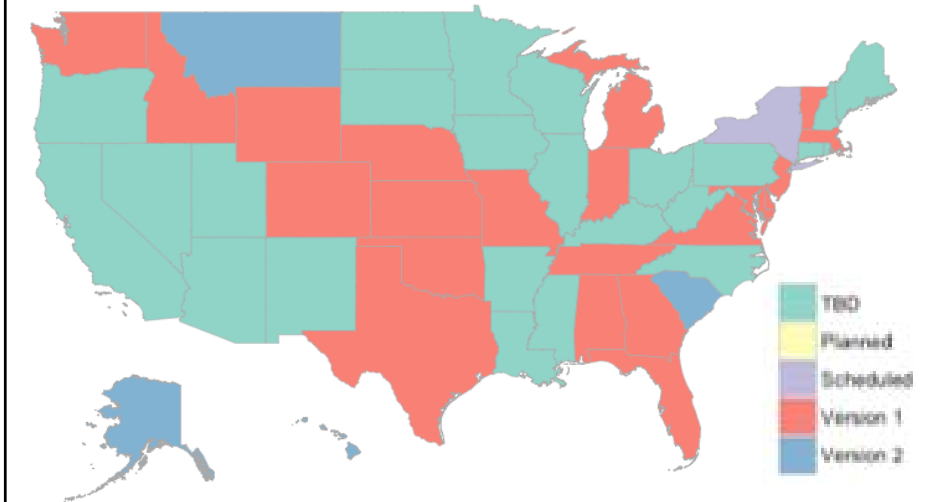
and

A Methodology for Determining Costs Associated with  
Noncriminal Justice Purpose Background Checks

Version 2 - February 2017

# QAP Participants

Status of State Efforts to Implement the Quality Assurance Checklist  
November 27, 2017



## State Progress in Record Reporting for Firearm-Related Background Checks

- Final publication in joint series between SEARCH and the National Center for State Courts
- Illegal Drug Use Records
  - Challenges
  - Success Stories
    - Connecticut
    - District of Columbia
    - Michigan

**State Progress in Record Reporting for Firearm-Related Background Checks: Unlawful Drug Users**  
By Benji Goggin, SEARCH, The National Consortium for Justice Information and Statistics and Shaina Strickland, National Center for State Courts | July 2017

**Introduction**

Under the Brady Handgun Violence Prevention Act of 1993 (Brady Act) as codified at 18 U.S.C. § 922(g)(2), being an unlawful user of or addicted to a controlled substance prohibits a person from receiving firearms.<sup>1</sup> The National Instant Criminal Background Check System (NICS) Improvement Amendments Act (NIAA) of 2007 defines “unlawful drug use” records as those that identify a person unlawfully using or addicted to a controlled substance, as demonstrated by specified arrests, convictions, and adjudications that are not protected from disclosure to the Attorney General by federal or state law.<sup>2</sup>

These include the following criminal history records that are typically available through the Interstate Identification Index (III):<sup>3</sup>

- Multiple arrests for use or possession of a controlled substance within the past 5 years if the most recent arrest occurred within the past year;
- Convictions for use or possession of a controlled substance within the past year (regardless of offense type);
- Certain convictions for possession of drug paraphernalia within the past year.

Unlawful drug use records may also be noncriminal history records, which can be made available through the NICS Index:<sup>4</sup>

- Persons who test positive for use of a controlled substance within the past year;
- Persons who admit to the use of a controlled substance within the past year.<sup>5</sup>

The NICS Index included nearly five times as many unlawful drug use entries in 2016 than it did in 2008, due to ongoing state and federal efforts to improve this category of records.

**Unlawful Drug Use Records in the NICS Index**

Year	Number of Records
12/2008	1,461
12/2016	22,611

0 5,000 10,000 15,000 20,000 25,000

More than 20 states have implemented laws to improve the accuracy of their background checking systems. SEARCH and the National Center for State Courts are working together to improve the accuracy of their background checking systems. SEARCH and the National Center for State Courts are working together to improve the accuracy of their background checking systems.

Many of these improvements are the result of funds awarded to states by the U.S. Department of Justice, Bureau of Justice Statistics (BJS) through the NICS Act Record Improvement Program (NARIP). This program administers the grant provisions of the NIAA that was signed into law on January 6, 2008, following the April 2007 shooting tragedy at Virginia Tech. The Virginia Tech shooter was able to purchase firearms from a Federal Firearms Licensee (FFL) because information about his prohibiting mental health history was not entered into the NICS Index. The NIAA is intended to address the gaps in information available to the NICS about prohibiting mental health adjudications, involuntary mental health commitments, and other prohibiting factors. BJS began awarding NARIP funds to states in 2008, and as of 2016, more than \$130 million in funding has been awarded to 27 states and one tribe.

While many of the records that are used to deny a firearms transfer based on unlawful drug use are available through III (i.e., arrests and convictions for controlled substance related crimes) noncriminal records are often missing. This information includes records for positive drug screens and persons’ admission of substance abuse. As of December 31, 2016, 26 states had no unlawful drug use entries in the NICS Index, which is where prohibiting noncriminal records should be included so they are available nationally for firearms related background checks.<sup>6</sup> Many other states had very few unlawful drug use records in the NICS Index.

**Footnotes:**

1. No one “intentionally” receives a drug or other substance, or receives possession, included in schedule I, II, III, IV, or V of part of 21 U.S.C. § 802.
2. 18 U.S.C. § 922(g)(2)(B)(i)(I).
3. 18 U.S.C. § 922(g)(2)(B)(i)(II).
4. 18 U.S.C. § 922(g)(2)(B)(i)(III).
5. 18 U.S.C. § 922(g)(2)(B)(i)(IV).
6. 18 U.S.C. § 922(g)(2)(B)(i)(V).

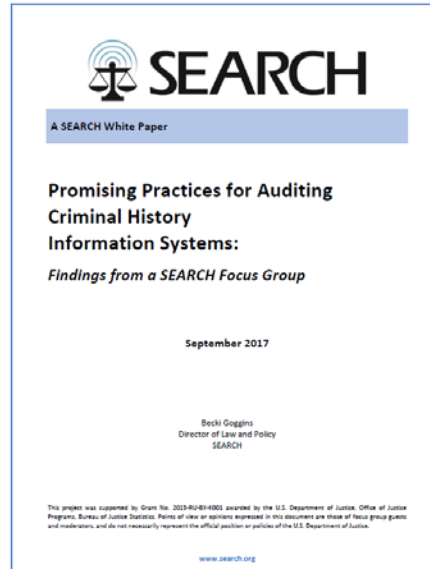
SEARCH NCSJ



## Findings from the SEARCH Focus Group on Criminal History Record Audits

### Promising practices

- Use of software to support quality assurance reviews
- Communication with contributing agencies regarding audit findings
- Publication of audit findings
- Ongoing outreach and training
- Stakeholder engagement



## Regional Multi-Disciplinary Meetings

- Facilitators – Federal Bureau of Investigation, BJS, National Center for State Courts and SEARCH
- Invitees – Law enforcement, courts, prosecutors, corrections, community supervision
- Topics
  - Disposition reporting
  - NICS prohibitors
  - National Criminal History Improvement Program (NCHP)
  - NICS Act Record Improvement Program (NARIP)

## Information Sharing Programs Update



### National Instant Criminal Background Check System (NICS) Technical Assistance

- SEARCH has funding from the Bureau of Justice Assistance to support technical assistance and development work in states seeking to increase the number of records available for firearms related background checks

## Computerized Criminal History (CCH) Analytics Proof Of Concept

- Not a “new” idea, but...
- Maine provided over 5 years of anonymized CCH data (January 1, 2012 – June 10, 2017)
- Measures/Metrics – arrests, disposition rate, re-arrest rate, average days to disposition
- Dimensions – dates, age, race, sex, agency, court, charge, disposition, etc.
- Operational and research capabilities

## Reasons to Use this Type of Tool

- **Anomaly detection**
  - Early problem identification
  - Potential data quality issues
- **Trend analysis**
  - Change in volume of arrests and dispositions
  - Changes in time elapsed between arrest and dispositions
- **Reporting**
  - Stakeholder reports
  - Funding requests

## Are there anomalies or trends in the data reported to the repository?

	2012	2013	2014	2015	2016	2017	
Parent Agency	Arrests	Arrests	Arrests	Arrests	Arrests	Arrests	
Belfast PD	96	181	213	195	208	82	
Calais PD	115	141	85	55	59	36	
Oakland PD	59	86	95	59	53	14	
Portland PD	1,653	2,208	1,876	1,669	1,719	669	

## Are we getting dispositions faster?

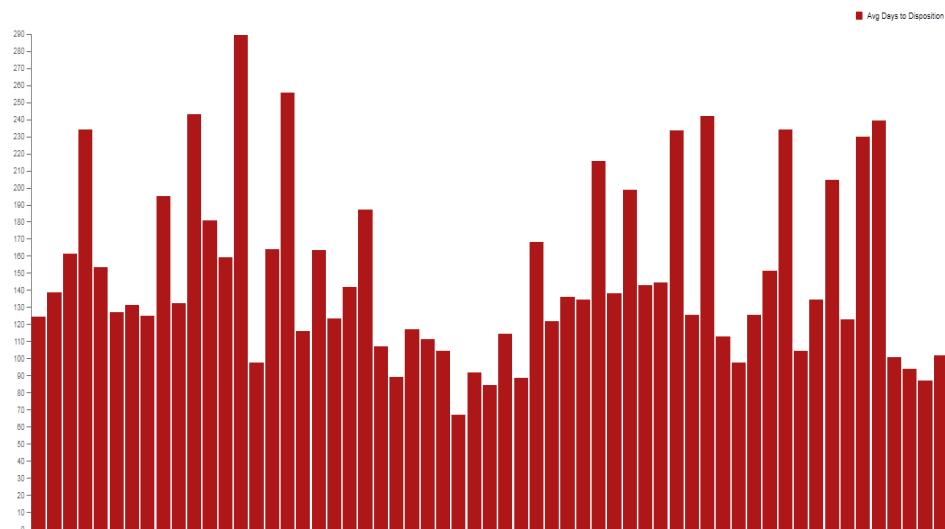
INFO: US:4 / / X 01 / U BUS

	2012	2013	2014	2015	2016	2017
Court	Avg Days to Disposition	Avg Days to Disposition	Avg Days to Disposition	Avg Days to Disposition	Avg Days to Disposition	Avg Days to Disposition
Biddeford District Court	68.21	90.36	112.03	170.44	494.33	568.75
Springvale District Court	72.08	106.03	123.03	189.46	516.96	540.30
York County Criminal Court		1.00		73.24	154.03	218.39
York County Superior Court - Alfred	112.43	172.29	224.83	273.70	575.86	1,019.50
York District Court	78.62	108.38	140.65	208.56	492.80	631.46
Bridgton District Court	68.63	88.63	115.38	174.05	353.10	524.20
Cumberland County Criminal Court	67.52	109.40	128.64	159.65	184.19	187.23
Cumberland County Superior Court - Portland			125.00			
Portland District Court	121.85	182.28	208.05	226.47	245.63	336.87
Androscoggin County Criminal Court				62.29	136.40	175.55
Androscoggin County Superior Court - Auburn	103.97	172.36	233.76	292.38	633.59	1,014.50
Farmington District Court	83.54	199.71	437.29	261.17	364.67	378.11
Franklin County Criminal Court		82.13	130.93	163.69	191.06	239.82
Franklin County Superior Court - Farmington	124.91	260.65	618.69	979.13	1,154.00	1,987.00
Lewiston District Court	66.22	92.53	89.16	131.38	449.72	331.94
Oxford County Criminal Court				61.83	156.97	229.11
Oxford County Superior Court - Paris	113.92	179.99	239.56	297.24	600.52	1,163.56
Rumford District Court	76.58	110.53	97.45	144.16	445.49	215.60
South Paris District Court	82.12	131.14	158.95	211.20	546.93	958.00
Augusta District Court	64.96	90.79	121.48	207.83	500.48	310.82

## What is the time between arrest and disposition by court region?

Region	Avg Days to Disposition
Region 1	169.16
Region 2	134.69
Region 3	153.04
Region 4	125.42
Region 5	110.38
Region 6	147.30
Region 7	141.59
Region 8	131.66

## Which courts average the longest time between arrest and disposition?



## Other Operational Questions

- How many arrests have dispositions? 129,575
- How many arrests are missing dispositions? 26,215

	2012	2013	2014	2015	2016	2017	None
Disposition Status	Arrests	Arrests	Arrests	Arrests	Arrests	Arrests	Arrests
Yes	18,301	27,454	27,391	23,358	23,405	9,614	
No							26,215

## Who gets arrested?

- **At what age are people arrested?**
  - Age Group – 20 – 24 years
  - Age – 21 years
- **Who gets arrested?**
  - Females – 45,459 (27%)
  - Males – 121,362 (73%)
  - Unknown – 67
- **Who gets re-arrested?**
  - Females – 45%
  - Males – 51%

## When do rearrests occur?

- **Within 6 months – 49,665**
- **Within 1 year – 13,342**
- **Within 2 years – 11,342**
- **> 2 years – 7,818**
- **Never\* – 84,825**

\* Not during time period covered by dataset.

## New Open Source Tools

- **National Crime Statistics Exchange (NCS-X) tools**
  - National Incident Based Reporting System (NIBRS) Pre-Certification Tool
  - XML input to Pre-Certification tool
  - NIBRS to summary conversion tool (coming soon!)
- **NIBRS analytics tool**

## NIBRS Pre-Certification Tool

- **Replicates validation process used by the FBI**
- **Features web-based drag and drop processing of NIBRS data files**
  - Currently supports flat-file submissions
  - SEARCH will build functionality to support XML submissions once the new IEPD is available
- **Tool is free and accessible at**  
<https://nibrs.search.org/nibrs-web/>



## Reasons to Use the Pre-Certification Tool

- **Allows agencies, state programs and industry partners to test NIBRS submissions prior to testing with FBI or state program**
- **Provides error reports similar to the FBI in a matter of seconds**
- **May speed certification process with the FBI**






## Pre-Cert Tool Limitations

- **Some rules require a comparison with pre-existing submissions**
  - Cannot check for updates
  - Cannot check for valid ORIs
  - Certain zero reports cannot be performed
- **Some rules are not being interpreted in the same way**
  - These differences will be resolved



## PCT Home Page

SEARCH

  
The National Incident-Based Reporting System  
(NIBRS) Pre-Certification Tool (Beta Version)

 Bureau of Justice Statistics  
U.S. Department of Justice

[Home](#) [Resources](#) [Tool Limitations](#) [Test Files](#) [About](#)

The NIBRS Pre-Certification Tool (PCT) provides law enforcement agencies, responsible for submitting Incident-Based Reports (IBR) data to State Uniform Crime Reporting (UCR) programs, the ability to test their submissions in advance of its formal delivery. State UCR programs may also use the NIBRS PCT to test their IBR submissions before beginning the NIBRS certification process with the FBI. The NIBRS PCT exercises the NIBRS data edit and validation rules and provides formatted output of errors, so that submitters may correct their data submissions and, ultimately, speed the FBI CJIS and/or state IBR certification process.

#### Important notes:

- The validation rules implemented by the NIBRS PCT only reflect the FBI's NIBRS rules and do not include state-specific data elements and rules. Likewise, the NIBRS PCT cannot validate some NIBRS rules specific to the submitting agency. See [Tool Limitations](#) for specific details.
- The NIBRS PCT is intended to assist the user in understanding how well its data aligns with the FBI NIBRS standard version 3.1. It is not intended to substitute for FBI NIBRS or State certification.

The NIBRS PCT is licensed under the open source Apache License, version 2.0. The source code is available [here](#).



Have questions? Ask SEARCH at [NIBRSPreCertToolHelp@search.org](mailto:NIBRSPreCertToolHelp@search.org)

## NIBRS Analytics Tool

- **Web-based analytics tool that uses Saiku business intelligence platform**
  - <https://nibrs.search.org/saiku-ui/>
- **Features easy drag-and-drop queries**
- **Supports advanced filtering**
- **Creates charts and graphs with a single click**
- **Allows queries to be saved**
- **Ingests standard NIBRS data**

## SEARCH Executive Director Update

- **On October 30, 2017, SEARCH Members confirmed David J. Roberts as the new SEARCH Executive Director**

## 2018 SEARCH Winter Membership Group Meeting

- **Tuesday, January 23 – Thursday, January 25, 2018**
- **Birmingham, Alabama**
- **Topics**
  - Government Affairs Update
  - Member Roundtable
  - FBI Rap Back
  - Criminal Justice Reform
  - And more!



**Thank You**

**Becki Goggins**

[becki@search.org](mailto:becki@search.org)

**334.201.3001**

© SEARCH, The National Consortium for Justice Information and Statistics | [search.org](http://search.org)



## SECURITY AND ACCESS SUBCOMMITTEE REPORT FALL 2017

Mr. Bradley Truitt, Chairman  
December 2017 CJIS APB Meeting  
Oklahoma City, Oklahoma



### SA Issue #1

*CJIS Security Policy Language Changes in  
Section 5.12*



***Purpose:***

To propose modifications to the *CJIS Security Policy* Section 5.12 to permit the vetting rules for personnel with access to criminal justice information to be applied consistently among criminal justice agency employees and contract personnel.



## SA Issue #1 Continued

### Available Options Considered



**Option 1:** Accept the following recommended changes within CJIS Security Policy Section 5.12 (item A) and Appendix J (B) as shown in the topic paper (additions in **red, bold italics**, deletions in ~~bold strikethrough~~).

**A. Proposed CJIS Security Policy Section 5.12 Language Changes:**

**5.12 Policy Area 12: Personnel Security**

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have **unescorted** access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

**Option 2:** Make no changes to the *CJIS Security Policy*.

3



## SA Issue #1 Continued



***Working Group Results:***

(5) Working Groups moved to endorse Option 1 as shown in the topic paper with Priority Tier 1.

***Subcommittee Motion:***

The SA Subcommittee moved to accept Option 1 as shown in the topic paper with Priority Tier 1.

4



## SA Issue #1 Continued

### Available Options Considered



#### **APB Motion:**

**Option 1:** Accept the following recommended changes within CJIS Security Policy Section 5.12 (item A) and Appendix J (B) as shown in the topic paper (additions in **red, bold italics**, deletions in ~~**bold strikethrough**~~).

#### **A. Proposed CJIS Security Policy Section 5.12 Language Changes:**

##### **5.12 Policy Area 12: Personnel Security**

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have **unescorted** access to unencrypted CJIS including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJIS.

**Priority Tier 1**

5



## SA Issue #2

**CJIS Security Policy Restriction for Criminal  
Justice Information Stored in Offshore  
Cloud Computing Facilities**



#### ***Purpose:***

The purpose of this topic was to propose language changes to *CJIS Security Policy* Section 5.10.1.5 to restrict where criminal justice information may be stored in cloud computing facilities.

6



## SA Issue #2 Continued

### Available Options Considered



**Option 1:** Accept the following recommended changes to CJIS Security Policy Section 5.10.1.5 and Appendix B as shown below (additions in **red, bold italics**, deletions in **bold strikethrough**).

- *The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).*

*Note: This restriction does not apply to exchanges of CJI with foreign criminal justice agencies under international exchange arrangements (i.e., the Preventing and Combatting Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).*

- **Proposed Additions to CJIS Security Policy Appendix B: Acronyms:**

Acronym	Term
<b>RCMP</b>	<b>Royal Canadian Mounted Police</b>

**Option 2:** Make no changes to the *CJIS Security Policy*.

7



## SA Issue #2 Continued



### **Working Group Results:**

(4 ) Working Groups moved to accept Option 1 as presented in the topic paper with Priority Tier 1.

(1) Working Group moved to accept Option 1 with amended language to replace “...foreign criminal justice agencies...” with “...foreign government agencies...”

8



## SA Issue #2 Continued



### **Subcommittee Motion:**

The SA Subcommittee moved to accept Option 1 with amended language to replace “foreign criminal justice agencies” with “foreign government agencies” with Priority Tier 1.

9



## SA Issue #2 Continued



**Option 1:** Accept the following recommended changes to CJIS Security Policy Section 5.10.1.5 and Appendix B as shown below (additions in **red, bold italics**, deletions in **bold strikethrough**).

- ***The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).***

***Note: This restriction does not apply to exchanges of CJI with foreign ~~criminal justice~~ government agencies under international exchange arrangements (i.e., the Preventing and Combatting Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).***

- **Proposed Additions to CJIS Security Policy Appendix B: Acronyms:**

Acronym	Term
<b><i>RCMP</i></b>	<b><i>Royal Canadian Mounted Police</i></b>

10





### SA Issue #3

Vetting of Non-U.S. Citizen Contractors/Vendors  
for Access to State Criminal Justice  
Information Systems



**Purpose:**

This topic paper was presented as information only to raise awareness of a new appendix to the *CJIS Security Policy* which provided information on suggested methods for vetting non-U.S. citizen contractors/vendors residing outside the United States or its territories who require access to state criminal justice information (CJI) systems.

Topic Canceled

11



### SA Issue #4 Cloud Task Force Update



**Topics of discussion:**

- Worked with the ISO Program to craft language for SA Issue #2. *CJIS Security Policy* Restriction for Criminal Justice Information Stored in Offshore Cloud Computing Facilities.
- Will discuss ideas to make the CSP easily understood and application to multiple 3<sup>rd</sup> party vendors.

**Subcommittee Action:**

Accepted for information only.

12



## SA Issue #4 Continued

### Mobile Task Force Update



#### **Topics of discussion:**

- Planning a meeting before the end of December.

#### ***Subcommittee Action:***

Accepted for information only.

13



## SA Issue #4 Continued

### Courts Task Force Update



#### **Topics of discussion:**

- Create use case scenarios for each chapter in Section 5.
- Do a risk assessment and identify potential mitigations to ensure criminal justice information is safeguarded.

#### ***Subcommittee Action:***

Accepted for information only.

14



## SA Issue #5

### Update on Fusion Center Access to CJIS Division Systems



#### ***Purpose:***

To provide an update regarding the CJIS Division's efforts to fulfill the CJIS Advisory Policy Board's (APB's) recommendations regarding fusion center access to CJIS Division systems.

The SA Subcommittee made a recommendation to the Identification Services Subcommittee Chair for Option 2.

15



## SA Issue #6

### Information Security Officer Symposium Review



#### ***Purpose:***

The purpose of this topic was to provide an update from the symposium held in Alexandria, VA, and to provide information regarding the next symposium in 2018.

#### ***Subcommittee Motion:***

Accepted for information only.

16



## AdHoc Discussion



**AdHoc Issue #1** – Use of the Regional Information Sharing System (RISS) and other Identity Data Providers

**Purpose:** Update on spring 2017 CJIS Action Item to provide information to the Subcommittee on the process for vetting Identity Data Providers.

**Subcommittee Recommendation:** Accepted for information only.

**AdHoc Issue #2** – FDLE Cloud Provider Audit Briefing

**Purpose:** The purpose of the topic was to provide an update on the results of the FDLE’s audit of cloud providers.

**Subcommittee Recommendation:** Accepted for information only.

17



## AdHoc Discussion



**AdHoc Issue #3** – FirstNet Discussion

**Purpose:** The purpose of this topic was to provide a briefing on the Los Angeles County Sheriff’s Department’s implementation of the FirstNet pilot.

**Subcommittee Recommendation:** Accepted for information only.

**AdHoc Issue #4** – LEEP Identity Management Discussion

**Purpose:** The purpose of this topic was to gather input regarding identity management at the federal, state, local, tribal and territorial level.

**FBI Action Item:** SA Subcommittee DFO will reach out to the members of the Subcommittee to elicit additional feedback regarding LEEP identity management.

18



## AdHoc Discussion



### **AdHoc Issue #5** – LEEP Enterprise Solution Discussion

**Purpose:** The purpose of this topic was to discuss non-criminal justice or private entities requesting access to CJIS Division services and how to differentiate those categories and those users from the information they should not be accessing.

**Subcommittee Recommendation:** Accepted for information only.

### **AdHoc Issue #6** – CAU Boundary Protection Discussion

**Purpose:** The purpose of the topic was to request guidance from the Subcommittee on how the CJIS Audit Unit assesses boundary protection.

**Subcommittee Recommendation:** Accepted for information only.

19



## Action Item



### **FBI Action Item:**

The CJIS ISO Program Office accepted an action item to explore the mobile applications taking the place of MDM compensating controls.

20

## CJIS APB Tribal Task Force

- ▶ William Denke, Chief of Police, Sycuan Tribal Police Department; Tribal Task Force Chair
- ▶ Francis E. Bradley, Chief of Police, Hualapai Nation Police Department
- ▶ Scott Desjaddon, Director, Yavapai Prescott Tribal Police Department
- ▶ Carlos Echevarria, Chief of Police, Tulalip Tribal Police Department
- ▶ Kathryn M. Monfreda, Chief, Alaska Department of Public Safety
- ▶ Dawn A. Peck, Manager, Idaho State Police
- ▶ Gene Thaxton, Director, Oklahoma Department of Public Safety
- ▶ Brian Wallace, Chief Civil Deputy, Marion County Sheriffs Office (OR)
- ▶ Jason O'Neal, Deputy Associate Director, Bureau of Indian Affairs
- ▶ Marcia Good, DOJ Office of Tribal Justice
- ▶ Donald W. Lee, FBI Indian Country Crimes Unit
- ▶ Christopher A. Nicholas, FBI Law Enforcement Support Section

UNCLASSIFIED

1

## What Are We Doing...

- ▶ NIBRS Conversion by January 2021
- ▶ National Use of Force Data Collection
- ▶ Reporting of Final Dispositions
- ▶ Disposition Reporting Guide

## Next step...

**January 2018 Teleconference**

UNCLASSIFIED

2

# CJIS Advisory Process Tribal Representatives

## Southern Working Group

Kendal Murphy  
Wyandotte Nation Police  
Department, Wyandotte OK  
<kmurphy@Wyandotte-nation-  
nsn.gov>  
918-678-6365

## Western Working Group

Scott Desjadon  
Yavapai Prescott Tribal Police  
Department, Prescott, AZ  
<sdesjadon@ypit.com>  
928-925-4581

## North Central Working Group

Gary Gaikowski  
Sisseton-Wahpeton Law  
Enforcement, Sisseton, SD  
<gaikowski@hotmail.com>  
605-698-7661

## Northeastern Working Group

Robert Bryant  
Penobscot Indian Nation Police  
Indian Island, ME  
<robert.bryant@penobscotnation.org>  
207-827-6336

## Federal Working Group

Jason O'Neal  
Bureau of Indian Affairs (BIA),  
Washington, DC  
<jason.oneal@bia.gov>  
918-221-1866

## Advisory Policy Board

William J. Denke  
Sycuan Tribal Police Department  
El Cajon, CA  
<bdenke@sycuan-nsn.gov>  
619-445-8710



UNCLASSIFIED

3

Tribal Task Force Chair  
William J. Denke  
<bdenke@Sycuan-nsn.gov>

CJIS Division Executive Management Tribal Liaison  
Law Enforcement Support Section  
Christopher A. Nicholas

CJIS Division Tribal Liaisons  
Kimberly K. Lough  
304-625-3855

Kristi A. Naternicola  
304-625-4701

<cjistribaloutreach@fbi.gov>



UNCLASSIFIED

4



**FBI Criminal Justice Information  
Services (CJIS) Division's  
National Instant Criminal Background  
Check System (NICS) Section**

Advisory Policy Board—December 2017

Robin A. Stark-Nutter  
Section Chief  
NICS Section

Unclassified//FOUO

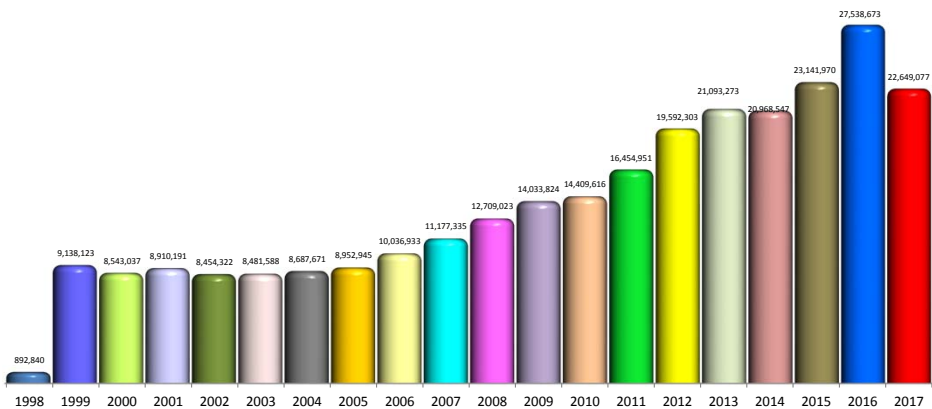


**Total NICS Background Checks**



Federal and State  
November 30, 1998 –November 30, 2017

Program-to-Date **275,866,242**



Unclassified//FOUO

2

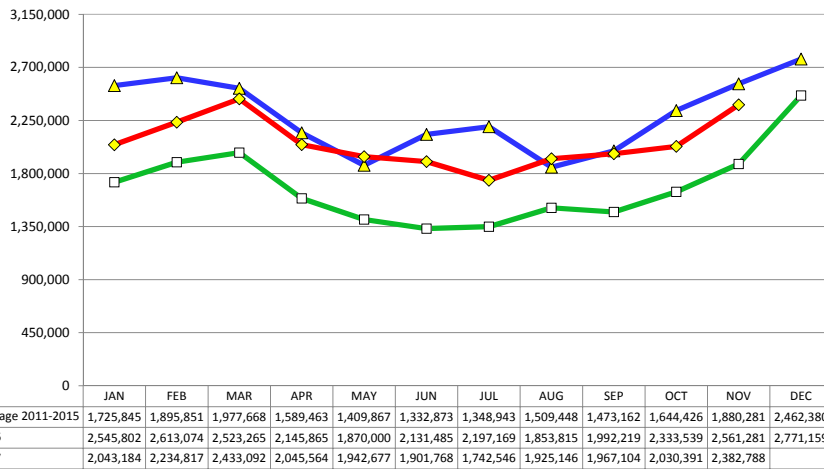




# Total NICS Background Checks



Federal and State  
November 30, 1998 – November 30, 2017

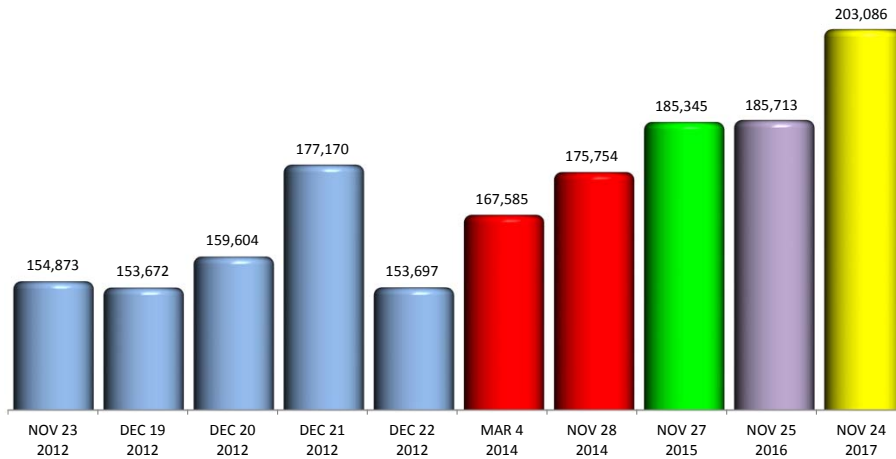


Unclassified//FOUO

3

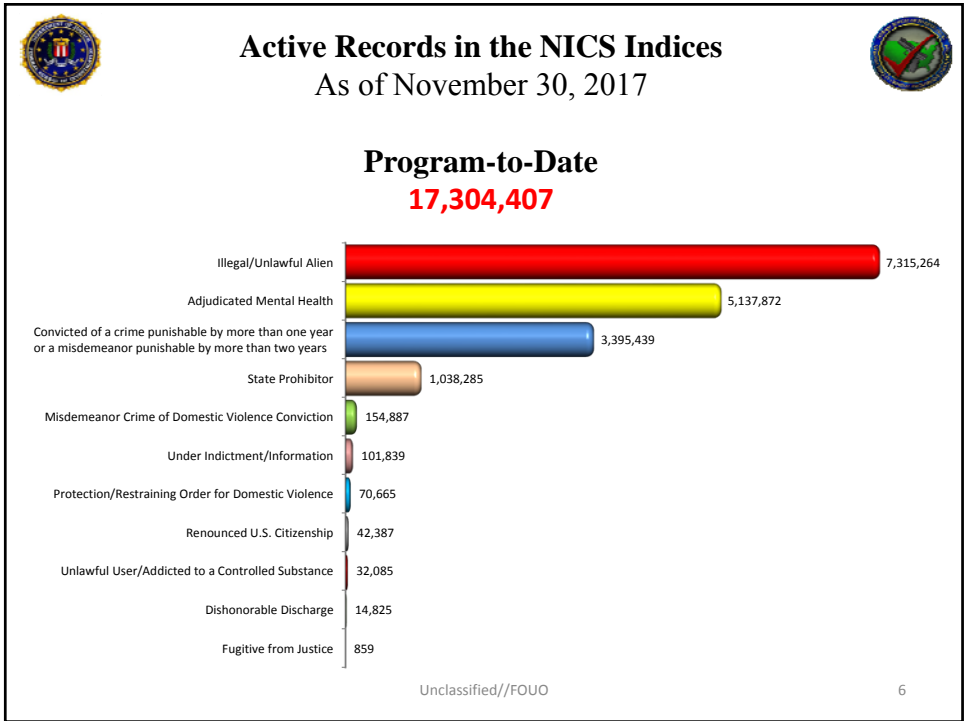
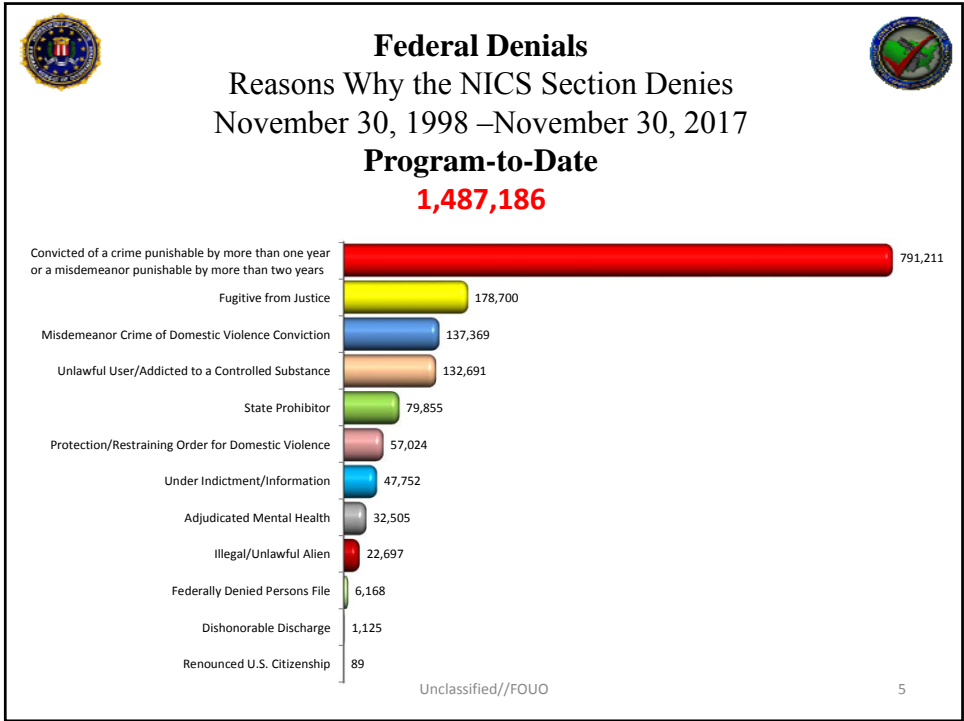


# Top 10 Highest Days November 30, 1998–November 30, 2017



Unclassified//FOUO

4





## NICS Section Backlogs

<b>NICS Indices Backlog:</b> <b>25,085</b>	<b>NICS Appeals Backlog:</b> <b>11,931</b>
<b>Explosives Backlog:</b> <b>22,372</b>	<b>Voluntary Appeal File Backlog:</b> <b>1,576</b>

Unclassified//FOUO

7



## Contact Information

FBI CJIS Division  
NICS Section  
E-mail: <[NICSLiaison@ic.fbi.gov](mailto:NICSLiaison@ic.fbi.gov)>

NICS Business Unit: 1-844-265-6716  
NICS Section Chief: Robin A. Stark-Nutter  
304-625-3500

Unclassified//FOUO

8



# Association of State Criminal Investigative Agencies

November 27, 2017

The Honorable Christopher A. Wray  
Director  
Federal Bureau of Investigation  
935 Pennsylvania Avenue, NW  
Washington, DC 20535-0001

Assistant Chief John Donohue  
Chair, Criminal Justice Information Services  
Advisory Policy Board  
Commanding Officer  
Intelligence Bureau  
New York City Police Department  
One Police Plaza  
New York, NY 10038

Dear FBI Director Wray and Assistant Chief Donohue:

On behalf of the membership of the Association of State Criminal Investigative Agencies (ASCIA), I am writing in support of efforts to address a current national security gap in information access and sharing that makes America vulnerable to terrorism and other violent criminal threats.

Currently, several of our nation's fusion centers are prohibited by Criminal Justice Information Services (CJIS) policy from accessing criminal history record information (CHRI) stored in the National Crime Information Center (NCIC). These fusion centers, as a part of the 79 federally recognized and governor-designated components of the National Network of Fusion Centers, operate as focal points for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, territorial, and private sector partners. Without access to CHRI, their ability to perform their required duties to support their fellow fusion centers, the FBI Joint Terrorism Task Force, the Terrorist Screening Center (TSC), and law enforcement partners is greatly diminished.

In May 2017, the Criminal Intelligence Coordinating Council (CICC), a group under the Global Justice Information Sharing Initiative (Global) that serves as a Federal Advisory Committee and advises the U.S. Attorney General on justice information sharing and integration issues, developed a white paper to address and mitigate this prohibition by identifying two overarching recommendations. The immediate access resolution was that the CJIS Advisory Policy Board (APB) authorize all fusion centers, including those that are not located within a criminal justice agency and that do not currently have access to CHRI, to enter into a memorandum of understanding (MOU) or a cooperative agreement with the state or local law enforcement agency that is involved at the fusion center.

The long-term policy resolution recommendation stated that 28 Code of Federal Regulations (CFR) Part 20 should be reevaluated to ensure that as the national security and criminal landscape changes, those entities, including fusion centers, operating in a criminal justice capacity are granted access to CHRI to ensure the safety and protection of the nation, including the detection of criminal activity. Specifically, the recommended change would focus on the addition of the words “prevention” and “criminal intelligence analysis” in section (b) of 28 CFR Part 20.3 and the addition of the words “initiative or program,” “criminal intelligence,” and “federally recognized state and major urban area-designated fusion centers, High Intensity Drug Trafficking Area-Investigative/Intelligence Support Centers, and Regional Information Sharing Systems’ Watch Centers” in section (g).

A version of the immediate access resolution was implemented as an interim solution (granting fusion centers access to CHRI through a management control agreement with a criminal justice agency); however, access issues remain, and there has been no resolution to the gap. In October 2017, the CJIS APB Identification Services (IS) Subcommittee met and discussed the issue, including proposed options to address the gap. The options presented do not address the long-term recommendation identified in the white paper but, rather, focus on a resolution similar to the immediate access recommendation.

The options presented by the CJIS APB IS Subcommittee serve only as a bandage, rather than addressing the problem of full access to CHRI by fusion centers as well as HIDTAs and RISS Watch Centers that represent our nation’s field-based information sharing entities; these options push the issue on to each field-based center to find an individual solution. All fusion centers perform the administration of criminal justice and allocate a substantial portion of their annual budget to the administration of criminal justice, including the detection of articulable or specified criminal or terrorist activity and, as such, should have access to CHRI. Further, fusion center personnel receive robust and extensive training on the security of classified information, the protection of personally identifiable information, and the protection of privacy, civil rights, and civil liberties.

As an example of this gap in operation, today each of the 79 fusion centers is mandated to support every request from the TSC for enhancing encounter information related to law enforcement, border crossing, and travel encounters of known or suspected terrorists (KSTs). The current CHRI data-access issue is inhibiting the National Network of Fusion Centers’ ability to gather all the data required to enhance KST encounters for the TSC. Fusion centers need criminal history data to develop a complete picture of individuals who pose the greatest threats to the communities they serve. Direct and full-file access to CHRI data via the NCIC is the only long-term option.

As a solution continues to be identified for fusion center access, we ask that the APB suspend the current IS Subcommittee proposal. We also request that CJIS and APB leadership meet as soon as possible with ASCIA, the National Governors Association, and other key law enforcement executives who represent most of America’s chiefs of police, sheriffs, and state law enforcement executives.

As the President of ASCIA, I have worked diligently with the associations that represent the major law enforcement organizations in America to find a resolution to the fusion center CHRI-access issue. The lack of progress to date requires my association and the other associations in America with members on the APB to reconsider the effectiveness of our representatives.

We appreciate our partnership with the FBI and look forward to addressing this issue with the members of the APB. The protection of our nation and the communities we serve requires state agencies operating criminal history information systems, fusion centers, and the FBI CJIS APB to work together to implement a recommendation that addresses the needs of fusion centers, HIDTAs, and RISS Watch Centers as they serve to detect and prevent criminal activity, including terrorist and mass-casualty threats.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark Gwyn". The signature is fluid and cursive, with the first name "Mark" and last name "Gwyn" clearly distinguishable.

Mark Gwyn  
*President – ASCIA*  
Director  
Tennessee Bureau of Investigation





November 27, 2017

Assistant Chief John Donohue  
Commanding Officer New York City Police Department  
Chair, CJIS Advisory Policy Board

Re: Criminal Justice Information Services (CJIS) data localization policy

Dear Chief Donohue,

The Computing Technology Industry Association (CompTIA) collectively represents vendors, innovators, and technology companies doing reputable and successful business in the criminal justice system.

It has come to our attention that the CJIS Advisory Policy Board (APB) is considering a new policy that would restrict the physical location of criminal justice information to the boundaries of the United States and Canada. We urge CJIS to consult with stakeholders, including CompTIA and its members before moving forward with this decision.

Data localization will not improve security outcomes and limits access to the latest cloud-based security innovations introduced to the commercial sector. Second, such a policy sends the wrong message to other countries that use data localization measures to discriminate against U.S. companies that provide leading technology and restrict market access by U.S. cloud computing companies.

First, CompTIA hopes that the CJIS Advisory Policy Board will consider other measures to improve security outcomes. Security solutions must protect networks, systems and data with continuous visibility, monitoring, detection and response. Deviating from best practices for the safety and security of cloud-based data storage, including redundant geographic storage of data and the usage of distributed security solutions, such as sharding and obfuscation, may undermine the security of U.S. criminal justice data.

Second, contract holders that provide secure and timely storage of CJIS data, as well as companies that aspire to hold such contracts, are often multi-national firms that deliver affordable yet secure services. Companies source and operate globally in order to offer products and services that are competitive in the market and of the best value to the customer. Enshrining a localization requirement into policy limits the flexibility that cloud services may be able to provide to the customer. Moreover, they serve as an excuse for other countries to adopt similar policies for protectionist, not security ends.



In August of 2017, the U.S. Trade Commission recognized that according to industry analysts, data localization rules that require data storage, management, and/or processing to occur in a single country are a major impediment for firms engaged in digital trade, because they prevent firms from taking advantage of the cost, speed, and security advantages offered by the distributed nature of cloud-based technologies. The ITC also found that “Location independence is a core aspect of the cloud delivery model. Policies that require providers to locate facilities in a given location may leave them with the choice of selecting a suboptimal location or not serving the target market at all.”

We would welcome a discussion on the points mentioned above before the APB makes any recommendations on this new policy. We look forward to working with you on this matter. You may contact me at [ehyman@comptia.org](mailto:ehyman@comptia.org) or 202-503-3621.

Sincerely,

A handwritten signature in blue ink, appearing to read "Elizabeth A. Hyman".

Elizabeth A. Hyman  
Executive Vice President, Public Advocacy  
CompTIA

## CJIS APB Minutes - Acronyms Listing

AD	Assistant Director
AFIS	Automated Fingerprint Identification System
AG	Attorney General
A-NFF	Alternate National Fingerprint File
APB	Advisory Policy Board
ASCIA	Association of State Criminal Investigative Agencies
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BJIS	Bureau of Justice Statistics
Brady Act	National Handgun Violence Prevention Act of 1993
BRAG	Biometric Risk Assessment Group
BSS	Biometric Services Section
C <sup>2</sup>	Community Connector
CAD	Computer Aided Design
CAR	Criminal Answer Required
CAU	CJIS Audit Unit
CBP	Customs and Border Protection
CCH	Computerized Criminal History
CDE	Crime Data Explorer
CDM	Crime Data Modernization
CE	Compliance Evaluation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CODIS	Combined DNA Index System
COMP	Compact Membership Program
Compact	National Crime Prevention and Privacy Compact
Council	National Crime Prevention and Privacy Compact Council
CSA	CJIS Systems Agency
CSO	CJIS System Officer
CSP	CJIS Security Policy
DAD	Deputy Assistant Director
DEA	Drug Enforcement Administration
DFO	Designated Federal Officer
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DNA	Deoxyribonucleic Acid
DOB	Date of Birth
DOF	Disposition of Firearms

DOI	Department of Interior
DOJ	Department of Justice
DPI	Director Priority Initiative
DQ	Driver's License Query
DTF	Disposition Task Force
EAD	Executive Assistant Director
EDDIE	EAGLE Directed Identification Environment
EPIC	El Paso Intelligence Center
ERO	Enforcement and Removal Operations
EXP	Date of Expiration
FBI	Federal Bureau of Investigation
FDLE	Florida Department of Law Enforcement
FISWG	Facial Identification Scientific Working Group
FY	Fiscal Year
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
ICAM	Integrated Computer Aided Manufacturing
ICD	Interface Control Document
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IFFS	Identification for Firearm Sales
III	Interstate Identification Index
INA	Immigration and Nationality Act
IPS	Interstate Photo System
IQ	CHRI Identity Query
IS	Identification Services
ISCG	Identification Services Coordination Group
ISO	Information Security Officer
IT	Information Technology
JD	Judicial District
LEEP	Law Enforcement Enterprise Portal
LENS	Law Enforcement Notification System
LEOKA	Law Enforcement Officer Killed and Assaulted
LinX	Law Enforcement Information Exchange
LEXS-SR	Logical Entity eXchange Specifications-Search and Retrieve
LTE	Long Term Evolution
MCA	Management Control Agreement
MFISs	Manual Fingerprint Identification Systems
MOU	Memorandum of Understanding
MQ	MQ series
N3G	NCIC Third Generation
NARIP	NICS Act Record Improvement Program
NCHIP	National Criminal History Improvement Program
NCIC	National Crime Information Center

NCSC	National Center for State Courts
NCS-x	National Crime Statistics Exchange
N-DEx	National Data Exchange
NDTF	NICS Denied Transaction File
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
NIEF	National Identity Exchange Federation
NIEM	National Information Exchange Model
Nlets	International Justice and Public Safety Network
NOPU	NCIC Operations and Policy Unit
NSO	Nonserious Offense
NSOR	National Sex Offender Registry
OCA	Originating Case Number
OGC	Office of General Counsel
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PAL	Public Access Line
PIA	Privacy Impact Statement
PO	Program Office
POC	Point of Contact
PPI	Pixels Per Inch
QAP	Quality Assurance Program
QW	NCIC Wanted Person
RAND	Random Access to Nlets Data
RDNA	Rapid Deoxyribonucleic Acid
RISC	Repository of Individuals of Special Concern
RISS	Regional Information Sharing
RQ	Registration Query
SA	Security and Access
SAC	Special Agent in Charge
SAML	Security Assertion Markup Language
S & P	Standards and Policy
S.C.An	Serial Crime Analysis
SEARCH	National Consortium for Justice Information and Statistics
SIB	State Identification Bureau
SID	State Identification Number
SIM	Subscriber Identity Module
SORN	Systems of Records Notification
STB	Science and Technology Branch
SWQ	State Warrant Query
TOU	Technical and Operational Updates

TTF	Tribal Task Force
TXDPS	Texas Department of Public Safety
UCR	Uniform Crime Reporting
UoF	Use of Force
USMS	U.S. Marshals Service
VIN	Vehicle Identification Number
XML	Extensible Markup Language