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

Minutes

Criminal Justice Information Services

Advisory Policy Board

December 4-5, 2019

Atlanta, Georgia

For Official Use Only

Intentionally Left Blank

Criminal Justice Information Services

Advisory Policy Board

March 3, 2020

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 4-5, 2019 Criminal Justice Information Services Advisory Policy Board meeting held in Atlanta, Georgia.

Sincerely yours,

Mr. Michael C. Lesko
Texas Department of Public Safety
Chairman, CJIS APB

Intentionally Left Blank

Criminal Justice Information Services (CJIS)
Advisory Policy Board
December 4-5, 2019
Atlanta, Georgia

Table of Contents

APPENDICES INDEX

Appendix Q	Item #14 Association of State Uniform Crime Reporting Programs (ASUCRP) Update
Appendix R	Item #15 Use of Force (UoF) Task Force Update
Appendix S	Item #16 CJIS Shared Management Progression
Appendix T	Item #17a APB Significant Achievements – Mr. Joseph P. Bonino
Appendix U	Item #17b APB Significant Achievements – Mr. David Gavin’s Letter
Appendix V	Item #17c APB Significant Achievements – Mr. William Casey
Appendix W	Item #17d APB Significant Achievements – Mr. William Casey
Appendix X	Item #17e APB Significant Achievements – Mr. Paul Heffner
Appendix Y	Item #17f APB Significant Achievements – Colonel Steve Cumoletti
Appendix Z	Item #17g APB Significant Achievements – Mr. Tom Turner
Appendix AA	Item #17h APB Significant Achievements – Mr. Jack Donohue
Appendix BB	Item #17i APB Significant Achievements – Mr. Dave Loesch’s Letter
Appendix CC	Item #18 Chairman’s Report on the Security and Access (SA) Subcommittee
Appendix DD	Item #20 Chairman’s Report on the NICS Subcommittee
Appendix EE	Item #21 Rapid DNA Update

Intentionally Left Blank

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

December 4-5, 2019
Atlanta, Georgia

Meeting Report

Mr. Michael C. Lesko, Texas Department of Public Safety (TXDPS) and the Federal Bureau of Investigation's (FBI's) CJIS APB Chair, called the meeting to order at 9:10 a.m., December 4, 2018, at the Marriott Marquis, Atlanta, Georgia.

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

Mr. Michael C. Lesko, TXDPS and CJIS APB Chair

Mr. Michael D. DeLeon, Assistant Director (AD), FBI, CJIS Division, Clarksburg, WV

Mr. Brian Wallace, Marion County Sheriff's Office, and CJIS APB First Vice Chair

Mr. Charles I. Schaeffer, Florida Department of Law Enforcement (FDLE), and CJIS APB Second Vice Chair

Ms. Kimberly J. Del Greco, Deputy Assistant Director (DAD), FBI, CJIS Division, Clarksburg, WV

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

Mr. Megna turned the meeting over to Mr. Lesko, who introduced new APB members:

Mr. Michael M. Brown, National Sheriffs' Association

Major Brandon Gray, New Jersey State Police

Mr. Maury Mitchell, Alabama Law Enforcement Agency (not in attendance)

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

Mr. Lesko noted appreciation to the vendors who sponsored breaks for the meeting. Gallery attendees then introduced themselves. ***(See Appendix B for a complete meeting attendee list.)***

Mr. Lesko introduced special guests, Mr. Oliver Rich, Assistant Special Agent in Charge, Atlanta Field Office, FBI; Deputy Chief, Mr. Scott Kreher, Atlanta Police Department; and Sheriff Ted Jackson, Atlanta Sheriff's Office, all who provided opening remarks.

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

APB ITEM #1 Executive Briefings

This agenda item was presented by Mr. DeLeon. ***(See Appendix E, PowerPoint)*** He relayed best wishes from Executive Assistant Director Piehota who was unable to attend. Mr. DeLeon mentioned seeing familiar faces from recent meetings, International Association of Chiefs of Police (IACP), Major City Chiefs (MCC), and the Association of State Criminal Investigative Agencies. He said these meetings were productive, collaborative meetings in which they exchanged great dialogue.

Mr. DeLeon aknowledged CJIS senior staff in attendance, DAD Ms. Kim Del Greco; Information Technology Management Section Chief, Mr. Brian Griffith; Global Law Enforcement Services Section Chief, Mr. Scott Rago; and Biometric Services Section (BSS) Chief, Mr. Bill McKinsey. Mr. DeLeon recognized the CJIS APB's 25th Anniversary. He shared that Director Wray was unable to attend but sent his greetings in a letter, which he then read. Director Wray congratulated the APB on the 25th Anniversary. He noted this milestone was yet another example of the strength of partnership working together to address pressing policy matters affecting communities across the country. He recognized the APB's recommendations have improved national services like National Crime Information Center (NCIC) checks, Fingerprint Identification, and Uniform Crime Reporting (UCR) for federal, state, local, and tribal partners. He thanked the group for their dedication and continued success and partnership.

Mr. DeLeon recognized the current and past leadership of the CJIS APB. There have been seven DFO's appointed by the FBI's Directors to facilitate the process. There were five in attendance; Mr. Nick Megna, Mr. Scott Trent, Mr. Mike McIntyre, Mr. Roy Weise, and Mr. Don Johnson. Mr. Dave Loesch and Mr. Demory Bishop were unable to attend. Mr. DeLeon recognized former CJIS APB chairs beginning in 1994. Seven were in attendance; Mr. Mike Lesko, Mr. Jack Donohue, Captain Tom Turner, Colonel Steve Cumoletti, Mr. Paul Heppner, Mr. William Casey and Mr. Joseph Bonino. Mr. David Gavin and Mr. Frank Sleeter were not able to attend.

Mr. DeLeon highlighted the Peace Tree Ceremony hosted at The CJIS Division on September 25, 2019. It was held in conjunction with the APB's Tribal Task Force (TTF) Meeting. A White Pine Tree was dedicated on the CJIS Division campus to commemorate the partnership with the Tribal Law Enforcement Community and serve as a reminder of the vital role tribal agencies have in supporting public safety.

Mr. DeLeon then provided an update on the CJIS systems. He began with the NCIC. An average of 10.9 million transactions a day were processed in FY19, with a response time of

1/100 of a second per transaction. From the NCIC perspective, they have been monitoring the growing interest around Extreme Risk Protection Orders (ERPOs). He spoke on the effort to modernize the current NCIC system with the NCIC 3rd Generation Project (N3G). An early deliverable of the N3G effort was the National Information Exchange Model (NIEM), and the base Extensible Markup Language (XML). It is available for testing in the operational environment. He expressed they have not observed much active testing and encouraged members to test. The NCIC is in the final stages of conducting market research to find a vendor to build the name search solution. One of the requests from the NCIC user canvas was to provide a more robust and accurate name search capability within the NCIC system.

The National Instant Criminal Background Check System (NICS) continued to see high volumes of transactions. The last five years have been the highest in volumes, with 2019 reaching a new record high of 27.48 million. It is speculated that the events of this year, San Francisco, Dayton, and El Paso, could be driving these increased transactions. Federal NICS staff denied more than 101,000 transactions in 2019. This does not include denials issued by the point-of-contact (POC) states that process their own NICS transactions. The number of federal transactions received via E-Check was 6.6 million. This accounts for approximately 80 percent of federal transactions. This has increased by 22 percent since 2015, making it a more efficient method benefiting both the FBI and NICS users.

Mr. DeLeon provided an update on Next Generation Identification (NGI). The CJIS Division processed more than 69 million fingerprints in FY19. In addition, they continue to grow and improve the facial recognition capabilities vital to providing investigative leads. He emphasized facial recognition was for investigative leads and not identification. The FBI received and tested the new face algorithm in October 2019 and on November 17, 2019; they were able to upgrade the new algorithm ahead of schedule. The enhancement increases accuracy from the previous 88.2 percent to the current 99.2 percent.

The National Data Exchange System (N-DEx), continues to provide a great venue to share incident information and other records. Two hundred additional criminal justice agencies began contributing to N-DEx in FY19. This increased the total number of contributors to more than 7,400 agencies. In 2019, N-DEx provided access to nearly 829 million records and users performed nearly 17 million searches.

The Law Enforcement Enterprise Portal (LEEP) continued to transform the way users access the system and its features. In 2019, LEEP added eight new services bringing the total to fifty-three. LEEP began the transition of its Special Interest Groups to the enhanced JusticeConnect application. JusticeConnect is a real-time collaboration and communication tool for criminal justice offering the ability to conduct business instantly and securely. The LEEP's Virtual Command Centers (VCC) continued to be vital to law enforcement investigations and event management. The top five uses for the VCC are operation centers for daily logs and activity tracking; event security for rallies and parades; arrest and warrant operations; investigations,; and sporting events.

Mr. DeLeon discussed a big priority for CJIS with two key initiatives in the UCR Program. They are the National Incident-Based Reporting System (NIBRS) and the National

Use of Force (UoF) Data Collection. The transition to NIBRS is slated for January 1, 2021. Approximately 7,000 law enforcement agencies have submitted NIBRS data to the UCR program dating back to 2017. There has been 4,500 additional agencies identified with their commitment to the transition to the NIBRS by the 2021 deadline. At the request of law enforcement partners, the FBI established the UoF Data Collection. This voluntary collection gathers law enforcement use of force incidents resulting in death, serious bodily injury of a person, or the discharge of a firearm in or at the direction of a person. The official launch of the National UoF Data Collection was January 1, 2019. There are currently 28.65 percent of the nation's non-federal law enforcement officers participating and releasing data to this collection; 27 federal agencies, including the FBI, are participating. Once states reach the 40 percent participation rate, the FBI will be able to publish the UoF data.

The National Threat Operation Center (NTOC) has fully transitioned from a tip line to a full-fledged operation center with expanded infrastructure. In FY19, the NTOC received more than 540,000 complaint calls and more than 727,000 E-tips. More than 74,000 leads have been submitted to FBI field offices. A video was shared with attendees. Mr. DeLeon explained that calls are received from countries such as Pakistan, Indonesia, and India and NTOC is obligated to reach back out to legal attaches and divisions who oversee foreign missions.

In closing, Mr. DeLeon thanked the CJIS APB for all they do to keep the nation, citizens, and communities safe. He noted, joint efforts equal great partnerships and usually produce positive results.

Mr. Klimavicz, provided an update on DOJ initiatives. He said he was honored to be speaking to the CJIS APB. He felt it was a great way to learn about new initiatives, discuss common challenges, share best practices and gain insights into how the department can better support law enforcement.

Mr. Klimavicz briefed on work with CJIS and law enforcement to continuously improve operations, data access, and security. Previously, he had spoken about DOJ's modernization strategy, which is based upon a desire to move to architecture that gives rapid elasticity and scale without constraint. It is a consumption-based service that provides flexibility to spending and managing the budget, broad network access to support mobility and access, and faster deployment of changes. They made an important step to make this architecture a reality when they awarded a contract for a NCIC access services. This contract, when fully deployed, will deliver a solution that requires no installation, local software and maintenance and software configuration will be handled remotely with zero footprint. Any agency can configure the application to their needs on any authorized device or network. This will save money from a deployment perspective and annual maintenance costs.

Next, they will work to replace their interface to the NGI so they can provide access to hundreds of different customers beyond just the DOJ. Mr. Klimavicz thought it was important to consider how they are managing data and how they are sharing information and usage. He highlighted an ongoing success with the Tribal Access Program (TAP). It was established in late 2015, to provide access to NCIC for both civil and criminal purposes and allows information to be shared with federal, state, local and tribal agencies. TAP allows tribes to serve and protect their nations' citizens more effectively by enabling exchange of critical data across national information systems. The TAP has been entering information into federal databases. They have entered 1,500 sex offender entries into the National Sex Offender Registry (NSOR); 400 entries to prohibit the purchase of a firearm, 1,300 orders of protection, and 8,800 fingerprint-based record checks for non-criminal justice purposes such as employment, travel, housing, personnel, and regular contact with children.

Mr. Klimavicz closed saying they would continue to improve on the responsible sharing of law enforcement information with components of their local, state, federal, tribal, and international partners.

APB ITEM #2 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 F, PowerPoint.)*** He reported the NCIC Subcommittee met on October 09, 2019. The subcommittee addressed eleven topics, with ten recommendations consolidated into five separate motions to present to the CJIS APB. Four topics were accepted for information only.

Mr. Neverman covered the information only topics first. They included the LEEP Status Report, the N3G Task Force update, the N3G Project recommendation update, and the NCIC Status Report.

He briefed the NCIC Issue # 5, Race Code Standardization across CJIS Systems, would be presented separately as APB Item # 4.

NCIC Issue # 1 was originally presented in the spring of 2019. Based on discussions, it was recommended proposed language be developed and returned to the CJIS APB process. The specific language and messages were included in the topic papers.

There were two options presented. Option 1 was to refine the wanted notification as indicated by the working groups ensuring the intent of the messages were clearly stated. Option 2 was to provide additional messages or suggest new messages. The working groups went with Option 1 and provided additional comments. The Identification Services (IS) Subcommittee reviewed the topic and weighed in with suggestions.

Regarding Section I: The NCIC Subcommittee endorsed the recommendation received from the IS Subcommittee to include the addition of the Universal Control Number (UCN), with a priority of 3M. The IS Subcommittee endorsed the recommendation of the Western Working Group, which was to accept the wanted notifications as indicated by the working groups, and outlined in the topic paper, Section I, options D, E, F, and accept the second proposed option which contained the action required language. Additionally under Section I, option G was to modify the language to the action required, your wanted notice X contains a UCN that has been deleted, please remove the UCN from your entity and replace if appropriate.

Regarding Section II: The NCIC Subcommittee endorsed the recommendation of the IS Subcommittee, with the addition of the UCN with a priority 3M. The IS Subcommittee endorsed the recommendation of the Northeastern Working Group, which was to adopt Option 1, refine the wanted notifications as indicated by the working groups ensuring the intent of the messages are clearly stated, recommended adding the UCN to all notifications, and using III instead of spelling out the Interstate Identification Index.

Regarding Section III: The NCIC Subcommittee endorsed the recommendation of the Northeastern Working group to adopt Option 1, refine the wanted notification as indicated by the working groups ensuring the intent of the messages is clearly stated. They recommended adding the UCN to all notifications and use III instead of spelling out Interstate Identification Index.

The APB made the following recommendations:

Regarding Section I - Automated Notifications during the Want Entry Process

APB MOTION: The CJIS APB moved to endorse the recommendation of the IS Subcommittee which agreed with the Western Working Group's recommendation, with the addition of the UCN with a priority of 3M to include the following:

Accept the proposed wanted notifications as indicated by the Working Groups for Options A, B, and C as outlined in the paper. For Section I, Options D, E, and F: Accept the 2nd proposed option which contains "Action Required".

Additionally for Section I, Option G, modify to "ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

Revised messages noting changes are listed below. Additions are noted in red text, deletions noted by strikethrough:

A. This message provides notification that the date of birth and the date of warrant in the wanted entry are the same.

Current automated message:
DATE OF BIRTH CONTAINED IN WANTED NOTICE IS THE SAME AS DATE OF WARRANT. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO REFLECT THE CORRECT INFORMATION TO UPDATE SUBJECT'S, XXXXXXXXX, CRIMINAL HISTORY RECORD.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE ENTERED DATE OF WARRANT AND DATE OF BIRTH ARE THE SAME. PLEASE REVIEW AND CORRECT THE MISENTERED FIELD.

B. This message provides notification that the UCN in the wanted entry is incorrect.

Current automated message:

PLEASE BE ADVISED UCN: XXXXXXXXX REFLECTED IN YOUR NCIC WANTED PERSON ENTRY, XXXXXXXXX, IS INCORRECT. PLEASE MODIFY YOUR NCIC ENTRY APPROPRIATELY.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE UCN, XXXXXXX, IN YOUR WANTED NOTICE IS INVALID. PLEASE DELETE THE NUMBER AND REPLACE, IF APPROPRIATE.

C. This message provides notification that the UCN entered in the wanted notice is invalid or doesn’t meet the biographic matching criteria; however, a potential match has been identified (fuzzy match).

Current automated message:
PLEASE BE ADVISED UCN: XXXXXXXXX REFLECTED IN YOUR NCIC WANTED PERSON ENTRY, XXXXXXXXX, IS INCORRECT. THE CORRECT UCN FOR YOUR WANTED SUBJECT MAY BE UCN XXXXXXXXX. PLEASE MODIFY YOUR NCIC ENTRY APPROPRIATELY. FOLLOWING COMPLIANCE WITH THIS REQUEST, THE SUBJECT’S IDENTITY HISTORY RECORD WILL BE UPDATED.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXX. THE UCN, XXXXXXX, IN YOUR WANTED NOTICE IS INVALID OR INCORRECT. THE CORRECT UCN MAY BE UCN XXXXXX. PLEASE DELETE THE CURRENT UCN AND REPLACE, IF APPROPRIATE.

D. Existing Deceased Notification - This message provides notification that the UCN entered in the wanted notice has been previously confirmed as deceased by fingerprints.

Current automated message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN VERIFIED AS DECEASED BY FINGERPRINTS. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO REMOVE THE FBI NUMBER TO UPDATE SUBJECT’S CRIMINAL HISTORY RECORD.
Note: Current message does not indicate the submitter of the information.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN, XXXXXXX, THAT HAS BEEN CONFIRMED DECEASED BY FINGERPRINTS. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

E. Existing Expunged Notification - This message provides notification that the UCN entered in the wanted notice is expunged.

Current automated message:
FBI NUMBER, XXXXXXXXX, CONTAINED IN WANTED NOTICE HAS BEEN EXPUNGED. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO CORRECT OR

REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN, XXXXXXX, THAT HAS BEEN PREVIOUSLY EXPUNGED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

F. Existing Consolidation Notification - This message provides notification that the UCN contained in the wanted entry was previously consolidated.

Current automated message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN CONSOLIDATED WITH XXXXXXXXX.   PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO CORRECT OR REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS UCN XXXXXXX. DUE TO A CONSOLIDATION THAT UCN HAS BEEN REPLACED WITH UCN XXXXXXX. PLEASE UPDATE THE UCN IN YOUR ENTRY TO XXXXXXX.

G. Existing Deleted Notifications - This message provides notification that UCN entered in the wanted notice was previously deleted due to a processing discrepancy.

Current automated message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN DELETED. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO CORRECT OR REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN, XXXXXXX, THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE. ~~A SEPARATE UCN MAY BE ADDED IF ANOTHER IDENTITY HISTORY RECORD IS IDENTIFIED.~~

Regarding Section II - Automated Subsequent Activity Notifications

APB MOTION: The CJIS APB moved to endorse the recommendation of the IS Subcommittee with a priority of 3M as follows:

To endorse the recommendation of the Northeastern Working Group to adopt Option 1: Refine the wanted notifications outlined in the proposed messages ensuring the intent of each message is clearly stated. Also recommend adding the UCN to all notifications and use III instead of spelling out Interstate Identification Index.

See below for the proposed automated messages:

A. **Existing Current Print Ident (CPI) and Criminal Ten-Print Notification - This message provides notification that a current criminal transaction or a NFF state has processed a current print with an identification to the UCN contained in the wanted entry.**

Current automated message:
ON YYYY/MM/DD, A FINGERPRINT CARD WAS IDENTIFIED WITH XXXXXXXXXXX, FBI/XXXXXXXXX BY XXXXXXXXXXXX (ORI/XXXXXXXXX), XXXXXXXXXXXX. OUR RECORD INDICATES YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX. FOLLOW-UP ACTION BY YOU WITH THE ARRESTING AGENCY MAY BE APPROPRIATE. CLEAR OR CANCEL YOUR NCIC RECORD WHEN SUBJECT IS NO LONGER WANTED. FBI CJIS DIVISION, CLARKSBURG, WV

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A FINGERPRINT CARD, DOA XXXX/XX/XX, FROM XXXXXXXX, WAS IDENTIFIED WITH UCN, XXXXXXX. THIS UCN IS CONTAINED IN YOUR WANTED NOTICE. SUBJECT'S IDENTIFICATION RECORD INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE III ~~INTERSTATE IDENTIFICATION INDEX~~. CONTACT THE ARRESTING AGENCY FOR MORE INFORMATION. IF THE SUBJECT IS NO LONGER WANTED, PLEASE CANCEL OR CLEAR THE NCIC ENTRY.

B. **Existing Civil Identification - This message provides notification that a non-criminal justice fingerprint card was idented to the UCN contained in the wanted notice.**

Current automated message:
ON XXXX/XX/XX, A CIVIL FINGERPRINT CARD WAS IDENTED TO FBI UCN XXXXXXX BY XXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC XXXXXXX).

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A CIVIL FINGERPRINT CARD FROM XXXXXXX WAS IDENTED TO UCN XXXXXXX CONTAINED IN YOUR WANTED NOTICE. PLEASE CONTACT THE AGENCY FOR MORE INFORMATION.

Section III - Manual Messages for Review

APB MOTION: The CJIS APB moved to endorse the recommendation of the Northeastern Working Group with a priority of 3M as follows:

To adopt Option 1: Refine the wanted notifications as indicated by the Working Groups, which are outlined in the following current and proposed messages ensuring the intent of each message is clearly stated. Also recommend adding the UCN to all notifications and use III instead of spelling out Interstate Identification Index.

A. **Consolidation Notification - This message provides notification that CJIS has taken action to consolidate two or more identity history records. The consolidation can be requested from a submitter or identified by internal CJIS processes. There are two different scenarios.**
    1. **The first is when the UCN in your want is retained as the primary identifier of the record.**

Current manual message:
ON XXXX/XX/XX, UCN XXXXXXX WAS CONSOLIDATED INTO UCN XXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC/XXXXXXX)

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE UCN, XXXXXXX, IN YOUR WANT WAS PART OF A CONSOLIDATION OF IDENTITY HISTORY RECORDS. ADDITIONAL DATA MAY BE AVAILABLE ON YOUR SUBJECTS RECORD IN THE III ~~INTERSTATE IDENTIFICATION INDEX~~. PLEASE REVIEW THE RECORD FOR MORE INFORMATION.

2. **The second is when the UCN in your want is *not* retained as the primary identifier of the record.**

Current manual message:
ON XXXX/XX/XX, UCN XXXXX WAS CONSOLIDATED INTO UCN XXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC/XXXXXXX) REFLECTING THE INACTIVE UCN/XXXXXXX. PLEASE REVIEW THE RECORD AND MODIFY YOUR NCIC ENTRY TO APPROPRIATELY REFLECT THE ACTIVE UCN/XXXXX.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXXX. UCN XXXXXX CONTAINED IN YOUR WANTED NOTICE HAS BEEN CONSOLIDATED INTO RETAINED UCN XXXXXXX. PLEASE MODIFY THE UCN IN YOUR WANT TO REFLECT THE RETAINED UCN. ALSO, ADDITIONAL DETAILS MAY BE AVAILABLE ON YOUR SUBJECT IN THE III ~~INTERSTATE IDENTIFICATION INDEX~~.

B. **Deceased Notification - This message is intended to provide notification that CJIS has received a fingerprint submission indicating the subject is deceased (DEK – known deceased submission) or a III message or hard copy documentation has been submitted indicating the state deceased the record based on biometric comparison (FII message).**

Current manual message:
ON XXXX/XX/XX, DECEASED INFORMATION WAS UPDATED TO UCN XXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC/XXXXXXX).

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. DECEASED INFORMATION WAS UPDATED TO UCN XXXXXXX CONTAINED IN YOUR WANTED NOTICE.

C. Disposition Notification - This message is intended to provide notification that a disposition has been added to an event on the identity history record indicated in the UCN in the wanted entry.

Current manual message:
ON XXXX/XX/XX, A DISPOSITION WAS UPDATED TO DOA XXXX/XX/XX, UCN/XXXXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING RECENT UPDATE IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A DISPOSITION WAS UPDATED TO DOA XXXX/XX/XX, UCN XXXXXXX. UPDATED IDENTITY HISTORY RECORD IS AVAILABLE VIA THE III ~~INTERSTATE IDENTIFICATION INDEX~~.

D. Probation/Supervision Notification - This message is intended to provide notification that a term of probation or supervised release has been added to the identity history record.

Current manual message:
ON XXXX/XX/XX, PROBATION/SUPERVISION WAS UPDATED TO DOA XXXX/XX/XX, UCN/XXXXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING RECENT UPDATE IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A SUPERVISED RELEASE OR PROBATION TERM HAS BEEN UPDATED TO UCN XXXXXXX BY AGENCY XXXXXXX. UPDATED IDENTIFICATION RECORD IS AVAILABLE VIA THE III ~~INTERSTATE IDENTIFICATION INDEX~~.

E. Modification to Name or Date of Birth Notification - This message is intended to provide notification that the master name or date of birth has been modified on the associated identity history record.

Current manual message:
ON XXXX/XX/XX, A NAME OR DATE OF BIRTH MODIFICATION WAS MADE TO

UCN/XXXXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING RECENT UPDATE IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX CONTAINS UCN XXXXXXX. THE CJIS DIVISION HAS MODIFIED THE NAME OR DATE OF BIRTH ASSOCIATED WITH THAT IDENTITY. PLEASE CONFIRM THE UCN IS STILL A MATCH FOR YOUR SUBJECT. IF SO, NO ACTION REQUIRED. IF NOT, REMOVE OR REPLACE THE UCN.

F. Last Criminal Event Expungement Notification - This message is intended to provide notification that the last criminal event has been expunged from the associated identity.

Current manual message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN EXPUNGED. THE IDENTITY WILL REMAIN ON FILE FOR REFERENCE PURPOSES ONLY UNTIL YOUR WANT IS CANCELLED.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE LAST CRIMINAL EVENT HAS BEEN EXPUNGED. THE UCN, XXXXXXX, WILL REMAIN ACTIVE FOR REFERENCE PURPOSES ONLY UNTIL YOUR WANT IS CANCELLED.

NCIC Issue # 4 was the Intra-Agency Sharing of NSOR Audit reports, findings, and accompanying documentation with the DOJ, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART) Office.

The SMART Office was mandated to assist jurisdictions in implementing the Sex Offender Registration Notification Act (SORNA). There are currently 18 states, four territories, and 134 American Indian and Alaska native tribes that have implemented SORNA. The SMART Office was mandated to assess whether a jurisdiction has implemented and continues to implement SORNA. By working with the CJIS Audit Unit (CAU) and the CJIS Systems Agency, it would eliminate the need for a second audit as well as eliminating any contradictory findings.

The NCIC Subcommittee determined it was prudent to have a Memorandum of Understanding (MOU) to cover safeguards with information sharing. Additionally, there would be traceability for future reference as to any decisions made regarding information sharing. It was proclaimed that the current audit process would not be modified or changed, and the information would be provided to the SMART Office as CJIS prepares it.

APB MOTION: The CJIS APB moved to endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required Sex Offender Registration and

Notification Act data fields with the USDOJ SMART office through the implementation of a Memorandum of Understanding that addresses the use and secondary dissemination of the data.

NCIC Issue No. 8 was the Inclusion of the Blue Alert Data in NCIC. This was a recommendation resulting from the N3G User Canvas. The data set is similar to the AMBER Alert that provides notification to law enforcement and to the public.

This request was submitted for changes to the current NCIC environment for the felony vehicle, wanted person, violent person, and the missing person files. The concept is that when a blue alert is placed as the first characters in the miscellaneous field, a caveat will generate a warning to the receiver.

The NCIC Subcommittee agreed with the working groups and endorsed Option 1 for both issues.

<u>Issue #1 Blue Alert Caveat</u>

<u>APB MOTION:</u> The CJIS APB moved to accept Option 1: Enable the use of "Blue Alert" as the first characters of the Miscellaneous field in the felony Vehicle, Wanted Person, Violent Person, and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. This should be a priority of 3H.

<u>Issue #2 APB Recommendation to DOJ Community Oriented Policing Services (COPS)</u>

<u>APB MOTION:</u> The CJIS APB moved to accept Option 1: Recommend that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

NCIC Issue No. 11 discussed the NICS Denied Transaction File (NDTF). This topic was presented in the fall of 2018, however it was not presented to the NCIC subcommittee at that time. With the new agile development methodology, resources are focused on prioritization. The topic was presented to the NCIC Subcommittee to determine the importance of the change in relation to other items that have been prioritized as part of the N3G project.

The NCIC Subcommittee moved to support the previously approved recommendations by the NICS Subcommittee regarding the NDTF dissemination caveat and the notification protocol with a priority of 3M.

APB Item #2 Chairman's Report on the NCIC Subcommittee, NCIC Issue #11 NDTF Dissemination Caveat and Notification Protocol Prioritization Request

(Note: This recommendation was previously approved by the Director as part of the December 2018 CJIS APB Recommendation Package. However, with the new agile methodology, resources are focused on prioritization. Subsequently, this topic was presented to the NCIC Subcommittee to determine the importance of this change in relation to other items that have been prioritized as part of the N3G Project.)

APB MOTION: The CJIS APB moved to endorse the previously approved recommendations by the NICS Subcommittee regarding the NDTF dissemination caveat and notification protocol with a priority of 3M.

Those recommendations were as follows:

Amend the Positive Hit Response caveat within the NDTF to include the following language, "DISSEMINATION OF SUPPLEMENTARY INFORMATION BY THE DENYING AGENCY MAY BE LIMITED UNDER STATE OR FEDERAL LAW."

Terminate the Delayed Inquiry Hit Notifications and Delayed Inquiry Hit Response Notifications when due to hits within the NDTF.

NCIC Issue No. 9 was a Request to Expand the NCIC Protection Order File Criteria to allow entry of the ERPOs. The topic was presented to the working groups as an information only topic. The NCIC Subcommittee was asked to provide any comments, suggestions, and feedback relating to the potential entry. The Subcommittee received an update related to a legal opinion that would potentially allow entry of the ERPOs in NCIC. They took action based on the assumption that a legal opinion to allow entry of the ERPOs into the NCIC would be forthcoming. Mr. Neverman allowed Mr. Todd Commodore, FBI, CJIS Division to give an update on the legal information received.

Mr. Commodore provided an update on the legal guidance received from the Office of General Counsel. He explained that ERPOs or red flag laws are civil orders where family members, or in some cases law enforcement, can petition courts to restrict an individual from purchasing or possessing a firearm. The CJIS Division Audit Unit, during their NCIC audits, discovered ERPOs during their data quality review. After discussion with General Counsel, they determined there was no authority for entry into NCIC.

The State of Maryland made a request to enter ERPOs into NCIC to have a national conversation, recognizing that it is critical to officer and public safety to have this information available. Mr. Commodore said they began with an information only topic paper in the working groups. As a work around, there was authority to enter this information into the NICS indices until they could explore if there was any legal action taken or any national authority underwent at least by Congress to allow the entry of ERPOs into NCIC. The working groups were emphatic that they look at these and do something quickly. Based on that, the Office of General Counsel was able to formalize their guidance so that the criteria for entry into NCIC would be based on the petitioner and type of court. Seventeen states have enacted ERPO legislation, all of them allow law enforcement to be the petitioner. The best answer to this issue would be national legislation. Several different drafts of legislation have been reviewed and the more recent ones have included provisions to allow entry into NCIC.

Discussion: The Chairman expressed his gratitude to CJIS staff and the NCIC Subcommittee for turning this around so quickly. A member asked for clarity, if it is a law enforcement petitioner, any court, it can be entered. If it is a non-law enforcement petitioner in a non-criminal justice court, it cannot be entered. Mr. Commodore replied that was correct. There are four different scenarios: 1) Criminal Justice petitioner in a criminal justice court, authorized 2) Noncriminal justice petitioner in a criminal justice court, authorized 3) Criminal Justice petitioner in a noncriminal justice court, authorized 4) noncriminal justice petitioner in a noncriminal justice court, not authorized.

APB MOTION 1: The CJIS APB moved to endorse the creation of a new NCIC file specifically for the entry of ERPOs with a priority of 3H.

APB MOTION 2: The CJIS APB moved to endorse the entry of all authorized ERPOs into the newly created NCIC file.

ACTION ITEM: The CJIS APB recommended the Chair of the APB draft a letter to the major law enforcement associations (IACP, MCC, NSA, etc.) encouraging endorsement of legislation and/or an Attorney General mandate that will authorize entry of all ERPOs (including, but not limited to, those issues by civil, military, federal, and state courts) into the NCIC system.

APB ITEM #3 N3G Task Force Update

Mr. Wyatt Pettengill, North Carolina State Bureau of Investigation, and Chair of the N3G Task Force provided this update.

Mr. Pettengill began his update by reminding the group that the NCIC is a mission critical system touching all members at some level. It has been nineteen years since the NCIC was updated. The N3G Task Force was established to provide guidance on modernizing the NCIC. He introduced the N3G Task Force members: Mr. Bill Guy, Rhode Island: Mr. Bob Sage, Kansas; Mr. Brad Truitt, Tennessee; Mr. Brian Wallace, Oregon; Mr. Chuck Murphy, Florida; Mr. Frank Minice, Nlets; Mr. Jeff Wallin, Vermont; Ms. Jennifer Armstrong, U.S. Marshals Service;
Mr. Joe Lapetina, Pennsylvania; Ms. Michelle Farris, Texas; Mr. Rick Wyffels, Minnesota; and Mr. Ted DeRosa, Colorado. Mr. Pettengill recognized CJIS Staff and their outstanding job in assisting the task force: Mr. Todd Commodore, Ms. Buffy Bonafield, Ms. Stephanie Manson, Mr. Zack Hartzell, Mr. Brian Nichols, Mr. Adam Epler, Ms. Joyce Wilkerson, and Ms. Valerie Evanoff.

Mr. Pettengill briefed that the task force began evaluating almost 2,000 functional requirements gathered from a stakeholders canvass. They assessed these functional requirements from a law enforcement perspective and sent those for further review. That task has been completed and several topics required further detail. Policy groups were created to take a deeper dive into some of these topics. The task force has held two meetings since the June 2019 CJIS APB Meeting. During those meetings, time was spent discussing updates and recommendations from the policy groups. There are five active policy groups: Warrant, Missing and Unidentified, Offline Search, Image Group, and the XML Group. Four policy groups have concluded; Blue Alert, Message Key, Supplemental and Gang.

APB ITEM #4 Race Code Standardization across CJIS Division Systems

This agenda item was presented by Mr. Todd Commodore, FBI, CJIS Division. **(*See Appendix G, PowerPoint.*)**

Mr. Commodore began by explaining this topic was an action item to both the NCIC and IS Subcommittees. Both subcommittees took action and recommended that this topic be presented separately. The primary issue was to standardize race codes across the CJIS Division systems. Currently, there are two sets of race codes being used. The NCIC, III and NGI use one set of codes and the NICS, N-DEx, and UCR use a different list of codes.

During the N3G user canvass, there were numerous requests to expand fields, change codes, etc. This was contained in Concept 9 of the N3G concepts, which included the biggest number of functional requirements. While reviewing this concept, the CJIS APB recommended the CJIS Division consider harmonization across their systems. The Director approved the recommendation. It was decided this was a significant effort that would not be accomplished in one topic paper. Mr. Commodore advised they are looking at each process and bringing them forward separately.

The state of Washington requested that the NCIC include a new race code. The NCIC, III, and the NGI are using a five-race code structure: A for Asian, B for African American, I for Native American or Alaskan Native, U for unknown and W for White. The NICS, UCR, and N-DEx capture all the same codes plus they capture race code P for Pacific Islander. This was a breakout from the Asian Category.

In 1997, the Office of Management and Budget issued a directive to separate the Pacific Islander, race code P, from Asian. After reviewing the guidance, the CJIS Division Executive Management asked for a variance for the NGI, the III, and the NCIC as these were not statistical systems. Mr. Commodore discussed the percentage of records that capture race codes A and P. All the systems capture race code A and that accounts for less than two percent. For the three systems that capture race code P it accounts for less than one percent.

Another consideration was how the race codes impact searches. The NCIC, filters between White and African American. If a search is conducted on white, it returns all codes except African American. If a search is conducted on African American, it returns all codes except white. The III contributes to the likeness score and the NGI is a biometric search that does not consider race during its fingerprint searches.

Additionally, this would be a table change for CJIS and a system change for the states. All fingerprint capture devices would have to capture the race code P. During the NCIC audits, race code is considered a critical field, which means they score and assess it. The CJIS Division would not be able to perform data remediation for the agencies.

The Federal, North Central, and Southern Working Groups chose Option 1, to bring consistency to the three systems and felt it was important to be specific on indicating an individual’s race. The Northeast and Western Working Groups opted for no change. They felt it was a significant programming effort to the local, state, and federal agencies and based on the number of potential subjects impacted versus the programming effort, it was too small. The NCIC and IS Subcommittees agreed with the Northeast and Western Working Groups.

Mr. Charlie Schaeffer, IS Subcommittee Chair, added that they discussed this topic at length. He said the fact the west, who has the greatest population of Hawaiians and Pacific Islanders, voted “no change” influenced their decision to vote the same.

APB MOTION: The CJIS APB moved to accept Option 2: No change.

APB ITEM #5 Nlets, The International Justice and Public Safety Network Update

Mr. Charlie Schaeffer, FDLE, and President of Nlets, provided an update. **(*See Appendix H, PowerPoint.*)**

Mr. Schaeffer provided background information on Nlets. For those who were not familiar, Nlets is the International Justice Public Safety Network. The CJIS APB shares information vertically with local, state, tribal, and federal law enforcement. In comparison, Nlets is more of a horizontal sharing between state and federal partners. Nlets is not directly involved with the locals. Nlets is a 501 (c) (3) not-for-profit corporation owned by the states and territories. It has been around for many years helping to share information. Many of the same people who serve on the Advisory Process and Compact Council are representatives of Nlets. They represent the states and federal partners who share information. Nlets is in a transition stage with Mr. Steve Correll retiring and Mr. Frank Minice selected to take his place.

Mr. Schaeffer noted he wanted to provide a different spin on his presentation and present information the CJIS APB may not be aware of. Nlets shares information among the states and internationally. Nlets will allow you to access Canadian Police Information Centre (CPIC) in Canada, INTERPOL, Mexico, and the Customs and Border Patrol. Their biggest customer is the Customs and Border Patrol. They search Nlets for tens of thousands of vehicle license plates crossing our borders.

New things are happening at the Nlets. They are able to search the stolen vehicle file from Mexico noting it works similar to the NCIC Stolen Vehicles File. There is a message key and a stolen vehicle query that can be sent to country code MX for Mexico. They have partners who are not government but government friendly. One of those partners is the National Insurance Crime Bureau (NICB**).** They have the ability to search the NICB for lien record information. Also, if a vehicle has a fancy lock and it cannot be accessed, you may query NICB for the key code to unlock the vehicle without breaking the glass.

There was international engagement with Australia and New Zealand to discuss information sharing. They were interested in the standard way of information sharing and noted they have been trusted partners with Canada for years. They did a follow-up trip in summer of 2019; their partners from Immigration and Customs Enforcement (ICE) manually shared information that was interesting to Australia and New Zealand. Mr. Schaeffer gave an example of a wanted person in the United States applying for a visa to enter into Australia through a third party country. Currently, Australia has to process it through an attaché who calls the State Department through a manual process. They demonstrated that within one week, 34 wanted people were granted access to their country. The next step, Phase II, will be to connect through Nlets, process an Illegal Alien Query (IAQ) and receive an Immigration Alien Response (IAR) that will provide the immigration status of a subject. This is something ICE wants to explore doing.

Another engagement they are working with ICE on is called Biometric International Query Service. It is a service that allows the Department of Homeland Security (DHS) to search an international biometric repository, send a transaction to one of our foreign partners, and receive a return response. This will be accomplished through the Nlets portal. An initiative has been funded by DHS and is in the pilot phase. When it becomes operational, the next logical phase would be to allow not just federal partners, but state partners' share that information.

Mr. Schaeffer shared some websites to find out more about Nlets. They have a wiki that explains how to build transactions. The main website conveys a marketing and business perspective, and Ngage is similar to LEEP. Ngage is a portal that can be logged into for secure communications with partners to discuss information sharing from a horizontal perspective.

Recently approved was the ability for Nlets to assign an Nlets Originating Agency Identifier (ORI). The fire community, who falls under the public safety umbrella, request to receive notifications from alarm companies. They are looking at how to construct a fire only ORI, which will enable sharing of the alarm company information.

Mr. Schaeffer concluded by providing his contact information and offering to answer any questions.

APB ITEM #6 Chairman's Report on the National Data Exchange (N-DEx) Subcommittee

Ms. Donna Uzzell, FDLE and Chair of the N-DEx Subcommittee, provided an update on the N-DEx Subcommittee. **(*See Appendix I, PowerPoint.*)**

Ms. Uzzell began by sharing background information on the N-DEx Subcommittee. The subcommittee was created as an answer to the 9/11 commission which called for better information sharing among local, state, and federal criminal justice agencies. The idea was to provide a more complete picture of the person, place, or thing investigated. In 2008-2009, it gained momentum. It was for law enforcement information only. There were 480 agencies, 65 million records, and 36 monthly users. They began a partnership with LInX and received the endorsement of the Major Chiefs and Sheriffs Association. The FBI began entering their own data and created a Use Code J for Criminal Justice Employment checks. INTERPOL data was entered and batch searches began. In 2014-2015, the DHS allowed access to their information. She noted, there are many great things planned for 2020.

Ms. Uzzell spoke on system participation. In 2019, N-DEX added two hundred agencies, three Department of Corrections, two Tribal Agencies and three of the top 100 law enforcement agencies, Oklahoma City Police Department, Colorado Springs, and Denver. There are over 37 million searchable records. The three state Department of Corrections added were Wyoming, New Mexico, and Missouri. Ms. Uzzell wanted to highlight the part N-DEx played in Operation Safe Summer. She encouraged others to look at N-DEx as a good source when trying to locate missing children. Ms. Uzzell encouraged those who work with sex offender files or corrections for persons who have absconded to work with the batch query process.

Ms. Uzzell then briefed on the following topics:

N-DEx Issue #1 N-DEX Program Status, User Assessment results were discussed. There were 1,400 criminal justice respondents in all 50 states and dozens of federal agencies. Eighty-five percent received a tangible benefit, including improvement of quality or quantity of information. The users offered suggestions to increase photo submission and to improve contact information on records. They were to re-examine the N-DEx policies of advanced permission and verification. The user assessment respondents have consistently voiced concerns with advanced permission and verification. The N-DEx system users indicated these policies were a deterrent to the timely use of system information. One-third of them offered some level of affirmative agreement to the statement, the N-DEx system policy for data use rules, specifically the need to both verify a record and receive permission to use the record from a record owning agency making it difficult to use N-DEx system information at all for their criminal justice needs. Twenty percent of respondents indicated it was difficult to reach the record owning agency based on the provided point of contact information. Further, not only has there been growing diversity in the primary roles of system users over the last few years, but traditionally investigative use of the system has been augmented by agency needs for data to support expanded analytical capabilities, time sensitive tactical or field activities, criminal justice suitability determinations, and continuous monitoring of supervision of high risk populations. The rules of engagement just have not kept up with the local agency needs.

APB MOTION: The CJIS APB moved to accept Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to “advanced permissions” and expanding the verification policy, as appropriate.

Revision No. 2 was to incorporate policy changes into the N-DEx policy and operating manual to clarify conditions under which preauthorized use of the N-DEx system information is permitted. The first thing was to remove the authorized pre-permission use policy and make it authorized use. The second thing was to expand the authorized use in the N-DEx policy to include relevant examples reflecting the current N-DEx system use cases. The best way would be to use cases and leave the language as broad as possible to give guidance. The main thing is not to take action until you validate it. They will add a plain language caveat to the authorized use policy to cover enforcement action and suitability determinations based on the N-DEx system information.

Discussion: A member asked Ms. Uzzell if she was speaking of suitability determination as in noncriminal justice placement of children. Ms. Uzzell answered this applied to suitability determinations such as employment suitability for criminal justice only.

Another member asked if it was going to be an administrative change to the policy document that would not return through the process. Ms. Uzzell advised it would come back through the process. Concepts will be done first and then returned through the spring 2020 round. There was discussion if this should be an action item and not a recommendation. The group agreed that Revisions 2 and 3 would be action items.

ACTION ITEM: The FBI will incorporate the changes for Revisions 2 and 3 and bring this topic back to the process in spring 2020.

Revision 2

Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of the N-DEx System information is permitted.

Revisions

- Remove *pre-permission* from *Authorized Pre-Permission Use* policy and make it *Authorized Use.*
- Expand authorized use paragraph in N-DEx Policy to include relevant examples reflecting current N-DEx System use cases, such as fusion center bulletins, threat assessments, and tactical situations.
- Add "plain language" caveat to authorized use policy to cover enforcement action and suitability determinations based on N-DEx System information.

Revision 3

Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the N-DEx policy (1.3.13**). ~~to remove the direct reference to exigent circumstances.~~**

The N-DEx Data Sharing Task Force update was discussed next. In the spring of 2019 this topic was presented as an ad hoc discussion to the N-DEx subcommittee. As the data contributors have grown, the application of the numerous data sharing rules and exceptions within the N-DEx system has become increasingly challenging. The subcommittee created a task force to review the complexity of the issues. Alan Peto, Las Vegas Metro Police Department was named the chair and Carol Gibbs from Illinois CJIS Systems office and N-DEx Committee member was named as the vice chair. The task force looked at all the various options within N-DEx and discovered so many exceptions that were developed to entice agencies to join. The task force reviewed in-depth analysis and made several recommendations. We want to return this because there are many changes to the policy language, changes to how agencies would share and what would be the basis for not sharing. The idea is to get as many agencies sharing with one another. So the subcommittee endorses the task force recommendation with the caveat of the N-DEx system is a national information sharing system where participating agencies are encouraged to share data with all approved criminal justice agencies, and with the understanding an agency may need to restrict in accordance with their laws.

ACTION ITEM: The FBI will present a topic paper at the spring 2020 round of meetings to address the N-DEx Subcommittee's recommended caveat as noted below:

The initial statement should read, “The N-DEx System is a national information sharing system where participating agencies ~~**should**~~ ***are encouraged*** to share data with all approved criminal justice agencies with the understanding an agency may need to restrict in accordance with laws, regulations, and policies.”

APB ITEM #7 Chairman’s Report on the (IS) Subcommittee

Mr. Charlie Schaeffer, FDLE and Chair of the IS Subcommittee presented this topic. ***(See Appendix J, PowerPoint.)***

Mr. Schaeffer began by thanking Mr. Joey Hixenbaugh and Ms. Brandy Meighan, FBI, CJIS Division for supporting the IS Subcommittee. Mr. Schaeffer first briefed on some of the information topics discussed at the IS Subcommittee and then addressed the action topics.

IS Issue #1 Miscellaneous Action Items Update

Extensive work has been done in the automation of disposition forms and the FBI continues to look at this for National Fingerprint File (NFF) states as well. Also discussed was searching the Criminal Master File (CMF) with a Repository of Individuals of Special Concern (RISC) transaction. RISC is a subset of the actual CMF. He noted only 2.5 to 3 million people are searched, when there are 70 - 80 million criminals in the CMF that RISC does not search. A study is being conducted about how to expand that capability to the CMF and return the response in a timely manner without an impact on other work.

IS Issue #2 Flats for Criminal Justice Purposes

There has been a debate on whether flats should be submitted for this criminal justice purposes. The FBI has researched the limitations and statistics relating to the submission of flats. During their research, it was found from a latent perspective 63 percent of the candidates are produced from a latent search coming from rolled impressions. The study also said that 40 percent of the identifications were made on the rolled impressions and not the plain impressions submitted. Based on that analysis, the recommendation was not to use flats as a way to update the CMF with arrest information. The discussion became that this will work for a booking however, with cite and release approximately 40 percent of arrests that occur do not result in a booking. There was discussion about the merits of capturing less than a full ten-print, the rolls, flats and palms with a misdemeanor crime where the person is most likely released opposed to booked. This resulted in an action item. The CJIS Division was asked to consider alternatives for capture of flats when it is a non-booking event or cite and release. Due to cite and release, the Disposition Task Force is looking at missing dispositions. If you do not have a booking event and the disposition comes in, there is nothing to match. This disposition does not make it to the state file or national file.

ACTION ITEM: The CJIS APB requested the CJIS Division provide additional policy options to address non-booking arrests.

IS Issue #3 Notifications for Wanted Notices on the NGI System

This topic was handled under APB Item #4.

IS Issue #8 Rapid DNA Update

Dr. Tom Callaghan, FBI Laboratory Division, provided an update to the IS Subcommittee on the progress with Rapid Deoxyribonucleic Acid (R-DNA). There is a big interest in being able to use Rapid DNA devices and the technology at the crime scene. An action item was assigned to the FBI to establish a Rapid DNA Crime Scene Task Force that would report to the IS Subcommittee. The task force will look into the viability of using this technology to process crime scenes and research if there could be a nexus established due to Rapid DNA Technology. The FBI was asked to work on this separately from the Rapid DNA Initiative.

IS Issue #9 Disposition Task Force Update

The Disposition Task Force Chair, Ms. Leslie Moore, Kansas Bureau of Investigation, provided an update to the IS Subcommittee. They are establishing a common way to count dispositions. This came from a report produced by the DOJ criticizing the disposition rate. Depending on how the disposition was counted, the reporting could look good or bad. The task force will be working on a standard way to count and report dispositions. Another crosswalk was taking all the statutes within states and mapping them to a standard definition. The NICS already does this and they will be assisting the task force moving forward.

IS Issue #10 Identification Services Coordination Group (ISCG) Update

Mr. Schaeffer advised that Mr. Brian Pittack provided the IS Subcommittee with an update of the ISCG. Twenty-one action items have been closed. The Electronic Biometric Transmission Specification (EBTS) is being updated to version 10.0.9. This will be the last update to EBTS Version 10 as they move towards implementing EBTS Version 11.

IS Issue #11 FBI Programs Research and Standards Unit (PRSU) Update

This unit is responsible for evaluating new technologies. Recently they reviewed card scanners and a Fujitsu Scanner was certified and approved for use. There was some discussion about contactless capture of fingerprints. During the FBI’s ongoing study, differences were discovered when comparing contactless versus rolled impressions. Contactless use is more for identification modality opposed to enrollment. Regarding the Iris Pilot; Accuracy has shown some merit and should become more mainstream as these standards are promulgated. The technology and testing are promising and improving closer to the friction ridge environment. PRSU will continue to explore the accuracy of facial recognition identification technologies.

IS Issue #12 – International Association for Identification (IAI) Update

Ms. Allison Miller, vice chair of the IS Subcommittee and IAI representative, briefed on what the Overseas Security Advisory Council (OSAC) is doing in regards to facial identification. The OSAC and the IAI are creating a source book and guide for those who want to enter the facial identification realm. They are creating proficiency testing and standards for facial identification.

The IAI has an Ad-Hoc item to create a quality metric when it comes to biometrics. When reporting accuracy, they have a false acceptance rate. They report what the statistic is but do not have a standard to compare it with. The Compact Council has been looking at the accuracy rate from an NFF Qualification Perspective but on the criminal side they don't have a metric. An action item was recommended that the FBI, in coordination with the IS Subcommittee and National Institute of Standards and Technology (NIST), begin developing those standards for biometric quality metrics.

The FBI distributes a list to check on unsolved latents and determine if they have been solved. This is not a capacity issue but a housekeeping issue. There was discussion about what should be done opposed to just sending out lists to everybody to clean up the Unsolved Latent File (ULF). They discussed setting boundaries when it comes to leaving something in the ULF. This was assigned as an action item to the FBI to see if there is a way to manage ULF better based on the number of minutia points stored for an unsolved case.

ACTION ITEM 1: The APB recommended the FBI in coordination with the IS Subcommittee begin researching and developing possible biometric quality metric standards with the NIST.

ACTION ITEM 2: The APB recommended the FBI review the previous recommendation pertaining to the minimum number of points required for storage within the ULF and possibly determine a way to manage data within the files.

IS Issue #4 Update the NGI Criminal Justice (CJ) Rap Back Policy and Implementation Guide to Show the Separation of "Death Notice with Fingerprints" and 'Death Notice without Fingerprints" Triggers

This was an action topic which came from the Compact Council, Standards and Policy Subcommittee, because of a change made to the noncriminal justice side for Rap Back. The change was made in 2017 and split out whether or not a death notice should be made based on a name or on fingerprints.

The subcommittee was provided two options, Option 1, to endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the NGI Criminal Justice (CJ) Rap Back Policy and Implementation (P&I) Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15 of the topic paper and Option 2, to make no changes to the NGI CJ Rap Back P&I Guide and perform a system enhancement returning the NGI CJ Rap Back Service "Death Notice Triggers to Death Notices with/without Fingerprints".

APB MOTION: The CJIS APB moved to recommend Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and

update the *NGI CJ Rap Back P&I Guide* to conform to the NGI System functionality as proposed in the NGI CJ Rap Back P&I Guide on pages 13-15.
(See Attachment A for details.)

IS Issue #6 Sex Offender Registration (SOR) Type of Transaction (TOT)

This topic originated from the TXDPS. The IS Subcommittee was asked to consider creating a TOT, for sex offender registration. Currently to create a registration event, it comes in as a booking or an arrest with a narrative. The recommendation requested the ability to send a separate TOT, for a sex offender registration event, that does not look like an arrest. The Working Groups and the IS Subcommittee approved Option 1, to have the FBI conduct the research needed to identify new business rules for a SOR TOT.

APB Item #7 Chairman's Report on the IS Subcommittee, IS Issue #6 SOR TOT

APB MOTION: Conduct the research needed to identify new business rules, policies, and privacy implications for a SOR TOT and bring the information back through the advisory process.

APB ITEM #8 Biometric Hit of the Year

Mr. William McKinsey, presented the Biometric Hit of the Year. ***(See Appendix K, PowerPoint.)***

Several years ago, the FBI developed the Biometric Identification Award. This award recognizes a law enforcement agency's good efforts, efforts that stand out, efforts to learn from in solving cases using the NGI System. The Biometric Identification Award is presented annually and promoted in conferences, conventions, and it is promoted on the FBI.gov website. The lessons it conveys are there for all to use.

On September 5, 1981, the Norfolk Police Department responded to an emergency call where a deceased female was found with more than 40 stab wounds. A fingerprint was found in the bathroom and was the only evidence that was available. The fingerprints were ran with no results. The case went cold. With the implementation of the automated fingerprint identification system in the 90's, the Commonwealth of Virginia requested assistance from other states to search the latent evidence against the fingerprint. Again, they received negative results. Finally, on January 28, 2015, the latent print evidence was searched against the NGI System, both criminal and civil prints and within 30 minutes, they identified a candidate. The individual was found and sentenced for his crime. Mr. McKinsey concluded with a video and presentation of the award.

APB ITEM #9 IAI Update

Mr. Ken Zercie, President of IAI, presented this topic. He noted IAI is a large organization and represents most of the law enforcement community, users of every system that

CJIS APB oversees, the people that implement the work, and the gracious work the FBI sponsors. **(*See Appendix L, PowerPoint.)***

Mr. Zercie provided history on the IAI. It was founded 105 years ago in California. It is international in scope. Out of the 68 divisions, there are divisions throughout the world. The most recent is in China. The international outreach through INTERPOL and some of the other partner agencies is critical. The IAI mission statement almost paraphrases the APB's, with the objective to advance the identification disciplines, get the information to the officers, and better serve our community.

The IAI annual education and training session was held in Reno, Nevada with over 1,500 attendees, national and international. They ran almost 600 presentations and multiple workshops, sharing information. Mr. Zercie complimented the bureau on sending their CJIS representatives to the meetings, acting as sponsors and providing information directly to the users. The members include administrators, functional technicians on the bench, laboratory people working in DNA, fingerprints, on the crime scene, collecting evidence, and recording the documentation. The IAI provides outreach throughout the country, the U.S., and internationally.

Another venture of the IAI is certification of the individual examiners. The IAI has been in the forefront of that for a number of years, whether it is latent fingerprint identification, ten-print identification, Facial Analysis Comparison and Evaluation (FACE), or Forensic Art. If you are an accredited operation through the Communications Assistance for Law Enforcement Act, International Organization for Standardization, American National Standards Institute National Accreditation Board, these programs will be recognized.

Mr. Zercie closed with a parting thought, "In any type of science, in anything that we do, we don't have any guilty to convict or innocent to acquit. It's a search for justice and truth." That is the main goal for everyone at this meeting. He also expressed his appreciation to the vendors for their support, sharing of ideas, techniques and technologies.

APB ITEM #10 National Consortium for Justice Information and Statistics (SEARCH) Update

Mr. David J. Roberts, Executive Director, SEARCH presented this agenda item. **(*See Appendix M, PowerPoint.)***

Mr. Roberts advised SEARCH was celebrating their 50th anniversary this year. He then briefed regarding solicitations for the National Criminal History Record Improvement Program (NCHIP) and NICS Act Records Improvement Program (NARIP) which were released in 2019 by the Bureau of Justice Statistics (BJS). He advised that 39 NCHIP and 19 NARIP applications were approved with an impressive 62 million dollars awarded for these programs. Funding for next year will be around 80 million with solicitations going out early in 2020.

The 2018 survey of state criminal history record information systems will soon be finalized. All states participated in the survey and results should be published early in 2020. SEARCH continues to work on the Quality Assurance Program (QAP) and Criminal History

Records Improvement Workshops. The QAP checklist developed in 2012 was revised in 2017. Several states have implemented the QAP. SEARCH would like to see those using the 2012 Version 1 upgrade to Version 2. They would like to see additional states come on board with the QAP. Two quality assessment workshops were completed in 2019 with funding from BJS. These workshops are effective and SEARCH plans to conduct two more of these in 2020.

Mr. Roberts briefed they are finding that states with centralized court case management systems have more complete criminal history records. The same goes for the states that have consolidated or centralized prosecutor case management systems.

SEARCH is expanding their work with the OPM Performance Accountability Council Project Management Office Defense Counterintelligence and Security Agency, previously known as the National Background Investigations Bureau. This effort focuses on understanding the gaps that exist in criminal history records. SEARCH is doing the mapping of and inventory of all the criminal history record systems to the Joint Task Force Standardized Rap Sheet, XML, Standard 4.1. Mapping has been completed for 37 states so far. Onsite detailed reviews will be done with two states and six local agencies. SEARCH will be providing state specific guidance for interpreting criminal history rap sheets as part of the gap analysis. They believe a guidebook that allows DCSA to understand and interpret criminal history record information across states will be very important.

SEARCH recently started a project with RAND Corporation, looking at replicating the 1999 report on name search efficacy. The Computerized Criminal Histories (CCH) metrics is another ongoing project which looks at CCH records for a broader criminological search to understand risk, recidivism and redemption. SEARCH has established a working group to identify the universal metrics that every repository ought to be looking at in terms of the quality of their criminal history records. The Arnold Foundation funded a very small amount last year to develop a research agenda. The agenda was presented at the July 2019 SEARCH Symposium. Mr. Roberts provided arrest and arrestee data obtained from their research.

Mr. Roberts closed by mentioning some of their upcoming meetings. In January, they will be meeting in Columbia, South Carolina for their Winter Membership Group meeting. Agenda items will include updates on the status of CCH upgrades, Automated Fingerprint Identification System updates, Clean Slate Act, the DCSA project, NIBRS update, and information system security in regard to recent ransomware attacks. The membership group will also meet July 20, 2020 in St. Louis, Missouri.

APB ITEM #11 National Crime Prevention and Privacy Compact Council Report

Mr. Wyatt Pettengill, North Carolina State Bureau of Identification and Chair of the Compact Council, presented this agenda item. ***(See Appendix N, PowerPoint.)***

The Compact Act, which is the National Crime Prevention and Privacy Compact Act, was established in the mid '90s. It provides an infrastructure for the sharing of criminal history record information for noncriminal justice purposes. The purpose is to vet those individuals who are seeking to work with the most vulnerable population. Whether it would be a nursing home, daycare, or a school, the goal is to make sure those individuals, working with our vulnerable population have been properly vetted and the Compact Act establishes an infrastructure for that.

The Compact Act established the Council itself. It allows the states to take advantage of those infrastructures created for the sharing of criminal history information. There are 34 states, who have ratified the Compact. Ten states have signed an MOU, which is the first step to becoming a Compact State. Delaware became the 34th state, ratifying on July 4, 2019. Ms. Lisa Voss was appointed as the first state Compact Officer. There are resources for anyone interested in becoming a member. A Compact Ratification Video and the Compact Mentorship Program is available for those interested. The mentorship program pairs representatives from non-compact states with representatives from compact states to discuss how to become a compact state and how to ratify it.

Ratifying the Compact brings a state one-step closer to providing the most comprehensive criminal history record information for noncriminal justice purposes. This is achieved through participation in the NFF program. This program places the management and responsibility of the effective control, collection, maintenance, and dissemination of state criminal history record files solely within the state. NFF participation results in both enhanced individual privacy protection and better security for the nation's most vulnerable population. To date, there are 20 states participating in the NFF program. Recently, the Council has approved an alternate NFF method, and several states are currently reviewing and taking advantage of that NFF alternate program.

Mr. Pettengill advised there were several Council initiatives. The first was the regional pilot meetings. The Council was established prior to September 11, 2001. After 9/11, data sharing changed causing the Council and infrastructure to look a lot different. The challenge for the Council has been staying true to their mission while evolving. With the addition of Compact States, the current meeting infrastructure, which included focused committees and a full Council meeting, was sustainable for the proper vetting and discussion of the topics that came before the Council. Regional Committee Meetings were established to include all state compact officers divided into two groups: eastern and western regions. It mimic's the APB working groups. The feedback received was positive. State Compact Officers found the small group structure facilitated more conversation, gave them more time to digest the information prior to the council meetings, and gave the states an opportunity to have a voice. It was a more comfortable environment making it less intimidating to speak. The pilot ends in February 2020 he hoped to transition these meetings from a pilot program into permanence.

One of the other initiatives is the privacy notice. One of the main goals was to strike a delicate balance between vetting an individual who wants to work with our vulnerable population with the importance for one's right to privacy. The privacy notices and disclaimers are an important piece. A great deal of time was spent the last round to update those privacy notifications appropriately.

The Compact Act defines immigration and naturalization matters as noncriminal justice purposes. Mr. Lee Bowes, DHS, highlighted challenges that the United States Citizenship and Immigration Services (USCIS) is experiencing as it pertains to criminal history. Those challenges include the inability to access state held criminal history from states that do no support Purpose Code I; the inability to access criminal history information sealed for noncriminal justice purposes; and the inability to access criminal history information because disposition information is incomplete. This conversation highlighted the importance of states having conversations about sealing and expunging data, and broadening our perspective to think about immigration and naturalization. The council motioned for the FBI CJIS Division to evaluate the level of effort to create a noncriminal justice purpose code for immigration and naturalization. This is an excellent example of the Council collaborating with federal agencies on noncriminal justice.

During the May 2018 presentation of the National Identity Services Summary Audit Summaries, the Council's Sanctions Committee requested additional tools and resources to assist the user community with understanding how to better prepare for audits and execute audits of their own. In response, the CAU explored options and concluded that in addition to creating a checklist or outline, it would be beneficial to consolidate this effort as part of a bigger project. As a result, an improved online audit resource was established to facilitate access to materials intended to assist noncriminal justice user community in preparing their audits. There were audit findings that were consistent across the board and we hope to provide a better set of resources for our noncriminal justice community that helps them move closer to compliance.

Mr. Pettengill briefed on two new task forces. The NFF Disposition Task Force. The goal is to develop recommendations for improving arrest and disposition reporting. Some states do not allow for the dissemination of the criminal history information if it does not contain a disposition. In order for those hiring agencies to make a determination of whether I want to hire that individual, they need and deserve a complete picture.

The second new task force is the Outsourcing Task Force. This task force is charged with proposing changes to the existing outsourcing standards and outreach documentation. The outsourcing issue was one of those frequent audit findings. In reviewing outsourcing standards and documentation, it was clear it needed to be updated to make it more helpful to non-criminal justice agency partners.

Mr. Pettengill said he was thankful and appreciative of the partnership between the CJIS APB and the Council. He introduced Ms. Leslie Moore, Compact Council representative on the CJIS APB. He also introduced Ms. Carol Gibbs, Illinois State Police, as the new State Criminal Justice Representative on the Council. He also advised that Mr. Mike Lesko serves as the APB representative Council. Mr. Pettengill shared the Compact Council meeting dates, Regional Meetings are slotted for February 26-27, 2020 in Clarksburg, WV; the Standards and Policy and Planning and Outreach meetings are scheduled March 25-26, 2020 in Clarksburg, WV, and the Compact Council Meeting will be May 13-14, 2020 location to be determined.

In conclusion, Mr. Pettengill thanked Ms. Chasity Anderson and the Compact Team for their help making them successful.

APB ITEM #12 Tribal Task Force (TTF) Update

This agenda item was presented by Mr. William Denke, Sycuan Tribal Police Department and Chair of the TTF. **(*See Appendix O, PowerPoint.)***

Mr. Denke began with the TTF mission, which is "To enhance officer and public safety by improving federal, state, local, tribal, and territorial participation in CJIS Division Systems. The task force reviews relevant issues that may prevent or discourage Tribal Law Enforcement agencies from entering records and/or data into CJIS Division systems, and make recommendations to address those issues." The TTF consists of 12 members. There are four tribal law enforcement representatives, four either state or local representatives, and four federal representatives. The task force was reconstituted adding three new members, Chief Ronnie Gilmore, Miami Nation in Oklahoma, Chris Sutter, Tulalip in Washington, and Colonel Tim Chung, Arizona Department of Public Safety. The task force has convened four times via teleconference and in person in September 2019 at the FBI's CJIS Division.

In April 2019, letters were sent to tribal leaders explaining the National UoF Collection and the need for participation. At that time, there were 12 tribes participating, as of December 2019, the number has increased to 30. There has been discussion concerning NIBRS. The primary reason being any tribal agency receiving funding from the Bureau of Indian Affairs (BIA) is required to send in Summary Reporting System (SRS) data via an Excel workbook every month. With only a year to go, there is concern with trying to bring that together. CJIS personnel has been working behind the scenes with BIA to ensure this is not an issue. It will be difficult for tribes, with the lack of resources in their records management systems, to bifurcate between the NIBRS and the SRS summary. The CJIS Division is working to create a portal through LEEP for tribes to report directly with a completion date by June 2020.

A disposition reporting guide, one-page document, will be sent to tribal leaders and copied to all tribal law enforcement chiefs. This comes after the first deliverable as a task force, the arrest and disposition reporting guide. They are trying to close the gap of disparity between arrests being reported versus a one-pager disposition and continue to remind the tribes how important it is to have these dispositions.

The Tribal Engagement Program continues to work hard visiting ten different tribes in California, Washington, Louisiana, and Maine this year. They continue to be active in tribal conferences attending approximately seven conferences. There has been work on the development of a CJIS Tribal Video. It will display six different CJIS programs, the UCR, the NICS, the N-DEx, the NGI, the LEEP, and the NCIC. It will highlight one tribe in Indian Country working within those CJIS programs. It will be a 45-minute video and is slated to be completed in June 2020. It will be sent to all 573 recognized tribes, different tribal associations, and upon request by any law enforcement entity.

Mr. Denke shared that the TTF met in September 2019 at the CJIS Division complex and it was one of their most productive meetings. They were able to visit most of the programs to include, the NCIC, the NICS, the NGI including the Facial Analysis, Comparison and Evaluation Services, Fingerprinting Image Comparisons, the LEEP, the UCR Program and the National Threat Operations Center. The Peace Tree Ceremony took place during the meeting. A member of the Seneca Tribe gave a background and cultural perspective of the planting of the White Pine Tree. The significance historically of the five tribes coming together to set their differences aside to work towards a common goal of peace for their people. It is sitting on campus for all to see with a plaque memorializing the efforts of the FBI CJIS Division working with the task force to advance public safety in Indian Country.

The FY2020 initiatives include the Tribal Access Project. This is not to be confused with the DOJ TAP kiosk. The Tribal Access Project is the research of issues, gaps or roadblocks of tribes participating in all of the FBI CJIS Programs. They are beginning to have dialogue with BJS, the National Institute of Justice, to find a group willing to work with the task force to survey the tribes and further promote the good steam moving forward with the tribes utilizing all CJIS programs. The task force would like to send another letter to tribal leaders explaining the NCIC is N3G, extradition codes for tribal agencies, and tribal fingerprint submission cascades of ULF. They would also like to continue outreach and support to the tribal partners.

In conclusion, Mr. Denke wanted to take a minute in the light of the 25-year anniversary to thank the CJIS AD and all his personnel. He reminded Chairman Lesko that his first step into this process was with the task force. At the first meeting, they knew there was a problem but not what the problem was. He said looking at how far we have come, it's beyond just solving problems, it's beyond certain people being in those positions, it's actually been woven into the CJIS APB process, and the fabric of what the FBI CJIS does with all its programs.

APB ITEM #13 Chairman's Report on the UCR Subcommittee

This agenda item was presented by Ms. Kathryn Monfreda, Alaska Department of Public Safety and Chair of the UCR Subcommittee. ***(See Appendix P, PowerPoint.)***

The UCR Subcommittee met on October 9, 2019 in Norfolk, VA. They discussed thirteen informational topics and one action topic.

UCR Issue # 2 Definition Revisions for the Federal NIBRS Offenses.

The purpose of this topic was to provide modifications and suggestions for the approved NIBRS offenses to enable federal agencies to accurately report crime data to the UCR Program. In 2017, the APB approved a list of crimes and codes associated with them to allow the federal government to report crime specific to them. Once approved, the UCR team began working on those and discovered some issues with how they were coded. This topic recommends changes to some of the codes previously approved. The UCR Subcommittee reviewed the options and inquired when a portion of these offenses would be available for state and locals. Several of the crimes are specific to federal government and some are applicable to the states. It was determined by the APB process in the spring of 2018 that states and locals would be allotted time to transition to NIBRS by the 2021 deadline. Following the transition, the states and locals will have the opportunity to request the ability to utilize these new offense codes.

<u>**APB MOTION:**</u> The CJIS APB moved to recommend Option 1: Accept the proposed revisions (Attachment B) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

Ms. Monfreda briefly went thru the information topics and then provided an update on the NIBRS transition. Thirty-nine states are currently NIBRS certified and ten states are developing a NIBRS certified system at state level. In August 2019, North Carolina became the 39th state certified as NIBRS. California has made great progress; they have received funds and are canvassing their local agencies for NIBRS commitments.

There have been significant commitments since September 2018. Florida provided their state's first update on local agencies committing. They moved from zero to two hundred fifty agencies committed to reporting by January 1, 2021. That will cover approximately 68 percent of the state's population. Other states with significant increases were Arizona, Louisiana, Minnesota, Mississippi, Nebraska, New York, Pennsylvania and Wyoming.

Ms. Monfreda reminded the group that there is only 12 months to go. The FBI encourages law enforcement agencies who have not yet started transitioning to do so by utilizing the available resources on the web page.

APB ITEM #14 Association of State Uniform Crime Reporting (ASUCRP) Programs Update

Mr. Derek Veitenheimer, Wisconsin Department of Justice and ASUCRP Representative presented this agenda item. **(*See Appendix Q, PowerPoint.)***

Mr. Veitenheimer began with the mission, values, and goals of the ASUCRP. Their mission is to represent State UCR Program's on a regional, local, and national level to move the program forward. Their goal is to improve the collection and the utility of UCR data soon to be NIBRS data. They partner with Justice Research and Statistics Association, an annual conference where they discuss the status of UCR Programs at a state level, identify areas of concern and areas of interest for state UCR programs, and foster partnerships and relationships with the FBI, to move the UCR program in a positive direction.

The ASUCRP sent an annual survey to state UCR programs and received an 85% response rate from their state and territory programs. Mr. Veitenheimer shared those results. He said one question always asked is how your program submits UCR data to the FBI. Just over 20 percent of agencies are still submitting via the SRS only. This provides an opportunity to reach out to states that have not yet transitioned and provide assistance, guidance, and help wherever needed. Half of state UCR programs, staff between two and five people. A quarter of state UCR programs have only one person making it difficult to transition to NIBRS. They would like to stress the importance of staffing a UCR program.

Although the UCR program is voluntary at the national level, three-quarter of states actually mandate the reporting of UCR data. For those states that mandate reporting, around half have no penalties for noncompliance. The submission of timely data from local agencies to the state UCR program is important. ASUCRP also promotes the importance of participating in the UCR Program at the local level. Approximately 87% of states offer some form of UCR training at the state level. This has improved from prior years.

A third of agencies do not have an audit process and don't plan to develop one. The ASCURP promotes complete, high quality data, and believes in the value of that crime data collected through the UCR program. To build trust in the data, it needs to be accurate. Training and auditing are two important issues the ASUCRP focuses on and promotes moving forward.

Another big ASUCRP topic is how the state programs are managing the UoF Data Collection effort. Half of the states are using the LEEP portal and the other half are developing their own statewide data collection effort and incorporating that with the UCR program. The survey asked states if they had implemented XML to collect data. The vast majority have not. This is an area of concern as it slows down the data collection process. As a follow up question, the states were asked when they plan to implement XML and 71 percent had no plans to do so in the next five years. This is no small task and an area that associations should focus on. The NIBRS program was not going anywhere until the CJIS APB recommended a cut off to SRS reporting. Mr. Veitenheimer suggested the CJIS APB consider a deadline for accepting flat file submissions to push this move to a more smooth data transmission. Another area of improvement needed is the use of UCR data to create public facing data visualizations. The FBI has invested a lot into their Crime Data Explorer, which introduces the entire nation to crime data. The ASUCRP would like to see states follow step and ensure they are presenting accurate information in a NIBRS format. He said the way they look at crime data is changing, and it will continue to change as NIBRS rolls out. Therefore, it is important to the association that they provide their members with information and good methodology to ensure the NIBRS data being presented accurately, and in a way that is usable.

Lastly, Mr. Veitenheimer updated the CJIS APB on areas of focus. The most important on the list from about every state was UoF Collection. Even if states are not participating, they are interested in where that program is going and how the state can implement with small staffs in an effective way. There is interest in the upcoming changes to NIBRS reporting. They are expecting post 2021 to see many improvements to the NIBRS program. Data quality is always important. It is about timely, accurate data, and what state UCR program managers can do to remove the burden from local law enforcement agencies to ensure the receipt of timely, complete data.

APB ITEM #15 Use of Force Task Force Update

Mr. Robert Sage, Augusta Department of Public Safety and Chair of the UoF Task Force presented this agenda item. ***(See Appendix R, PowerPoint.)***

Mr. Sage started by thanking UoF Task Force members and FBI staff for the extensive work in getting UoF data collection live on January 1, 2019.

Mr. Sage provided the background on UoF data collection. It was established at the request of federal, state, local, tribal, college, university, and major law enforcement agencies. High profile events involving the law enforcement community and general public, highlighted the need for better crime data and an additional collection of law enforcement and use-of-force incidences. Mr. Sage said trust and transparency are paramount between law enforcement and the community they serve and this data collection is intended to promote that transparency. This data will provide the public with necessary facts about law enforcement use-of-force in the course of their duties and ultimately strengthen the nation's confidence in law enforcement. The data derived from the collection can also be used to enhance law enforcement training for such things as de-escalation techniques when officers are faced with combative subjects. It is designed to protect privacy and confidentiality by including quantifiable data only and omitting narratives and personally identifiable information.

UoF data collection involves three types of use-of-force incidents, death, serious bodily injury, and the discharge of a firearm at or in the direction of another person, whether or not the person was struck. Mr. Sage said what constitutes serious bodily injury is a question frequently asked by law enforcement. Serious bodily injury is defined based in part on Title 18 United States Code, Section 2246 Part 4 which states 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 definition of a firearm is based in part on the Bureau of Alcohol, Tobacco, Firearms and Explosives definition in 18 USC 921(a)(3) which means any weapon, including a starter gun, which will or is designed to or may readily be converted to expel a projectile by the action of an explosive.

Mr. Sage said they continue to get more and more partners enrolling and participating in the data collection. The task force continues to meet and discuss incidents that are coming in and questions from law enforcement agencies on what is reportable and how the information should be classified. Mr. Sage said it is imperative the FBI reaches the OMB's mandated 40, 60, and 80 percent participation thresholds and they are definitely on track to hit those percentages. Participating agencies may contribute data via the free Use-of-Force Portal Application housed on the LEEP or via bulk submissions. He said data should be submitted within 48 hours of an incident, even if the facts are not all there. The incident should be started in the system and agencies can then come back later and add other data sets that were pending or unknown at the initial entering, zero reports should be entered by the 15th day of the following month, these are used when there is no reportable incident. These reports demonstrate an agency's active participation and establish that no incident occurred in the jurisdiction. Zero reports also assist the FBI in computer valid statistics and take less than a minute to submit.

Several states are managing the collection by submitting a bulk file, allowing local agencies to submit directly into the Use-of-Force Portal or entering data into the Use-of-Force Portal on behalf of local agencies, or they can do it in a combination, they can enter for some and allow others to enter for themselves. Responsibilities come with managing the collection, states must ensure that all agencies are submitting monthly data, they must identify and request missing data and they need to monitor data for pending information, and request pending information when it is in there. State must also review and approve incident reports and zero reports, and serve as an intermediary between the locals and the FBI.

Mr. Sage provided information on several states that plan to participate in collection and want to manage the data by June 2020. He also provided information on the challenges states face, which include technical issues and lack of funding to acquire resources, personnel, and equipment to develop systems as well as encountering delays in obtaining LEEP accounts in order to access the Use-of-Force Portal. Mr. Sage said webcasts are being offered to state programs and local law enforcement agencies to demonstrate the portal and it’s utility. Because of these webcasts, some states have elected to use the portal until their state systems are finalized. The Crime Statistics Management Unit (CSMU) has received great feedback on the webcasts. The CSMU is working with LEEP staff on new enhancements as well to include the capability to see the applicant's online application when the applicant calls to obtain their user ID and password. A recent enhancement allows applications for Use-of-Force Portal access only to receive special attention and lessen delays in the processing of LEEP applications.

The FBI continues to provide outreach with their law enforcement partners in an effort to increase participation in this collection. There have been over 80 speaking engagements since the date the collection was launched. Mr. Sage urged anyone with questions to reach out to the FBI by phone or email or visit <www.fbi.gov> for resources and information on use-of-force collection.

APB ITEM #16 CJIS Shared Management Progression

Former and present FBI Designated Federal Officer’s (DFOs) presented this agenda item. ***(See Appendix S, PowerPoint.)*** Mr. Megna, current DFO, began the presentation with trivia questions. The first question being what was the location of the first CJIS APB meeting? The answer was Atlanta, Georgia. He said the location for the current meeting was not by design as it was originally planned for San Antonio and solely by chance it was held again in Atlanta. The second question was what was the number of members on the original CJIS APB in 1994? The answer, 29 members, current membership consists of 35 members. The third question, what was the highest number of recommendations from a single APB meeting. He noted, the average is 33 recommendations per round. The lowest has been 10 and the highest 74.

Advisory committees have historically played an important part in the history of the U.S. Government’s ability to form policy and approaches surrounding programs, dating all the way back to the days of George Washington attempting to address the whiskey rebellion. The value of advisory committees was memorialized in the Federal Advisory Committee Act (FACA) in 1972, that act established law dictating or governing those advisory bodies. It required charters, specific rules, and the appointment of a DFO to be appointed to each FACA within the government. Mr. Megna was honored to have been appointed to this FACA that he believes is the gold standard within the federal government. He was pleased that several past DFOs would be present to assist with memorializing the shared management approach that was executed not only for the past 25 years with the CJIS APB, but all the way back to the original NCIC APB established 50 years ago.

Mr. Megna introduced Mr. Scott Trent who served as the DFO from 2011 to 2017. Mr. Trent thought today was not only a celebration of 25 years but also a celebration of and an acknowledgement of the important foundational pillars of this partnership. In 1969, the NCIC APB was established. It worked so well that by 1989 the UCR Data Providers started an advisory board. In 1994, FBI Director Louis Freeh decided only one advisory board was needed for CJIS, resulting in the CJIS APB of today. Mr. Trent believed that 50 years of shared management is what makes this successful. It is the partnerships with criminal justice agencies, law enforcement agencies, court systems, tribal agencies, and the vendor community. All of which are part of the shared management process. The FBI had the systems and the services to effectively protect citizens and their property but did not have the data. Law enforcement and criminal justice agencies have that data. An agreement was made that if law enforcement and criminal justice agencies would provide the data, the FBI would place it in their systems and make it available. At the same time, agencies would have a say in how that data was used, accessed and the policies surrounding that data. This was the foundation of the shared management concept and a model for the entire nation. It has been the basis of a strong partnership continuing today.

Criminal justice is a team sport. One agency cannot do it alone; it takes everyone working together to be effective at criminal justice to protect lives and properties. Mr. Trent reminded the group of three key elements that every partnership must have. The first was to care about your partner. The people sitting at this meeting care about the mission and the involvement in meeting this goal of protecting our citizens. The second was that both parties must trust each other. Mr. Trent said the third, while we may not always agree, both parties have to be willing to listen to one another. To have the conversation, to understand the perspectives, to come together, and at times be willing to compromise to reach the greater good. The shared management process has those three elements. He said we don't always agree and there has been heated debates over the years but this is a sign of a healthy relationship. It shows people are passionate about the process.

Mr. Trent quoted Howard Thurman, "We need to ask ourselves, what makes you come alive, then go do that. Because what the world needs is people who have come alive." He said as the past APB Chairs and DFO's met prior to this meeting, it turned into a free-flowing discussion about the important efforts of the APB over the past decade. These passionate men came alive talking about the challenges that were overcome in order to do what was right and was not always easy. That is shared management. Mr. Trent felt fortunate to be a part of something extraordinarily special from the former and current members sitting at the table, to the FBI leadership, to the hard working people behind the scenes at the CJIS Division, to the vendor community who listens to what is said and makes it happen. That is a community of service, a shared management, and the APB is able to bring that altogether.

The next guest speaker was Mr. Roy Weise. Mr. Weise served as a DFO for more than a decade. Mr. Weise was a programmer, software engineer, and program manager within the NCIC and retired from the FBI with 45 years and 10 months of service. Mr. Weise spoke on the roots of the NCIC system and the APB. He said it began as an informal group of local, state, and federal law enforcement officers and officials who met under the auspices of the IACP and the NSA in the early 1960's. The consensus of the group was that law enforcement needed the NCIC system. They concurred that the FBI should be the agency to house the system. Mr. Weise believed two agents, Mr. Jerry Daunt and Mr. Frank Buhl, were the fathers of NCIC and represented the bureau at the meetings of IACP and the NSA.

The first step was to build a system. Mr. Daunt met with the director and after some contentious meetings; he agreed to fund the system. Once the system began operation, they realized that a more formal and subject matter specific board was needed to define the system and the policies governing it. This was an even harder sell as the shared management concept was new to the FBI and against their mindset to propose an advisory body to assist in the development and operation of the NCIC.

Mr. Weise shared three of the recommendations made in the first meeting. He felt they illustrated the foresight and the vision of an advisory board. The UCR APB recommended that all state and metropolitan area computerized Law Enforcement Information Systems should interface with the NCIC and must be under the management and control of a law enforcement agency. The second was pertaining to misuse and abuse of the system. While not a problem at the time, the NCIC APB noted it was a possibility that future information could be misused or improperly divulged by a participating police agency. Title 28, Section 534 of the U.S. Code provided the FBI the authority to cancel service to an agency for divulgence of criminal record information for unauthorized reasons. The third referred to the NCIC support and expansion. The NCIC APB recommended that the NCIC, including new file applications, be expanded as rapidly as possible, specifically requesting that this recommendation include FBI consideration of message switching and police communications in an expanded NCIC network.

Mr. Weise then described the first APB meeting in 1974. The meetings were smaller. They met in a small room with one banquet style table. All the board members sat at the table and two or three FBI staff sat along the wall. There were no guests or contractors as there were very few private companies at that time. Mr. Weise received his indoctrination to the passion of the APB at this meeting. The Assistant Director attended due to a hot topic regarding the continuance of FBI support and participation in the automation of criminal histories. The manual conversion process or the building of the CCH system was a huge effort for the FBI and the states too. For resource reasons, the FBI considered pulling out and this was a sore spot with the states because they had already committed resources. The board had a lively discussion and then it was decided that only those people involved would meet later for a special meeting. The FBI agreed to study the CCH program and decide whether it would be a centralized database or a pointer system. This was the forerunner for the current subcommittee meetings.

He noted the NCIC APB influenced the creation of other Advisory Groups. The Laboratory Division modeled their Combined DNA Index System (CODIS) Advisory Group after the NCIC APB. The CPIC Advisory Board was formed in 1972. Mr. Weise was the FBI representative to that body and was told that the NCIC APB influenced the creation of the CPIC APB.

The next speaker was Mr. Don Johnson who had over 31 years of law enforcement experience at the federal, state, and local level. He was the FBI CJIS Division, Program's Development Section Chief as well as the DFO.

Mr. Johnson's presentation was about the UCR Advisory Board. He noted they were celebrating 90 years of UCR, 50 years of NCIC, and 25 years of the CJIS APB. Mr. Pat Fitzsimons was the first chair of the UCR APB. Mr. Johnson contacted him prior to the meeting and they talked about how the people came together on the UCR APB to be a voice of the police agencies and support the FBI. There were battles but the best memories involved the resolution, when it finally got to the APB after going through the UCR Working Groups.

Mr. Johnson shared a life-changing moment as a rookie police officer in Beaumont, Texas, when the NCIC went online January 27, 1967. He located an abandoned vehicle and checked it through the local databases. When he ran it through the NCIC he received a hit that it had been stolen two weeks prior. He processed the paperwork and was proud of himself until he opened the afternoon paper, it read in bold letters "FBI locates stolen vehicle". That was a life changing moment; he went to school and was blessed with the opportunity to work for the FBI. Mr. Johnson said coming together on many issues and finding resolutions thru the shared management process was amazing. There is compromise and negotiating but the process works. Mr. Johnson encouraged CJIS APB members to continue their good work.

Mr. Megna added that the NCIC APB and the UCR APB set the foundation for the current NCIC and Uniform Crime Reporting Program, as well as NCIC 2000 and the Integrated Automated Fingerprint Identification Systems (IAFIS), which ultimately became the NGI. Both paved the way and set the foundation for the CJIS APB. He asked Mr. Weise to speak about the formation of the CJIS APB as it is currently.

Mr. Weise pointed out that Director Louis Freeh established the CJIS APB in 1994 and recognized the benefit provided by NCIC and UCR boards as well as the fact the DOJ needed to reduce the number of advisory committees. They combined the two into one overarching board to provide guidance on the operation of all program services administered by the FBI's CJIS Division. The NCIC APB's responsibility was expanded in 1988 to include criminal history matters. This became much more of an issue when the automated fingerprint systems came about. The final meeting of the NCIC APB and the first meeting of CJIS APB were held in Atlanta, Georgia in December of 1994 with Director Freeh in attendance.

Mr. Weise heard many times that the successes of the system that CJIS operates would not have been possible without the CJIS APB board. There is a much greater impact to the local law enforcement agencies than the FBI. He noted the measure of any organization is growth, and the CHIS APB has certainly grown. He concluded by saying, the motions and recommendations made by this body has helped the FBI set priorities and its success is a result of the dedication, the wisdom, and the vision of this CJIS APB.

Mr. Trent recapped the APB's evolution. He said an advisory board has to do two things: 1) remain consistent to the mission and 2) find a way to evolve to meet the changing needs of the communities it serves. The CJIS APB's first female board member was Ms. Sandra O'Connor, a state attorney for Baltimore County who represented the National District Attorney's Association. In the early 90's, there were not many female sheriffs, but the NCIC APB actually had a female sheriff on one of the working groups, was elected vice chair of the working group, and served on nearly every subcommittee. She eventually made her way to the APB where she served as 2nd vice chair and she serves today. He then recognized Sheriff Kathy Witt, the longest sitting member on the CJIS APB. Mr. Trent thanked her for her dedication to the process and belief in the community of shared management since 1991.

In 1996, the MCCA was added as a member to the APB. In 1997, a member for the Major County Sheriffs Association was added. In 1999, representatives from the American Society of Crime Lab Directors (ASCLD), and the Conference of Chief Justices was added. The FBI Director had the ability to add someone to each working group. Former chair, Mr. Jack Donohue, was a director appointee in the northeast and then elected to the APB. In 2003, the

Virgin Islands and Guam were added as voting members to the regional working groups. The N-DEx Subcommittee was formed in 2003. In 2005, there were interesting conversations with the DHS and a representative was added for national security. Tribal representatives were added to each of the working groups in 2006. In 2009, a tribal member was added to the APB. In 2014, a Compact Council member was added and the chair of the Federal Working Group was no longer an automatic member but sat with the chairs of the other working groups. The Federal Working Group elected a person to sit on the board. With the evolution of changes, the CJIS APB managed to stay consistent to mission and evolve as the times have changed. Mr. Trent concluded by thanking the people around the horseshoe, the people at CJIS, the people in the gallery, and the ones that came before us for doing a phenomenal job of showing how community law enforcement should be handled.

Mr. Megna then introduced former DFO Mike McIntyre. He served as the DFO in 2017 and continues to engage the advisory process as the CAU Chief.

Mr. McIntyre said he believed the success of this shared management ensures there is a common set of standards and rules moving this community into a common direction. He said we may not always agree on the same path but it leads to vigorous, robust debate throughout the process. It is crucial to have diverse perspectives from all the members of the community as we consistently work to build toward those common goals, in crime data modernization, building the next version of the NCIC, modifying or modernizing policy, and creating a CJIS Security Policy to address emerging technologies or security threats.

Mr. McIntyre briefed on the membership of the CJIS APB. It consists of 20 members representing the four regional working groups from state and local law enforcement. A member elected from the Federal Working Group. A representative from the prosecutorial, judicial, correctional, and national security sectors. A tribal law enforcement community representative, association representatives from the American Probation and Parole, IACP, Major County Sheriffs of America, MCC, National District Attorneys Association (NDAA), NSA, ASCLD, and the Conference of Chief Justices and a member representing the Compact Council. There have been more than 2,200 recommendations with 98 percent completed. This speaks volumes to the work and the dedication put into this process and to the amount of importance, debate, and consideration that goes into each recommendation moving forward. Mr. McIntyre concluded by thanking the CJIS APB board for their time, dedication, and effort put into the process in order to keep the community moving forward and keep the public safety of this nation strong.

Mr. Megna wrapped up this topic. With these comments, made at the first meeting of the CJIS APB by then Director Freeh. He said these statements still ring true 25 years later. "Deliberations of this new board in the months and years to come will directly impact policing into the 21st century which is an awesome challenge. We have had in this country, and I see them every day, hundreds and thousands of dedicated law enforcement people who protect the streets and the country roads. They need more than ever your dedication, your intelligence, your commitment, your innovation, your ability to predict where we will be in a very, very short time, and to give us the informational systems to prepare better." Mr. Megna commended the APB and thanked them for their participation and dedication. He said it was clear that 25 years ago, Director Freeh, understood where the CJIS APB was going.

A video was played to commemorate the past 25 years.

APB ITEM #17 APB Significant Achievements

Former APB Chairs recognized significant achievements occurring during their tenures. Mr. Lesko introduced Mr. Joseph P. Bonino, retired Los Angeles Police Department and the first chair of the CJIS APB. Mr. Bonino joined the NCIC Western Working Group back in 1985 and was elected to the NCIC APB board in 1988. He served as first vice chair of the NCIC board from 1992 to 1994, which transitioned into the CJIS APB in 1994. Mr. Bonino served over 30 years with the Los Angeles Police Department and served two terms as the APB chair from 1994 to 1998.

Mr. Bonino provided a summary of significant APB achievements during his tenure as chair of the CJIS APB. ***(See Appendix T, PowerPoint.)*** He briefed most were in regard to NCIC 2000 or IAFIS, highlighted several key stories of shared management. In the early part of Mr. Bonino's term, NCIC had difficulties that sent a three-person team to directly address issues with the vendor. At the direction of Director Freeh, the team was given full authority to resolve those issues. During his term, there was discussion concerning name checks versus fingerprint checks. He said this was a definitive study which determined there were critical problems with false positives and false negatives and fingerprint checks were possibly the only way to resolve this. There were important recommendations relating to missing and unidentified files, establishment of a dental task force with emphasis on forensic work and analysis, missing and exploited children, DNA, and the flagging of estranged and abducted children. Mr. Bonino concluded that the most important thing was the regular involvement with the senior leadership of the FBI and their full support in what was being done. He said he would like to see this continue into the future because it is the essence of shared management.

Mr. Megna read comments provided by Mr. David Gavin, retired Assistant Chief of Administration of the Texas Department of Public Safety who was unable to attend the meeting. ***(See Appendix U.)*** Mr. Gavin was a member of the CJIS APB for 18 years and served as chair of the CJIS APB from 1998 - 2000.

Mr. Lesko then introduced Mr. William Casey who served on the CJIS APB for 16 years and served two terms as chair of the CJIS APB. Mr. Casey was with the Boston Police Department for over 20 years.

Mr. Casey began by reviewing significant achievements from David Gavin's tenure, 1998 to 2000. ***(See Appendix V, PowerPoint.)*** Two of the largest systems, the IAFIS system and NCIC 2000 went live back to back during this time. Numerous recommendations were made related to the NCIC 2000, however Mr. Gavin was most proud of was the work on XML. The IAFIS Interface Evaluation Task Force was established and multiple recommendations came from this task force regarding latent capabilities, interstate photos, rap sheet standardization, and fingerprint transmission specifications. The NICS sanctions framework was one of Mr. Gavin's most meaningful CJIS APB achievements and the encryption standards and establishment of background check policies with regard to individuals with access to systems.

Mr. Casey continued with the significant achievements during his tenure from 2000-2004. ***(See Appendix W, PowerPoint.)*** There were 440 recommendations during that four-year period. Two things happened back to back. The first was the transition between Director Freeh who served as the FBI Director from 1993 until June 2001 to Director Mueller who replaced him on September 4, 2011. Then the events of 9/11 happened. The CJIS APB went from providing input on systems like the NCIC and the IAFIS, to supporting law enforcement as they dealt with the new issues of terrorism. The CJIS APB established polices regarding states transitioning to the NCIC 2000. He noted, Mr. Bonino did much of the work in getting these huge systems going, however they went live under Mr. Gavin, and were maintained under Mr. Casey's tenure as CJIS APB Chair. Design review for the NGI also began during this tenure.

Mr. Lesko introduced Mr. Paul Heppner as the next speaker. ***(See Appendix X, PowerPoint.)*** Mr. Heppner served as the Georgia CJIS Systems Officer from 1993 to 2009. He served on the CJIS APB beginning in 2000 and was elected chair in 2006, serving through 2008.

Mr. Heppner reminded the group it is important to remember those tangible things that are hard to measure. He said we cannot measure how much mayhem and carnage has been averted every time a criminal is arrested because of these systems. Mr. Heppner reviewed the significant achievements recommended during his tenure. In conclusion, Mr. Heppner said he was honored to serve on this APB and wished them luck going forward and accomplishing many more things in the future.

Mr. Lesko next introduced Colonel Steve Cumoletti who served with the New York State Police for more than 33 years. He served two terms as the APB Chair from 2008-2012. ***(See Appendix Y, PowerPoint.)***

Colonel Cumoletti said that during his term there were 359 recommendations, which included the endorsement of significant Warrant Task Force recommendations. The evolution of the N-DEx was a huge topic. The CJIS APB explored and embraced a variety of methods for agencies to integrate their systems into the N-DEx.

Mr. Lesko introduced Captain Tom Turner who served at the Virginia State Police for 50 years. He served as chair of the APB from 2012 -2016. ***(See Appendix Z, PowerPoint.)***

Captain Turner said he was pleased to have been a part of the CJIS APB and meet the people he had. During his term, there were 224 recommendations and he highlighted the significant achievements. Captain Turner commended the audience/vendors who take their ideas and develop these processes as well as the people that do the research. He said being a member and a part of this organization was one of the most important things in his life. He asked them to keep up the good work and to remember, if you want to go fast, go by yourself, if you want to go far, go as a group.

Mr. Lesko then introduced Mr. Jack Donohue who served over 30 years with the New York City Police Department. He was a director appointee to the CJIS APB and assumed the chair's role from 2016-2018. ***(See Appendix AA, PowerPoint.)***

Mr. Donohue spoke on the importance of being vocal and speaking up in the process, whether in the working groups, task forces, or subcommittees. He said this is the only way we accomplish what we need to accomplish. Collaboration brings people together, builds trust, and forms relationships. Mr. Donohue shared at one point they almost lost the charter for the APB but after numerous phone calls to high-level people and because we had a relationship and trust, we were able to salvage the charter. Some of the significant achievements during his tenure included establishing a policy to use N-DEx as a NICS resource, and standardizing N-DEx audits to ensure the system was reliable. With regard to NCIC, the CJIS APB continued to establish requirements for N3G. He said while his term only had 94 recommendations, the work of the N3G Task Force probably generated hundreds of hours of work and hundreds upon hundreds of individual requirements. He recognized the incredible work Mr. Pettengill and the people on the task force did.

Mr. Donohue said with regard to the *CJIS Security Policy (CSP)*, is one of those items that will be on the agenda for perpetuity, because of the need for security related to trust in the availability and reliability as a system. It will always be an issue requiring continuous improvement.

As for the NICS, he said they strengthened the need for a packed record to ensure there is as much valuable information as possible for law enforcement and the FBI to make good recommendations regarding people who should or should not possess weapons. Lastly, in regard to the NGI, they established required training for face recognition searches through the NGI Interstate Photo System and endorsed moving forward on iris recognition technology. He said make no mistake about the importance of policy before running forward with embracing new technologies.

Mr. Donohue shared a quote attributed to Ben Franklin, "If we are all thinking alike, then no one is thinking". He charged the CJIS APB to be thoughtful about what they do and how they embrace policy, because it matters.

Mr. Lesko said a constant presence was an individual who always introduces himself as a friend of CJIS, former Assistant Director Dave Loesch. Mr. Loesch retired from the FBI after a distinguished career of more than 29 years. He served as the DFO in 1998. Unfortunately, he was unable to attend but provided comments to share with APB attendees. Ms. DelGreco read his comments. ***(See Appendix BB.)***

Mr. Lesko then opened the floor for comments. Mr. Bonino mentioned Judge Manuel Real who served from 1976 to 1994 on the NCIC APB and chaired the Sanctions Committee for many years. He said he was an institution and strong leader who was concerned that the FBI's fingerprint Identification capability needed some work and pressed hard with Director Sessions to do something. This resulted in both the state liaison conference in 1988, which generated the Inspection Division sending three agents out for a whole year to research this issue with the police departments. Then in 1989, Director Sessions attended the NCIC APB meeting to ask the APB to provide advice on identification services and more. He asked that a committee come to Washington for a week to provide advice and guidance. Mr. Bonino believed Judge Real deserved a tremendous amount of credit in the background for having done what he did to enhance fingerprint identification. He said Judge Real passed in 2019, at the age of 94.

Mr. Brandon Gray said as one of the newest members of the APB and a police officer for the last 27 years, he wanted to recognize those that came before him and thank them for paving the road.

Mr. DeLeon provided the following comments. He said the products and benefits resulting from this board are officer safety, protection of our citizens, protection of our communities and our nation, intelligent policing, proactive posture for law enforcement, preventing acts of violence, global awareness, projecting crime trends, and trust. He said if you think about our technology improvements, like radio transmissions versus the Mobile Data Terminal's we work with today, CJIS systems promote urgency and speed, Be on the Lookout, AMBER Alerts, silver alerts, all those things that we take for granted. He said the actions of the CJIS APB and commitment to this board save lives and protect our nation. He closed by thanking the APB for their constant pursuit of efficiency and thanked them for their partnership on behalf of the FBI, specifically the CJIS Division.

APB ITEM #18   Chairman's Report on the Security and Access (SA) Subcommittee

Mr. Bradley D. Truitt, Tennessee Bureau of Investigation, and Chair of the SA Subcommittee presented this agenda item. ***(See Appendix CC, PowerPoint.)***

Mr. Truitt advised the subcommittee agenda included three action topics, six informational topics, one action item, and one ad hoc issue. He thanked Ms. Cindy Johnston, who prepared the report, Mr. Chris Weatherly and the Information Security Officer (ISO) Program Office (PO) for preparing the topic papers, providing information to the SA Subcommittee, and answering their questions. He also commended the SA Subcommittee for their work addressing many of the technical topics.

He then provided an update on a couple related efforts. The CJIS APB chair and vice chairs are close to establishing the interpretive task force discussed at the previous CJIS APB meeting. The planning for the *CSP* modernization effort is underway. He advised more information should be presented at the next meeting.

Mr. Truitt briefed on Issue # 1, Action Item Review. The ISO PO accepted an action item during the spring 2019 SA Subcommittee meeting to obtain the FBI's interpretation of the changes made to the CSP, Section 4.1, regarding the protection of criminal justice information (CJI) indirectly released into open judicial proceedings. Specifically, the ISO PO was asked to clarify the timeframe in which CJI remains under the protection of the courts after adjudication. The revised language approved by the CJIS APB in June 2018, states the intent of the *CSP* is to ensure the protection of the aforementioned CJI until the information is released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; or released in the interest of public safety), purged, or destroyed in accordance with applicable record retention rules. He advised the language in question is: CJI introduced into the court system pursuant to a judicial proceeding and can be released to the public via a public records request is not subject to the *CSP*. The FBI informed the subcommittee that discussions were underway within the DOJ, and additional information will be provided once it becomes available. This topic was accepted as information only.

The following information only topics were discussed at the SA Subcommittee meeting. Issue #2 provided an update on the activities of the task forces under the SA Subcommittee. Issue #5 informed the subcommittee of the FBI's cloud implementation status and future plans. Issue #6, was a discussion on the different implementations of *CSP*, Section 5.12 relative to background screening requirements for cloud service provider staff. Issue #8, was a review of the August 2019 ISO Training Symposium held in conjunction with the working group meetings in St. Louis, Missouri. Issue #9 was an informational briefing on how risk-based security assurance may be accomplished, and Issue #10, was an update on the LEEP and other services managed by the FBI's Online Services and Operational Unit.

SA Issue #3 Mobile Device Management (MDM) Requirements in the *CSP*

Mr. Truitt advised this topic request was for clarification to the *CSP* to more clearly depict whether the service provider or the user agency bears responsibility for complying with the MDM requirements for direct access to CJI. In limited cases, the interpretation of the *CSP*, Section 5.13.2, as it is currently written, has placed the responsibility of ensuring compliance with MDM requirements on the service provider, allowing direct access, rather than the user agency. The CJIS Division and the SA Subcommittee agree this interpretation is inconsistent with intent, spirit and long-standing audit practices which hold the user agency responsible.

The SA Subcommittee made two motions on this issue. The subcommittee debated some of the specific wording and amended Option 1 to include the word directly, and then include in the *CSP* modernization new requirement options which include, but are not limited to, containerization, application virtualization, and secure web servers. However, during their discussion, the subcommittee determined and/or language could result in the user agency placing responsibility on the device owner and vice versa, rendering the requirement impossible to audit. The subcommittee voted down that motion and presented Option 3, which added the word directly, but removed and/or device owners.

APB MOTION: The CJIS APB moved to accept Option 3 as follows:

5.13.2 Mobile Device Management

User ~~A~~*a*gencies shall implement the following controls when ***directly accessing*** ~~**allowing**~~ CJI ~~**access**~~ from devices running a limited-feature operating system:
Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

SA Issue #4 *CSP* Advanced Password Standards

Mr. Truitt advised the purpose of this topic was to propose modifications to the advanced password standards in *CSP* Section 5.6.2.1.1.2 to align the length and expiration requirements with NIST 800-63B. The NIST advanced password standard calls for adopting a non-expiring 8- to 64-character password, and the password should be compared against a list of banned passwords. The June 2018 APB approved the SA Subcommittee's recommendation to set the minimum character limit to 20, and to expire the password yearly. The rationale for the 2018 motion was the absence of a clear method of checking passwords against a banned password list, and concern that an 8-character password may not be sufficiently stringent. Therefore, this topic was brought back to the subcommittee to consider updating the *CSP policy* to reference a NIST-recommended website containing a list of breached passwords, require agencies to maintain a listing of a minimum 1,000 banned passwords, reconcile directory services against the banned password list, and reconsider adopting the 8- to 64-character password length with no annual password expiration as recommended by the NIST.

One member noted this was a recent decision as far as the CJIS APB endorsing the current polices, and there hasn't been an update or change in the NIST standards. He asked what prompted this topic to come back through the Advisory Process so quickly, resulting in four working groups and the CJIS ISO PO endorsing Option 2. He then asked what information the SA Subcommittee had access to that the Working Groups did not that caused the subcommittee to recommend no change, while four of the Working Groups recommended Option 2.

Mr. Truitt responded he believed it came back up so quickly because there was a new idea on how to access, or to provide this banned password list. He relayed the subcommittee debated the topic, trying to align these advanced password standards with the NIST policy. The NIST guidance, the implementation of the banned password list and how it is written would be difficult for many agencies. He stated that is what prompted the subcommittee to consider revisiting this topic with the exploration of the modernization piece.

Mr. Megna advised this met the historic minimum requirement for bringing a paper back through the Advisory Process. Mr. Weatherly added they decided to bring the paper back through the process because when it was passed by the CJIS APB in 2018, there was some resistance to going stronger than the NIST standards. He waited the appropriate amount of time to bring it back through the Advisory Process, to more align the *CSP* with the NIST recommendations. He stated another reason to bring it back through the process was while there was a requirement to have a banned password list, there was no direction on how many must be on this banned password list, or how to get the authoritative source of truth for that password list. He advised the SA Subcommittee did not access to the working groups did not have. There was some concern with including the authoritative source of truth, and having the banned password list as a shall statement versus having it in the appendices. He advised this was one item of contention from the briefings he presented to the working groups, the SA Subcommittee, and the Compact Council. Another member commented his working group had voted for no change because of the reason Mr. Weatherly brought up, the actual URL link inside the policy, and the understanding that 1,000 passwords did not make much sense, since the website has five billion passwords that have been compromised. Mr. Truitt stated that was why the subcommittee decided on no change, as well; but it was mostly around the issues and implementation of the password list.

A member asked Mr. Truitt if the SA Subcommittee would re-examine this as they work on refreshing the policy. Mr. Truitt responded, with the two efforts underway, specifically the modernization effort, they will bring it back because it does align with that NIST standard. He also noted as they get into data categorization, there would be an opportunity to come up with a way to implement the aligned NIST standard much easier than they currently can with the way the security policy is constructed. Mr. Weatherly pointed out this has to do with advanced password standards. The basic password standards are still within the policy and agencies are compliant if they continue to follow those password standards as well.

This topic was taken as an action item to take back to the SA Subcommittee and the Working Groups to see how they can better align the NIST standards with the *CSP*.

ACTION ITEM: The CJIS APB requested this topic be brought back thru the process to see how password standards can better align with the *CSP*.

SA Issue #7 Audit of Vendor Contracts with Authorized Criminal Justice Agencies

Mr. Truitt advised the purpose of this topic is to inform and elicit feedback on the CJIS Division's plan to include vendor contracts as part of the criminal justice information technology security (ITS) audit. He noted this issue was an external request for the CAU to review vendor contracts for appropriate *CSP* language during the ITS audit. The rationale for the request was specific language in the contract would ensure vendors were truly CJIS contractors, enabling security issues to be more effectively addressed. Additionally, the issue suggests adding a template previously included in *CSP*, *V*ersion 4. The template has been helpful in creating appropriate contract language. He advised the CJIS Division deemed this request a change to practice rather than policy as the requirement currently exists, but the audit only extends to a review of the signed certification page of the CJIS Security Addendum for each unescorted contractor performing a criminal justice function on behalf of criminal justice agencies. The audit questionnaire was revised to include a review of the entire contract to confirm reference to the *CSP*, and that the contract language states the purpose and scope of services that will be provided by the contractor.

One member asked why the subcommittee felt this should be treated as a new policy, given it is existing policy. Mr. Truitt responded that was part of the debate, but they has come up with a new way to look at it. It is existing policy, but the CAU has not reviewed it that way previously. It was decided doing it this way would give agencies time to adjust to it. Another member commented when a new policy is established, there's usually a zero cycle where it is looked at, but is not sanctionable. While it existed in policy, it was not looked at, so the agencies were not expecting it to be looked at. He commented an agency couldn't suddenly do a new contract with their vendor just because the audit unit is looking at it. This gives them a warning that they have from now until October 2020 before it becomes sanctionable. This provides agencies an opportunity to renew their contract and add the appropriate *CSP* language, if necessary. Another member voiced disagreement with the philosophy. She commented there is a lot of policy that is not looked at every year at every audit. Every three years she is audited, the auditors look at something different. She stated it is wrong to say it is new and should not be considered as policy as it has been standing. Just because the audit unit chose to look at it this time, but not last time, does not make it new policy.

A member stated this issue was raised by his state. They changed the way they were handling vendor backgrounding, and in the process, they started looking at contracts. There were large national companies that had no contract containing the correct language pursuant to the *CSP*. Many of these companies had been doing business handling their state CJI for decades. While he was concerned this was an existing standard in the policy, he also understood it would take time for people to get used to this. He hoped businesses that store CJIS data are given three years. He noted three years is not much time in the contracting world.

APB MOTION 1: The CJIS APB moved to accept Option 1A: CAU will evaluate the existing contractor agreement requirements as "new policy". (The requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)

APB MOTION 2: The CJIS APB moved to accept Option 2A: Include the Attachment 1 (previously included in the *CSP* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Mr. Truitt advised Option 2A called for adding the template in appendix H, but makes no changes to the policy.

Mr. Truitt relayed the SA Subcommittee discussed one ad hoc topic, which was to gauge the committee's interest in a topic paper for the spring 2020 working group meetings. The discussion was around a request from the National Association of State Chief Information Officers for CJIS and the Internal Revenue Service to work together to align three security controls: frequency of training, account inactivity lockout, and audit records retention. So the concern is in situations where state information technology consolidations have resulted in the Health Insurance Portability and Accountability Act, or HIPAA, the Internal Revenue Service, and CJI all becoming collocated. Due to the different categorizations and purposes of the data, the SA Subcommittee did not express an interest in moving this request forward at this time.

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

This topic was presented by Ms. Carol Gibbs, Acting Chair of the CE Subcommittee, Illinois State Police.

Ms. Gibbs acknowledged it was former CE Chairman, Mr. James Slater's idea to provide a handout of the results of the CE Subcommittee meeting prior to the presentation of the report. She commended the CAU and the CE Subcommittee for the volume of work they do in preparation for the meeting so that the subcommittee can review and come to conclusions within a one-day meeting. She then presented the following findings.

Follow-up to Governor/Attorney General/City Mayor Letters

Alabama (IT)

Arkansas (NSOR) Call/Close or Follow-up
Florida (IT)
Maine (NCIC)
Minnesota (IT)
Montana (IT)
Nebraska (IT) Call/Close or Follow-up
Nevada (IT) – elevation
New Mexico (IT) Call/Close or Follow-up
New York (NCIC, NSOR, IT)
North Carolina (IT)
North Dakota (NSOR) Call/Close or Follow-up
Ohio Bureau of Criminal Investigation (NSOR, IT, NICS - F/U to superintendent) – Elevation
Oregon (NSOR)
Puerto Rico (NCIC) – Elevation
Rhode Island Repository (IT)
South Carolina (IT)
South Dakota (NSOR)
Virginia (NSOR)

Closure to Governor/Attorney General/City Mayor
South Dakota (IT)
Vermont (IT)
West Virginia (IT)

Follow-up to CSA Head
Alaska (IT)
Idaho (IT)
Indiana (IT) – Elevation
Kentucky (IT) Call/Close or Follow-up
Louisiana (NSOR) Call/Close or Follow-up
Maryland (IT)
Massachusetts (NCIC, NSOR, IT, NICS) – Elevation
Michigan (IT) Call/Close or Follow-up
Minnesota (IT) – Elevation
Missouri (NCIC, NSOR, IT)
Montana (NSOR, IT)
Rhode Island (IT)
South Carolina (NSOR and IT)

Closure to CSA Head
Alaska (NCIC)
Puerto Rico (IT)
Tennessee (IT)
Utah (NCIC)

Follow-up to CJIS Systems Officer (CSO)/Bureau Chief/POC

Administrative Office of the United States Courts (NCIC)
Arkansas (NSOR)
Arkansas SIB (NIS)
California (NSOR, IT) Call/Close or Follow-up
Colorado (NCIC, NSOR, IT)
Connecticut (IT, and NIS Follow-up to Repository POC)
Florida (NSOR, IT)
Guam (NSOR, IT)
Hawaii (NCIC)
Illinois (NCIC, NSOR, IT, NIS)
Iowa (NSOR, IT)
Kansas (IT)
Maine (NCIC)
Massachusetts State Identification Bureau (IT, NIS Follow-up to Repository POC)
New Hampshire (NCIC, IT, N-DEx, NIS)
New York (NCIC, NSOR, IT)
North Carolina (IT, NICS)
Ohio Bureau of Criminal Investigation (NSOR, IT, NIC Follow-up to Superintendent) – Elevation
Oregon (NSOR, IT)
Pennsylvania (IT)
United States Airforce Office of Special Investigation (NCIC, IT)
Utah (IT) Call, Close or Follow-up
Virginia (NSOR, IT) Call/Close or Follow-up
Washington (IT)
West Virginia (NCIC, IT)
Wisconsin (IT, NSOR) Call/Close or Follow-up

Closure to CSO/ POC
Administrative Office of the Unites States Court (IT)
Arkansas (NCIC)
District of Columbia (NIS)
Illinois (N-DEx)
Indiana (NSOR)
Iowa (NICS, N-DEx)
New York (NICS, N-DEx)
North Carolina (NCIC, N-DEx)
Ohio (NCIC)
Oregon (NCIC)
Pennsylvania (NSOR)
U.S. Department of the Army (IT)
U.S. Department of Justice (NCIC)
U.S. Naval Criminal Investigative Service (NCIC)
Virginia (NCIC, NICS, N-DEx)
Washington (NSOR, NICS)
West Virginia (NSOR, NICS, N-DEx)

Commendation to CSO/State Identification Bureau Director/POC

Arkansas (IT, NICS, N-DEx)
Arkansas SIB (IT)
Illinois (NICS)
North Carolina (NSOR)
Virginia (NIS)

APB MOTION: Accept the actions of the CE Subcommittee as presented.

APB ITEM #20 Chairman's Report on the NICS Subcommittee

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

She began by thanking the NICS Section for all they do to assist the NICS Subcommittee and to process background checks in a timely manner. The NICS Subcommittee met October 10, 2019, in Norfolk, Virginia. She stated there were no voting topics this round, but there was a lot of discussion with an agenda that included much feedback to the NICS Section.

Ms. Rolin briefed on the informational topics presented to the subcommittee, they included race code standardization, expansion of the Protection Order File (POF), the NICS audit update, and an update on the LEEP. She did not provide a brief on these topics, but she thanked the FBI CJIS Division, the NCIC Subcommittee, and the Office of General Counsel for their work on expanding the POF. She noted the NICS audit issues routinely found were related to Immigration Alien Queries, use of proper purpose codes, and multiple drug use issues.

She briefed on NICS Issue #1, which covered old action items. There was an update on identifying multiple jurisdictional agencies. The NICS is currently researching multiple jurisdictional agencies and has identified approximately 760 agencies during that research. The NICS is establishing a POC for these agencies to contact when additional research is required for locating needed information. The NICS has been advised by the legal administrative team that the section cannot provide the multi-jurisdictional agency information as a resource to external agencies. She advised a paper on the reconceptualization of the structure of the NICS Indices would be presented at the spring 2020 round of meetings.

Another topic heard by the subcommittee was the process of receiving technical updates. The subcommittee asked the NICS why they are receiving technical enhancement documents and not Technical and Operational Updates. The subcommittee asked if the NICS could reevaluate the process of receiving technical updates to bring everyone into alignment and harmonization so they will receive the updates in the manner that everyone else is as far as other updates. In order to identify any changes in the Interface Control Document, a side by side comparison of the old and new are needed.

NICS Issue #2 regarded information on NICS enhancements. The subcommittee received information on the POC states' access to the complete III, or criminal history record. The BSS began a new study to take an in-depth look at any inconsistencies between state and federal records and the reason for those inconsistencies. The subcommittee also discussed access to the Disposition Document File (DDF). The subcommittee was advised authorized local, state, tribal, and federal agencies could access the DDF via existing CJIS systems by entering a separate query. She relayed a task force has been developed consisting of staff from the NICS, the BSS, and the ITMS to review information retained in the DDF and any potential legal issues that may arise from that. The subcommittee also received an N-DEx update with some discussion about the N-DEx Program's use as a secondary search for NICS background checks. She advised both programs are working towards implementation. Due to the increase in workload and needed staffing, the deployment of the N-DEx for secondary searches will take longer than originally expected.

NICS Issue #3 was a NICS Operational Update. One of the issues discussed was about how agencies and regions are notified of Alcohol, Tobacco, and Firearms (ATF) and ATF-sponsored Federal Firearm Licensee seminars. These seminars are sponsored by the ATF, who is responsible for planning and scheduling those seminars. Ms. Stely, ATF, indicated she would follow up with the field division for outreach. The NICS Section will coordinate with the ATF to discuss ways the ATF and/or the NICS Section can notify state POCs when seminars will be hosted in their area. She stated these are very beneficial seminars. Usually the state is invited to speak at these regional ATF meetings. Another update presented was the Fix NICS Act of 2018 and the CJIS Division's role in supporting the DOJ as well as federal and state agencies. A strategic plan has been developed for outreach to federal and state agencies to assist in addressing questions and concerns agencies may have regarding the development of implementation plans and updates. She relayed information should be coming out in 2020. She advised a NICS User Conference is tentatively scheduled for August 2020, with a tentative location of Columbus, OH.

NICS Issue #8 involved discussion on some ad hoc topics. One topic was Identification for Firearm Sales (IFFS) Marketing. The NICS Section shared some of the standards and benefits of using the IFFS Program on state criminal history records and the current flag settings. Twenty-three states are currently participating in the IFFS program. Another ad hoc topic was NICS downtime. A subcommittee member inquired about receiving quicker system down or degraded notice. Messages are received; however, sometimes they are not received timely enough. Another ad hoc discussion was related to federal firearm restrictions. One hurdle is the NICS is not able to deny on firearm restrictions that exist during active federal probation. There has been no avenue to deny previously; therefore, the NICS Section has historically canceled transactions when a federal firearm prohibition exists. She advised a topic paper will be prepared regarding this issue for the spring 2020 round of meetings.

APB ITEM #21 Rapid Deoxyribonucleic Acid (DNA) Update

This agenda item was presented by Mr. Thomas Callaghan, FBI Lab Division **(*See Appendix EE, PowerPoint.*)**. He briefed on the first two milestones of rapid DNA. In 2008, the joining of the Department of Defense, the DOJ, the FBI, and the DHS to come up with a set of standards, or eight requirements, and the use of the CODIS led to the development of the technology that is hoped to spawn a booking station industry. The second milestone was the recommendation by the December 2009 CJIS APB that the FBI establish a Rapid DNA Task Force. The recommendations that have come out over the last ten years drove the development of rapid DNA.

In September 2019, six federal offenders were uploaded into the national database in the Washington Field Office, and if it wasn't for the Advisory Process and the Biometric Center of Excellence, they would not have this technology. But a change in federal law was needed after they had the technology. Prior to August 18, 2017, federal law required all DNA profiles that went into the national database be developed in an accredited laboratory. Using rapid DNA after August 18, 2019 the FBI was authorized to issue standards and procedures for rapid DNA instruments to develop DNA profiles outside of an accredited laboratory. He advised they are currently in the pilot phase, and when the pilot phase is completed, they will be able to issue those standards and procedures.

In 2009, the last recommendation dealing with rapid DNA had nothing to do with the booking station. As the legislation moved forward, there was a lot of direct marketing from the rapid DNA manufacturers to police departments and police agencies to use rapid DNA for crime scene analysis. He advised more than 1,000 recommendations have been made to the FBI. The APB requested the FBI educate state and local law enforcement on federal law and what was and was not allowed with regard to rapid DNA and the booking station. The Accelerated Nuclear DNA Equipment (ANDE) 6C, is approved by the FBI for use in an accredited laboratory for reference samples. A convicted offender or arrestee, if analyzed with this instrument in one of the 202 CODIS laboratories, can go directly into the national database. He noted it is fast, but expensive. Kentucky is currently the only state using this and on a very limited basis. He advised nothing has been approved for routine use.

Mr. Callaghan relayed the CODIS and the national database modeled its governance in line with the structure of the Advisory Process. Federal law in 1994 established the national DNA index system, and it required the FBI to have a DNA advisory board similar to the CJIS APB. Members were appointed by the director of the FBI, given a five-year term, and a Nobel laureate geneticist was the original chair. Since they didn't get their work done in five years, Director Freeh extended it for one year. The last FBI recommendation was to sunset and create the scientific working group on DNA analysis.

In 2010, Mr. Callaghan went to Australia to speak about the success of the international database. He told them about the CJIS APB, which the DNA community emulated for their governance. Laws, standards, and documents make up the foundation. Activities by people are the pillars and then they have the CODIS unit or the FBI CJIS Division that protects the national database. The CJIS APB created and paved the road for the national DNA database, and what they have done over the past ten years is protect genetic privacy of arrestees and convicted offenders, and integrated that into the Advisory Process.

The schematic of the criminal justice system is if you collect a conviction, you do not collect everyone that enters the criminal justice system. If you collect arrests, you obtain more people who may otherwise fall through the cracks. This is the same idea with arrestee DNA. In 2008, the NIST was a four-hour process to amplify DNA and was converted to 22 minutes.

Over the last decade, they were able to eliminate the mailing of a million samples each year and process those in the booking station. When there is a hit against the DNA Index of Special Concern, there is an immediate notification sent to the arresting agency and the booking agency, if it is different. The investigating agency is able to contact the booking location for a status of that individual. Some jurisdictions do not have many violent crimes and don't have experience with the CODIS so they want the CODIS laboratory involved as a safety net for law enforcement.

The DNA Index of Special Concern is based on the RISC. There will not be many hits but every arrestee who has rapid DNA will be searched against every unsolved crime in the United States within 24 hours. The DNA Index of Special Concern is limited to homicide, sexual assault, kidnapping, and terrorism investigations. If it is a perfect match, then that information is sent. It's not only lights out rapid DNA analysis, its lights out DNA notification. They would like to increase their locations to put reference samples in the national database from fifty-four to thousands.

The unsolicited DNA notification was based on a want or warrant notification. The issue is that information has to be collected electronically, and 48 states and the federal government still collect and mail inked fingerprints for a DNA sample. Mr. Callaghan said they need to go paperless in booking stations. When the task force was created in 2010, law enforcement had requirements: do not tell us how to run our booking stations, no new numbers, no new networks, set requirements and let us determine how to meet them, and protect genetic privacy. The task force decided that they would enter the DNA Index of Special Concern information from the CODIS laboratory into the national database that resides at CJIS. They would use the national fingerprint submission network to branch off to the state identification number, link it to the swab along with other information, and put it into the rapid DNA instrument. It's the state's responsibility to obtain the information from the local booking station, deliver it to the CJIS switch, and from there it will be placed into the national database. There will be no need for new networks and the notifications will be pushed out over Nlets. The current rapid DNA Instruments are an early prototype from IntegenX, the ANDE 6CA, and the IntegenX RapidHIT. A test of the system was performed in April 2019.

The DNA Identification Act and the Advisory Process began 25 years ago. This process started 50 years ago. Twenty-five years ago, there was nothing in CODIS and today they make about 130 associations a day. Last year they aided over 50,000 investigations. The federal law passed two years ago for Rapid DNA is the bridge taking DNA into the booking station. In 2013, the Supreme Court ruled that taking DNA from an arrestee for a serious crime was constitutional. There are 30 states, the Army, federal law enforcement, and the FBI who have the authority to collect an individual when they are arrested for a serious crime. Mr. Callaghan's PowerPoint provided a breakdown on the 30 states. The green states can collect and analyze as soon as the sample is collected from the arrestee. The red states can collect, but they cannot analyze until there is an indictment. The Supreme Court ruled that taking DNA at arrest is an administrative procedure just like fingerprints and booking. There are seventeen rapid DNA states available.

Mr. Callaghan asked Mr. Lesko if he would like to comment about Texas becoming a green state as of September 1, 2019. Mr. Lesko remarked that since September 1, 2019, they have had 16 CODIS hits for arrest-collected DNA. The first one, September 1, 2019, was on an individual that was arrested for burglary with a hit against a sexual assault. On September 5, 2019, they had an arrest for theft over $2,500 that hit on a CODIS entry for murder. He thought the ability to collect arrest DNA coupled with rapid DNA allows for adjudication of those individuals while they are in jail. By having the rapid DNA technology in place at the booking station, it will arm law enforcement with the ability to incarcerate or retain those individuals and ensure they receive justice.

Mr. Callaghan advised, the arrest offense is what triggers the collections. The states treat juveniles and misdemeanors differently. There are other issues around arrestee DNA that don't exist with mug shot and fingerprints. He said they are running a national database where 20 states do not collect and 13 states do collect at arrest. This is like collecting fingerprints and mug shots but not being able to use them until the individual is indicted. He said the green states are our pool and the way they look at fingerprints in the booking station is identity verification that answers these questions: Have we seen you before? Has law enforcement seen you before? Who are you? Are you who you say you are? It then searches the unsolved latent file. DNA is identity discovery. We know who you are but what have you done. Where have you been? That is the DNA modality. There are five states participating in the rapid DNA pilot, Arizona, California, Florida, Louisiana, and Texas.

He advised rapid DNA could be a problem if not used in a responsible manner with regard to crime scenes. They do not want cases to be jeopardized, so when Congress passed the law, the report stated that at present rapid DNA technology can only be used for identification purposes, not crime scene analysis. There are many challenges with mixtures and low quantity DNA. There was a movement for the FBI to set CODIS free and lessen the requirements for crime scene rapid DNA direct access to the national database for one-time search.

In March 2018, the FBI had a national meeting, which involved IACP, MCCs, NSA, Major County Sheriffs, the APB, NIST, and Scientific Working Group on DNA Analysis Methods. At this invitation only meeting, the FBI announced they would set up a rapid DNA task force to address nonCODIS rapid DNA analysis of crime scenes. Task Group 1 will drive the development and work with industry and law enforcement to develop an expert system for looking at DNA analysis in the booking station and transport it over to crime scenes outside of a laboratory. Task group 2 will bring all of the people currently using rapid DNA in nonCODIS applications together with the National District Attorneys Association, the ASCLD, and the CJIS APB. This group compiled a document, which is posted on the FBI CODIS site on the Rapid DNA page. This document provides considerations for law enforcement agencies who want to use rapid DNA on crime scenes outside of CODIS. When the law was passed in 2017, the FBI had three steps to get rapid DNA into the national database. They have accomplished step 1 and 2, and in doing that they realize they need to address the crime scene issue creating dual paths. For crime scene analysis, two task groups have been established within a task force. The next step over the next number of years is to move forward to crime scene in the booking station.

The initial interactions between the DNA community and the APB occurred in 1998 or 1999, and it was to get a DNA indicator put on a missing person file in NCIC. That was the first time the Lab Division began attending these meetings, and they have been involved for 21 years.

Mr. Callaghan said they gave briefings with CJIS background slides on rapid DNA. This was the wake-up call that the CJIS APB put forward to let industry and law enforcement know they were serious about rapid DNA. Ten years ago, there were six companies involved in rapid DNA and only two of those companies are still around today. There is an existing rapid DNA task force, however a number of people have retired or left the task force. There is an action item to explore expanding the task force to continue with rapid DNA in the booking station and with crime scene rapid DNA.

Mr. Callaghan stated rapid DNA would not currently exist without the Advisory Process. He opined that state criminal history needs improvement. There are many states that want to use rapid DNA as another justification to improve or enhance their IAFIS systems.

Mr. Callaghan concluded his presentation by acknowledging several individuals who significantly contributed to rapid DNA over the past decade.

ACTION ITEM: The CJIS APB recommended the FBI stand up the Rapid DNA Crime Scene Task Force as a logical extension to the Rapid DNA Task Force under the umbrella of the CJIS APB's IS Subcommittee.

APB ITEM #22 ASCLD Update

This agenda item was presented by Mr. Bruce Houlihan, Director, Orange County Crime Laboratory and ASCLD representative on the APB. He briefed that crime laboratories across the country have experienced increased involvement in biometrics not only new modalities, such as face and iris, but also forensic operations for comparisons. Since their experience involves accreditation and the forensic operations they are used to with traditional disciplines, they are increasing their involvement in WatchNET.

The ASCLD recently published a status update on sexual assault evidence throughout the country. Approximately 90,000 sexual assault kits are untested and unsubmitted to laboratories across the country. They have been working with law enforcement to have these historical, legacy kits submitted and tested. A big part of this is the tracking and reporting of the status of these kits. Victims want to know the status of their kits, so IT services that provide that information, both at the state and local levels, are extremely important. Since most of these kits are still in law enforcement agencies, the ASCLD is trying to facilitate getting these kits to the crime laboratories a lot quicker, as well as disseminating information about the results of the kits. He noted tracking is done at the state, local, and federal levels. Tracking systems and analysis are mandated in some states. For instance, in California, the kit analysis is mandated within 120 days, and reported or submitted to the crime laboratories within 90 days. Typically, these mandates are non-funded, but they are considering deadlines for getting these kits done.

He advised ASCLD's relationships with the FBI and the CODIS are the most important they have in crime laboratories. With respect to rapid DNA, they appreciate the work the FBI is doing to ensure accredited crime laboratories are involved in using rapid DNA for crime scene evidence. The ASCLD is working with the FBI and preparing for crime scene evidence to be part of their rapid DNA programs in the next couple of years.

The ASCLD is involved not only with giving advice and consultations on the use of DNA in the booking stations, but they are also involved with mass disaster use. He stated an issue for ASCLD is the appropriate use of genetic genealogy information, which can also be used for cold cases. It is important for its integrity to be maintained as it is going to be used in court.

He advised one of the most critical issues they are dealing with is the call for probability studies and statistical analyses on the work they are doing. Their ability to give historical conclusions on pattern matching disciplines, specifically related to firearms, fingerprinting, shoe prints and tire tracks, is being challenged by academic institutions and the judicial system. They are being asked to curtail the conclusions they traditionally have been able to give until they have the ability to demonstrate full probability with black and white box studies. He relayed there have been a couple of recent cases in firearms where the conclusions were disallowed. An identification was made by an examiner associating bullets and cartridge cases with firearms, but the judge disallowed the conclusions because there was no probability backing the specific conclusions. The analyst was only able to give results and not give an opinion about whether the bullet was associated with the firearm. The ASCLD's use of characteristic databases is being challenged until they can come up with these kinds of probability studies.

Chair Lesko stated Texas is confronted with the U.S. Farm Act, new legalization regarding hemp farming and the ability or inability by labs to be able to do quantitation of tetrahydrocannabinol (THC) levels within that plant material. Mr. Houlihan stated this is being seen across the board. Laboratories are not currently funded to do THC testing in plant-submitted material. There's a lot of discussion about dry weights and wet weights; what happens when hemp is transported across the borders; and inconsistent jurisdictional laws about the amount of THC content in the plant material. Mr. Houlihan commented progress is being made by some laboratories on methods, and some are getting to the point they are prepared to do this testing, if necessary. He noted there is some movement toward more logical laws on hemp versus marijuana. Chair Lesko predicted once the plant material issue is dealt with, consumables will be another issue to consider. Mr. Houlihan agreed with his prediction.

APB ITEM #23 IACP Update

This topic was not presented.

APB ITEM #24 Major Cities Chiefs Association Update

This topic was not presented.

APB ITEM #25 Major County Sheriffs of America Update

This topic was not presented.

APB ITEM #26 NSA Update

This topic was presented by Mr. Michael Brown, Director of Professional Development, NSA. **(*See Appendix FF, PowerPoint.)***

Mr. Brown provided an update, as well as some history, on the NSA. The NSA started in 1940 as a professional association dedicated to serving all sheriffs and its affiliates through law enforcement education and training, through the provisions of general law enforcement informational resources. The NSA's roots can be tracked back to 1888, when a group of sheriffs in Minnesota and surrounding states formed an organization, which they named the Interstate Sheriffs Association. The purpose of this association was to give opportunity for a wider, mutual acquaintance to exchange ideas for more efficient service and to assist one another in apprehension of criminals. The NSA has approximately 18 committees, one of which is the NSA CJIS committee, chaired by retired Sheriff David Goad from Maryland.

He noted during his 17 year affiliation with NSA, the association has supported numerous FBI CJIS projects; most notably the N-DEx. He advised former NSA Deputy Director John Thompson supported the NIBRS, and he had asked Vermont Sheriff Bill Bohnyak to work with CJIS to help make NIBRS successful.

He relayed one of the things the NSA can do better is to use their publications to get information out to its members. For example, they could publish success stories illustrating how biometrics have worked. He opined this could help push the charge for what they are trying to accomplish.

He advised retired Sheriff David Goad, the current chair of the NSA CJIS committee, asked him to provide information to the group regarding the NSA Law Enforcement Cyber Investigators Program. Their mission is to precipitate a more robust law enforcement response to cybercrime. They are interested in sustainable Software as a Service transaction platform for reporting cybercrime offenses and threat intel data, and for sharing that information with federal partners. The NSA also has a newly formed Unmanned Aircraft System (UAS) subcommittee. The first meeting of the UAS subcommittee will be at the NSA Winter Conference in February, 2020. He advised they are trying to establish a direct line of communication with the Federal Aviation Administration to prepare law enforcement for the challenges ahead as it relates to UAS and drones.

Recognition of Members

Mr. Lesko recognized Ms. Donna Uzzell, Florida Department of Law Enforcement and Mr. Wyatt Pettengill, North Carolina State Bureau of Investigation, both retiring. AD DeLeon presented both with a certificate recognizing their service.

Closing Remarks

Mr. Lesko concluded the meeting by thanking the CJIS staff for supporting the APB. He felt that Topics 16 and 17, which had to do with the evolution of the APB, and bringing in former members was a worthwhile accomplishment. The meeting was adjourned.

Intentionally Left Blank

APPENDICES

Intentionally Left Blank

Advisory Policy Board Roll Call

Atlanta, Georgia -- 12/04-05/2019

Name	Agency	Serving as a proxy for:	
Mr. Andrew R. Black	Federal Bureau of Prisons Washington, DC	Sonya Thompson	□
Mr. William G. Brooks, III	Norwood Police Department Norwood, MA		□
Mr. Michael M. Brown	National Sheriffs' Association Alexandria, VA		□
Mr. Kevin C. Cockrell	Montgomery County Attorney Mount Sterling, KY		□
Mr. Donald Conroy	National Targeting Center, Department of Homeland Security Sterling, VA		□
Mr. Dwayne D. "Rusty" Cooper	Kingman Police Department Kingman, AZ		□
Ms. Veronica S. Cunningham	American Probation and Parole Association Lexington, KY		□
Mr. William J. Denke	Sycuan Tribal Police Department El Cajon, CA		□
Mr. Edward J. "Ted" DeRosa	Colorado Bureau of Investigation Denver, CO		□
Ms. Carol A. Gibbs	Illinois State Police Joliet, IL		□
Captain B. Kyle Gibbs	Stillwater Police Department Stillwater, OK		□

Name	Agency	Serving as a proxy for:	
Major Brandon Gray	New Jersey State Police West Trenton, NJ		□
Mr. Jeremy Hansford	Ohio State Highway Patrol Columbus, OH		□
Mr. Darryl J Hayes	Connecticut Department of Emergency Services and Public Protection Middletown, CT	Not Attending	□
Mr. Bruce T. Houlihan	Orange County Crime Laboratory American Society of Crime Lab Directors Santa Ana, CA		□
Mr. Michael C. Lesko	Texas Department of Public Safety Austin, TX		□
Ms. Lynda G. Lovette	Baltimore City Police Department Baltimore, MD		□
Mr. Gary M. Lyons	Monroeville Police Department Monroeville, OH		□
Mr. Edward A. Mello	Jamestown Police Department Jamestown, RI		□
Mr. Maury Mitchell	Alabama Law Enforcement Agency Montgomery, AL	Not Attending	□
Ms. Kathryn M. Monfreda	Alaska Department of Public Safety Anchorage, AK		□
Ms. Leslie Moore	Kansas Bureau of Investigation Topeka, KS		□
Mr. Walt Neverman	Wisconsin Department of Justice Madison, WI		□
Mr. Scott G. Patterson	Talbot County State's Attorney Easton, MD		□

Name	Agency	Serving as a proxy for:	
Mr. Brian Pittack	Office of Biometric Identity Management - DHS Washington, DC		□
Colonel Edwin C. Roessler, Jr.	Fairfax County Police Department Fairfax, VA		□
Mr. Robert S. Sage	Augusta Department of Public Safety Augusta, KS		□
Mr. Charles I. Schaeffer	Florida Department of Law Enforcement Tallahassee, FL		□
Mr. Corey R. Steel	Nebraska State Court Administrator Lincoln, NE	Not Attending	□
Mr. Bradley Truitt	Tennessee Bureau of Investigation Nashville, TN		□
Mr. Brian Wallace	Marion County Sheriff's Office Salem, OR		□
Honorable Nathan E. White, Jr.	American Judges Association McKinney, TX		□
Mr. Anthony Wickersham	Macomb County Sheriff Mt. Clemens, MI		□
Mr. Scott Wilcox	New York State Police Albany, NY	James Slater	□
Ms. Kathy Witt	Office of the Fayette County Sheriff Lexington, KY		□

Intentionally Left Blank

Meeting Attendee List - Advisory Policy Board – December 4-5, 2019 - Atlanta, Georgia

Name		Agency/Company
Ali	Aamir	FreeAlliance, LLC
Brenda	Abaya	Hawaii Criminal Justice Data Center
Yusuf	Abdul-Salaam	DHA Group, Inc.
Melissa	Abel	Federal Bureau of Investigation
Scott M.	Adams	Unisys Corporation
Peter J.	Ahearn	Seneca Holdings
Kevin	Ahearn	Paradyme Management
William	Alderson	IntePros Federal
Albert	Alston	Microsoft
Christopher	Anderson	Unisys Corporation
Nichole	Anderson	GuidePoint Security
Chuck	Archer	Grabba
Jennifer A.	Armstrong	U.S. Marshals Service
Jessica	Augustine	U.S. Immigration and Customs Enforcement
Zalmai	Azmi	IMTAS
Joseph M.	Baker	Federal Bureau of Investigation
Christopher	Barker	Griaule Corporation
Charles S.	Barnett	IntelliWare Systems, Inc.
Fiona	Barshow	Koniag Government Services
Brian	Bear	Accenture Federal Services
Nathan	Beckham	Microsoft
Andreas	Beebe	Nutanix
Ajay	Bhatia	IMTAS
Olivia	Blackburn	DMI
Amy	Blasher	Federal Bureau of Investigation
Kenneth	Blue	Tennessee Bureau of Investigation
Elizabeth	Bodell	ServiceNow
Buffy M	Bonafield	Federal Bureau of Investigation
Katherine	Bond	Federal Bureau of Investigation
Joseph P	Bonino	Los Angeles Police Department - Retired
John	Boyd	Perspecta
Keri	Brady	CBP
Tracy	Brown	Noblis
Keith	Bryars	NTT Data Federal Services
James W	Buckley Jr.	Computer Projects of Illinois
Jay	Burke	Huntington Ingalls Industries
Marion	Burrows	ATF

Tom	Bush	Tom Bush Consulting, LLC
Larry	Byers	Amazon Web Services
Thomas	Callaghan	Federal Bureau of Investigation Lab
Frank	Campbell	Highland Strategies
Melissa	Carson	Unisys Corporation
William	Casey	ANDE
Alvaro	Castillo	ManTech International Corporation
Zackery	Chang	Kroleo
William D.	Chase	EnProVera, Inc.
Barbara	Clouser	Federal Bureau of Investigation
Charles M. "Monty"	Coats, Jr.	South Carolina Law Enforcement Division
James	Coffee	Diverse Computing, Inc.
Todd	Commodore	Federal Bureau of Investigation
Joseph	Courtesis	IDEMIA
Tyler L.	Cox	Federal Bureau of Investigation
Kathy	Cox	DHA Group, Inc.
Steven F.	Cumoletti	New York State Police - Retired
Chad	Damerell	Cadence Group
Roy	Davis	Unisys Corporation
Dennis	DeBacco	SEARCH Group, Inc.
Kimberly J.	Del Greco	Federal Bureau of Investigation
Michael D.	DeLeon	Federal Bureau of Investigation
Brian	DeMore	U.S. Immigration and Customs Enforcement
Karen	DeSimone	NTT DATA
Kaustubh	Despande	IDEMIA Identity & Securit N.A.
Paul	DiPietra	NEC Corporation of America
Lorie	Doll	Federal Bureau of Investigation
John K.	Donohue	New York Police Department
Matt	Dryer	World Wide Technology
Jim	Dufford	Xcelerate Solutions
Jeff	Edgell	TMC Technologies
Mohamed A.	Elansary	Buchanan & Edwards
Robert	English	Federal Bureau of Investigation
Adam	Epler	Federal Bureau of Investigation
Valerie	Evanoff	Consultant
Mike	Fabling	Time Solutions, LLC
Patrick D.	Fagan	Motorola Solutions, Inc.
Adam	Farry	Nutanix
Amber J.	Fazzini	Federal Bureau of Investigation
Timothy	Fermanis	VMware Inc.
Elizabeth	Flaherty	Accenture Federal Services

Michael	Flynn	Transportation Security Administration
Denise	Ford	Federal Bureau of Investigation
John	Fortunato	IDEMIA
Gena	Fortune	Perspecta, Inc.
Jody	Fuller	STEALTHbits Technologies
Cheley A.	Gabriel	Enterprise Information Services, LLC
Cathy	Gallagher	Red Hat
Kelly	Gallagher	NEC Corporation of America
Gerard	Gallant	Amazon Web Services
Viraj	Gandhi	Paradyme Management
Luis	Garcia	Cisco Systems, Inc.
JoAnn	Garrison	Federal Bureau of Investigation
Ronnie	George	Federal Bureau of Investigation
James	Gerst	Federal Bureau of Investigation
Craig	Gibbens	Diverse Computing, Inc.
Becki	Goggins	SEARCH Group, Inc.
Ben	Goss	Quadrint
Mary	Gostel	Tygart Technology, Inc.
Todd	Graham	AnaVation LLC
Robert	Greeves	National Criminal Justice Association
Brian D.	Griffith	Federal Bureau of Investigation
Melvin O.	Grover III	Norfolk Police Department
Harry	Halden	IDEMIA
Lee	Hall	Leidos
Christian	Hall	Salient CRGT
Katie	Hanley	DHS/ICE
John	Harley	Leidos
Zachary P.	Hartzell	Federal Bureau of Investigation
Richard	Hauf	Ernst & Young
Daryl	Haugh	LexisNexis Special Services Inc.
Paul	Heppner	Georgia Bureau of Investigation - Retired
David J.	Hicks	Defense Counterintelligence and Secuirty Agency
Joey L.	Hixenbaugh	Federal Bureau of Investigation
Ricky	Hodson	David Hale Associates
Unice Y	Hsu	DHS/ICE
Michael	Hulme	Unisys Corporation
Eric	Ingersoll	Ingersoll Consulting, Inc.
Alex	Issac	MarkLogic Corporation
Ted	Jackson	Atlanta Sheriff's Office
Loma	Jamil	FreeAlliance, LLC
Don	Johnson	Federal Bureau of Investigation - Retired

Cyhthia	Johnston	Federal Bureau of Investigation
Kenneth E. (Casey)	Jones III	Thales Defense & Security Inc.
Michael	Kato	IDEMIA
Ryan N.	Keyes	Microsoft
Lee	Kicker	NEC of America
Jared	Kim	AnaVation LLC
Scott	Kirby	Immigration & Customs Enforcement
Joe	Klimavicz	U.S. Department of Justice
Michael P.	Klopp	ASHA IT Solutions Inc.
Brian	Knobbs	REDLattice
Thomas	Kohler	Full Visibility, LLC
Thomas	Krall	CGI Federal
Brian	Lamont	INTEGRITYOne Partners
Scott	Lamoreux	Dorrean, LLC
Stan	Larmee	Highlight Technologies
Thomas	Lee	OctoConsulting Group
Marty	Leeth	Venturi, LLC
Tom	Lehosit	Federal Bureau of Investigation
John	Leonard	Bi2technologies, LLC
Brian	Lester	Technica Corporation
Andrew	Levitt	HP
Brett	Lincoln	Federal Bureau of Investigation
Denise	Lindsey	DHA Group, Inc.
Kyle	Linscheid	Federal Bureau of Investigation
Brad	Long	Datamaxx Group, Inc.
James	Loudermilk	IDEMIA National Security Solutions
Katie	Loughran	IntelliWare Systems, Inc.
Steven	Ly	ServiceNow
Sarah	Lynn	U.S. Department of Justice
Kreher	M.	Atlanta Police Department
Kimberly A	Mackey	Tanium
Rachel	Maloney	RedSeal
Virginia "Ginger"	Manning	Unisys Corporation
Stephanie	Manson	Federal Bureau of Investigation
Jerry A	Marco	Federal Bureau of Investigation
William L	Marosy	MSM Security
Sherrie	Masden	Louisville Metro Police/MetroSafe 911 Communications Center
Christina	Mason	Federal Bureau of Investigation
Jeff	Matthews	OffenderWatch
Robert	May	IJIS Institute
Andrea	McCarthy	HARP

Luke J.	McCormack	DHS - Retired
Tricia	McCree	Cisco Systems, Inc.
Heather	McDade	Thomson Reuters
Marla	McDonald	Federal Bureau of Investigation
Donna	McIntire	Google
Michael D.	McIntyre, Jr.	Federal Bureau of Investigation
William G.	McKinsey	Federal Bureau of Investigation
Jairobe	McPherson	Google
Aimee	Medonos	AnaVation LLC
Nick	Megna	Federal Bureau of Investigation
Roger D.	Miller	Federal Bureau of Investigation
Michael	Miscio	General Dynamics Information Technology
Carol	Monroe	RedSky
Nichole	Moore	Diverse Computing, Inc.
Michelle	Moore	South Carolina Law Enforcement Division
Brian	Mortweet	Unisys Corporation
Charles	Murphy	Florida Department of Law Enforcement
Scott Eric	Myers	Federal Bureau of Investigation
Monte D.	Newton	Seneca Nation Group (SNG)
Patricia	Nunez	Federal Bureau of Investigation
Paulina T.A.	Orlikowski	Perspecta, Inc.
Jenna	O'Steen	Accenture Federal Services
Kimberly	Parsons	Federal Bureau of Investigation
Darrin A.	Paul	Federal Bureau of Investigation
Daniel	Pedowitz	IBM Corporation
Gigi	Pereira	SAIC
Wyatt	Pettengill	North Carolina State Bureau of Investigation
Shanon	Pitsenbarger	Fusion Technology
David	Popelier	Oracle Corporation
Kimberly	Portik	Canyon State Reporting Services, LLC
Lea	Post	Federal Bureau of Investigation
Mark	Potter	Ernst & Young
Jennifer	Pratt	Ernst & Young
Charles	Prouty	General Dynamics Information Technology
Steve	Psarakis	Dorrean, LLC
Cary	Quinn	Thomson Reuters
Catherine	Quinn	DHS/ICE
Dan	Radke	Gigamon
Scott	Rago	Federal Bureau of Investigation
Amanda	Rasinski	CBP
Kevin	Razzaghi	Koniag Government Solutions

James F.	Reed	BAE Systems
Kevin	Reid	Fusion Technology
Mike	Reid	DHS/ICE
Dyson	Richards	Xcelerate Solutions
Jonnianne	Ridzelski-McCombs	KBR Government Services
David J.	Roberts	SEARCH Group, Inc.
Evelyn "Lynn"	Rolin	South Carolina Law Enforcement Division
Lou	Ronca	AKIMA, LLC
Brian	Rosenthal	Full Visibility, LLC
Derek	Sabatini	Los Angeles County Sheriff's Department - LACRIS
Eric J.	Schiowitz	DHA Group, Inc.
Chris	Schraf	Microsoft
Shivaji	Sengupta	Magnus Management Group, LLC
Anil K.	Sharma	IBM
Kate	Silhol	Nlets
Samuel J.	Smith	Transportation Security Administration
Wesley	Smith	World Wide Technology
Barry	Smith	BAE Systems
Zachary	Snyder	National Background Check, Inc.
Elaine A.	Solomon	SAIC
Michael	Spellings	Novetta Solutions
Shaun I.	Squyres	Norfolk Police Department
Brian Scott	Swann	IDEMIA National Security Solutions
Wayne	Sweeney	Esri
Edward James	Talbert	IMTAS
Michael	Tang	Leidos
Mark	Tanner	General Dynamics Information Technology
Donald	Taylor	Perspecta
Cong Sinh	Tham	IMTAS
Christopher	Trainor	IBM
James	Travelstead	Federal Bureau of Investigation
R. Scott	Trent	Federal Bureau of Investigation
Patty	Trexler	Tanium
Amaha	Tsegaye	DHA Group, Inc.
Paul	Tselepis	IDEMIA National Security Solutions
Nathan	Tsoi	Transportation Security Administration
Robert	Turnbaugh	REDLattice
Thomas	Turner	Virginia State Police - Retired
Jeff	Tyler	US Marshals Service
Ryan	Tyrrell	Cisco Systems, Inc.
Donna M.	Uzzell	Florida Department of Law Enforcement

Derek	Veitenheimer	Bureau of Justice Information and Analysis
Mandar	Vengurlekar	Google Cloud Platform
Carey D.	Vereen	Data Systems Analysts (DSA) Inc.
Lisa A.	Vincent	Federal Bureau of Investigation
Brandon	Vincent	Federal Bureau of Investigation
Maria	Voreh	Federal Bureau of Investigation
Michael	Waddell	INTEGRITYOne Partners
Jeffrey	Wallin	Vermont Department of Public Safety
Troy	Walter	Salient CRGT
Roland	Walters	Oracle
Dale	Watson	Booz Allen Hamilton
John C.	Weatherly	Federal Bureau of Investigation
Roy G	Weise	Federal Bureau of Investigation - Retired
Tony	West	Forcepoint
Charlotte	Whitacre	Department of Commerce/First Responder Network Authority
Daniel	White	Xator Corporation
Missy	Willett	Red Hat
Karl W	Wilmes	AT&T First Net
Michelle	Wingate	GuidePoint Security
Glenn	Wood	Oracle National Security Group
Patrick J.	Woods	Amazon Web Services
Teresa	Wu	IDEMIA
Richard	Wyffels	Alexandria Police Department
Brian	Yanagi	Los Angeles County Sheriff's Department - LACRIS
Michael V.	Yates	Federal Bureau of Investigation
John	Yearty	Peak Performance Solutions
Theodore K.	Yoneda	Federal Bureau of Investigation
Christopher D.W.	Young	Hawaii Criminal Justice Data Center
Derek	Zaugg	Ingersoll Consulting, Inc.
Kenneth B.	Zercie	International Association for Identification

Intentionally Left Blank

Criminal Justice Information Services (CJIS)
Advisory Policy Board (APB)
December 4, 2019
Atlanta, Georgia
FINAL AGENDA

Wednesday, December 4, 2019
9 a.m.

Board Convenes

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

Roll Call

Mr. Michael C. Lesko
APB Chairman
Director
Law Enforcement Support Division
Texas Department of Public Safety

Introduction of Attendees and Special Guests

Mr. Lesko

Welcoming Remarks

Mr. Oliver Rich
Assistant Special Agent in Charge
Atlanta Field Office
Federal Bureau of Investigation

Mr. Theodore Jackson
Sheriff
Fulton County Sheriff's Office

Mr. Scott Kreher
Deputy Chief
Atlanta Police Department

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #1*
Executive Briefings

Mr. Michael D. DeLeon
Assistant Director
CJIS Division
Federal Bureau of Investigation

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

Item #2
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 #3*
NCIC 3rd Generation (N3G) Task Force Update

Mr. Wyatt A. Pettengill - **Chair**
Special Agent in Charge
Criminal Information and Identification Section
North Carolina State Bureau of Investigation

Item #4
Race Code Standardization across CJIS Division Systems

Mr. Todd C. Commodore
Acting Assistant Section Chief
Global Law Enforcement Support Section
CJIS Division
Federal Bureau of Investigation

*No staff paper

<u>**CJIS Advisory Policy Board**</u>
<u>**Wednesday, December 4, 2019**</u>

Item #5*
Nlets, The International Justice and Public Safety Network Update

Mr. Charles L. Schaeffer
President, Nlets
Director
Criminal Justice Information Services
Florida Department of Law Enforcement

Item #6
Chairman's Report on the National Data Exchange (N-DEx) Subcommittee

Ms. Donna Uzzell - **Chair**
Special Agent in Charge
Investigations and Forensics
Florida Department of Law Enforcement

Item #7
Chairman's Report on the Identification Services (IS) Subcommittee

Mr. Schaeffer - **Chair**

Item #8*
Biometric Hit of the Year

Mr. William G. McKinsey
Chief
Biometric Services Section
CJIS Division
Federal Bureau of Investigation

Item #9*
International Association for Identification (IAI) Update

Mr. Ken Zercie
IAI President

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #10*
National Consortium for Justice Information and Statistics (SEARCH) Update

Mr. David J. Roberts
Executive Director
SEARCH

Item #11*
National Crime Prevention and Privacy Compact Council Report

Mr. Pettengill - **Chair**

Item #12*
Tribal Task Force Update

Mr. William Denke - **Chair**
Chief of Police
Sycuan Tribal Police Department
El Cajon, CA

Item #13
Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee

Ms. Kathryn M. Monfreda - **Chair**
Chief
Criminal Records and Identification Bureau
Alaska Department of Public Safety

Item #14*
Association of State Uniform Crime Reporting (ASUCRP) Programs Update

Mr. Derek Veitenheimer
ASUCRP Representative to the APB
Wisconsin Department of Justice

Item #15*
Use of Force Task Force Update

Mr. Robert Sage - **Chair**
Director
Augusta Department of Public Safety
Augusta, KS

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #16*
CJIS Shared Management Progression

Mr. David Loesch
DFO/Assistant Director (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. Don Johnson
DFO/Section Chief (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. Roy Weise
DFO (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. R. Scott Trent
Unit Chief/Former DFO
Executive Support Unit
CJIS Division
Federal Bureau of Investigation

Mr. Michael McIntyre
Unit Chief/Former DFO
CJIS Audit Unit
Federal Bureau of Investigation

Mr. Nicky J. Megna
DFO
CJIS Division
Federal Bureau of Investigation

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #17*
APB Significant Achievements

Mr. Joseph P. Bonino
Commanding Officer (Retired)
Records and Identification Division
Los Angeles Police Department
APB Chair, December 1994 – December 1998

Mr. David Gavin
Assistant Chief (Retired)
Texas Department of Public Safety
APB Chair, December 1998 – December 2000

Mr. William Casey
Superintendent (Retired)
Boston Police Department
APB Chair, December 2000 – December 2004

Chief Frank Sleeter
Chief (Retired)
Sun Prairie Police Department
Sun Prairie, WI
APB Chair, December 2004 – June 2006

Mr. Paul Heppner
Director (Retired)
Georgia Bureau of Investigation
APB Chair, December 2005 – December 2008

Colonel Steven Cumoletti
Deputy Superintendent (Retired)
New York State Police
APB Chair, December 2008 – December 2012

Captain Tom Turner
Division Commander (Retired)
Criminal Justice Information Services Division
Virginia State Police
APB Chair, December 2012 – December 2016

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #17 Continued

Mr. John “Jack” Donohue
Chief
Strategic Initiatives
New York City Police Department
APB Chair, December 2016 - December 2018

Mr. Michael Lesko
Chief
Law Enforcement Support Division
Texas Department of Public Safety
APB Chair, December 2018 - present

*No staff paper

CJIS Advisory Policy Board
Thursday, December 5, 2019

Item #18
Chairman's Report on the Security and Access (SA) Subcommittee

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

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

Ms. Carol Gibbs - **Chair**
Chief, Program Administration Bureau
Illinois State Police

Item #20
Chairman's Report on the National Instant Criminal Background Check System (NICS) Subcommittee

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

Item #21*
Rapid DNA Update

Mr. Thomas Callaghan
Senior Physical Scientist
Laboratory Division
Federal Bureau of Investigation
Quantico, VA

Item #22*
American Society of Crime Laboratory Directors' Update

Mr. Bruce Houlihan
Director
Orange County Crime Laboratory
Santa Ana, CA

*No staff paper

CJIS Advisory Policy Board
Thursday, December 5, 2019

Item #23* ***(was not presented)***
International Association of Chiefs of Police Update

Mr. William G. Brooks, III
Chief of Police
Norwood, Massachusetts Police Department

Item #24* ***(was not presented)***
Major Cities Chiefs Association Update

Colonel Edwin C. Roessler, Jr.
Chief of Police
Fairfax County Police Department
Fairfax, VA

Item #25* ***(was not presented)***
Major County Sheriffs of America Update

Mr. Anthony Wickersham
Sheriff
Macomb County Sheriff's Office
Mt. Clemens, MI

Item #26*
National Sheriffs' Association (NSA) Update

Mr. Michael Brown
Director
Professional Development
NSA

Other Business

Adjourn

*No staff paper

Intentionally Left Blank

Criminal Justice Information Services (CJIS)
Advisory Policy Board (APB)
December 4, 2019
Atlanta, Georgia
AGENDA as of 11/12/2019

Wednesday, December 4, 2019
9 a.m.

Board Convenes

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

Roll Call

Mr. Michael C. Lesko
APB Chairman
Director
Law Enforcement Support Division
Texas Department of Public Safety

Introduction of Attendees and Special Guests

Mr. Lesko

Welcoming Remarks

Mr. J.C. Hacker
Special Agent in Charge
Atlanta Field Office
Federal Bureau of Investigation

Mr. Theodore Jackson
Sheriff
Fulton County Sheriff's Office

Mr. Scott Kreher
Deputy Chief
Atlanta Police Department

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #1*
Executive Briefings

Mr. Michael D. DeLeon
Assistant Director
CJIS Division
Federal Bureau of Investigation

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

Item #2
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 #3*
NCIC 3rd Generation (N3G) Task Force Update

Mr. Wyatt A. Pettengill - **Chair**
Special Agent in Charge
Criminal Information and Identification Section
North Carolina State Bureau of Investigation

Item #4
Race Code Standardization across CJIS Division Systems

Mr. Todd C. Commodore
Acting Assistant Section Chief
Global Law Enforcement Support Section
CJIS Division
Federal Bureau of Investigation

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #5*
Nlets, The International Justice and Public Safety Network Update

Mr. Charles L. Schaeffer
President, Nlets
Director
Criminal Justice Information Services
Florida Department of Law Enforcement

Item #6
Chairman's Report on the National Data Exchange (N-DEx) Subcommittee

Ms. Donna Uzzell - **Chair**
Special Agent in Charge
Investigations and Forensics
Florida Department of Law Enforcement

Item #7
Chairman's Report on the Identification Services (IS) Subcommittee

Mr. Charles L. Schaeffer - **Chair**

Item #8*
Biometric Hit of the Year

Mr. William G. McKinsey
Section Chief
Biometric Services Section
CJIS Division
Federal Bureau of Investigation

Item #9*
International Association for Identification (IAI) Update

Mr. Ken Zercie
IAI President

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #10*
National Consortium for Justice Information and Statistics (SEARCH) Update

Mr. David J. Roberts
Executive Director
SEARCH

Item #11*
National Crime Prevention and Privacy Compact Council Report

Mr. Pettengill - **Chair**

Item #12*
Tribal Task Force Update

Mr. William Denke - **Chair**
Chief of Police
Sycuan Tribal Police Department
El Cajon, CA

Item #13
Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee

Ms. Kathryn M. Monfreda - **Chair**
Chief
Criminal Records and Identification Bureau
Alaska Department of Public Safety

Item #14*
Association of State Uniform Crime Reporting (ASUCRP) Programs Update

Mr. Derek Veitenheimer
ASUCRP Representative to the APB
Wisconsin Department of Justice

Item #15*
Use of Force Task Force Update

Mr. Robert Sage - **Chair**
Director
Augusta Department of Public Safety
Augusta, KS

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #16*
CJIS Shared Management Progression

Mr. Demery Bishop
Designated Federal Employee (DFE) (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. Don Johnson
DFE (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. Roy Weise
DFO (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. David Loesch
DFE/Assistant Director (Retired)
CJIS Division
Federal Bureau of Investigation

Mr. R. Scott Trent
Unit Chief
Executive Support Unit
CJIS Division
Federal Bureau of Investigation

Mr. Michael McIntyre
Unit Chief
CJIS Audit Unit
Federal Bureau of Investigation

Mr. Nicky J. Megna
DFO
CJIS Division
Federal Bureau of Investigation

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #17*
APB Significant Achievements

Mr. Joseph P. Bonino
Commanding Officer (Retired)
Records and Identification Division
Los Angeles Police Department
APB Chair – December 1994 – December 1998

Mr. William Casey
Superintendent (Retired)
Boston Police Department
APB Chair – December 2000 – December 2004

Chief Frank Sleeter
Chief (Retired)
Sun Prairie Police Department
Sun Prairie, WI
APB Chair – December 2004 – June 2006

Mr. Paul Heppner
Director (Retired)
Georgia Bureau of Investigation
APB Chair – June 2006 – December 2008

Colonel Steven Cumoletti
Deputy Superintendent (Retired)
New York State Police
APB Chair – December 2008 – December 2012

Captain Tom Turner
Division Commander (Retired)
Criminal Justice Information Services Division
Virginia State Police
APB Chair – December 2012 – December 2016

Mr. John “Jack” Donohue
Assistant Chief
Executive Officer
Intelligence Bureau
New York City Police Department
APB Chair - December 2016 - December 2018

*No staff paper

CJIS Advisory Policy Board
Wednesday, December 4, 2019

Item #17 Continued

Mr. Michael Lesko
Chief
Law Enforcement Support Division
Texas Department of Public Safety
APB Chair - December 2018 - present

*No staff paper

CJIS Advisory Policy Board
Thursday, December 5, 2019

Item #18
Chairman's Report on the Security and Access (SA) Subcommittee

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

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

Mr. James F. Slater, III - **Chair**
Commissioner
Massachusetts Department of Criminal Justice Information Services

Item #20
Chairman's Report on the National Instant Criminal Background Check System (NICS) Subcommittee

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

Item #21*
Rapid DNA Update

Mr. Thomas Callaghan
Senior Physical Scientist
Laboratory Division
Federal Bureau of Investigation
Quantico, VA

Item #22*
American Society of Crime Laboratory Director's Update

Mr. Bruce Houlihan
Director
Orange County Crime Laboratory
Santa Ana, CA

*No staff paper

Item #23*
International Association of Chiefs of Police Update

Mr. William G. Brooks, III
Chief of Police
Norwood, Massachusetts Police Department

Item #24*
Major Cities Chiefs Association Update

Colonel Edwin C. Roessler, Jr.
Chief of Police
Fairfax County Police Department
Fairfax, VA

Item #25*
Major County Sheriffs of America Update

Mr. Anthony Wickersham
Sheriff
Macomb County Sheriff's Office
Mt. Clemens, MI

Item #26*
National Sheriffs' Association Update

Mr. Michael Brown
Director
Professional Development
NSA

Other Business

Adjourn

*No staff paper

Intentionally Left Blank

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA

STAFF PAPER

APB ITEM #2

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

NCIC ISSUE #1
Notifications for Wanted Notices on the Next Generation Identification (NGI) System

NCIC ISSUE #2
Law Enforcement Enterprise Portal Status Report

NCIC ISSUE #3*
N3G User Transition Fundamentals - NIEM XML Update

NCIC ISSUE #4
The Intra-Agency Sharing of National Sex Offender Registry Audit Reports, Findings, and Accompanying Documentation with the United States Department of Justice, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking

NCIC ISSUE #5 ***(See APB Item #4 for staff paper)***
Race Code Standardization across CJIS Division Systems

NCIC ISSUE #6*
NCIC Third Generation (N3G) Task Force Status Update

NCIC ISSUE #7
N3G Project

NCIC ISSUE #8
Inclusion of Blue Alert Data in the NCIC

NCIC ISSUE #9
Request to Expand the NCIC Protection Order File Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders

NCIC ISSUE #10** ***(See Informational Topic E for staff paper)***
CJIS Division NCIC Status

*No staff paper

NCIC ISSUE #11*
NICS Denied Transaction File Dissemination Caveat and Notification Protocol
Prioritization Request

*No staff paper

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC)
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

NCIC ISSUE #1

Notifications for Wanted Notices on the Next Generation Identification (NGI) System

PURPOSE

The purpose of this paper is to review manual and automated notifications for specific maintenance transactions in the NGI System for agencies with an active want, and determine if those should be continued with automation when required, or discontinued. Also, modify language as needed.

POINT OF CONTACT

Biometric Services Section, Biometric Support Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to review the alternatives presented and recommend one alternative for the FBI staff to pursue for each of the messages.

BACKGROUND

The topic of notifications generated during identity history record maintenance activities was originally presented to the advisory process in the spring of 2019. Based upon those discussions, it was recommended that a second version be returned to the Working Groups to include the subsequent process, encompassing a review of the messages, as well as the language of those messages, and the language and value of the current automated messages. Currently, automated notifications are transmitted to wanting agencies when ten-print submissions update to a record in the NGI System. This practice is expected to continue. Criminal Justice Information Services (CJIS) Division staff performs a manual review of Identity History Record Summaries when other activities occur on a record in the NGI System, which contains an active Want; such as consolidations, deceased, dispositions, probation/supervision, modifications related to name and date of birth, and expungement of the last criminal event. Staff review these transactions and determine if the updated information could be of value to the wanting agency. If staff determines there is value, a message is sent to the wanting agency utilizing the International Justice and Public Safety Information Sharing Network also known as Nlets.

DISCUSSION AND ANALYSIS

The manual review preceding any notification to wanting agencies increases the delay time prior to notification and allows for individual interpretation regarding the value of information. It is the intent of the CJIS Division to automate those notifications. This effort created the opportune time to review the message content as well as the usefulness of the data.

During the Spring 2019 Working Group Meetings, Subsequent Activity Notifications for Wanted Notices on the NGI System was discussed. In June 2019, the APB recommended pursuing the development of automated messages to replace manual notifications to wanting agencies for disposition, modification, and expungement transactions in the NGI System. The APB provided guidance to the FBI that the intent of the messages should be made clear to message recipients.

The APB motioned to this option with additions: Pursue development of automated messages to wanting agencies on each of these updates: dispositions, modification of name or date of birth, expungement of last criminal event within the Universal Control Number, and flashes. Also revisit the messages currently being sent as well as any new messages to clarify the intent of the messages and recommend a record review. Proposed message revisions will be brought through the Advisory Process.

This topic paper provides current and proposed message revisions in option 1 to support the regional working group's discussions to clarify the intent of messages. The subcommittee is also requested to eliminate any investigative messages deemed not valuable.

OPTIONS

Option 1:
Refine the wanted notifications as indicated by the Working Groups which are outlined in the following current and proposed messages ensuring the intent of the messages is clearly stated.

If Option 1 is approved, the system enhancements necessary to implement the proposal should be assigned the priority:___(enter 0-5) and categorized as: __ (enter High, Medium, or Low).

Section I - Automated Notifications during the Want Entry Process

A. This message provides notification that the date of birth and the date of warrant in the wanted entry are the same.

Current automated message:
DATE OF BIRTH CONTAINED IN WANTED NOTICE IS THE SAME AS DATE OF WARRANT. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO REFLECT THE CORRECT INFORMATION TO UPDATE SUBJECT'S, XXXXXXXXX, CRIMINAL HISTORY RECORD.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE ENTERED DATE OF WARRANT AND DATE OF BIRTH ARE THE SAME. PLEASE REVIEW AND CORRECT THE MISENTERED FIELD.

B. This message provides notification that the UCN in the wanted entry is incorrect.

Current automated message:
PLEASE BE ADVISED UCN: XXXXXXXXX REFLECTED IN YOUR NCIC WANTED PERSON ENTRY, XXXXXXXXX, IS INCORRECT. PLEASE MODIFY YOUR NCIC ENTRY APPROPRIATELY.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE UCN IN YOUR WANTED NOTICE IS INVALID. PLEASE DELETE THE NUMBER AND REPLACE, IF APPROPRIATE.

C. This message provides notification that the UCN entered in the wanted notice is invalid or doesn't meet the biographic matching criteria; however, a potential match has been identified (fuzzy match).

Current automated message:
PLEASE BE ADVISED UCN: XXXXXXXXX REFLECTED IN YOUR NCIC WANTED PERSON ENTRY, XXXXXXXXX, IS INCORRECT. THE CORRECT UCN FOR YOUR WANTED SUBJECT MAY BE UCN XXXXXXXXX. PLEASE MODIFY YOUR NCIC ENTRY APPROPRIATELY. FOLLOWING COMPLIANCE WITH THIS REQUEST, THE SUBJECT'S IDENTITY HISTORY RECORD WILL BE UPDATED.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXX. THE UCN IN YOUR WANTED NOTICE IS INVALID OR INCORRECT. THE CORRECT UCN MAY BE UCN XXXXXX. PLEASE DELETE THE CURRENT UCN AND REPLACE, IF APPROPRIATE.

D. Existing Deceased Notification - This message provides notification that the UCN entered in the wanted notice has been previously confirmed as deceased by fingerprints.

Current automated message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN VERIFIED AS DECEASED BY FINGERPRINTS. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.
Note: Current message does not indicate the submitter of the information.

Proposed automated message:
UCN, XXXXXXX, CONTAINED IN WANTED NOTICE HAS BEEN VERIFIED AS DECEASED BY FINGERPRINTS BY XXXXXXXXX. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXX, TO CORRECT OR REMOVE THE UCN.
Or
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN CONFIRMED DECEASED BY FINGERPRINTS. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

E. Existing Expunged Notification - This message provides notification that the UCN entered in the wanted notice is expunged.

Current automated message:
FBI NUMBER, XXXXXXXXX, CONTAINED IN WANTED NOTICE HAS BEEN EXPUNGED. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO CORRECT OR REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.

Proposed automated message:
#1 UCN, XXXXXXX, ENTERED IN WANTED NOTICE HAS BEEN EXPUNGED. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXX, TO REMOVE THE UCN.
Or
#2 ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN PREVIOUSLY EXPUNGED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

F. Existing Consolidation Notification - This message provides notification that the UCN contained in the wanted entry was previously consolidated.

Current automated message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN CONSOLIDATED WITH XXXXXXXXX. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO CORRECT OR REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.

Proposed automated message:
#1 UCN XXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN CONSOLIDATED WITH UCN XXXXXXX. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXX, TO CORRECT OR REMOVE THE UCN.
Or
#2 ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS UCN XXXXXXX. DUE TO A CONSOLIDATION THAT UCN HAS BEEN REPLACED WITH UCN XXXXXXX. PLEASE UPDATE THE UCN IN YOUR ENTRY TO XXXXXXX.

G. Existing Deleted Notifications - This message provides notification that UCN entered in the wanted notice was previously deleted due to a processing discrepancy.

Current automated message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN DELETED. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXXXX, TO CORRECT OR REMOVE THE FBI NUMBER TO UPDATE SUBJECT'S CRIMINAL HISTORY RECORD.

Proposed automated message:
#1 UCN XXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN DELETED. PLEASE MODIFY YOUR NCIC ENTRY, XXXXXXX, TO REMOVE THE UCN.
Or
#2 ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY. A

SEPARATE UCN MAY BE ADDED IF ANOTHER IDENTITY HISTORY RECORD IS IDENTIFIED.

Section II - Automated Subsequent Activity Notifications

A. Existing Current Print Ident (CPI) and Criminal Ten-Print Notification - This message provides notification that a current criminal transaction or a NFF state has processed a current print with an identification to the UCN contained in the wanted entry.

Is this notification valuable?

Current automated message:
ON YYYY/MM/DD, A FINGERPRINT CARD WAS IDENTIFIED WITH XXXXXXXXXXX, FBI/XXXXXXXXX BY XXXXXXXXXXXX (ORI/XXXXXXXXX), XXXXXXXXXXXX. OUR RECORD INDICATES YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX. FOLLOW-UP ACTION BY YOU WITH THE ARRESTING AGENCY MAY BE APPROPRIATE. CLEAR OR CANCEL YOUR NCIC RECORD WHEN SUBJECT IS NO LONGER WANTED. FBI CJIS DIVISION, CLARKSBURG, WV

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A FINGERPRINT CARD, DOA XXXX/XX/XX, FROM XXXXXXXX, WAS IDENTIFIED WITH UCN XXXXXXX. THIS UCN IS CONTAINED IN YOUR WANTED NOTICE. SUBJECT'S IDENTIFICATION RECORD INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX. CONTACT THE ARRESTING AGENCY FOR MORE INFORMATION. IF THE SUBJECT IS NO LONGER WANTED, PLEASE CANCEL OR CLEAR THE NCIC ENTRY.

B. Existing Civil Identification - This message provides notification that a non-criminal justice fingerprint card was idented to the UCN contained in the wanted notice.

Is this notification valuable?

Current automated message:
ON XXXX/XX/XX, A CIVIL FINGERPRINT CARD WAS IDENTED TO FBI UCN XXXXXXX BY XXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC XXXXXXX).

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A CIVIL FINGERPRINT CARD FROM XXXXXXX WAS IDENTED TO UCN CONTAINED IN YOUR WANTED NOTICE. PLEASE CONTACT THE AGENCY FOR MORE INFORMATION.

Section III - Manual Messages for Review

A. **Consolidation Notification - This message provides notification that CJIS has taken action to consolidate two or more identity history records. The consolidation can be requested from a submitter or identified by internal CJIS processes. There are two different scenarios.**

   1. **The first is when the UCN in your want is retained as the primary identifier of the record.**

Is this notification valuable?

Current manual message:
ON XXXX/XX/XX, UCN XXXXXXX WAS CONSOLIDATED INTO UCN XXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC/XXXXXXX)

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE UCN IN YOUR WANT WAS PART OF A CONSOLIDATION OF IDENTITY HISTORY RECORDS. ADDITIONAL DATA MAY BE AVAILABLE ON YOUR SUBJECTS RECORD IN THE INTERSTATE IDENFICATION INDEX. PLEASE REVIEW THE RECORD FOR MORE INFORMATION.

   2. **The second is when the UCN in your want is *not* retained as the primary identifier of the record.**

Current manual message:
ON XXXX/XX/XX, UCN XXXXX WAS CONSOLIDATED INTO UCN XXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC/XXXXXXX) REFLECTING THE INACTIVE UCN/XXXXXXX. PLEASE REVIEW THE RECORD AND MODIFY YOUR NCIC ENTRY TO APPROPRIATELY REFLECT THE ACTIVE UCN/XXXXX.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXXX. UCN XXXXXX CONTAINED IN YOUR WANTED NOTICE HAS BEEN CONSOLIDATED INTO RETAINED UCN XXXXXXX. PLEASE MODIFY THE UCN IN YOUR WANT TO REFLECT THE RETAINED UCN. ALSO, ADDITIONAL DETAILS MAY BE AVAILABLE ON YOUR SUBJECT IN THE INTERSTATE IDENTIFICATION INDEX.

B. **Deceased Notification - This message is intended to provide notification that CJIS has received a fingerprint submission indicating the subject is deceased (DEK – known deceased submission) or a III message or hard copy documentation has been submitted indicating the state deceased the record based on biometric comparison (FII message).**

Current manual message:
ON XXXX/XX/XX, DECEASED INFORMATION WAS UPDATED TO UCN XXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL IN NCIC (NIC/XXXXXXX).

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. DECEASED INFORMATION WAS UPDATED TO UCN XXXXXXX CONTAINED IN YOUR WANTED NOTICE.

C. Disposition Notification - This message is intended to provide notification that a disposition has been added to an event on the identity history record indicated in the UCN in the wanted entry.

Is this notification valuable?

Current manual message:
ON XXXX/XX/XX, A DISPOSITION WAS UPDATED TO DOA XXXX/XX/XX, UCN/XXXXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING RECENT UPDATE IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A DISPOSITION WAS UPDATED TO DOA XXXX/XX/XX, UCN XXXXXXX. UPDATED IDENTITY HISTORY RECORD IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

D. Probation/Supervision Notification - This message is intended to provide notification that a term of probation or supervised release has been added to the identity history record.

Is this notification valuable?

Current manual message:
ON XXXX/XX/XX, PROBATION/SUPERVISION WAS UPDATED TO DOA XXXX/XX/XX, UCN/XXXXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING RECENT UPDATE IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.
Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A SUPERVISED RELEASE OR PROBATION TERM HAS BEEN UPDATED TO UCN XXXXXXX BY AGENCY XXXXXXX. UPDATED IDENTIFICATION RECORD IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX

E. **Modification to Name or Date of Birth Notification - This message is intended to provide notification that the master name or date of birth has been modified on the associated identity history record.**

Current manual message:
ON XXXX/XX/XX, A NAME OR DATE OF BIRTH MODIFICATION WAS MADE TO UCN/XXXXXXXXX. OUR RECORDS INDICATE YOUR AGENCY HAS AN ACTIVE WANT FOR THIS INDIVIDUAL AS XXXXXXXXXXXXXXXXXXXXX, CASE NUMBER XXXXXXXXXXX, ENTERED IN NCIC (NIC/XXXXXXXXXX). SUBJECT'S IDENTIFICATION RECORD INCLUDING RECENT UPDATE IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX CONTAINS UCN XXXXXXX. THE CJIS DIVISION HAS MODIFIED THE NAME OR DATE OF BIRTH ASSOCIATED WITH THAT IDENTITY. PLEASE CONFIRM THE UCN IS STILL A MATCH FOR YOUR SUBJECT. IF SO, NO ACTION REQUIRED. IF NOT, REMOVE OR REPLACE THE UCN.

F. **Last Criminal Event Expungement Notification - This message is intended to provide notification that the last criminal event has been expunged from the associated identity.**

Is this notification valuable?

Current manual message:
FBI NUMBER, XXXXXXXXX CONTAINED IN WANTED NOTICE HAS BEEN EXPUNGED. THE IDENTITY WILL REMAIN ON FILE FOR REFERENCE PURPOSES ONLY UNTIL YOUR WANT IS CANCELLED.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE LAST CRIMINAL EVENT HAS BEEN EXPUNGED. THE UCN WILL REMAIN ACTIVE FOR REFERENCE PURPOSES ONLY UNTIL YOUR WANT IS CANCELLED.

Option 2: Provide additional messages or suggest new messages for wanted notifications.

If Option 2 is approved, the system enhancements necessary to implement the proposal should be assigned the priority:__(enter 0-5) and categorized as: __ (enter High, Medium, or Low).

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 with a priority level 3M.

Option 1: Refine the wanted notifications as indicated by the Working Groups which are outlined in the topic paper ensuring the intent of the messages is clearly stated. Accepting the second message for D, E, F, and G of Section I which begin with "Action Required."

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept a new Option.

Option:

Refine the wanted notifications as indicated in the paper with exception of Section III – C (Dispositions) & F (Expungement of Last Criminal Event) which will be eliminated. In Section I: D, E, F, & G to adopt the proposed language #2 which begins with "Action Required."

Section I - Automated Notifications during the Want Entry Process

A. This message provides notification that the date of birth and the date of warrant in the wanted entry are the same.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE ENTERED DATE OF WARRANT AND DATE OF BIRTH ARE THE SAME. PLEASE REVIEW AND CORRECT THE MISENTERED FIELD.

B. This message provides notification that the UCN in the wanted entry is incorrect.

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE UCN IN YOUR WANTED NOTICE IS INVALID. PLEASE DELETE THE NUMBER AND REPLACE, IF APPROPRIATE.

C. This message provides notification that the UCN entered in the wanted notice is invalid or doesn't meet the biographic matching criteria; however, a potential match has been identified (fuzzy match).

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXX. THE UCN IN YOUR WANTED NOTICE IS INVALID OR INCORRECT. THE CORRECT UCN MAY BE UCN XXXXXX. PLEASE DELETE THE CURRENT UCN AND REPLACE, IF APPROPRIATE.

D. Existing Deceased Notification - This message provides notification that the UCN entered in the wanted notice has been previously confirmed as deceased by fingerprints.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN CONFIRMED DECEASED BY FINGERPRINTS. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

E. Existing Expunged Notification - This message provides notification that the UCN entered in the wanted notice is expunged.

Proposed automated message:
#2 ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN PREVIOUSLY EXPUNGED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

F. Existing Consolidation Notification - This message provides notification that the UCN contained in the wanted entry was previously consolidated.

Proposed automated message:
#2 ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS UCN XXXXXXX. DUE TO A CONSOLIDATION THAT UCN HAS BEEN REPLACED WITH UCN XXXXXXX. PLEASE UPDATE THE UCN IN YOUR ENTRY TO XXXXXXX.

G. Existing Deleted Notifications - This message provides notification that UCN entered in the wanted notice was previously deleted due to a processing discrepancy.

Proposed automated message:
#2 ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY. A SEPARATE UCN MAY BE ADDED IF ANOTHER IDENTITY HISTORY RECORD IS IDENTIFIED.

Section II - Automated Subsequent Activity Notifications

A. Existing Current Print Ident (CPI) and Criminal Ten-Print Notification - This message provides notification that a current criminal transaction or a NFF state has processed a current print with an identification to the UCN contained in the wanted entry.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A FINGERPRINT CARD, DOA XXXX/XX/XX, FROM XXXXXXXX, WAS IDENTIFIED WITH UCN XXXXXXX. THIS UCN IS CONTAINED IN YOUR WANTED NOTICE. SUBJECT'S IDENTIFICATION RECORD INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX. CONTACT THE ARRESTING AGENCY FOR

MORE INFORMATION. IF THE SUBJECT IS NO LONGER WANTED, PLEASE CANCEL OR CLEAR THE NCIC ENTRY.

B. Existing Civil Identification - This message provides notification that a non-criminal justice fingerprint card was idented to the UCN contained in the wanted notice.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A CIVIL FINGERPRINT CARD FROM XXXXXXX WAS IDENTED TO UCN CONTAINED IN YOUR WANTED NOTICE. PLEASE CONTACT THE AGENCY FOR MORE INFORMATION.

Section III - Manual Messages for Review

A. Consolidation Notification - This message provides notification that CJIS has taken action to consolidate two or more identity history records. The consolidation can be requested from a submitter or identified by internal CJIS processes. There are two different scenarios.

1. **The first is when the UCN in your want is retained as the primary identifier of the record.**

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE UCN IN YOUR WANT WAS PART OF A CONSOLIDATION OF IDENTITY HISTORY RECORDS. ADDITIONAL DATA MAY BE AVAILABLE ON YOUR SUBJECTS RECORD IN THE INTERSTATE IDENFICATION INDEX. PLEASE REVIEW THE RECORD FOR MORE INFORMATION.

2. **The second is when the UCN in your want is *not* retained as the primary identifier of the record.**

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXXX. UCN XXXXXX CONTAINED IN YOUR WANTED NOTICE HAS BEEN CONSOLIDATED INTO RETAINED UCN XXXXXXX. PLEASE MODIFY THE UCN IN YOUR WANT TO REFLECT THE RETAINED UCN. ALSO, ADDITIONAL DETAILS MAY BE AVAILABLE ON YOUR SUBJECT IN THE INTERSTATE IDENTIFICATION INDEX.

B. Deceased Notification - This message is intended to provide notification that CJIS has received a fingerprint submission indicating the subject is deceased (DEK – known deceased submission) or a III message or hard copy documentation has been submitted indicating the state deceased the record based on biometric comparison (FII message).

Proposed automated message:
ACTION REQUIRED. WANTED NOTICE XXXXXXX. DECEASED INFORMATION WAS UPDATED TO UCN XXXXXXX CONTAINED IN YOUR WANTED NOTICE.

~~C. Disposition Notification - This message is intended to provide notification that a disposition has been added to an event on the identity history record indicated in the UCN in the wanted entry.~~

D. Probation/Supervision Notification - This message is intended to provide notification that a term of probation or supervised release has been added to the identity history record.

Proposed automated message:
INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A SUPERVISED RELEASE OR PROBATION TERM HAS BEEN UPDATED TO UCN XXXXXXX BY AGENCY XXXXXXX. UPDATED IDENTIFICATION RECORD IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX

E. Modification to Name or Date of Birth Notification - This message is intended to provide notification that the master name or date of birth has been modified on the associated identity history record.

Proposed automated message:
ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX CONTAINS UCN XXXXXXX. THE CJIS DIVISION HAS MODIFIED THE NAME OR DATE OF BIRTH ASSOCIATED WITH THAT IDENTITY. PLEASE CONFIRM THE UCN IS STILL A MATCH FOR YOUR SUBJECT. IF SO, NO ACTION REQUIRED. IF NOT, REMOVE OR REPLACE THE UCN.

~~F. Last Criminal Event Expungement Notification - This message is intended to provide notification that the last criminal event has been expunged from the associated identity.~~

Action: Motion carried

Motion: To assign a Priority 3M.
Action: Motion carried

<u>NORTHEASTERN WORKING GROUP ACTION:</u>

Motion: To adopt Option 1 with the addition of adding the UCN to all notifications and III instead of spelling out Interstate Identification Index. Priority level 3L.
Action: Motion carried

<u>SOUTHERN WORKING GROUP ACTION:</u>

Section I:

Motion 1: To adopt Option 1: Refine the wanted notifications as indicated by the Working Groups which are outlined in the paper ensuring the intent of the messages is clearly stated. Adopt proposed language for A, B, and C as stated in the paper.

A. ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE ENTERED DATE OF WARRANT AND DATE OF BIRTH ARE THE SAME. PLEASE REVIEW AND CORRECT THE MISENTERED FIELD.

B. ACTION REQUIRED. WANTED NOTICE XXXXXXX. THE UCN IN YOUR WANTED NOTICE IS INVALID. PLEASE DELETE THE NUMBER AND REPLACE, IF APPROPRIATE.

C. ACTION REQUIRED. WANTED NOTICE XXXXXX. THE UCN IN YOUR WANTED NOTICE IS INVALID OR INCORRECT. THE CORRECT UCN MAY BE UCN XXXXXX. PLEASE DELETE THE CURRENT UCN AND REPLACE, IF APPROPRIATE.

Adopt the second proposed option in D, E, F, & G which begin with "Action Required."

D. ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN CONFIRMED DECEASED BY FINGERPRINTS. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

E. ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN PREVIOUSLY EXPUNGED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.

F. ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS UCN XXXXXXX. DUE TO A CONSOLIDATION THAT UCN HAS BEEN REPLACED WITH UCN XXXXXXX. PLEASE UPDATE THE UCN IN YOUR ENTRY TO XXXXXXX.

G. ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY. A SEPARATE UCN MAY BE ADDED IF ANOTHER IDENTITY HISTORY RECORD IS IDENTIFIED

Action: Motion carried.

Section II:

Motion 2: Adopt Option 1: Adopt proposed language as stated in the paper for A & B.

A. INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A FINGERPRINT CARD, DOA XXXX/XX/XX, FROM XXXXXXXX, WAS IDENTIFIED WITH UCN XXXXXXX. THIS UCN IS CONTAINED IN YOUR WANTED NOTICE. SUBJECT'S IDENTIFICATION RECORD INCLUDING CURRENT ARREST INFORMATION, IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX. CONTACT THE ARRESTING AGENCY FOR MORE INFORMATION. IF THE SUBJECT IS NO LONGER WANTED, PLEASE CANCEL OR CLEAR THE NCIC ENTRY.

B. INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A CIVIL FINGERPRINT CARD FROM XXXXXXX WAS IDENTED TO UCN CONTAINED IN YOUR WANTED NOTICE. PLEASE CONTACT THE AGENCY FOR MORE INFORMATION.

Action: Motion carried.

Section III:

Motion 3: Adopt Option 1: Adopt proposed language as stated in the paper for A through F.

A1. INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE UCN IN YOUR WANT WAS PART OF A CONSOLIDATION OF IDENTITY HISTORY RECORDS. ADDITIONAL DATA MAY BE AVAILABLE ON YOUR SUBJECTS RECORD IN THE INTERSTATE IDENFICATION INDEX. PLEASE REVIEW THE RECORD FOR MORE INFORMATION.

A2. ACTION REQUIRED. WANTED NOTICE XXXXXXXX. UCN XXXXXX CONTAINED IN YOUR WANTED NOTICE HAS BEEN CONSOLIDATED INTO RETAINED UCN XXXXXXX. PLEASE MODIFY THE UCN IN YOUR WANT TO REFLECT THE RETAINED UCN. ALSO, ADDITIONAL DETAILS MAY BE AVAILABLE ON YOUR SUBJECT IN THE INTERSTATE IDENTIFICATION INDEX.

B. ACTION REQUIRED. WANTED NOTICE XXXXXXX. DECEASED INFORMATION WAS UPDATED TO UCN XXXXXXX CONTAINED IN YOUR WANTED NOTICE.

C. INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A DISPOSITION WAS UPDATED TO DOA XXXX/XX/XX, UCN XXXXXXX. UPDATED IDENTITY HISTORY RECORD IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

D. INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. A SUPERVISED RELEASE OR PROBATION TERM HAS BEEN UPDATED TO UCN XXXXXXX BY AGENCY XXXXXXX. UPDATED IDENTIFICATION RECORD IS AVAILABLE VIA THE INTERSTATE IDENTIFICATION INDEX.

E. ACTION REQUIRED. YOUR WANTED NOTICE, XXXXXXX CONTAINS UCN XXXXXXX. THE CJIS DIVISION HAS MODIFIED THE NAME OR DATE OF BIRTH ASSOCIATED WITH THAT IDENTITY. PLEASE CONFIRM THE UCN IS STILL A MATCH FOR YOUR SUBJECT. IF SO, NO ACTION REQUIRED. IF NOT, REMOVE OR REPLACE THE UCN.

F. INVESTIGATIVE VALUE. WANTED NOTICE XXXXXXX. THE LAST CRIMINAL EVENT HAS BEEN EXPUNGED. THE UCN WILL REMAIN ACTIVE FOR REFERENCE PURPOSES ONLY UNTIL YOUR WANT IS CANCELLED.

Action: Motion carried.

Motion 4: Assign a priority 4M.
Action: Motion carried.

WESTERN WORKING GROUP ACTION:
Motion 1: To adopt a new Option. Priority 3M.
Option:
Accept the wanted notifications as indicated by the Working Groups which are outlined in the paper. Section I options D, E, and F accept the 2nd proposed option which contains "Action Required." Section I option G modify to "ACTION REQUIRED. YOUR WANTED NOTICE, XXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.
Action: Motion carried.

FALL 2019 SUBCOMMITTEE ACTIONS:

IDENTIFICATION SERVICES (IS) SUBCOMMITTEE ACTION:
Section 1 - Automated Notification during the Want Entry Process
Motion: Endorse the Western Working Group motion to adopt a new Option.
Option:
Accept the wanted notifications as indicated by the Working Groups which are outlined in the paper. Section I options D, E, and F accept the 2nd proposed option which contains "Action Required." Section I option G modify to
"ACTION REQUIRED. YOUR WANTED NOTICE, XXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.
Action: Motion carried.

Section 2 – Automated Subsequent Activity Notifications
Motion: Endorse to accept the Northeastern Working Group motion to adopt Option 1 with the addition of adding the UCN to all notifications and III instead of spelling out Interstate Identification Index.
Action: Motion carried.

Section 3 – Manual Messages
Motion: Endorse original proposal in A-F with the exception of replacing Interstate Identification Index with III.
Action: Motion carried.

NCIC SUBCOMMITTEE ACTION:

Section 1

Motion: To endorse the recommendation of the IS Subcommittee (as noted above) with the addition of adding the UCN to all notifications. Priority of 3M.

Action: Motion carried.

Section 2

Motion: To endorse the recommendation of the IS Subcommittee (as noted above).
Priority of 3M.

Action: Motion carried.

Section 3

Motion: To endorse the recommendation of the Northeastern Working Group (as noted above).
Priority of 3M.

Action: Motion carried.

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC)
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

NCIC ISSUE #2

Law Enforcement Enterprise Portal (LEEP) Status Report

PURPOSE

To provide a status report on activities and initiatives.

POINT OF CONTACT

Global Law Enforcement Support Section (GLESS), Online Services and Operations Unit (OSOU)

Questions regarding this topic should be directed to <agmu@leo.gov>.

BACKGROUND

OSOU is responsible for the management of LEEP, SIGs, Virtual Command Center (VCC), @leo.gov email, and JusticeConnect. In support of the progression of LEEP and its Service Providers (SPs), OSOU has planned, developed and implemented several initiatives to enhance the effectiveness of LEEP, SIGs, VCC, @leo.gov email, and JusticeConnect. OSOU has prepared this status report on its activities and initiatives for the purpose of CJIS APB awareness.

LEEP Identity and Access Management

OSOU is currently developing a participation strategy for partnership expansion at the federal, state, local, tribal, and territorial (FSLTT) level. OSOU's strategy includes identifying key agencies for onboarding to LEEP and leveraging the CJIS Advisory Process and the FBI's existing partnerships. LEEP participation is measured by the number of Identity Providers (IdPs) as well as the number of offered services.

New LEEP Identity Providers

Identity Provider-Agencies	Type of System
Department of the Interior, Incident Management and Analysis Reporting System (IMARS)	Federal
Pima County Sheriff's Office, AZ	Local

IdPs are FSLTT agencies which create, maintain, manage and authenticate the identity information for their users to LEEP. Agencies must provide appropriate documentation and meet specific technical and operational requirements to become an IdP.

Identity Provider Requirements

Documentation	Technical	Operational
Initial On-boarding Meeting discussion of documentation and overview of technical process. Includes review of: SPs, IdPs, attributes, **Security Assertion Markup Language (SAML)**, LEEP Frequently Asked Questions, etc.	Review technical document **Metadata and SAML Information**.	**Must have Remote Access to LEEP.** Users will need to have secure access to LEEP remotely.
Review the **LEEP Procedures and Operations Manual**.	Initial Technical Meeting to determine tentative schedule for deployment, testing, and go-live dates.	**No need for LeepID Accounts.** An IdP's users will need to use their IdP accounts and therefore, LeepID accounts will no longer be given out to those users.
Review the **CJIS Security Policy**	Exchange and review metadata.	
Complete **LEEP IdP Participant Questionnaire**	Determine attribute format and type to send to LEEP.	Provide agency icon
Must receive **CJIS Systems Officer concurrence** (via email) and review copy of **CJIS User Agreement**.	Schedule dates and times testing.	Provide a brief description of service.
A technical review completed by the CJIS Audit Unit.	Perform test assertion; additional testing may be required.	Communications Plan: Agency Help Desk and user notifications

LEEP identity management is bifurcated between CJIS partner agency IdPs and the CJIS Division managed IdP known as LeepID Accounts. Currently, a majority of users access LEEP through the LeepID Accounts IdP. The GLESS strategic vision and goal for CJIS identity management is to draw down LeepID Accounts while transitioning primary access to CJIS Systems Agency (CSA) IdPs. The purpose of this effort is to focus CJIS identity management support on the small, local, tribal, and territorial agencies with limited resources, who have no other options for access to LEEP SPs.

LEEP SPs

SPs provide access to their databases, or information services, in accordance with their established policies and procedures, to authorized users accessing LEEP.

New LEEP Service Providers

Services	Providers
Symbol Affiliation Library (SAL)	FBI CJIS Division
National Use-of-Force Data Collection	FBI CJIS Division
VALOR, Officer Safety Initiative	Institute for Intergovernmental Research

OSOU Accomplishments

- **CJIS Services Portlet –** LEEP users can now set their preferences to view only CJIS SPs when they access the portal by selecting the CJIS Services Portlet button on the LEEP view filter.

- **Chat –** This instant messaging feature within JusticeConnect, allows real-time communication with individuals or group collaboration, with an option to share files.

- **LeepID Accounts –** The password expiration requirement was extended from 90 to 180 days. The account inactivity requirements were extended from 35 to 90 days.

OSOU Initiatives

OSOU is facilitating several initiatives to enhance the users' information sharing experience and expedite access to the services they need.

- **Mobility –** OSOU is working with the FBI Mobility Program Office and CJIS internal stakeholders to develop mobility services for all LEEP users. The end goal is to provide IdPs with access to LEEP SPs through a LEEP Mobility App. This project is contingent upon technical development capabilities and security policy requirements. Currently the plan for mobility development is conceived in three phases. Phase one should deliver single sign on mobility app access to all FBI users. Phase two will develop and test single sign on capability for all other LEEP IdPs. Phase three will involve consideration of the CJIS Security Policy for proper governance of mobility app access to CJIS Systems.

- **LeepID Account Management Redesign –** OSOU is developing a new identity management system to automate the LeepID Accounts IdP. The new identity management system will further automate the CJIS Division's vetting and re-vetting process. Phase two of this project will facilitate the CSA's role in validating the identities of their respective users. The identity management redesign will include: collection of required user information; users' supervisor data; users' employer information; automation of email notifications; validation of required user attributes; user preferences; PII encryption in transit; audit capabilities; role-based, enhanced user interfaces with intuitive dashboard capabilities; duplicate record detection; active Point of Contact management; and preferred method of contact.

- **FirstNet -** FirstNet is an independent authority within the U.S. Department of Commerce. Authorized by Congress in 2012, its mission is to develop, build and operate the nationwide, broadband network that equips first responders with dedicated, priority access; preemption; and more network capacity. OSOU is exploring FirstNet federation with LEEP. If successful, FirstNet would become a LEEP IdP. OSOU is working with FirstNet to validate their vetting procedures in compliance with the CJIS Security Policy to ensure only criminal justice agency users obtain access to LEEP through FirstNet devices. OSOU will onboard FirstNet under a Memorandum of Understanding (MOU) for *a federal agency without a CJIS Systems Officer*. The MOU will authorize roles and responsibilities, leveraging FirstNet agency administrators' duties for access and usage. Once FirstNet is federated with LEEP, OSOU will explore how users may be permitted to access CJIS data through FirstNet.

- **CSO Tool –** OSOU is exploring the development of a CSO identity and access management tool to empower CSOs with direct management of user access, auditing, training, application tracking, information dissemination, CSO centric attributes, and role-based access to CJIS Services.

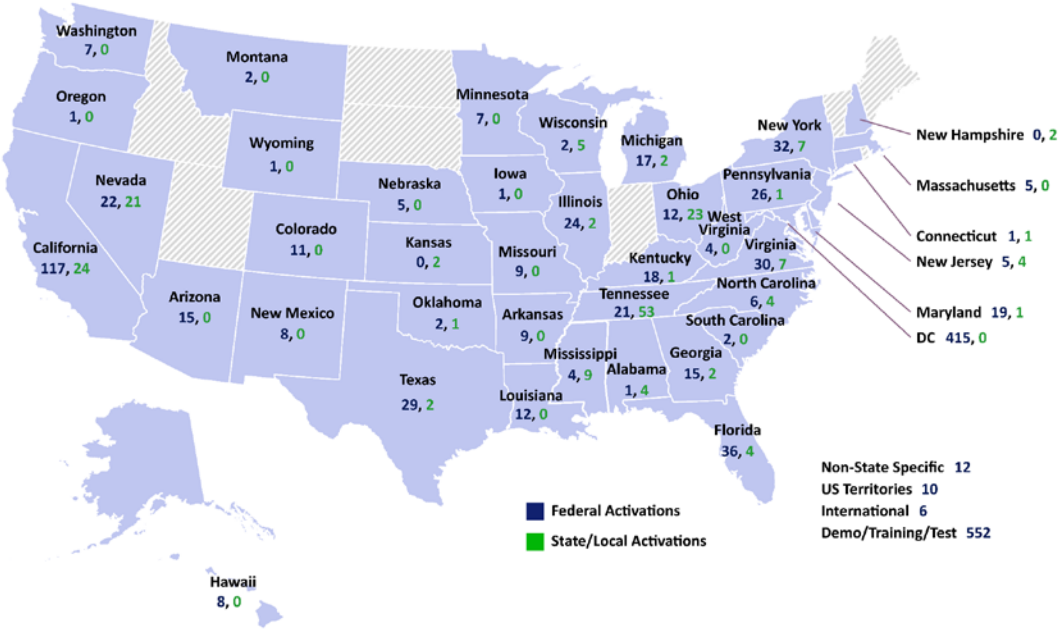
<u>OSOU Managed Services</u>

JusticeConnect – a criminal justice network designed to facilitate collaboration, among LEEP users.

- A collaborative environment featuring wikis, blogs, communities of interest, and activities (taskings).
- Available to LEEP users since May 21, 2018.
- JusticeConnect is replacing SIGs as the primary hub for information sharing on LEEP.
- The Content Team is available to provide moderators with assistance in replacing their SIGs with JusticeConnect Communities.

VCC – event management applications for critical incidents, law enforcement operations, natural and manmade disasters, special events, and operations centers. VCC provides real-time situational awareness and event management, fostering multi-agency collaboration and allowing FLSTT users to share intelligence resources. From May 2018 to May 2019 there were over 1700 VCC activations, see *VCC Activations* map at the top of page 5.

VCC Activations
(May 2018 - May 2019)



OSOU is working to complete the following 2019 user driven VCC initiatives and priorities:

- FBI OPS Centers
- Geospatial interface (phase one)
- Blue force tacking system integration (phase two)
- Geographic Information System (GIS) integration (phase two)
- Personnel roster (Phase two)
- VCC Dashboard Custom View
- Calendar
- Incident reminders
- Bulk upload of data
- Linking or merging incidents
- Multiple locations per incident
- Chat
- VCC mapping upgrades: street view to satellite view; icon layering.
- VCCs and @leo.gov email are transitioning to Amazon Web Services (AWS) by 2020.

In the past year, the following VCC enhancements have been implemented:

- Multi VCC Unified Viewer

- Map layers, drawing tool, Google Street View
- Notifications and emails
- Personnel roster
- Command Center Accounts – 8 hour sessions
- TRAX - more custom fields
- Blue force tracking program integration (phase one)
- Incident log
- Access management
- Customization of all fields
- Fixes

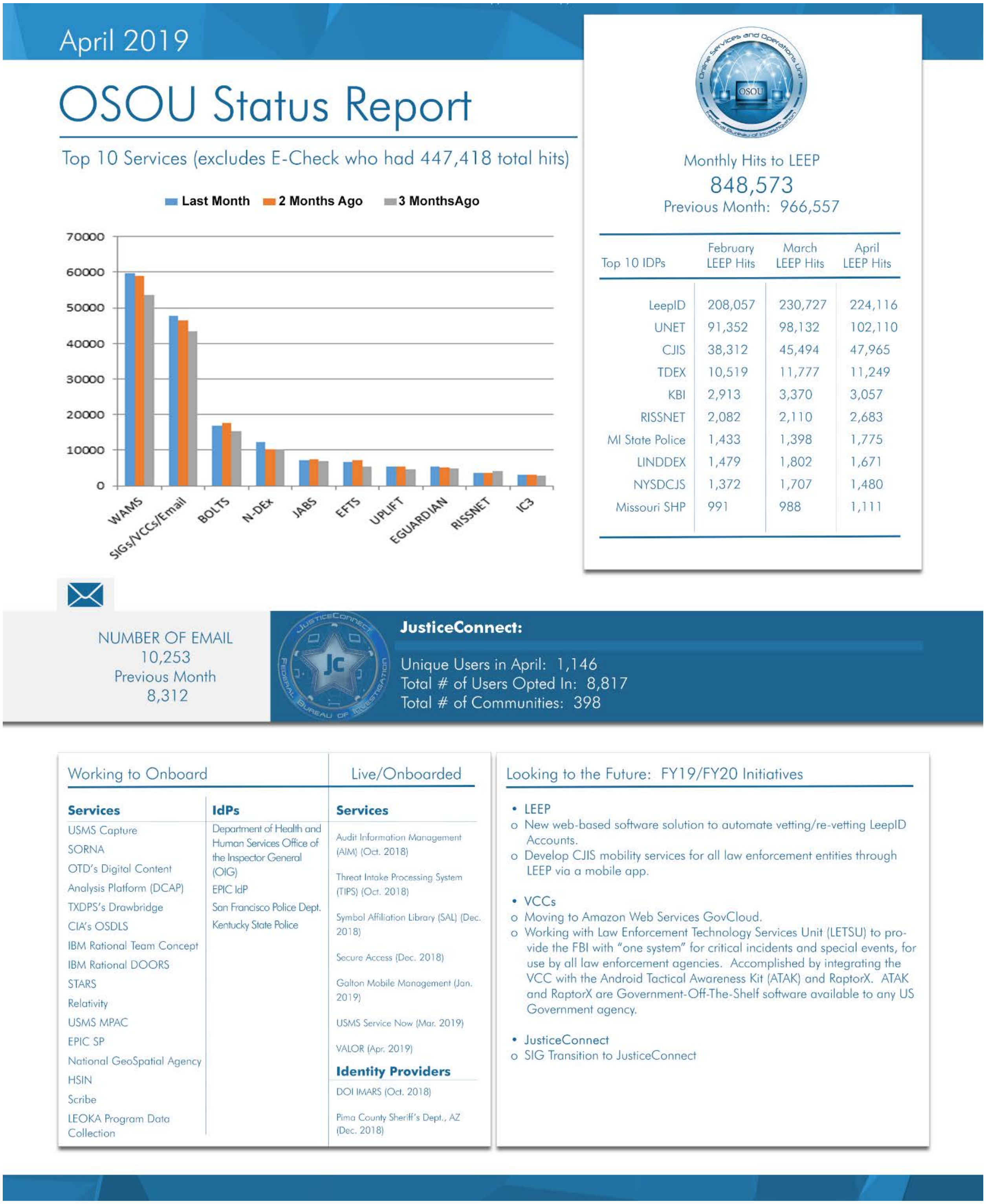
SIGs – This system will be decommissioned and its users transitioned to JusticeConnect. Transition from SIGs to JusticeConnect will be completed by September 30, 2019. SIG Moderators should contact the Content Team, via email at <content@leo.gov>, or by phone at (225) 578-9287, for assistance with transitioning SIG information to JusticeConnect.

OSOU Reporting and User Analysis

To improve program management and enhance system development, OSOU collects information on its systems and users from two sources, automated system reports and user feedback assessments.

OSOU collects statistics on the usage of LEEP, @leo.gov Email, VCCs, JusticeConnect, and SIGs. Beginning in 2017, OSOU established a monthly report for all OSOU Services. Due to increased system prominence within the FBI, OSOU added a standalone VCC monthly report in January, 2019. These two monthly reports are produced from automated system usage statistics but also include current projects, initiatives, or events, see attachments, pages 7 and 8.

OSOU conducts an annual analysis of user activity to determine: the types of users who access the systems; the reasons they access the systems; and what services or functionality the users would like to see added to the systems. From the results of the analysis, the majority of users are law enforcement who use LEEP for investigative support and intelligence sharing. The functionality users would most like to see added to the system is mobility app access, see attachment, page 9.


Last Month
2 Months Ago
3 MonthsAgo
70000
60000
50000
40000
30000
20000
10000
0
WAMS
SIGs/VCCs/Email
BOLTS
N-DEx
JABS
EFTS
UPLIFT
EGUARDIAN
RISSNET
IC3
OSOU
Online Services and Operations Unit
Federal Bureau of Investigation
JusticeConnect
Federal Bureau of Investigation
JC

April 2019

OSOU Status Report

Top 10 Services (excludes E-Check who had 447,418 total hits)

Monthly Hits to LEEP
848,573
Previous Month: 966,557

Top 10 IDPs	February LEEP Hits	March LEEP Hits	April LEEP Hits
LeepID	208,057	230,727	224,116
UNET	91,352	98,132	102,110
CJIS	38,312	45,494	47,965
TDEX	10,519	11,777	11,249
KBI	2,913	3,370	3,057
RISSNET	2,082	2,110	2,683
MI State Police	1,433	1,398	1,775
LINDDEX	1,479	1,802	1,671
NYSDCJS	1,372	1,707	1,480
Missouri SHP	991	988	1,111

NUMBER OF EMAIL
10,253
Previous Month
8,312

JusticeConnect:

Unique Users in April: 1,146
Total # of Users Opted In: 8,817
Total # of Communities: 398

Working to Onboard

Services

USMS Capture
SORNA
OTD's Digital Content
Analysis Platform (DCAP)
TXDPS's Drawbridge
CIA's OSDLS
IBM Rational Team Concept
IBM Rational DOORS
STARS
Relativity
USMS MPAC
EPIC SP
National GeoSpatial Agency
HSIN
Scribe
LEOKA Program Data Collection

IdPs

Department of Health and Human Services Office of the Inspector General (OIG)
EPIC IdP
San Francisco Police Dept.
Kentucky State Police

Live/Onboarded

Services

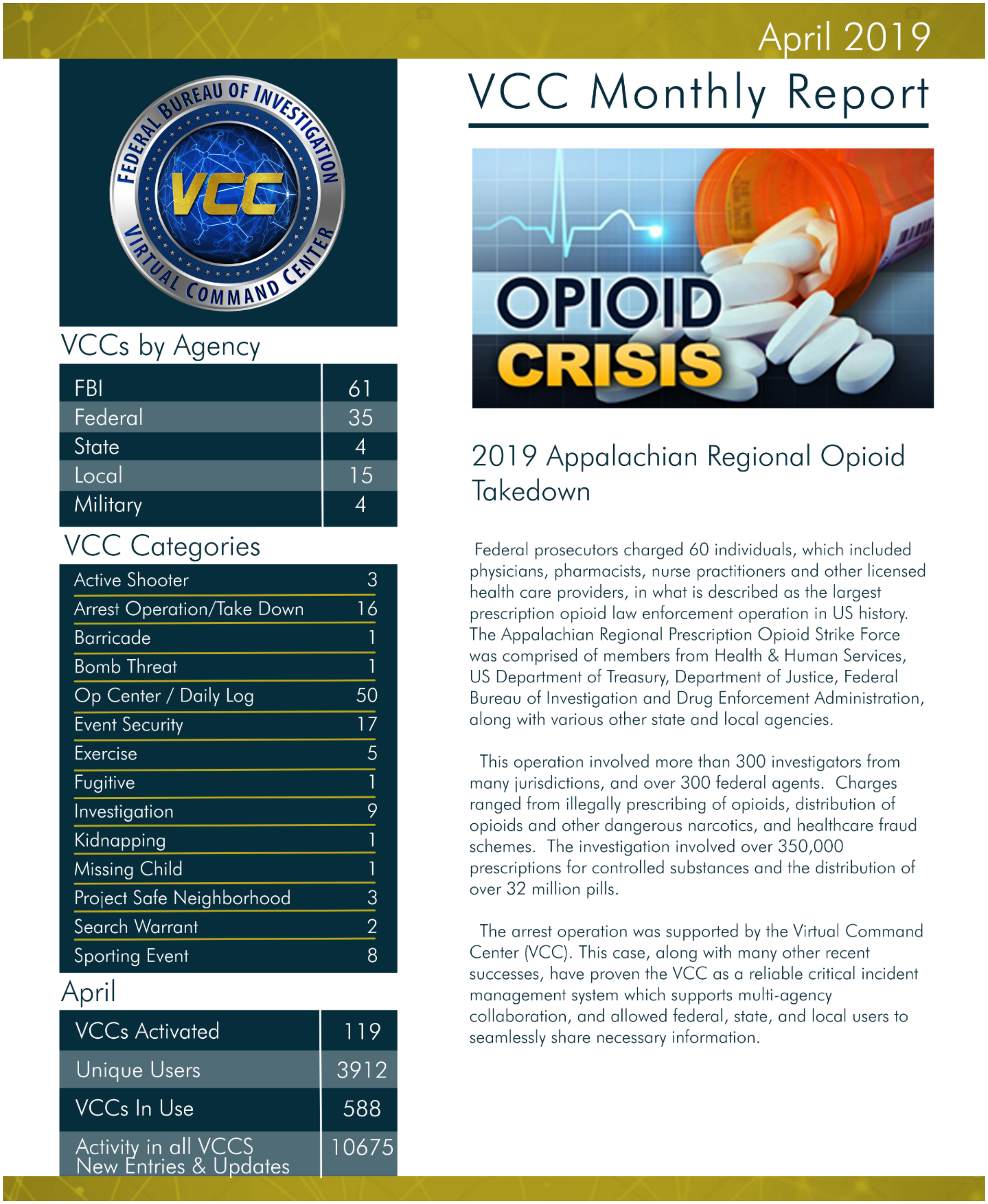
Audit Information Management (AIM) (Oct. 2018)
Threat Intake Processing System (TIPS) (Oct. 2018)
Symbol Affiliation Library (SAL) (Dec. 2018)
Secure Access (Dec. 2018)
Galton Mobile Management (Jan. 2019)
USMS Service Now (Mar. 2019)
VALOR (Apr. 2019)

Identity Providers

DOI IMARS (Oct. 2018)
Pima County Sheriff's Dept., AZ (Dec. 2018)

Looking to the Future: FY19/FY20 Initiatives

- LEEP
  - o New web-based software solution to automate vetting/re-vetting LeepID Accounts.
  - o Develop CJIS mobility services for all law enforcement entities through LEEP via a mobile app.
- VCCs
  - o Moving to Amazon Web Services GovCloud.
  - o Working with Law Enforcement Technology Services Unit (LETSU) to provide the FBI with "one system" for critical incidents and special events, for use by all law enforcement agencies. Accomplished by integrating the VCC with the Android Tactical Awareness Kit (ATAK) and RaptorX. ATAK and RaptorX are Government-Off-The-Shelf software available to any US Government agency.
- JusticeConnect
  - o SIG Transition to JusticeConnect



April 2019

VCC Monthly Report

OPIOID
CRISIS

VCCs by Agency

FBI	61
Federal	35
State	4
Local	15
Military	4

VCC Categories

Active Shooter	3
Arrest Operation/Take Down	16
Barricade	1
Bomb Threat	1
Op Center / Daily Log	50
Event Security	17
Exercise	5
Fugitive	1
Investigation	9
Kidnapping	1
Missing Child	1
Project Safe Neighborhood	3
Search Warrant	2
Sporting Event	8

April

VCCs Activated	119
Unique Users	3912
VCCs In Use	588
Activity in all VCCS New Entries & Updates	10675

2019 Appalachian Regional Opioid Takedown

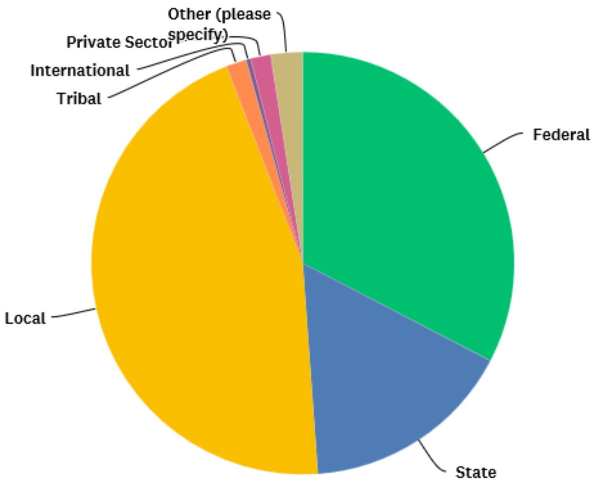
Federal prosecutors charged 60 individuals, which included physicians, pharmacists, nurse practitioners and other licensed health care providers, in what is described as the largest prescription opioid law enforcement operation in US history. The Appalachian Regional Prescription Opioid Strike Force was comprised of members from Health & Human Services, US Department of Treasury, Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration, along with various other state and local agencies.

This operation involved more than 300 investigators from many jurisdictions, and over 300 federal agents. Charges ranged from illegally prescribing of opioids, distribution of opioids and other dangerous narcotics, and healthcare fraud schemes. The investigation involved over 350,000 prescriptions for controlled substances and the distribution of over 32 million pills.

The arrest operation was supported by the Virtual Command Center (VCC). This case, along with many other recent successes, have proven the VCC as a reliable critical incident management system which supports multi-agency collaboration, and allowed federal, state, and local users to seamlessly share necessary information.

What is your primary jurisdiction type? (Please select the one jurisdiction type most in line with your employer)

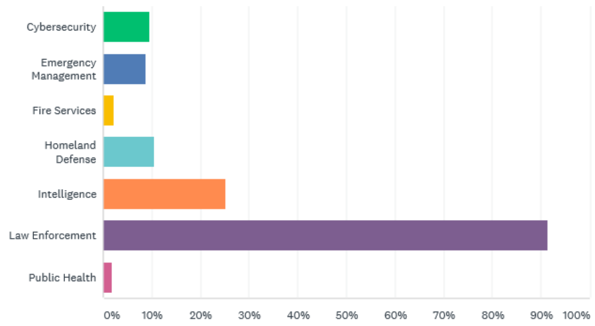
Answered: 579 Skipped: 4



FY18 LEEP Annual Assessment

What is your primary mission area? (Select all that apply)

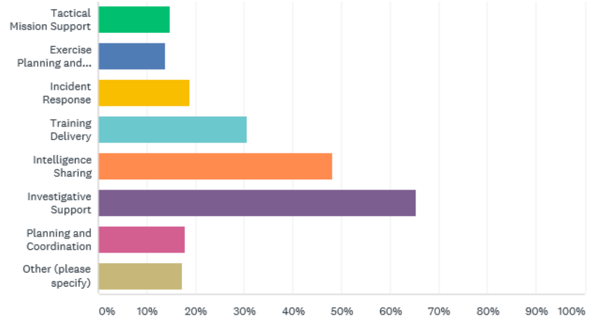
Answered: 580 Skipped: 3



FY18 LEEP Annual Assessment

In what ways do the LEEP services support your operational needs? (S...

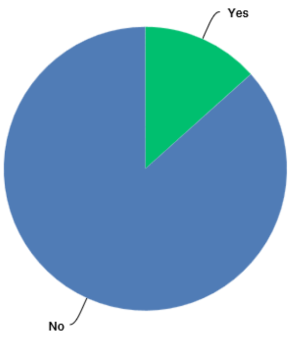
Answered: 577 Skipped: 6



FY18 LEEP Annual Assessment

Do you use LEEP on your mobile device?

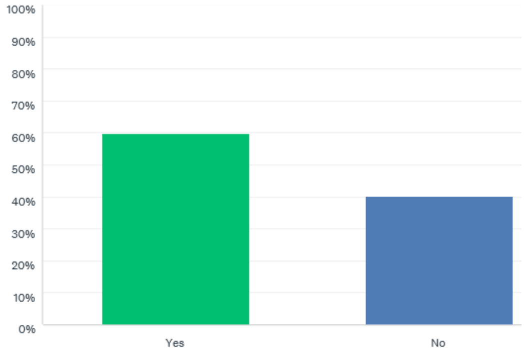
Answered: 560 Skipped: 23



FY18 LEEP Annual Assessment

Would a LEEP mobile app improve efficiencies in your job?

Answered: 566 Skipped: 17



FY18 LEEP Annual Assessment

FALL 2019 WORKING GROUP ACTIONS:

This topic was accepted as information only by all five working groups.

FALL 2019 SUBCOMMITTEE ACTIONS:

This topic was accepted as information only by all of the subcommittees.

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC)
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

NCIC ISSUE #4

The Intra-Agency Sharing of National Sex Offender Registry (NSOR) Audit Reports, Findings, and Accompanying Documentation with the United States Department of Justice (USDOJ), Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (SMART)

PURPOSE

The USDOJ, SMART is requesting access to FBI Criminal Justice Information Services (CJIS) Division National Crime Information Center (NCIC) NSOR audit reports, findings, and accompanying documentation for the states, territories, and the District of Columbia (D.C.). This will facilitate statutorily mandated Sex Offender Registration and Notification Act (SORNA) implementation assurance reviews for all SORNA implemented jurisdictions as well as eliminate the need for an additional audit by the SMART Office regarding jurisdictional data entries into the NCIC NSOR File.

POINT(S) OF CONTACT

USDOJ SMART Office, (202) 307-0783

Questions regarding this topic should be directed to <agmu@leo.gov>

REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to review the information in this paper and provide comments, suggestions, and recommendations to the CJIS APB regarding the intra-agency sharing of the NSOR audit reports with the USDOJ SMART Office.

BACKGROUND

Under the Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (codified as amended at 34 U.S.C. § 20901 *et seq*. (2012)) (hereafter "AWA"), the Attorney General is mandated to assess and determine jurisdictions' efforts in implementation of the SORNA. The SMART Office is tasked by the Attorney General with determining the initial implementation of, and adherence to, the SORNA standards by the states and territories, as well as the District of Columbia. Once a jurisdiction has been found to have substantially implemented SORNA, the Attorney General is statutorily required to ensure that the respective jurisdiction continues to comply with the SORNA standards in each subsequent year. Part of this implementation assurance process requires that the SMART Office determine whether a jurisdiction is submitting the SORNA required sex offender registration information to the National Sex Offender Public Website (NSOPW), which is administered by the SMART Office, and to the law enforcement accessible NCIC NSOR File, which is administered by the FBI CJIS Division. The FBI CJIS Audit Unit (CAU) performs triennial audits of the jurisdictions submitting data into the NSOR File. The CAU collects and assesses information during the course of these audits that relates directly to and may significantly inform the SMART Office's assessment as to a jurisdiction's ongoing substantial implementation of the SORNA requirement to submit sex offender information into the NSOR File. The SMART Office is requesting access to NSOR audit reports, findings, and accompanying documentation for the states, territories, and D.C. as part of its statutorily required implementation assurance process.

The scope of audit report, findings, and accompanying documentation sharing will include all SORNA implemented states, territories, and the District of Columbia. The SMART Office will work directly with the state or territory sex offender registration points of contact and collateral professionals responsible for the collection and entry of sex offender registration information.

The CAU NSOR audits primarily evaluate NSOR entries at the registry level. The scope of this state-wide audit provides limited information about the NSOR entries from SORNA participating American Indian or Alaska Native Tribes and a United States Commonwealth. The SMART Office is aware of this limitation and is working to identify other means for assessing the compliance with sex offender data sharing requirements by these jurisdictions.

DISCUSSION AND ANALYSIS

The SMART Office, on behalf of the Attorney General, is mandated to assess jurisdictions' continued substantial implementation of SORNA's requirements and is requesting the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation.

To complete the mandated task, the SMART Office is requesting that the NSOR audit reports, findings, and accompanying documentation of a jurisdiction's NSOR audit be shared with the SMART Office in order for the SMART Office to determine compliance with the national sex offender data sharing requirements under the SORNA. The specific field information requested is listed in the chart below:

SORNA Required Information	Corresponding NSOR Fields
Name and Aliases	Name (NAM) Alias (AKA)
Social Security Number	Social Security Number (SOC)
Internet Identifiers	Internet Identifiers (IID) Email Address (EML)
Date of Birth	Date of Birth (DOB)

Driver's License Information	Operator's License Number (OLN) Operator's License State (OLS) Operator's License Year of Expiration (OLY)
Vehicle Information	License Plate Number (LIC) License Plate State (LIS) License Plate Year of Expiration (LIY) License Plate Type (LIT) Vehicle Identification Number (VIN) Vehicle Year (VYR) Vehicle Make (VMA) Vehicle Model (VMO) Vehicle Style (VST)
Passport, Identification and Immigration Documents Information	Miscellaneous Number (MNU) to include passport, personal identification, and alien registration numbers
Residence Address	State (STA) Street Number (SNU) Street Name (SNA) City Name (CTY) County (COU) Zip Code (ZIP) Address Type (ADD)
Employment Name and Address	Employer Name (EMP) Supplemental address data and indicate the address type (ADD) is Employer
School Name and Address	School Name (SHN) Supplemental address data and indicate the address type (ADD) is School
Physical description	Scars, Marks, Tattoos, and Other Characteristics (SMT) Sex (SEX) Race (RAC) Height (HGT) Weight (WGT) Eye Color (EYE) Hair Color (HAI)
Telephone Number	Telephone Number (TNO)
Professional Licensing Information	Professional License Number (PLN) Professional License Type (PLT)
Registration Offense and Criminal History Information	Conviction Resulting in Registration (CRR) Date of Conviction (CON)
International Travel Information	No corresponding NSOR Field although if offender indicates he/she is relocating to an international location, Offender Status (OFS) field allows for "Relocated to an International Location" code.

Temporary Lodging Information	Supplemental address data and indicate the address type (ADD) is “Temporary Lodging” Offender Status (OFS) could also be entered as “Vacation”, “Visiting”, or “Visitor” code
SORNA requires NSOR to be updated within three days if offender has failed to register or is an absconder, etc.	Offender Status (OFS) allows for “Failure to Register” and “Absconder”, etc.
Fingerprints and Palm Prints or “identifying numbers” that “provide access to fingerprint and palm print information in other databases” (i.e. FBI/UCN number)	FBI Number/UCN (FBI)

The above information is what the SMART Office would want to learn from an FBI NSOR audit so that they can follow up with the jurisdictions who are not complying as part of their implementation assurance review. Since FBI NSOR audits already look at timeliness as defined under SORNA and completeness, the SMART Office believes it covers most of the fields already. The SMART Office would like to know if the jurisdiction is collecting the information and submitting the information into the relevant NSOR fields and if not, what are the issues. This will enable the SMART Office to offer grant assistance to jurisdictions that may need financial support/additional technology or resources to complete these tasks, and work with non-implemented jurisdictions who apply for reallocation funds to use some or all of those funds to meet their NSOR requirements.

Access to the NSOR audit reports, findings, and accompanying documentation on required SORNA data fields will allow the SMART Office to identify which jurisdictions are entering sex offender information into the NSOR File completely, accurately, and in a timely manner, as required by the SORNA. As part of the NSOR audits, the CAU requests that jurisdictions detail the sex offender registration information that is collected and submitted to the NSOR File through the pre-audit questionnaire. The CAU verifies that this information is entered by the jurisdiction and that it is submitted to the NSOR File. The CAU also audits the NSOR entries for accuracy, completeness, and timeliness as part of their mission to ensure the integrity of data contained in the NCIC.

The SMART Office’s access to the CAU’s NSOR audit reports and findings will eliminate a duplication of effort by a fellow Department of Justice agency and will reduce the likelihood of contrary findings or miscommunication to jurisdictions about their NSOR File entries. This will also assist the SMART Office in working with the SORNA jurisdictions on issues that may affect accuracy, completeness, and timeliness of NSOR File entries.

The NSOR audit reports and findings, including the pre-audit questionnaire, contain the majority of the information that the SMART Office needs to assess implementation assurance with the data sharing requirements of the SORNA. Receiving the questionnaire, reports, findings, and accompanying documentation ensure that the SMART Office will have the most recent and complete materials from which to make a compliance determination and will eliminate the need for the jurisdiction's CJIS Systems Agency to provide the state's Governor's Office this documentation during SORNA implementation assurance reviews.

A SORNA jurisdiction may or may not be aware of current problems with data loss or completeness in the NSOR File fields and having access to these reports will enable the SMART Office to assist the jurisdiction in the development of solutions for creating a more robust system of data collection and sharing. The SMART Office has grant funds available for jurisdictions that want to update or expand the criminal justice information systems that are integral to the collection, retention and communication of sex offender registration data. Currently the SMART Office does not become aware of the need to offer assistance to SORNA jurisdictions for needed technology upgrades unless a jurisdiction specifically notifies the SMART Office of the issues and requests assistance.

Costs:

No additional costs would be associated with this request as the CAU currently collects and records this information. Sharing of the information with the SMART Office could be accomplished in the manner currently utilized by the CAU when sharing files and would require no additional equipment. Sharing files and data digitally between Department of Justice agencies does not incur any additional costs or approvals.

Alternatives:

The alternative to the CAU sharing the audit reports and findings would be for the states, territories, and D.C. to undergo a second audit. The second audit would include providing the most recent NSOR audit report and findings for review by the SMART Office. This would be part of the implementation assurance process currently being conducted by the SMART Office and involves the Governor of each SORNA implemented state providing documentation as part of their certification of continued SORNA implementation.

Scheduled implementation date:

The SMART Office is requesting that the sharing of the NSOR audit reports and findings will begin upon the FBI Director's approval of the CJIS APB's Recommendation and execution of the Memorandum of Understanding.

Coordination of services:

This proposal will involve a coordinated effort between the CAU and the SMART Office to share the information contained in the CAU's audit reports, findings, and accompanying documentation on required SORNA data fields. Additionally, the SMART Office shall work with the states and territories to find solutions to any existing sex offender data sharing problems. The SMART Office will consult with the FBI CJIS Division, as needed, as part of assisting the jurisdiction's sex offender registry personnel. This could include discussions of best practices or problem solving of technological issues when collecting the required sex offender registration information, retaining that information, and inputting this data into the NSOR File in the most effective manner.

OPTIONS

The Subcommittee is requested to discuss the proposal, provide the necessary input, and choose one of the following options:

Option 1: Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office.

Option 2: No change.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt a new Option 3: Hold on an endorsement until such time the Working Groups have an opportunity to review and comment on the proposed MOU between the DOJ and FBI. Further, the Working Group requests that the MOU will include language specifically related to secondary dissemination of FBI CJIS Audit reports, findings, and accompanying documentation.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2: No change.

Action: Motion carried.

FALL 2019 NCIC SUBCOMMITTEE ACTION:

Motion: To accept a new option, Option: Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART office through the implementation of a Memorandum of Understanding that addresses the use and secondary dissemination of the data.

Action: Motion carried.

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC)
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

NCIC ISSUE #7

NCIC Third Generation (N3G) Project

PURPOSE

To provide a status on recommendations of the N3G Task Force

POINT OF CONTACT

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to agmu@leo.gov

BACKGROUND

The purpose of the N3G Project is to identify requirements which will improve, modernize, and expand the existing NCIC system to continue providing real-time, accurate, and complete criminal justice information in support of law enforcement and criminal justice communities.

In June 2016, the APB approved, for further exploration, 14 high-level concepts as representation of more than 5,500 user requests. Functional requirements correlating to those high-level concepts were subsequently forwarded for further review and are listed with the status of the approval process.

Concept 1: Flexible Data Format – Director Approved
Concept 2: Tailored Functionality – Director Approved
Concept 3: Access Data Repositories – Director Approved
Concept 4: Name Search Algorithm – Director Approved
Concept 5: Enhanced Data Search – Director Approved
Concept 6: System Search - Director Approved
Concept 7: Enhanced Training Resources – Director Approved
Concept 8: Enhanced Testing Environment – Director Approved
Concept 9: Record Content - Director Approved
Concept 10: Enhanced Multimedia – Director Approved
Concept 11: Improved Data Management – Director Approved
Concept 12: Alternative Outbound Communications – Director Approved
Concept 13: Alternative Access – Director Approved
Concept 14: Improved Outbound Communications - Director Approved

An N3G Task Force was established to assist with the development of the N3G Project. The purpose of the N3G Task Force is to offer continuous subject matter expertise and user experience to the CJIS Division project personnel during the development of N3G. The APB also granted the N3G Task Force the discretion to provide the initial review, acceptance, and disposition or disposal of the concepts and their associated functional requirements before introducing them through the CJIS Advisory Process. The inaugural N3G Task Force meeting was held on 08/18/2015, and meetings have routinely been conducted both in person and telephonically since the initial meeting. As a result of the collaborative efforts of the N3G Project Team and the N3G Task Force, over 1200 functional requirements associated with the 14 high-level concepts were identified.

The N3G Task Force dispositioned all 1200 of the initial functional requirements and recommended 376 move forward for further exploration. Those functional requirements were approved by the APB during meetings held in June 2017 through December 2018. None of the initial functional requirements proposed for Concept 13 were approved by the N3G Task Force. This recommendation was subsequently endorsed by the APB at the December 2017 meeting.

N3G Functional Requirement Exploration Strategy

Since the initial Advisory Process review of N3G Task Force approved functional requirements has concluded, the N3G Task Force has moved into its next area of responsibility to further explore APB approved functional requirements in conjunction with the NCIC Program Office. The method to further explore the remaining N3G functional requirements and an agile Advisory Process approval strategy were adopted by the APB in June 2018. The APB recognized that a streamlined approval process was necessary to ensure the successful and timely deployment of N3G functionality using the Agile Development Methodology.

As a reference, the APB approved process, for moving functional requirements forward, allows the N3G Task Force to determine if a functional requirement falls into either the “straight forward” or “needs further research” category. As described in the spring 2018 topic paper, many of the APB-approved “for further exploration” functional requirements are very straight forward and need no further policy-related information for development. For instance, a requirement may read “expand the name field to 50 characters.” This requirement is straight forward, needing no further policy review for development. As such, it can be turned over to developers as currently defined. The N3G Task Force has identified approximately 150 requirements which fall into the straight-forward category. Other functional requirements do need further policy, legal, and technical refinement such as the ability to enter “multiple warrants for the same subject by the same ORI.” Further research, legal review, and technical impact analysis on 260 of those types of requests will be conducted by the N3G Task Force and the CJIS Division NCIC Program Office collectively. Once completed, those identified as adding value and benefit to NCIC stakeholders will move to the development stage.

As a reminder, any requirements needing major modifications or new requirements identified by the N3G Task Force will be forwarded through the Advisory Process for final approval. Functional requirements no longer supported by the N3G Task Force will not be moved forward for inclusion in N3G project development. Functional requirements excluded after the N3G Task Force further exploration are identified in an addendum to this paper for traceability purposes. These items will continue to be included with the N3G Project staff paper for the next several rounds of the Advisory Process meetings until all the exclusions are exhausted.

N3G Functionality Approval Strategy

As the N3G Task Force continues exploring the APB approved functional requirements, new system functionality emerges. This includes an emphasis on streamlining processes when possible, coupled with the development of new or modified policy definitions. In accordance with the APB agile approval process, as N3G Task Force approved functionality advances to the development effort and is ready to demonstrate, the N3G Task Force will confirm functionality (virtually or in person) meets the original intent, as approved by the APB. Their decisions will be forwarded to the NCIC Subcommittee for advisement and endorsement. If the NCIC Subcommittee concurs with the Task Force decision, the recommended N3G functionality will advance to the non-operational environment or directly to the APB for final disposition. Conversely, if the N3G Task Force determines the functionality requires further refinement, it will be returned to a development program backlog and then reintroduced into the development process once necessary changes are identified. Although this approach places considerable responsibility on the N3G Task Force up front, it will pave the way for continued user engagement in the N3G development effort.

The N3G Task Force has established and continues to reiterate several “guiding principles” to be taken into consideration as the requirements are further analyzed and developed. One such principle is to ensure current system performance and response times are not degraded with the introduction of new functionality. Another principle established is continued support of legacy functionality. Since CJIS Systems 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. This will ensure vital services remain available to all users. The intent of the N3G project is to be forward looking, but backward compatible. Additional guiding principles include the integration of national standards, when applicable, and scalability. The next generation of the NCIC system should provide scalable capacity for additional input, storage, processing, and output functionality. Furthermore, the N3G Task Force determined enhancements to the NCIC system should be established as user friendly and intuitive as possible. Providing a more intuitive system could simplify training new users and allow current users to be more efficient and effective.

N3G User Transition Fundamentals

During the spring 2019 N3G project update, CJIS Division staff clarified that the N3G project is an enhancement effort rather than a full system replacement. Based on this premise, the N3G Task Force supported two fundamental N3G transition requirements. These are based on the understanding in which NCIC will continue to release newly developed functionality in the operational environment consistent with the annual enhancement build schedule and associated notification process existing today. They are also in keeping with the "guiding principles" as described previously. During their June 2019 meeting, the APB approved the following two N3G User Transition Fundamentals as recommended by the N3G Task Force:

Extensible Markup Language (XML) User Transition Timeframe

a. All CSAs and direct interface agencies must convert to the National Information Exchange Model (NIEM) data processing format, using web service applications, from the current NCIC socket supported dot delimited and Global Justice Data Model (GJXDM) formats by **September 30, 2022**.
b. Dot delimited and GJXDM XML formatted messages, along with Transmission Control Protocol/Internet Protocol socket and MQ Series Protocols will no longer be supported effective **September 30, 2022**.

1. **Availability of New Functionality**
   a. N3G developed functionality, to include improved and streamlined capabilities, along with new files, fields and codes will only be available for entry and maintenance using the NIEM XML data processing format. However, dot delimited and GJXDM XML users must be able to accept new data in responses.

DISCUSSION AND ANALYSIS

N3G Project – Functionality Approved by the N3G Task Force for Development

As the N3G Task Force further explores approximately 260 functional requirements associated with the original 14 high-level N3G concepts, policy subgroups are formed to thoroughly investigate all aspects of the proposed functionality. Thus far, seven policy groups including a Gang, Warrant, Supplemental Data, Message Key, Missing and Unidentified Persons, XML and a Blue Alert subgroup have been established, meet on a regular basis and some have concluded. Each group is represented by members of the N3G Task Force in addition to other law enforcement and criminal justice community subject matter experts. As the groups presented recommendations to the N3G Task Force for further consideration, it became evident that individual functional requirements have inter-dependencies. As such, holistic functionality has emerged which encompasses some, or even many individual functional requirements. Individual functional requirements will no longer be presented individually through the Advisory Process with the understanding that the functionality approved by the N3G Task Force satisfies all of the associated functional requirements. Conversely, as discussed previously, functional requirements the N3G Task Force excludes will be identified in the addendum at the end of the staff paper for traceability purposes. The N3G Task Force approved functionality, as described below, is being provided for your information and awareness as it will move forward to the agile development process.

Blue Alert

Throughout the N3G user canvass, there were many requests to enhance officer safety. One specific request was to create a Blue Alert Missing Person Circumstance (MPC) code in NCIC.

Although, the request was specific to functionality that currently exists in the NCIC Missing Person File, the N3G Task Force determined that it would be beneficial to explore Blue Alerts in a more comprehensive manner. The group discussed the sharing opportunities that are currently available for Blue Alerts and determined that it would be beneficial to include a Blue Alert flagging mechanism in NCIC. The N3G Task Force approved the following functionality related to the Blue Alert issue:

- An Alert field will be created in the Vehicle, Wanted Person, Missing Person and Violent Person files.
- The caveat generated when Blue Alert is entered in the Alert field in the Vehicle, Wanted Person and Violent Person files will be returned on record responses in the respective files to indicate: **BLUE ALERT WARNING. USE EXTREME CAUTION IN APPROACHING THIS INDIVIDUAL/VEHICLE.**
- The caveat generated when Blue Alert is entered in the Alert field in the Missing Person file will be returned on record responses to indicate: **BLUE ALERT WARNING. THE INDIVIDUAL OF RECORD IS AN OFFICER MISSING IN THE LINE OF DUTY.**

Missing and Unidentified Files

The Missing and Unidentified (M/U) Policy Group was established out of the N3G Task Force to review the NCIC Missing Person File and the Unidentified Person File; as well as the automatic comparison process between the files known as the NCIC Cross-Match. The initial objective of the M/U group is to simplify record entry into the Missing Person File. Although the group is putting forth a recommendation in this regard, ongoing discussions continue on several issues related to streamlining the record entry process identified during the N3G user canvass. The M/U group dispositioned numerous requests for the creation of codes to account for elderly individuals which have gone missing and individuals that may pose a threat to law enforcement. The M/U Policy Group reviewed existing fields wherein this information could be included. It was decided that the new code requests would align with codes available in the Missing Person (MNP) field; however, the field would best be identified as an “Alert” field since most information entered generates a notification, or an alert. As a result, the N3G Task Force approved the following functionality related to the Missing Person issue:

- Eliminate the MNP field in lieu of an “Alert” field.

Gang File

The Gang File Policy Group was created to review the use of the NCIC Gang File and explore methods to promote record entry. User requests focused on the process for Group Name (GNG) and Subgroup Name (SGP) code assignment and enhancing entry capability. The group questioned if the GNG and SGP codes provided benefit to tactical users. The Gang File Policy Group further identified investigative users as secondary users able to obtain further information by contacting the record owner. The group considered numerous alternatives to decrease the amount of time needed to assign group codes and allow state systems to seamlessly exchange gang names with NCIC.

The Gang File Policy Group additionally examined the criteria for entry in the Group Member Capability (GMC). Changes to the GMC entry criteria have been considered on numerous occasions by the APB. Entry criteria for the national repository of gang members is especially difficult to approach due to the lack of a consistent membership standard across jurisdictions. The policy group discussed the addition of a new Entry Criteria (ECR) field code to address the issue. The N3G Task Force approved the following functionality related to the NCIC Gang File:

- Change the GNG and SGP fields to free-text allowing codes or naming conventions to be passed from the state repository.
- Remove the mandatory requirement for a Group Reference Capability record to exist for active group members to be entered.
- Create a new primary ECR code to identify a subject meeting the state definition of "gang member".

Felony Boat

During the N3G user canvass, it was recommended that felony boat records be allowed in the NCIC Boat File. A felony boat record would contain information on a boat that has been used in the commission of a felony and the location of the boat is unknown. The N3G Task Force approved the following functionality related to the Felony Boat issue:

- Felony boat records will be allowed to be entered in the NCIC Boat File.
- Retention for felony boat records will be a maximum of 90 days from the day of entry.
- The mandatory fields for entry will mimic the mandatory fields for entry for stolen boat records.

FALL 2019 WORKING GROUP ACTIONS:

This topic was accepted as information only by all five working groups.

FALL 2019 NCIC SUBCOMMITTEE ACTION:

This topic was accepted as information only.

National Crime Information Center (NCIC) Third Generation (N3G) Project Addendum

Functionality excluded after Program Office Research

Concept 9

- **Create a Blue Alert MPC Code.**

The N3G Task Force moved to exclude the request to create a Blue Alert MPC code in the NCIC Missing Person File. This was based on the recommendations from the Blue Alert Policy group and the decision to include Blue Alert in a newly created Alert Field.

- **Create a Missing Vulnerable Adult MNP Code**

During the N3G user canvass, there were numerous requests for codes to be included in fields describing the circumstances in which an individual is deemed to be missing. The N3G Task Force elected to exclude the request to create a Missing Person Vulnerable Adult code and recommended that a "Silver Alert" code be considered for the newly created Alert field. Codes for the Alert field (to include Silver Alert) are currently being reviewed and will be proposed in a future N3G topic paper.

Concept 11

- **Provide the ability to pull gang data from other files for ease of entry.**

After considering the improvements to record entry recommended by the Gang File Policy Group, the N3G Task Force reviewed the functional requirements for further exploration concerning the Gang File. The task force concluded the other files lacked the necessary data for a valid GMC entry and determined the proposed changes to the group name codes and entry criteria would sufficiently improve the entry process.

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC)
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

NCIC ISSUE #8

Inclusion of Blue Alert Data in the NCIC

PURPOSE

To request approval for the inclusion of Blue Alert data in NCIC

POINT OF CONTACT

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

REQUEST OF THE SUBCOMMITTEE

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

BACKGROUND

Throughout the NCIC Third Generation (N3G) user canvass, there were many requests to enhance officer safety. One specific request was to create a Blue Alert Missing Person Circumstance (MPC) code in NCIC. Although, the request was specific to functionality that currently exists in the NCIC Missing Person File, the N3G Task Force determined that it would be beneficial to explore Blue Alerts in a more comprehensive manner. The N3G Blue Alert Policy Group (hereafter referred to as the Group) was established by the N3G Task Force and held its first meeting on March 13, 2019. Throughout several teleconferences, the Group discussed the sharing opportunities that are currently available for Blue Alerts and determined that it would be beneficial to create a flagging mechanism for Blue Alert data in the current NCIC operational environment as well as part of the N3G modernization effort.

A Blue Alert, as depicted in Public Law 114-12, is defined as "information sent through the network relating to: (1) the serious injury or death of a law enforcement officer in the line of duty, (2) an officer who is missing in connection with the officer's official duties, or (3) an imminent and credible threat that an individual intends to cause the serious injury or death of a law enforcement officer." While states may have adopted unique definitions within their respective states, for NCIC purposes, recommendations will refer to the federal definition.

Although, one of NCIC's primary roles is providing data that assists in the protection of law enforcement officers, currently no Blue Alert information is captured in any NCIC System record. NCIC currently maintains a flagging mechanism for Amber Alerts in the Missing Person File and also includes a MPC code that provides additional information surrounding the circumstances of the missing person. NCIC also maintains several files that provide data used for the protection of law enforcement. Furthermore, the Violent Person File was established in 2012 exclusively to alert law enforcement officers that an encountered individual may have the propensity for violence against law enforcement.

DISCUSSION AND ANALYSIS

As mentioned in the Background section of this document, the request for the inclusion of Blue Alert information in NCIC was addressed in a broad manner. Prior to determining if it would be beneficial to include Blue Alert data in NCIC, the Group had the opportunity to learn of the current Blue Alert initiatives to determine if a gap exists or if the current functionality can be improved upon using NCIC.

During the first teleconference, Mr. Vince Davenport, Deputy National Blue Alert Coordinator, DOJ (Department of Justice) COPS (Community Oriented Policing Services), provided an overview of the Blue Alert Act and the DOJ's roles and efforts in administrating the National Blue Alert Network. Additionally, Ms. Jennifer Viets, Montana Amber Alert/Missing Persons Clearinghouse Manager shared the current Blue Alert initiatives from the state perspective. Subsequently, the Group members participated in open dialogue regarding current initiatives and potential NCIC benefit. Ultimately, it was determined that the inclusion of Blue Alert data in NCIC could potentially benefit law enforcement and enhance officer safety.

Several NCIC files were explored for possible inclusion of Blue Alert data including: the Vehicle, Wanted Person, Violent Person and Missing Person files. Although, the Group determined that it would be beneficial for an Alert field to be created as part of the N3G initiative, it was recommended that due to the potential benefit to officer safety, the inclusion of Blue Alert data in the current environment be considered. The N3G Task Force approved the recommendations to include an Alert field with a corresponding Blue Alert code as part of the N3G initiative. The Blue Alert code would generate a caveat to be returned in the record response. However, the N3G Task Force recommended that the suggestion to consider incorporating Blue Alert data in the current environment was out of the scope of the N3G Task Force and should be forwarded through the Advisory Process as a separate topic. Hence, the recommendations outlined in this paper will focus solely on the current NCIC operational environment. The N3G Task Force recommends this topic be considered, recognizing that it is an exception to the recommendation approved through the Advisory Process that new functionality only be available using the National Information Exchange Model (NIEM) Extensible Markup Language (XML) data processing format. This exception was considered based on the importance of the data to officer safety and the presumption that it would not require programming by the CJIS Systems Agencies.

The Vehicle File discussion focused on the felony vehicle records due to the minimum required fields for entry, allowing an entry to be made in an expedited manner. It was determined that adding "Blue Alert" in the record could generate a caveat to be returned with the record response, warning the officer to use extreme caution when approaching the vehicle. Due to the potential impact to officer safety, it was recommended that entering Blue Alert as the first characters of the Miscellaneous (MIS) field in the current environment would generate the following caveat: **BLUE ALERT WARNING. USE EXTREME CAUTION IN APPROACHING THIS VEHICLE.**

Due to the importance of the entering the Blue Alert data quickly, the Wanted Person File discussion primarily focused on the entry of temporary felony want records in the Wanted Person File. A temporary felony want record may be entered to establish a "want" entry when a law enforcement agency desires to take prompt action to apprehend a person who has committed, or the officer has reasonable grounds to believe has committed, a felony. The record can be entered prior to obtaining a warrant, allowing an expedited entry. The Group determined that it would definitely be beneficial to add a Blue Alert flag to the Wanted Person File. However, it was recommended that the inclusion **not** be limited to the felony want records but also include traditional Wanted Person File records. This decision was based on the fact that some states are not be programmed for the temporary felony records, preventing them from taking advantage of the new functionality. Due to the importance of the Blue Alert data, it was recommended that entering Blue Alert as the first characters of the MIS field in the current environment would generate the following caveat: **BLUE ALERT WARNING. USE EXTREME CAUTION IN APPROACHING THIS INDIVIDUAL.**

The Violent Person File serves solely for the purpose of alerting law enforcement officers that an individual they are encountering may have the propensity for violence against law enforcement. Accordingly, it is probable that most Blue Alert incidents would also meet the criteria for entry into the Violent Person File. However, it was determined that the additional Blue Alert caveat could provide additional caution that the incident is current. Hence, it was recommended that entering Blue Alert as the first characters of the MIS field in the current environment would generate following caveat: **BLUE ALERT WARNING. USE EXTREME CAUTION IN APPROACHING THIS INDIVIDUAL.**

Furthermore, it was determined that the unique benefit for the Violent Person File could be after the Blue Alert broadcast has been activated or even canceled. The recommendation falls outside the NCIC system. The N3G Task Force supports a recommendation by the APB to the DOJ COPS to establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled. This could be implemented as an automatic notification from the respective Blue Alert systems or as a notification outside the system. It was suggested that the notification would provide benefit, especially in those situations where a Blue Alert may have been canceled prior to the subject being apprehended. Many jurisdictions have a 24-48 hour time frame for dispersing Blue Alert information and the alert will automatically be canceled by the system upon reaching that time.

The Group also discussed alternatives for flagging Blue Alerts in the Missing Person File. Although, a Blue Alert may be issued in the situation where an officer goes missing in the line of duty, it was suggested that the benefit for entering this information in NCIC would be in very specific circumstances and ultimately minimal. It was also mentioned that including the information in this file does not correlate with the intent of a Blue Alert, which is apprehending a suspect. However, the N3G Task Force determined that the inclusion of Blue Alert data in the Missing Person File could provide benefit and recommended that entering Blue Alert as the first characters of the MIS field in the current environment would also generate the following caveat: **BLUE ALERT WARNING. THE INDIVIDUAL OF RECORD IS AN OFFICER MISSING IN THE LINE OF DUTY.**

Current NCIC functionality allows for the first characters of the MIS field to be used for noting specific conditions. For example, using SVIN in the MIS field indicates that the VIN used in the record is a state assigned or non-conforming VIN. It may be necessary for agencies to prioritize information entered in those first characters of the MIS field if more than one condition is met.

OPTIONS

ISSUE 1 – BLUE ALERT CAVEAT

Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle File (felony vehicle), Wanted Person, Violent Person and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. **Selecting this option will prioritize this NCIC System change above all planned N3G development work items.**

Option 2: No change in current NCIC environment. An Alert Field will be created as part of N3G development.

ISSUE 2 – APB RECOMMENDATION TO DOJ COPS

Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

Option 2: No change.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Issue 1 – Blue Alert Caveat

Motion 1: To accept Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle File (felony vehicle), Wanted Person, Violent Person and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. **Selecting this option will prioritize this NCIC System change above all planned N3G development work items.**

Action: Motion carried**.**

Motion 2: Assign a priority 1H.

Action: Motion carried.

Issue 2 – APB Recommendation To DOJ COPS

Motion 3: To accept Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Issue 1 – Blue Alert Caveat

Motion 1: To accept Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle File (felony vehicle), Wanted Person, Violent Person and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. **Selecting this option will prioritize this NCIC System change above all planned N3G development work items.**

Action: Motion carried.

Issue 2 – APB Recommendation To DOJ COPS

Motion 2: To accept Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Issue 1 – Blue Alert Caveat

Motion: To adopt Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle File (felony vehicle), Wanted Person, Violent Person and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. Priority 3-H.

Action: Motion carried

Issue 2 – APB Recommendation To DOJ COPS

Motion: To adopt Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert | broadcast being canceled.

Action: Motion carried

SOUTHERN WORKING GROUP ACTION:

Issue 1 – Blue Alert Caveat

Motion 1: To adopt Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle File (felony vehicle), Wanted Person, Violent Person and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. Selecting this option will prioritize this NCIC System change above all planned N3G development work items.

Action: Motion carried.

Motion 2: Assign a priority 3H.

Action: Motion carried.

Issue 2 – APB Recommendation To DOJ COPS

Motion 3: To adopt Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Issue 1 – Blue Alert Caveat

Motion 1: To accept Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle File (felony vehicle), Wanted Person, Violent Person and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. **Selecting this option will prioritize this NCIC System change above all planned N3G development work items.**

Action: Motion carried.

Issue 2 – APB Recommendation To DOJ COPS

Motion 2: To accept Option 1**:** The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

Action: Motion carried.

FALL 2019 NCIC SUBCOMMITTEE ACTION:

Issue 1

Motion: To accept Option 1: Enable the use of "Blue Alert" as the first characters of the MIS field in the Vehicle (felony vehicle), Wanted Person, Violent Person, and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. Priority 3H.

Action: Motion carried.

Issue 2

Motion: To accept Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.

Action: Motion carried.

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL CRIME INFORMATION CENTER (NCIC)
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

NCIC ISSUE #9

Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPO)

PURPOSE

To present the status of the allowance of ERPO entries into the NCIC System.

POINT OF CONTACT

Global Law Enforcement Support Section, NCIC Operations and Policy Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to review this paper and provide appropriate comments, suggestions, or recommendations to the Criminal Justice Information Services (CJIS) APB.

BACKGROUND

The NCIC POF was established in 1997 as a result of the Violent Crime Control and Law Enforcement Act of 1994 (Crime Control Act). Title IV, Subtitle F, Section 40601 of the Crime Control Act, stipulates the following:

- Information from national crime information databases consisting of identification records, criminal history records, protection orders, and wanted person records may be disseminated to civil and criminal courts for use in domestic violence and stalking cases.

It also authorizes federal and state criminal justice agencies to enter information into criminal information databases, including:

- Arrests, convictions, and arrest warrants for stalking or domestic violence or for violations of protection orders for the protection of parties from stalking or domestic violence; and
- Protection orders for the protection of persons from stalking or domestic violence provided such orders are subject to periodic verification.

Following the signing of the Crime Control Act, the CJIS Brady Act Task Group made recommendations for the development and design of the NCIC POF. These recommendations were subsequently forwarded through the Advisory Process in 1995. Among the recommendations were the original POF criteria for entry. The original entry criteria were based on provisions of the Crime Control Act and codified in Title 18 United State Code (USC) §§ 2265-2266 (full faith and credit provisions). The Violence Against Women Act (VAWA) of 2000 and the VAWA of 2005 amended the protection order definition, and the CJIS APB recommended the NCIC POF entry criteria be changed to reflect the amended statute each time. The POF was created to contain court orders issued to prevent acts of domestic violence against a person or to prevent a person from stalking, intimidating, or harassing another person, as outlined in the previously identified legislation.

The *NCIC Operating Manual* provides the following criteria for entry for POF records:

“Each record in the POF must be supported by a protection order (electronic or hard copy). Protection orders must meet the following criteria before an entry can be made into the file:

1. The protection order includes:

    a. any injunction, restraining order, or any other order issued by a civil or criminal court for the purpose of preventing violent or threatening acts or harassment, sexual violence or contact or communication with, or proximity to another person including any temporary and final orders issued by civil or criminal courts whether obtained by filing an independent action or as a pendente lite order in another proceeding so long as any civil order was issued in response to a complaint, petition, or motion filed by or on behalf of a person seeking protection and

    b. any support, child custody or visitation provisions, orders, remedies, or relief issued as part of a protection order, restraining order, or stay away injunction pursuant to local, state, tribal, or territorial law authorizing the issuance of protection orders, restraining orders, or injunctions for the protection of victims of domestic violence, dating violence, sexual assault, or stalking.

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

In recent years, mass shootings and other types of gun violence have prompted states to enact legislation attempting to prevent gun tragedies before they occur. Many states have passed “red flag” laws which permit law enforcement or family members to petition state courts to order the temporary removal of firearms from a person based on the belief they may present a danger to themselves or others. Many red flag laws have identified these orders as Extreme Risk Protection Orders.

In the fall of 2018, representatives of the National Instant Criminal Background Check System (NICS) Section presented an information-only topic paper through the Advisory Process. The paper advised of the CJIS Division's awareness of ERPOs and ongoing review of NCIC policy to determine if ERPOs qualify for entry into the NCIC POF. In addition, the paper provided guidance for states with ERPO laws specific to firearm prohibitions in the interim. To assist in the determination of firearm eligibility, the NICS Section recommended states enter the information into the NICS Indices. Entry into the NICS Indices would prohibit the transfer of a firearm in the state in which the entry was submitted; however, 18 U.S.C. § 2265 stipulates full faith and credit is only given to full and ex parte protection orders meeting the criteria proving protection against abuse by a spouse or intimate partner. Therefore, if the individual were to move to another state and attempt to purchase a firearm in the new state of residence, the state prohibitor from the previous state would not apply.

DISCUSSION AND ANALYSIS

The Maryland State Police has requested an additional category be added to the criteria for entry policy in the NCIC POF, or the creation of a new NCIC File, to allow for the entry of ERPOs. In addition to making ERPO issuance available for firearm prohibition purposes, representatives from the Maryland State Police expressed the importance of making this information available in the NCIC System for officer and public safety. As of June 2019, at least 16 states have enacted ERPOs or similar red flag laws (Connecticut, Indiana, California, Washington, Oregon, Florida, Vermont, Maryland, Rhode Island, New Jersey, Delaware, Massachusetts, Illinois, New York, Colorado, and Hawaii). Other states have plans to introduce similar legislation in the near future. Although legislation varies from state to state regarding ERPOs, the same general principles apply nationwide. An ERPO (generally):

- makes it illegal for the respondent to purchase or possess firearms
- is filed against a person who poses a significant danger of causing personal injury to self or others in the near future by possessing firearms
- is initiated by law enforcement or a family or household member
- may not exceed one year

Similar to restraining orders, ERPO legislation establishes other guidelines within each respective state. The process widely includes the issuance of a temporary ERPO followed by a court review of all documentation provided by the petitioner. During this review process, some of the factors a judge may consider prior to issuing a full ERPO are:

- History of suicidal threats
- Recent threat or act of violence by the respondent towards others
- Prior convictions for assault
- Prior convictions for weapons offense
- Recent unlawful use of controlled substance
- Prior violation of restraining order
- Evidence of recent acquisition of firearms
- History of displaying or brandishing a deadly weapon

State ERPO legislation also mirrors typical protection order legislation in requiring the respondent has reasonable notice and the opportunity to be heard. Some State ERPO laws specifically indicate records must be shared with the databases operated by the U.S. Attorney General for distribution across state jurisdictions. As such, a statistical analysis conducted in June 2019 showed there were 245 POF record entries in NCIC in which “Extreme Risk Protection Order” was entered into the Miscellaneous (MIS) field. An additional 74 entries contained “ERPO” in the same manner, while there were more than 2,000 MIS field entries of “Risk Protection Order.” Upon review of a selection of existing entries in the national system, it was determined only few met the criteria for entry into the POF.

Federal ERPO Authority

A comprehensive analysis (including a legal review) of state ERPO legislation and NCIC record entries found that ERPOs are considered civil orders because they affect the private rights of citizens as compared to administering penal justice. As a result, and similar to that for stalking and domestic violence protection orders, entry into the NCIC System requires specific Federal statutory authority. This is to recognize Congress’s intention to restrict the use of data (within the NCIC System) to that stated in the law and to prevent its use from becoming limitless in scope. Currently, no Federal legislation authorizes civil ERPOs (and/or any other red flag laws) to be entered into NCIC. However, each ERPO should be reviewed to determine if it meets the criteria for entry of another file of the NCIC System.

Expansion of POF Criteria for Entry

As mentioned, the POF entry criteria was created from language derived from the Crime Control Act and other federal legislation. In addition to defining a protection order, the legislation contains language authorizing entry into the NCIC System (relevant provisions of the Crime Control Act were codified in the notes of 28 U.S.C. § 534). ERPOs are not generally intended to protect a specific individual from domestic violence, harassment, or stalking; but rather are issued to protect society or the community at large from the harm an individual may impose. Because the intended purpose of red flag laws is to temporarily restrict an individual’s access to firearms rather than to prevent stalking and domestic violence incidents, the CJIS Division, in consultation with the Federal Bureau of Investigation’s (FBI) Office of the General Counsel has determined not all ERPOs meet the criteria for entry into the NCIC POF. Additionally, and unlike the law which exists for stalking and domestic violence protection orders, there is no federal law supporting the entry of civil ERPOs into the NCIC System. Thus, the criteria for entry into the POF may not be expanded at this time. However, a review of protection orders identified as ERPOs already entered into the POF found records which specifically identified a protected person and indicated there was a viable threat of domestic violence (or other criteria); therefore meeting the criteria for entry despite being issued as ERPOs. Each ERPO should be carefully reviewed to determine if the current POF entry criteria can be met.

Entry into the Violent Person File (VPF)

The NCIC VPF was created to alert law enforcement officers an individual they are encountering may have the propensity for violence against law enforcement. An entry into the VPF may be made when at least one of the following criteria has been met:

1. Offender has been convicted for assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement.
2. Offender has been convicted of a violent offense against a person to include homicide and attempted homicide.
3. Offender has been convicted of a violent felony against a person where a firearm or weapon was used.
4. A law enforcement agency, based on its official investigatory duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community.

The FBI CJIS Division explored the potential for creating a fifth category for entry into the VPF to account for ERPOs. Again, it was determined that, unlike stalking and domestic violence protection orders, not all ERPOs would meet the requirements for entry into the NCIC System since they are civil orders and there is no federal law to provide authority for entry. However, upon review of ERPOs already entered into the POF, it was determined the criteria for entry into the VPF in some cases may be appropriate. Many ERPOs are initiated by law enforcement. This indicates law enforcement believes an individual is a potential threat to commit an act of violence with a firearm. If the respondent was previously convicted of a crime that met any of the first three criteria, then an entry into the VPF would be substantiated. In addition, if a law enforcement official reasonably believed a threat has been made against law enforcement, the subject should be entered into the VPF under the fourth criteria.

Proposed Federal Legislation

In 2018 and again in 2019, a number of federal ERPO bills were introduced into Congress but have not become law. The language in most of the proposals is similar to many of the laws passed in state ERPO legislation. Proposed legislation includes grant funding for states considering implementing ERPO laws and amending the Brady Act to include a new federal firearm prohibition for state-issued ERPOs. The inclusion of this prohibitive measure in federal legislation would nullify legal concerns regarding ERPO issuance only being considered for firearm prohibitions in the state in which the order is issued. A significant omission from proposed federal legislation reviewed by the FBI CJIS Division is authorization for entry of both state and federally-issued ERPOs into the NCIC System where they are available to law enforcement across jurisdictional lines for officer and public safety.

CJIS Division Guidance

The FBI CJIS Division’s mission is to equip law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties. The main objective of the NCIC System is to assist law enforcement officers in performing their duties more safely and provide information necessary to protect the public. There has been a growing number of mass shootings across the nation. Red flag laws (including ERPOs) are a manner in which to combat these unpredictable acts of violence. In some cases, individuals posing a potential danger to him/herself or the general public show signs of being a threat prior to committing an act of violence. Currently, there are instances when law enforcement has limited ability to take action unless an actual crime is committed. Similarly, unless there is a reasonable belief a serious threat has been made against law enforcement, or one of the other criteria is met for entry into the VPF, law enforcement may be unable to make an entry into the NCIC System. The FBI CJIS Division recognizes the difficulties the criminal justice community faces with becoming aware of potential threats; regardless of against whom they may be directed. The FBI will continue to collaborate with federal and state partners in anticipation of a comprehensive solution for allowing the entry of state-issued ERPOs in the NCIC System.

Absent federal authority supporting entry into the NCIC System, most ERPOs will not meet the criteria for entry. An initial review of ERPOs already entered into the national system indicates some of these orders do meet criteria for entry into the POF as well as the VPF. However, based on ERPOs found in the POF during recent audit assessments, many have been entered which do not meet the current criteria. The FBI CJIS Division encourages entering agencies to assess each ERPO to determine if the criteria is met for entry into an existing NCIC File. Until authority supporting entry into NCIC exists, ERPOs not meeting present entry criteria should be removed.

The POF currently allows agencies to reflect firearm prohibition via the Brady Indicator (BRD) field, or by entering NCIC code “07” in the Protection Order Conditions (PCO) field. The BRD field may be populated with “Y” to indicate the subject of record is federally disqualified from possessing, purchasing, or receiving a firearm per Title 18, USC § 922. The PCO field is used to indicate terms and conditions of a protection order. PCO Code 07 should be entered when a judge indicates the subject (respondent) of an order is prohibited from possessing a firearm based on a state prohibition or other considerations. Since ERPOs are not currently disqualifying under Brady Act provisions, if POF criteria is met, PCO Code 07 should be applied to appropriate records.

As advised by representatives of the NICS Section in the fall of 2018, ERPOs should be entered into the NICS Indices. The state prohibition for the ERPO is disqualifying for NICS purposes if the subject of the order is attempting to purchase or is residing in the state of issuance. However, if the individual moves to another state and attempts to purchase a firearm in the new state of residence, the ERPO would not apply. Entry of ERPOs into the NICS Indices ensures state prohibitive information is available for NICS background checks in applicable scenarios.

As previously mentioned, federal ERPO legislation has been drafted but has not yet become law. The language in proposed ERPO laws does not recognize the necessity for entry of state or federally issued ERPOs into the NCIC System. The FBI is proactively seeking opportunities to share identified gaps with Congressional staff members.

The NCIC Program Office will continue to monitor closely state red flag laws and federal legislation for additional opportunities to support the entry of ERPOs into the NCIC System.

RECOMMENDATION

Please provide any comments, suggestions, and feedback relating to the potential entry of ERPOs into the NCIC System.

FALL 2019 WORKING GROUP ACTIONS:

This topic was accepted as information only by all five working groups.

FALL 2019 SUBCOMMITTEE ACTIONS:

NCIC SUBCOMMITTEE ACTION:

Motion: To endorse the creation of a new NCIC file specifically for the entry of Extreme Risk Protection Orders (ERPOs).

Action: Motion carried.

Motion: Assign a priority of 3H.
Action: Motion carried.

Motion: To endorse the entry of ALL authorized Extreme Risk Protection Orders (ERPOs) into the newly created NCIC file.
Action: Motion carried.

Motion: To recommend the Chair of the Advisory Policy Board draft a letter to the major law enforcement associations (IACP, MCC, NSA, etc.) encouraging endorsement of legislation and/or an Attorney General mandate that will authorize entry of ALL Extreme Risk Protection Orders (ERPOs) (including, but not limited to, those issued by civil, military, federal, and state courts) into the NCIC system.
Action: Motion carried.

NICS SUBCOMMITTEE ACTION:

Accepted as information only.

Intentionally Left Blank

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA

STAFF PAPER

APB ITEM #4

Race Code Standardization across Criminal Justice Information Services (CJIS) Division Systems

PURPOSE

The purpose is to present a proposal to standardize Race Codes across CJIS Division Systems by adding Race Code P for Native Hawaiian or Other Pacific Islander

POINT OF CONTACT

Global Law Enforcement Support Section, National Crime Information Center Operations and Policy Unit and the Programs Research and Standards Unit

Questions regarding this topic should be directed to <agmu@leo.gov>.

REQUEST OF THE APB

The APB is requested to review the information provided in this paper and provide appropriate comments, suggestions or recommendations to the FBI Director.

BACKGROUND

In June 2018, the APB recommended the CJIS Division to further explore cross walking the new National Crime Information Center (NCIC) 3rd Generation (N3G) specifications with the Next Generation Identification (NGI) System and the Interstate Identification Index (III) specifications regarding demographic and biographic data elements entered into the NCIC and NGI at booking, then subsequently searched by each system. Although this motion mentions NCIC, NGI and III specifically, the intent is to look across all CJIS Division Systems. Subsequent topic papers will come as the CJIS Division continues to support this cross walk effort.

The first demographic data element reviewed for standardization is the race code. Although leveraged by nearly all CJIS systems, race codes vary somewhat from system to system. The CJIS Division analyzed applicable race codes for each of the following systems: NCIC, III, NGI, National Instant Criminal Background Check System (NICS), Uniform Crime Reporting (UCR), and National Data Exchange (N-DEx). While each of these systems has its own clearly defined mission, race codes A, B, I, U, and W are common among them (*see table on page 3 for code definitions*). However, race code P, which specifically defines Native Hawaiian or Other

Pacific Islander, is an acceptable code for only NICS, UCR, and N-DEx. Currently, for NCIC, NGI, and III, in the absence of a race code P, persons who identify as Native Hawaiian or Other Pacific Islander could be included under race code A for Asian or U for Unknown. The following paragraphs will provide historical insight as to why each system is programmed to accept their respective race codes.

In March 2002, the CJIS Division was granted a variance from the Office of Management and Budget (OMB) for the NCIC, III, and Integrated Automated Fingerprint Identification System (IAFIS) (now NGI) Systems. The following is an excerpt from the 2002 letter to FBI CJIS from the OMB:

> *After reviewing the information provided in your letter, we agree that the systems of records in the NCIC, the III/IAFIS, and the NICS are not maintained to provide statistics or to furnish administrative or compliance reports, but rather contain individual data that are intended to identify persons engaged in criminal activity; hence, they are not subject to the provisions of the 1997 standards.*

The NICS accepts race codes based upon the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Form 4473. This form is utilized and required with each attempted firearm purchase. The prospective buyer must complete, sign and provide the completed form to the gun dealer. The Form 4473 collects descriptive information utilized by the NICS for the biographic name search. In 2016, the ATF updated their Form 4473 to comply with the OMB Standards, and likewise NICS made changes, to collect both ethnicity and the additional race code.

The UCR Program's primary objective is to generate reliable statistical information for use in law enforcement administration, operation, and management. As of January 1, 2013, the UCR Program began to collect the expanded race categories for all data collections to comply with the race categories as described by the OMB 1997 Revision (listed on page 3).

The N-DEx system is an investigative lead system to assist law enforcement with connecting the dots of a case or criminal activity. All information contained within or disseminated by the N-DEx system is already collected by criminal justice agencies when fulfilling their official criminal justice functions like law enforcement encounters or judicial proceedings. Therefore, the N-DEx was programmed to accept the expanded list of race codes identified in the OMB Standard, as an optional entry field from their contributing agencies.

CJIS System	Race Codes	Race Code Description
NCIC	A, B, I, U, W	Asian or Pacific Islander, Black, American Indian or Alaskan Native, Unknown, and White
III	A, B, I, U, W	Asian or Pacific Islander, Black, American Indian or Alaskan Native, Unknown, and White
NGI	A, B, I, U, W	Asian or Pacific Islander, Black, American Indian or Alaskan Native, Indeterminable, and White
NICS	A, B, I, U, W, P	Asian, Black, American Indian, Unknown, White, and Pacific Islander
UCR	A, B, I, U, W, P	Asian, Black, American Indian or Alaskan Native, Unknown, White, and Native Hawaiian or Pacific Islander
N-DEx	A, B, I, U, W, P	Asian, Black, American Indian or Alaskan Native, Unknown, White, and Native Hawaiian or Pacific Islander

As referenced above, in 1997, the OMB issued the Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity. The revised standards contain five minimum categories for Race: American Indian or Alaska Native, Asian, Black or African American, Native Hawaiian or other Pacific Islander, and White. The OMB Directive defines each racial category as follows: Asian, Black or African American, American Indian or Alaskan Native, White, and Native Hawaiian or Other Pacific Islander.

DISCUSSION AND ANALYSIS

The State of Washington Administrative Office of the Courts (AOC) is requesting race code P, for Native Hawaiian or Other Pacific Islander, be added to the following CJIS Systems: NCIC, III, and NGI. There is currently no race code P in these systems, therefore, any Native Hawaiian or Other Pacific Islander would have to be entered as either an A for Asian or U for Unknown. The Washington AOC's system is based on the standard set forth by the OMB in 1997 which includes race code P.

The Washington AOC believes the uniformity of data standards within the FBI CJIS Division Systems will increase criminal justice data analysis at the local, state, federal, and national levels. Similar to the various CJIS Division Systems, the Washington AOC can enter race code P in their statistical records data base, but that information must be translated into another code when sent to the Washington State Patrol's criminal justice system which is based on NCIC Standards and does not include race code P.

Law enforcement may leverage race codes when performing biographic identity queries in NCIC and III. When race is entered as part of an NCIC Wanted Person search, results are filtered according to one of two scenarios: a query with race code B will search all records except those with a race code W, and a query with race code W will search all records except those with a race code B. For Wanted Person queries submitted with race codes A, I, and U, all records are searched without any filter applied.

When race is entered as part of an III biographic query, the element will contribute to the overall likeness score produced which directly impacts the candidates returned in the response to the query. Unlike NCIC and III biographic queries, the race code provided as part of an NGI biometric search has no influence on the identification process where the specific candidate is returned.

Based on CJIS's cursory review of current NCIC, III, and NGI functionality with regard to the race code; no major negative impacts or benefits were identified which would change the law enforcement community's ability to make more accurate subject identifications by leveraging race code P.

If this proposal is approved, agencies will have the capability to enter race code P in all CJIS Division Systems. System programming will be necessary on behalf of CJIS as well as each state to enable both submissions and receipt of race code P for various transaction associated with NCIC, III, and NGI. Any recommendation from this topic will suffice the N3G Task Force Recommendation to revisit race codes.

The APB is requested to review the information in this paper and provide feedback on the following options:

RECOMMENDATIONS

Option 1: Standardize the Race Codes across CJIS Division Systems to include the addition of Race Code P for Native Hawaiian or Other Pacific Islander.

Option 2: No change.

The CJIS staff performed a technical assessment of this enhancement and determined that it is a ______ to ______ (TBD weeks) change to the NCIC system.

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

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion 1: To accept Option 1: Standardize the Race Codes across CJIS Division Systems to include the addition of Race Code P for Native Hawaiian or Other Pacific Islander.
Action: Motion carried.

Motion 2: To accept Priority Level 3M
Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion 1: To accept Option 1: Standardize the Race Codes across CJIS Division Systems to include the addition of Race Code P for Native Hawaiian or Other Pacific Islander.
Action: Motion carried. 15 Yay; 7 Nay.

Motion 2: To assign a Priority 4L.
Action: Motion carried

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 2. No change.
Action: Motion carried

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Standardize the Race Codes to include the addition of Race Code P for Native Hawaiian or Other Pacific Islander. Priority 4M
Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 2: No change.
Action: Motion carried. 28 Yay; 1 Nay.

FALL 2019 SUBCOMMITTEE ACTIONS:

IDENTIFICATION SERVICES SUBCOMMITTEE ACTION:

Motion: To adopt Option 2: No change
Action: Motion carried. 1 opposed.

NCIC SUBCOMMITTEE ACTION:

Motion: To accept Option 2: No Change.
Action: Motion carried. 1 opposed.

N-DEx SUBCOMMITTEE ACTION:

Accepted as information only.

NICS SUBCOMMITTEE ACTION:

Accepted as information only.

UCR SUBCOMMITTEE ACTION:

Accepted as information only.

Intentionally Left Blank

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA

STAFF PAPER

APB ITEM #6

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

N-DEx ISSUE 1
N-DEx Program Office Update

N-DEx ISSUE 2
Re-examine the N-DEx Policies of Advanced Permission and Verification

N-DEx ISSUE 3*
N-DEx Data Sharing Task Force Update

N-DEx ISSUE 4 (See APB Item #2, NCIC Issue #2 for staff paper)
LEEP Status Report

N-DEx ISSUE 5*
User Assessment Results

N-DEx ISSUE 6 (See APB Item #4 for staff paper)
Race Code Standardization across CJIS Division Systems

*No staff paper

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL DATA EXCHANGE (N-DEx) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 10, 2019

STAFF PAPER

N-DEx ISSUE #1

National Data Exchange (N-DEx) Program Office (PO) Update

PURPOSE

To provide a program status update on activities and initiatives.

POINT OF CONTACT

Global Law Enforcement Support Section (GLESS), N-DEx PO.

Questions regarding this topic should be directed to <agmu@leo.gov>.

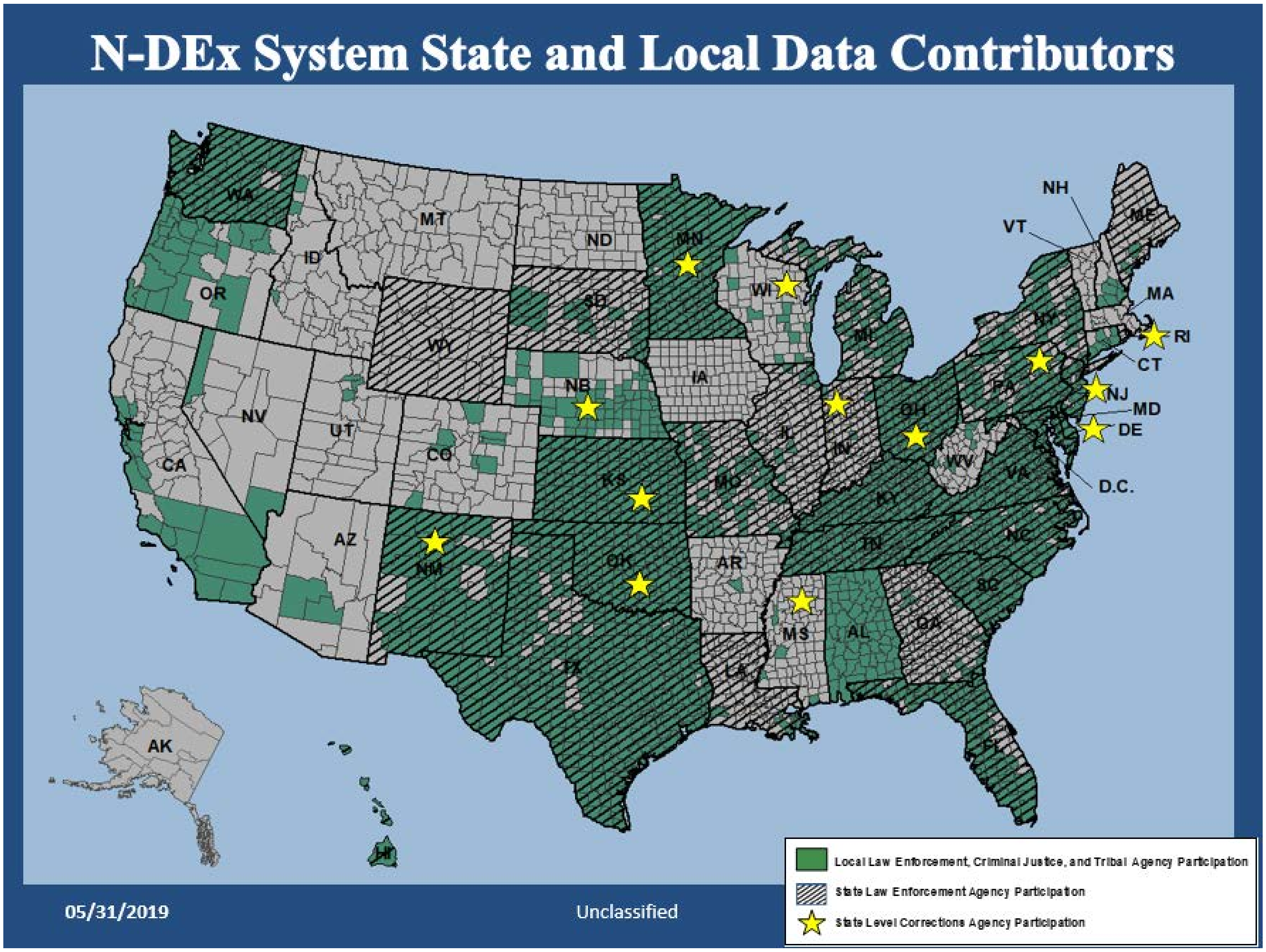
BACKGROUND

The N-DEx PO is currently planning, developing, and implementing numerous initiatives, which will further support the growth and effectiveness of the N-DEx System. The N-DEx PO is providing the CJIS Advisory Policy Board (APB) with status updates on the following program activities and initiatives: N-DEx System Participation; Stakeholder Relationships, Outreach, and Customer Support; N-DEx Subcommittee Action Items; Technical Management, to include Data Quality and Standards and Build Enhancements; and Brand Management, to include the Success Story Program, Publications, and N-DEx System Training and Resources.

N-DEx System participation

The following information is as of May 31, 2019:

- 7,359 Agencies.
- 819+ Million Searchable Records.
- 18,300+ Active Users.
- 1.39 Seconds Average Monthly Search Response Time.
- 73 of the top 100 largest law enforcement agencies are contributing data to the N-DEx System. (added Denver Police Department FY19).
- The Violent Crimes Against Children/Innocence Lost Database/Web Archival Tool federated database is now available to criminal justice users.



N-DEx System State and Local Data Contributors

🟩 Local Law Enforcement, Criminal Justice, and Tribal Agency Participation

▨ State Law Enforcement Agency Participation

☆ State Level Corrections Agency Participation

05/31/2019

Unclassified

STAKEHOLDER RELATIONSHIPS, OUTREACH, AND CUSTOMER SUPPORT

The N-DEx PO is actively leveraging strategic partnerships with additional large-scale information sharing systems to enhance the N-DEx System's visibility and increase system use and criminal justice data.

Naval Criminal Investigative Service (NCIS) Law Enforcement Information Exchange (LInX)

- 15 User Connections.
- 14 Data Connections.

COPLINK

- Nine User Connections.
- Nine Data Connections.

Regional Information Sharing Systems (RISS)

- Six Regional Centers working toward full User Connections

High Intensity Drug Trafficking Areas (HIDTA)

- All 29 Directors have approved user access.
- One User Connection.
- One Data Connection.
- Currently working with Washington/Baltimore HIDTA for user connection.

Institutional and Community Corrections (ICC)

Recognizing the need to support an information sharing environment spanning the entire criminal justice lifecycle, the N-DEx PO continues to engage ICC stakeholders to increase both ICC data contributions and usage of the system.

- Currently, 13 state departments of corrections directly contribute data to the N-DEx System (Delaware, Indiana, Kansas, Mississippi, Minnesota, Nebraska, New Jersey, New Mexico, Ohio, Oklahoma, Pennsylvania, Rhode Island, and Wisconsin) with several additional states involved in either data integration or planning implementation efforts with the N-DEx PO.
- ICC agencies continue to rank among the most prolific users of the N-DEx System Batch Search feature, which has prompted the N-DEx PO to develop specific distance learning courses to demonstrate how ICC agencies can use batch search to locate absconders.

N-DEX SUBCOMMITTEE ACTION ITEMS

ACTION ITEM	STATUS	DETAILS	TENTATIVE COMPLETION
Questionnaire to 20 percent of CJIS Systems Officers (CSOs) limiting N-DEx System access.	Pending	Pending acquisition of survey tool purchase (Summer 2019).	Fall 2019
Criminal Intelligence information via the N-DEx System	On-going	Deployment beginning late Summer 2019.	Summer 2019
NICS Accessing the N-DEx System as a Secondary Search.	On-going	On track to meet the NICS Sections FY 2020 implementation plans.	FY 2020
Email Notifications for Ingestion	On-going	Pending Amazon Web Services (AWS) Cloud migration.	Summer 2020

TECHNICAL MANAGEMENT

Data Quality and Standards

Formation of the N-DEx Data Sharing Task Force

The current N-DEx System data sharing capabilities and policies create a myriad of options by design, but as the system has matured and expanded over the years, the original design has proven to be unsustainable. After lengthy discussion on the data sharing complexities during the N-DEx Subcommittee during the Spring 2019 meeting, it was decided a task force should be created to conduct a more detailed review of the data sharing policy and capability within the N-DEx System. The N-DEx Data Sharing Task Force will assess the current data sharing policy with the expectation of revising the policy to reflect a less complex data sharing structure and possibly creating standards and/or best practices. The task force will also review statistics and current implemented data sharing rules to make recommendations for future data sharing development.

Members of the N-DEx Data Sharing Task Force include: (* current N-DEx Subcommittee member)

- Mr. Alan Peto, Las Vegas Metro Police Department.*
- Ms. Carol Gibbs, Illinois CSO.*
- Ms. Wendy Easterbrook, Michigan State Police.
- Mr. Brandon Gray, New Jersey CSO.*
- Mr. Luke Thompson, Chief of Byram Police Department, Mississippi.*
- Ms. Pamela Thrift, Georgia Department of Community Supervision.
- Mr. Mike Roosa, Department of Justice.*
- Ms. Danielle Bell, Florida Department of Law Enforcement.

The task force will meet bi-weekly via teleconference for the foreseeable future to complete this project. Representatives from the N-DEx PO and the Information Technology Management Section will also participate.

Release of N-DEx 4.0 Information Exchange Package Documentation (IEPD)

The N-DEx 4.0 IEPD was released for public review and comments. The goal of this IEPD is to simplify, streamline, and increase efficiency in performing data integration efforts between criminal justice agencies and the N-DEx System.

Key features:

- Combined the N-DEx IEPDs v2.1 Incident and Arrest (IA) and v2.1 Incarceration Booking Probation and Parole (IBP2) IEPDs.
- Updated code tables (to include new code values and elements within National Information Exchange Model, National Incident Based Reporting System).
- Removal of extraneous elements within the IEPD (to decrease the size and complexity of the IEPD).

- Offers a generic information report type, “Information” Report Type, allowing any report type approved by N-DEx policy but not in the IEPD to be generated.
- Created an all-inclusive structured payload option (to provide integrators the option of using Logical Entity eXchange Specifications (LEXS) 5.0 for data submissions (Publish/Discover (PD)).

Based on the feedback received, deployment of the new IEPD into the N-DEx System is anticipated during the mid-year 2020 timeframe.

Completed Build Enhancements

- Coordinated with the FBI NICS Section to develop enhancements, which support a secondary N-DEx System search for Use Code “F” checks using the N-DEx System Portal.
- Addition of federated searches to criminal intelligence data sources (once approved). This includes developing a capability, which verifies a user has completed training to access 28 CFR Part 23 Data.
- Received CJIS Security approval and began transition of the N-DEx System to the AWS Cloud.
- Enhanced the Records tab functionality.
- Enhanced the saved records functionality.
- Provided the ability to print multiple records at once.
- Implemented an enhancement to allow users to save records via the Batch Search Results screen.
- Implemented the Training Administration redesign.
- Added the course complete date to training reports, which is available to N-DEx System users having the Training Management Role.
- Redesigned the user interface for Federated Data Sources.
- Created a Training tab beside Resources tab on N-DEx home page.
- Implementation of Use Code “S” (pending validation of user access).
- Addition of Federated Searches for Innocence Lost Database/Web Archival Tool.

Upcoming System Enhancements

- Implement CSO notifications for affirmations to the Data Access Agreement page (new users only).
- Implement email notifications for Data Submissions.
- Automatically update the Originating Agency Identifier (ORI) in a user’s account when coming from the same identity provider. If an identity provider changes a user’s ORI, N-DEx will provision a new account.
- Create the capability to disable e-mail notifications for batch searches.
- Implement the Audit Reports redesign.
- Migrate Entity Intelligent Data Operating Layers to AWS.
- Development of the N-DEx System manual ingest tool.

BRAND MANAGEMENT

Success Story Program – Celebrating Success

2019

- All 2019 success story awards have been presented to the winners. Below is a highlight from the N-DEx Success Story of the Year Award presentation:

The CJIS Division's Global Law Enforcement Support Section Chief, Scott A. Rago, presented the 2019 N-DEx Success Story of the Year Award to Wayland, Michigan, Police Department. Officer Mark Riemersma was selected for the award based upon his investigative use of the N-DEx System to assist with a child predator case, which ultimately led to the arrest and subsequent federal indictment on 16 counts of child sex crimes. Officer Riemersma praised the N-DEx System: "I have used N-DEx to expand and solve many cases that may have gone unsolved otherwise, ranging from organized retail fraud crime groups to identifying numerous victims of sex trafficking in large scale online escort operations. N-DEx is an invaluable tool for any law enforcement officer, and it should be a part of every investigator's toolbox."

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

2020

- The N-DEx PO is actively gathering successes for the 2020 Success Story of the Year Awards. Please submit your successes via the N-DEx System User Feedback or via email at ndex@leo.gov.

N-DEx System Publications

- The N-DEx System was featured in the CJIS Link and CJIS Connection numerous times celebrating success and sharing information related to the N-DEx System.
- The N-DEx PO is drafting a special CJIS Link article for the announcement of the 2019 N-DEx Success Story of the Year Award.
- The N-DEx System is featured in the monthly FBI E-Brief.
- An article featuring the N-DEx System has been published for the Corrections Today publication of the American Correctional Association.
- The N-DEx N-Focus newsletter is distributed quarterly to the N-DEx System user community.
- The N-DEx PO is drafting a submission for the Law Enforcement Bulletin.
- The N-DEx PO has submitted an article for the Corrections One online publication.

Training Resources

The tiered approach to outreach provides multiple levels of complementary resources, depending on the end user's needs. The web-based and on-demand resources provide short, concise, and dynamic digital resources tailored to specific needs of the users, while leveraging technology to provide specific training topics users may access when the need arises. Training resources include:

- Computer Based Training Modules (CBTs).
- User Workshops.
- Video Tutorials.
  - These videos provide a method for delivering content in small, very specific bursts. This creates an on-demand resource that allows the user to decide what and when to learn. Video tutorials are created and updated to reflect any changes to the system. Videos will run for no longer than 10 minutes.
  - Videos created and maintained include:
    - System Tour.
    - Search.
    - Batch Search.
    - Subscription and Notification.
    - Preferences.
    - Setting Sharing Policies.
    - Audit.
    - User Administrator.
    - Training Administrator.
- Web-based Information Sessions available via Skype for Business.
  - Regularly scheduled sessions such as Batch Search, Fugitive Finder, and N-DEx Overview.
  - CSO administrative sessions, such as Audit and User Management.
  - Agency requested sessions for specific topics, assistance, or demonstrations.

FALL 2019 WORKING GROUP ACTIONS:

This topic was accepted as information only by all five working groups.

FALL 2019 N-DEx SUBCOMMITTEE ACTION:

This topic was accepted as information only.

CJIS ADVISORY POLICY BOARD (APB)
NATIONAL DATA EXCHANGE (N-DEx) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 10, 2019

STAFF PAPER

N-DEx ISSUE #2

Re-examine the N-DEx Policies of Advanced Permission and Verification (AP&V)

PURPOSE

To review and discuss changes to the current policies regarding AP&V within the *N-DEx Policy and Operating Manual.*

POINT OF CONTACT

Global Law Enforcement Support Section (GLESS) N-DEx Program Office (PO).

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, and recommendations regarding changes to the current policies referencing AP&V Requirements within the *N-DEx Policy and Operating Manual.*

BACKGROUND

The N-DEx PO reviews the *N-DEx Policy and Operating Manual* on an annual basis. This review is to ensure policies within the manual remain consistent with the *Criminal Justice Information Services (CJIS) Division Security Policy (CSP),* N-DEx System development, N-DEx stakeholder feedback, and resultant lessons from N-DEx System audits. When necessary, recommended revisions are provided to the CJIS Advisory Policy Board (APB) for review and approval.

The existing AP&V policies within the *N-DEx Policy and Operating Manual Version 5.0,* along with the accompanying authorized pre-permission policy, read as follows:

- *Policy 1.3.9* – Authorized Pre-Permission Use: N-DEx System information may be viewed, output, or discussed without advance authorization of the record-owning agency, within the record-requesting agency or another agency, if the other agency is an authorized recipient of such information, by virtue of meeting the requirements for N-DEx System access and is being serviced by the record-requesting agency. However, any recipient of N-DEx System data must obtain advanced permission from the record-owning agency prior to acting upon any data obtained through the N-DEx System.

- *Policy 1.3.10* – Advanced Permission Requirement: Terms of N-DEx System information use must be obtained from the record-owning agency prior to reliance or action upon, or secondary dissemination. 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.

- *Policy 1.3.11* – Verification Requirement: 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.

N-DEx System policy also provides exigent exceptions to the above requirements as follows:

- *Policy 1.3.13* – Immediate use of N-DEx System information can be made without the advanced permission of the record-owning agency if there is an exigent circumstance - an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect, or destruction of evidence. The record-owning agency shall be immediately notified of any use made as a result of exigent circumstances.

Executive Order 12862 directs federal agencies to provide service to the public matching or exceeding the best service available in the private sector. In response to this mandate, the N-DEx PO regularly administers user assessments to collect baseline performance information on N-DEx System service delivery and to offer users a mechanism to provide qualitative feedback on specific system improvement topics.

In the Fall 2018 *N-DEx System User Assessment*, in which feedback was collected from more than 1,400 active users, respondents were asked questions specific to N-DEx System AP&V requirements. In short, some N-DEx System users indicated the AP&V policies were a deterrent to the timely use of system information. One-third of respondents offered some level of affirmative agreement with the following statement: "The N-DEx System policy for Data Use Rules, specifically the need to both verify a record and get permission to use a record from the record-owning agency, makes it difficult to use N-DEx System information for my criminal justice needs." On a related question, twenty percent of respondents indicated they had "a difficult time reaching the record-owning agency based on the provided point of contact (POC) information." Respondents were also asked to provide further qualitative feedback on any data use rule difficulties they experienced, either with, "the general verifying/permission requirements, or the specific point of contact information on the record(s)."

These results prompted the N-DEx PO to document concerns with the AP&V policies and present assessment data at the Spring 2019 N-DEx Subcommittee Meeting, to obtain additional stakeholder insight on the topic. The subcommittee members provided the N-DEx PO with an action to further examine the AP&V issue and to offer the APB with specific policy or technical solutions to mitigate user concerns with the current iteration of the requirements.

DISCUSSION AND ANALYSIS

Further analysis of stakeholder feedback by N-DEx PO staff, to include data from a variety of quantitative and qualitative sources, revealed concerns about the compatibility of AP&V processes with the evolving needs of the criminal justice community. Not only has there been growing diversity in the primary roles of system users over the last few years, but traditional investigative use of the system has been augmented by agency needs for data to support expanded analytical capabilities, time-sensitive tactical or field activities, criminal justice suitability determinations, and continuous monitoring or supervision of high-risk populations. These compatibility concerns have been exacerbated by the low quality of POC information associated with some N-DEx System records. The following sample of respondent quotes from the *N-DEx System User Assessment* highlight these concerns:

> *"While providing tactical 24/7 intel to officers on patrol, there are often times when we call to verify a record, and the agency in question is not staffed 24/7 for that task."*
>
> *"We have contacted agencies asking to utilize the information in their record, and the POC has no idea what we are talking about, or they no longer work at that agency."*
>
> *“When I actually get through to someone, it can take days and sometimes more than a week to get permission.”*

Additional feedback on AP&V requirements cited a lack of clarity on certain policy language components, leading to user uncertainty on which "reliance," "action," or “secondary dissemination” should result in AP&V. This latter point was a particular concern among those working in analytical roles involving the creation and dissemination of products containing N-DEx System information to other criminal justice entities.

Another point of concern expressed by some stakeholders was the resource impact AP&V requirements had on record-owning agencies, particularly for agencies sharing large numbers of records. One particular user noted the record POC for their agency, working in an administrative role, was uncertain how to correctly address AP&V requests, as it was the agency’s position that “permission” to use N-DEx System information for specific authorized purposes and roles was previously established via the agency’s initial data sharing agreements.

After synthesizing comments from both the *N-DEx System User Assessment* and additional stakeholder feedback, the N-DEx PO determined most AP&V concerns broadly revolve around the perceived inability, due in part to language clarity, to use N-DEx System information in a manner fully supporting criminal justice needs of a time-sensitive, but non-exigent nature. Any ambiguity or uncertainty with policy language was further exacerbated by the inability of the user to satisfy requirements by way of the established POC contact information. This dynamic suggests an indirect way to mitigate user concerns with AP&V is to implement system improvements to POC information within a record. Additionally, technical solutions might also help record-owning agencies better address verification or permission policy requirements. For example, record-owning agencies with frequent (e.g., daily) submission feeds might "opt-in" to a system in which receipt of their records within the N-DEx System establishes their agreement to the timeliness, completeness, and accuracy of the records contained within. The feasibility of these technical solutions, which fall outside the scope of the current paper, has not been thoroughly examined and would need to be further researched by the N-DEx PO.

Although implementing technical improvements to satisfying AP&V requirements can mitigate a large number of stakeholder concerns, modifications to existing policy language would also address important user issues with AP&V processes. The recommended policy areas to address via language modification are as follows:

Clarify user authorization requirements by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate.

A theme explored during the review of AP&V feedback, particularly among record-owning agencies, was the lack of language clarity on means to establish permission of use for N-DEx System information. While there is consensus on the importance of establishing the veracity of system information via verification procedures, a belief among many stakeholders is necessary N-DEx System permission rules governing use, protection, and sharing of records are established on the front end of the data sharing process, by the record owner, and the permission requirement in policy *1.3.10* is redundant. The *N-DEx Policy and Operating Manual* defines the responsibilities of record-owning agencies, and the protections they are provided for those records, as listed below:

- *Policy 1.2.14* N-DEx System participants shall contribute or allow access to information via the N-DEx System, and agree to permit the access, dissemination, and/or use of such information by other parties pursuant to the provisions of this policy. The record-owning agency has the sole responsibility and accountability for ensuring that it is not constrained from permitting this access by any laws, regulations, policies, or procedures.
- *Policy 1.4.1* Record-owning agencies that make available records in the N-DEx System are responsible for their timeliness, accuracy, completeness, and providing point-of-contact (POC) information.
- *Policy 1.4.2* Each record-owning agency controls how and with whom their data is shared, thus retaining responsibility, control, and ownership.
- *Policy 1.4.3* Agency-Configurable Data Sharing Controls: The N-DEx System is designed to allow record-owning agencies to protect their data in accordance with the laws and policies that govern dissemination and privacy for their jurisdictions. All data is presumed sharable unless the record-owning agency restricts data access, in accordance with their sharing policy. N-DEx enables data sharing at the following data item (i.e. reports) dissemination criteria values:
  1.4.3.1 Green: Data is viewable.
  1.4.3.2 Yellow: Data consists of record ID and record-owning agency POC information. To obtain access, contact the record-owning agency.
  1.4.3.3 Red: Data is not viewable.

In short, this raises the hypothetical question, "if terms and limitations on use of records are established via data sharing rules upon initial submission to the N-DEx System, what is the exact purpose and substance of additional permissions requirements from an authorized N-DEx user to a record-owning agency?" Further review suggests the intent of the policy is to less establish permission than to ensure any additional considerations or restrictions of use can be properly conveyed to the user.

To address these concerns from stakeholders, the N-DEx PO recommends the removal of the advanced permission policy *1.3.10*, on the grounds the requirement is adequately addressed elsewhere in the *N-DEx Policy and Operating Manual*. The N-DEx PO also recommends the modification of the verification policy, as necessary, to include any language safeguards record-owning agencies might want to maintain to convey additional considerations of use.

Clarify conditions under which pre-authorized use of N-DEx System information is permitted.

Recent user feedback data suggest a stronger role delineation between users who compile, create, and disseminate criminal justice information products, and those who rely or act upon them. This is both a function of stronger interagency information sharing over the last several years, and the growing diversity of the N-DEx System user base. This has also resulted in AP&V confusion among users whose sole responsibility is the compilation of information to others within an agency, or to another agency with which a formal information exchange agreement exists: which party is ultimately responsible for satisfying AP&V requirements? Those who collect and disseminate products, including N-DEx System information, the recipients who act or rely upon the information, or both? While dissemination of both criminal history record information (CHRI) and National Crime Information Center (NCIC) restricted files to authorized recipient agencies is clearly defined within the *CJIS Security Policy* (4.2.1 and 4.2.2), the current N-DEx System authorized pre-permission policy is unclear on the act of dissemination under these conditions. This has led some to confuse dissemination with *secondary dissemination*, which governs use between agencies lacking formal agreements, and is currently included as an action requiring advanced permission and verification of N-DEx System information.

To alleviate ambiguity with existing language, the N-DEx PO's recommendation is to explicitly state dissemination as an acceptable pre-authorization use condition, alongside viewing, outputting, or discussing N-DEx System information. The form of dissemination should also clearly articulate the AP&V requirements to any authorized recipients of disseminated information. This recommendation could ultimately be accomplished through the inclusion of a cover letter containing current AP&V requirements. This would not apply to secondary dissemination, which would require explicit permission from a record-owning agency to ensure the agency's terms for the user who initially compiled the information are the same as the recipient of the compilation.

Clarify language in the "immediacy" policy (1.3.13) to remove the direct reference to exigent circumstances.

Feedback suggests the specific requirement of an exigent or emergency circumstance can have a possible deterrent effect on the use of N-DEx System information, by opening up the interpretation of appropriate use during time-sensitive, tactical situations in which the threat to danger of life might be present. Similar policy language referring to permission exceptions in the Law Enforcement Information Exchange (LInX) *Remote Data Access Agreement*, for example, specifies immediate dissemination of information without permission can be made if:

- There is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to the national security; and
- It is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such a threat, danger, or harm.

Revising the policy to remove the exigent term, while specifying conditions in a manner consistent with the LInX language, would maintain the spirit of the exception, while potentially broadening the application of N-DEx System information to other public safety situations requiring immediacy of N-DEx System Use.

OPTIONS

The Subcommittee is requested to recommend one of the options for each of the proposed revision types to the *N-DEx Policy and Operating Manual*. Agreement with the proposed revision type would result in the N-DEx PO preparing specific policy language to be submitted through the next round of the Advisory Process. .

Revision 1, Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate.

Revision 1, Option 2 – No changes.

Revision 2, Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted.

Revision 2, Option 2 – No changes.

Revision 3, Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the "immediacy" policy (1.3.13) to remove the direct reference to exigent circumstances.

Revision 3, Option 2 – No changes.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1 on Revisions 1, 2 and 3.
Revision 1, Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by

removing the reference to “advanced permissions” and expanding the verification policy, as appropriate.
Revision 2, Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted.
Revision 3, Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the “immediacy” policy (1.3.13) to remove the direct reference to exigent circumstances.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion 1: To accept Option 1 on Revisions 1, 2 & 3.
Revision 1, Option 1:
Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to “advanced permissions” and expanding the verification policy, as appropriate.
Revision 2, Option 1:
Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted.
Revision 3, Option 1:
Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the “immediacy” policy (1.3.13) to remove the direct reference to exigent circumstances.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Revision 1

Motion: To adopt Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to “advanced permissions” and expanding the verification policy, as appropriate.

Action: Motion carried

Revision 2

Motion: To adopt Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted.

Action: Motion carried.

Revision 3

Motion: To adopt Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the “immediacy” policy (1.3.13) to remove the direct reference to exigent circumstances.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Revision 1: Clarify user authorization requirements by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate.

Motion 1: To adopt Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate.

Action: Motion carried.

Revision 2: Clarify conditions under which pre-authorized use of N-DEx System information is permitted.

Motion 2: To adopt Option 1: Incorporate policy Changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted.

Action: Motion carried.

Revision 3: Clarify language in the "immediacy" policy (1.3.13) to remove the direct reference to exigent circumstances.

Motion 3: To adopt Option 1A with changes in **red bold** and **bold strikethrough**: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the "immediacy" policy (1.3.13)**.** ~~**to remove the direct reference to exigent circumstances.**~~

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion 1: To accept Option 1 on Revision 1.
Revision 1, Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate**.**

Action: Motion carried.

Motion 2: To accept Option 1 on Revision 2.
Revision 2, Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted.

Action: Motion carried.

Motion 3: To accept Option 1 on Revision 3.
Revision 3, Option 1: Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the "immediacy" policy (1.3.13) to remove the direct reference to exigent circumstances.

Action: Motion carried.

<u>FALL 2019 N-DEx SUBCOMMITTEE ACTION:</u>

Motion: <u>Revision 1</u>

To accept Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate.

<u>Revision 2</u>

To accept Option 1 revised - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of the N-DEx System information is permitted.

Revisions:

- Remove *pre-permission* from *Authorized Pre-Permission* Use policy and make it *Authorized Use*
- Expand authorized use paragraph in N-DEx Policy to include relevant examples reflecting current N-DEx use cases, such as fusion center bulletins, threat assessments, and tactical situations.
- Add "plain language" caveat to authorized use policy to cover enforcement action and suitability determinations based on N-DEx information

<u>Revision 3</u>

To accept (new) Option 3 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the N-DEx policy (1.3.13)**.** ~~**to remove the direct reference to exigent circumstances.**~~

Action: Motion carried.

Intentionally Left Blank

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA

STAFF PAPER

APB ITEM #7

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

IS ISSUE #1*
Miscellaneous Action Items Update

IS ISSUE #2
Flats for Criminal Justice Purposes

IS ISSUE #3 ***(See APB Item #2, NCIC Issue #1)***
Notifications for Wanted Notices on the Next Generation Identification (NGI) System

IS ISSUE #4
Update the NGI Criminal Justice Rap Back Policy and Implementation Guide to Show the Separation of "Death Notice with Fingerprints" and "Death Notice without Fingerprints" Triggers

IS ISSUE #5 ***(See APB Item #4 for staff paper)***
Race Code Standardization across CJIS Division Systems

IS ISSUE #6
Sex Offender Registration Type of Transaction

IS ISSUE #7 ***(See APB Item #2, NCIC Issue #2 for staff paper)***
Law Enforcement Enterprise Portal Status Report

IS ISSUE #8** ***(See Information only topic F for staff paper)***
Rapid Deoxyribonucleic Acid (Rapid DNA) Update

IS ISSUE #9*
Disposition Task Force Update

IS ISSUE #10*
Identification Services Coordination Group Update

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

IS ISSUE #11** ***(See Information only topic G for staff paper)***
FBI Programs Research and Standards Unit Update

IS ISSUE #12*
International Association for Identification (IAI) Update

IS ISSUE #13*
Ad hoc Items

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

CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 8, 2019

STAFF PAPER

IS ISSUE #2

Flats for Criminal Justice Purposes

PURPOSE

To provide results of studies concerning flat only images for criminal submissions.

POINT OF CONTACT

Biometric Services Section, Biometric Identification and Analysis Unit

Questions regarding this topic should be directed to agmu@leo.gov

BACKGROUND

As a result of APB Recommendation #1076 made in 2009, an operational assessment was performed concerning the use of flat capture fingerprint events for criminal justice purposes. The assessment was initially placed on hold until deployment of the NGI System. The CJIS Division has since performed additional research comparing the occurrences in which the latent matching algorithm produces flat versus rolled fingerprint impressions within responding candidate lists produced by the NGI System.

The capture of rolled fingerprint impressions allows for the inclusion of nail-to-nail friction ridge information while plain or flat impressions are simultaneously captured and typically exclude friction ridge detail beyond the surrounding center pattern area of the fingers. The NGI System retains both rolled and plain fingerprint impressions within the Friction Ridge Investigative File for latent search purposes and also cascades both against the Unsolved Latent File. The availability of clear and present friction ridge detail is vital in order for the NGI System to produce new investigative leads and for subsequent examination by the latent user community. The CJIS Division performed analysis of candidates produced by the NGI System within both Latent Friction Ridge Images and Feature Searches during December 2016 through December 2017. The Fingerprint Position (FGP) Field along with other corresponding information from approximately 3.5 million candidates were reviewed to determine the rate at which rolled versus flat impressions returned as candidates. The results concluded 63.49% of candidates produced were of rolled finger impression while 36.51% were associated within flat impressions.

Due to the possibility of duplicate Universal Control Numbers (UCNs) returning in a single candidate list with a combination of both rolled and flat impressions, additional analysis was performed to identify those within the candidate lists. Because the NGI System returns both rolled and plain impression codes within the FGP Field, but converts the plain impression codes to those of rolled impressions within the Candidate Investigative List (CNL) Field combined with the fact that the CNL Field includes duplicate candidates while being removed from the FGP Field, the assessment did not consider duplicate candidates. Please note only 2.07% of the 3.5 million candidates included as part of this assessment were associated with duplicate UCNs.

In response to a suggestion that the FBI require rolled capture biometric events for establishment of a criminal identity and allow for all subsequent events to include only flat fingerprint impressions, analysis was performed to determine the number of candidates produced from new versus subsequent biometric events within the NGI System. Based upon the UCN and Biometric Set Identifier of highest scoring candidates within each latent search response, 68.51% were of subsequent events while only 31.49% were associated with the original event that established the identity within the NGI System. Furthermore, 44.26% of all highest scoring candidates included subsequent events submitted with rolled fingerprint impressions.

In the absence of comparing all 3.5 million referenced candidates, a similar review of approximately 2,700 **confirmed** identifications reported by the Laboratory Division and other local, state, and federal law enforcement agencies was performed, which concluded the rate of flat versus rolled occurrences were consistent with those from the original sample. Of the confirmed identifications, 68.26% were to rolled impressions while only 31.74% resulted from flat impressions. In addition, 40.35% of the total identifications were associated with a rolled impression included as part of an event submitted after establishment of a biometric identity within the NGI System.

RECOMMENDATIONS

Based on the aforementioned operational assessment, the CJIS Division does not recommend the capture of flat only impressions for criminal justice purposes as the availability of both rolled and plain fingerprint impressions increases latent search accuracy within the NGI System and provides additional friction ridge details often times necessary for examination by the latent user community. The overall quality and integrity of biometrics submitted to or retained within the NGI System is essential in producing new leads to law enforcement and the U.S. Intelligence Community attempting to solve crime and identify suspects within terrorism investigations.

FALL 2019 WORKING GROUP ACTIONS:

This topic was accepted as information only by all five working groups.

FALL 2019 IS SUBCOMMITTEE ACTION:

This topic was accepted as information only.

CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 8, 2019

STAFF PAPER

IS ISSUE #4

Update the Next Generation Identification (NGI) Criminal Justice (CJ) Rap Back Policy and Implementation (P&I) Guide to Show the Separation of “Death Notice with Fingerprints” and “Death Notice without Fingerprints” Triggers

PURPOSE

An enhancement was made to the NGI System affecting the NGI Rap Back Services, Triggering Event Notification, “Death Notice with/without Fingerprints” separating this into two triggering events – “Death Notice with Fingerprints” and “Death Notice without Fingerprints.”

To conform to the functionality of the NGI System the NGI CJ Rap Back P&I Guide needs updated to show the proper programming format for agencies developing their system to participate in the NGI CJ Rap Back Service.

POINT OF CONTACT

Biometric Services Section, Biometric Support Unit, NGI Rap Back Services

Questions regarding this topic should be directed to <agmu@leo.gov>

REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to review, discuss, and endorse the revisions to the NGI CJ Rap Back Service P&I Guide.

BACKGROUND

Prior to the deployment of the NGI Rap Back Services on September 7, 2014, the FBI CJIS Division had been unable to fully leverage the value of their Criminal History Record Information repository on a national scale. The primary function of NGI Rap Back Services is to notify authorized agencies when a person, whose fingerprints are retained within the NGI System and has an NGI Rap Back Subscription has been arrested or has other criminal activity. These notifications are a result of the triggering events the authorized agency has selected to receive. The NGI CJ Rap Back Service provides pertinent notifications to criminal justice agencies regarding relevant triggering events reported to the NGI System pertaining to individuals currently under active investigation or under court ordered supervision. The NGI Noncriminal

Justice (NCJ) Rap Back Service provides suitable notifications to NCJ entities regarding relevant triggering events which are reported to the NGI System regarding their applicants, employees (including law enforcement employees), volunteers, licensees, etc.

With the implementation of the NGI Rap Back Services, the Subscribers choose one, some, or all of the operational triggering events (with the option for future programming of up to 40 triggering events) to generate a Rap Back Activity Notification:

1. Criminal Retain Submission – Default Trigger
2. Dispositions
3. Civil Retain Submission – only available to authorized federal agencies
4. Expungement/Partial Expungement
5. Warrant Addition
6. Warrant Deletion
7. Warrant Modification
8. Sex Offender Registry Addition
9. Sex Offender Registry Deletion
10. Sex Offender Registry Modification
11. External (Intentionally skipped as this number is not operational)
12. Death Notices with/without Fingerprints

During the Spring 2017 National Crime Prevention and Privacy Compact Council Meetings, a topic was presented and endorsed to separate the Death Notice Trigger Notification. On August 14, 2018, this enhancement was made to the NGI System affecting the NGI Rap Back Services Triggering Event Notification number twelve "Death Notice with/without Fingerprints" separating this into two triggering events – "Death Notice with Fingerprints" and "Death Notice without Fingerprints." When the enhancement was made, it affected both the NCJ and CJ Rap Back Services.

This topic paper was written to notify the user community of the enhancement, and update the NGI CJ Rap Back P&I Guide accordingly.

To conform to the functionality of the NGI System, the NGI CJ P&I Guide needs to be updated to reflect this enhancement.

DISCUSSION AND ANALYSIS

This enhancement to the NGI System allows the NGI Rap Back subscribing agencies the ability to select the Rap Back Triggers based upon Death Notices supported and/or not supported by fingerprints. Therefore, the Rap Back subscribing agency can opt in/opt out of these triggering event notifications similar to the other available triggering event selections (i.e., Triggers for Want Addition, Deletion, and Modification and Triggers for Sexual Offender Registration Addition, Deletion, and Modification).

The NGI CJ Rap Back P&I Guide will be updated to show the correct format for the NGI Rap Back Triggering Events to allow prospective NGI Rap Back participating agencies the ability to build their Rap Back Systems using accurate triggering event options currently available in the NGI System.

1. Criminal Retain Submission (Default)
2. Dispositions
3. Civil Retain Submission (Security Clearance Information Act Only)
4. Expungement/Partial Expungement (No longer an NGI Noncriminal Justice Rap Back Service Trigger Option)
5. Want Addition
6. Want Deletion
7. Want Modification
8. Sexual Offender Registration Addition
9. Sexual Offender Registration Deletion
10. Sexual Offender Registration Modification
11. External (Intentionally skipped as this number is not operational)
12. Death Notice With Fingerprints
13. Death Notice Without Fingerprints

14-40. Reserved for FBI Future Use

OPTIONS:

Option 1:
To endorse the separation of the “Death Notice with Fingerprints” and the “Death Notice without Fingerprints” Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Option 2:
Make no changes to the NGI CJ Rap Back P&I Guide and perform a system enhancement returning the NGI CJ Rap Back Service Death Notice Triggers to Death Notices with/without Fingerprints.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: To endorse the separation of the “Death Notice with Fingerprints” and the “Death Notice without Fingerprints” Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: To endorse the separation of the “Death Notice with Fingerprints” and the “Death Notice without Fingerprints” Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Action: Motion carried.

FALL 2019 IS SUBCOMMITTEE ACTIONS:

Motion: To endorse Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the NGI CJ Rap Back P&I Guide to conform to the NGI System functionality as proposed in the NGI CJ P&I Guide on pages 13-15.

Action: Motion carried.

5. Criminal Justice Subscribers may identify the triggering events for Rap Back notifications.

By default, all Subscribers will be notified when the subscribed person is arrested and the arresting agency notifies the FBI CJIS Division with the Criminal Retain Submission (the first Trigger listed, below). In addition, the Subscribing Criminal Justice Agency may elect to have other listed events trigger Rap Back notifications. The choice must be made on each Rap Back subscription and may be modified at any time through a Rap Back maintenance request transaction. The triggering event choices are placed in the Rap Back Trigger field (2.2040 RBT). The available triggering events are:

1. Criminal retain submission
   This trigger will activate whenever a retained criminal tenprint identification submission transaction or National Fingerprint File (NFF) Criminal Print Identification (CPI) transaction matches against a subscribed NGI Identity. This trigger is automatically set for all subscriptions, regardless of whether it is requested or not.
2. Dispositions
   This trigger will activate whenever a reported disposition transaction is matched against a subscribed NGI Identity. The disposition transactions included are:
   - Disposition Fingerprint Search Request;
   - Disposition Submission Request;
   - Disposition Maintenance Request.
3. Civil Retain Submission
   This trigger will activate when a retained civil Tenprint Fingerprint Identification Submission matches against a subscribed NGI Identity and it will provide notification of civil event information. This trigger is limited to certain federal agencies that have specific statutory authority per the SCIA, 5 United States Code Section 9101 to receive this information.
4. Expunge/Partial Expungement
   This trigger will activate whenever all or a portion of a subscribed NGI Identity is expunged and provide notification of the information being removed from the record.
5. Want Addition with FBI number/UCN included
   This trigger will activate whenever a record containing an FBI/UCN matches a subscribed NGI Identity is entered into the NCIC Wanted Person file or Immigration Violator file.
6. Want Deletion
   This trigger will activate whenever a record containing an FBI/UCN matches a subscribed NGI Identity is deleted from the NCIC Wanted Persons file or Immigration Violator file. This trigger will be activated by NCIC Cancel, Clear, or Locate transactions.

7. Want Modification

   This trigger will activate whenever a record containing an FBI/UCN matches a subscribed NGI Identity is modified within the NCIC Wanted Persons file or Immigration Violator file.

8. Sexual Offender Registry Addition with FBI number/UCN included

   This trigger will activate whenever a record containing an FBI/UCN matches a subscribed NGI Identity is entered in the NCIC Sex Offender Registry.

9. Sexual Offender Registry Deletion

   This trigger will activate whenever a record containing an FBI/UCN matches a subscribed NGI Identity is deleted from the Sex Offender Registry. This trigger will be activated by Cancel or Clear transactions.

10. Sexual Offender Registry Modification

   This trigger will activate whenever a record containing an FBI/UCN matches a subscribed NGI Identity is modified within the Sex Offender Registry. Transactions that will cause this trigger to activate are limited to modification of any of the following fields:

   - Name;
   - Case Number;
   - Registration Date;
   - Registry Expiration Date;
   - Registering Agency.

11. External (Intentionally skipped as this number is not operational)

~~11. Death Notices~~

~~This trigger will activate whenever CJIS receives a death notice and associates it with a subscribed NGI Identity. This will include both fingerprint-based and non-fingerprint-based death notice submissions. The Rap Back Activity Notification will include whether it was a fingerprint supported death notice or not. The NGI does not remove the Rap Back subscription as result of a fingerprint based or non-fingerprint based death notice.~~

12. Death Notice with Fingerprints

   This trigger will activate when NGI System receives a death notice and associates it with a subscribed NGI Identity. This will include any fingerprint-based death notice submission. The Rap Back Activity Notification will include "Deceased's fingerprints were provided." The NGI System does not remove the subscription as result of a fingerprint based death notice.

13. Death Notice without Fingerprints

   This trigger will activate when the NGI System receives a death notice and associates it with a subscribed NGI Identity. This will include any non-fingerprint-based death notice submission. The Rap Back Activity Notification will include "Deceased's fingerprints were not provided." The NGI System does not remove the subscription as a result of a non-fingerprint based death notice.

Note: The NGI will also provide a Rap Back Activity Notification for all subscriptions regardless of the set triggers for the following conditions:

1. Consolidation: Consolidation may trigger a Rap Back notification for any of the Identities involved in the consolidation. This process is described further in the NGI Rap Back Service Transactions Section, Item #6: Receiving Rap Back Activity Notifications for Consolidations of Subscribed Identities.
2. Identity Deletion: FBI CJIS will send the Submitting Agency a Rap Back Activity Notification when a subscribed Identity is deleted from the NGI. The associated subscription(s) are automatically deleted whenever an Identity is deleted.

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
IDENTIFICATION SERVICES (IS) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 8, 2019

STAFF PAPER

IS ISSUE #6

Sex Offender Registration (SOR) Type of Transaction (TOT)

PURPOSE

To discuss the benefits and risks of creating a new Electronic Biometric Transmission Specification (EBTS) TOT to be utilized for SOR submissions to establish a biometric-based event in the Next Generation Identification (NGI) System.

POINT OF CONTACT

Biometric Services Section, Biometric 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 provided in this paper and provide appropriate comments, suggestions, or recommendations to the APB). Also, the Subcommittee should indicate what priority should be assigned to any recommendation.

BACKGROUND

In December 2010, the FBI Criminal Justice Information Services (CJIS) Division published a CJIS Information Letter which advised users the FBI CJIS Division would begin accepting and maintaining SOR fingerprints. Prior to this change, SOR fingerprints were not accepted solely on registration of the offender and were not able to be used to establish a criminal history record. The change permitted agencies to positively identify an offender and obtain an FBI Universal Control Number (UCN) if one was not already established.

Pursuant to the 2010 guidance, SOR transactions submitted for the purpose of creating an FBI UCN are submitted as a Criminal Ten-Print Submission Answer Required (CAR) TOT and may include a free text disposition to comply with the expectation of court data to complete the event. These are processed as criminal events which update the Identity History Summary (IdHS) or establish an FBI UCN, and are included in responses disseminated to the contributors. The responses will always contain the positive identification/non-identification decision and may contain the electronic IdHS, if requested, in accordance with the CAR TOT. Once the FBI UCN is established, it is available for the inclusion in the National Crime Information Center (NCIC) National Sex Offender Registry (NSOR) entry by the entering agency.

As a matter of information, an FBI UCN is not a mandatory field for entry when creating an NCIC NSOR record. However, an FBI UCN must be included in the NCIC NSOR record for the sex offender notice to be appended to a criminal history record in the NGI System. Without the FBI UCN in the NCIC NSOR, the sex offender notice will not be available in response to fingerprint-based criminal or civil checks, or via name-based checks of the Interstate Identification Index (III).

While it seems unlikely for a registered sex offender to not have a criminal event retained in the NGI System, and thus an FBI UCN, it does occur for various reasons. A few examples include non-retainable juvenile offenses, state laws preventing the entry of juvenile offenders, arrest fingerprints not being captured at the time of arrest, or poor image quality fingerprints which are rejected by the NGI System and not resubmitted. One specific example is when an offender relocates to a new state and must register in that state and an FBI UCN has not been established in the state the offenses occurred. The following proposal would create a new TOT to add SOR events to the NGI System and establish an FBI UCN, if necessary.

DISCUSSION AND ANALYSIS

The Texas Department of Public Safety (DPS) is requesting the Subcommittee discuss creating a new TOT that would support the submission of a SOR record type. Currently, SOR events are submitted as criminal events by utilizing the CAR TOT; however, SOR events are neither a true arrest event nor an applicant event. Per the Texas DPS, the SOR TOT would clearly define the registration event and remove the criminal event requirement of a final disposition. The Texas DPS envisions the new SOR TOT will also establish a record or event in the NGI System. Establishing an FBI UCN will enable the NSOR owner to update the NCIC NSOR accordingly, as well as enable the NGI System to append the NCIC NSOR to the IdHS.

In addition, the new SOR TOT could allow the states to submit and retain fingerprints for all SOR records through the NGI System. States will need to program for the new SOR TOT and acquire fingerprints to submit using this TOT. Rules regarding the dissemination of registration events will need to be established.

As a matter of information, the CJIS Division is currently in the final stages of development and implementation of a process to eliminate unsynchronized data between the NGI System and the NCIC. This development was in response to an outstanding 2006 APB recommendation and the plan was presented to the APB in fall 2018 (see Topic Paper #D-42). The NCIC is the primary system for NSOR records and the NGI System is linked to enhance response data. The creation of a new EBTS TOT to allow SOR data to be included in the NGI System would not align with this initiative.

If it is determined a new SOR TOT should be pursued, additional items will require research and resolution. The below list is not all-inclusive but does address some of those items:

- Creation of a new TOT and rules related to the TOT (i.e., retention, expiration date, deletion, cascading, maintenance, required fields, and any associated fees.)
- Creation of audit rules to ensure a clear understanding of what the expectations are from a program office perspective prior to formally incorporating into an existing audit methodology for the new TOT.
- Dissemination and usage rules for the new TOT and any criminal or non-criminal IdHS which contain an SOR transaction.
- Determine if programming of the new TOT will be mandatory or optional.
- Determine if current NGI System SOR events submitted as CAR TOTs would have to be changed or remain as is.

If the current processes need redefined or changes to the dissemination rules are required, a technical review will be conducted to properly assess the expectations and provide the level of effort.

OPTIONS

Option 1: Conduct the research needed to identify new business rules for a SOR TOT.

Option 2: No change.

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

RECOMMENDATION

The FBI CJIS Division has no recommendations.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion 1: To accept Option 1: Conduct the research needed to identify new business rules for a SOR TOT.
Action: Motion carried.

Motion 2: To accept Priority Level 2H.
Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion 1: To accept Option 1: Conduct the research needed to identify new business rules for a SOR TOT.
Action: Motion carried.

Motion 2: To assign a Priority 4M.
Action: Motion carried

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 1. Conduct the research needed to identify new business rules for a SOR TOT. Priority 3M.
Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Conduct the research needed to identify new business rules for a SOR TOT. Priority 3M
Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Conduct the research needed to identify new business rules for a SOR TOT. Priority 3M.
Action: Motion carried.

FALL 2019 IS SUBCOMMITTEE ACTION:

Motion: Conduct the research needed to identify new business rules, policies, and privacy implications for a SOR TOT. (Notes: juveniles, rejects, etc.)
Action: Motion carried.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA

STAFF PAPER

APB ITEM #13

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

UCR ISSUE #1* ***(See Informational Topic K for staff paper)***
UCR Status Report

UCR ISSUE #2
Definition Revisions for Federal National Incident-Based Reporting System (NIBRS) Offenses

UCR ISSUE #3 ***(See APB Item #4, for staff paper)***
Race Code Standardization across CJIS Division Systems

UCR ISSUE #4**
Beyond 2021 Task Force Update

UCR ISSUE #5**
Women's Law Project Request for Topic

UCR ISSUE #6**
Unfounded and Case Disposition Options Research Update

UCR ISSUE #7
Why Participation Matters in the National Use-of-Force Data Collection

UCR ISSUE #8**
Law Enforcement Officers Killed or Assaulted Update

UCR ISSUE #9
Status of the NIBRS Transition

UCR ISSUE #10**
NIBRS Estimation Project

UCR ISSUE #11**
Crime Data Explorer Update

UCR ISSUE #12 ***(See APB Item #2, NCIC Issue #2 for staff paper)***
Law Enforcement Enterprise Portal Status Report

UCR ISSUE #13**
Quality Assurance Review Update

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

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING SUBCOMMITTEE (UCR)
NORFOLK, VA
OCTOBER 8, 2019

STAFF PAPER

UCR ISSUE #2

Definition Revisions for Federal National Incident-Based Reporting System (NIBRS) Offenses

PURPOSE

To provide modifications and suggestions for the approved NIBRS offenses to enable federal agencies to accurately report crime data to the Uniform Crime Reporting (UCR) Program.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to consider the modifications and suggestions presented in this paper and attachment for revising the NIBRS offenses for federal reporting.

BACKGROUND

The UCR Program has been working with federal agencies to assist them in complying with the Uniform Federal Crime Reporting Act 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 a 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 collaborating with federal agencies, the UCR Program identified a need to develop additional offenses to enable federal agencies to accurately report crime data. In addition, the UCR Program organized a Federal Task Force consisting of representatives from the Department of Homeland Security, the United States Marshals Service, the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Environmental Protection Agency, the Department of the Interior, and the Drug Enforcement Administration. The task force discussed the need to expand the Group A and B offenses in order to capture details of crime for federal reporting. The results of these discussions led to a topic paper containing 20 additional NIBRS offenses for federal and tribal reporting. The topic paper was reviewed, discussed, and recommended for approval during the Fall 2017 Criminal Justice Information Services (CJIS) Division APB.

DISCUSSION AND ANALYSIS

Following the approval by the FBI Director of the 20 additional NIBRS offenses, the UCR Program began the process to implement them into policy, user manual, and technical documentation. During this process and in collaboration with UCR, NIBRS, and CJIS Training subject matter experts, it was determined a portion of the definitions and codes may need revised. The reasoning was to ensure compatibility with existing NIBRS offenses and understanding by the federal and tribal user community.

The UCR Program decided to revisit the NIBRS offenses and codes in question and collaborate with the Federal Task Force on recommended definitions and codes for the Subcommittee to review. The UCR Program has provided an attachment (NIBRS Offenses Attachment) outlining the original APB approved definitions and codes in conjunction with the proposed revisions. As stated in the 2017 approved APB language, these offenses would only be reported by federal and tribal agencies. In the future, these additional offense types could be made available for reporting by local and state law enforcement agencies if recommended and approved by the APB. The UCR Program is anticipating these changes will be made to the NIBRS prior to January 1, 2021.

OPTIONS

Option 1 – Accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

Option 2 – Accept the recommended NIBRS UCR offense definitions and codes (NIBRS Offenses Attachment) for federal and tribal reporting with the following modifications.

Option 3 – No Change

RECOMMENDATIONS

The UCR Program recommends accepting all the modifications for the NIBRS offenses and codes for federal and tribal reporting.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 3: No change.

Action: Motion carried. 14 Yay; 8 Nay.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Accept the proposed revisions (NIBRS UCR offense definitions and codes for federal and tribal reporting.)

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting

Action: Motion carried.

FALL 2019 UCR SUBCOMMITTEE ACTION:

Motion: Approve Option 1, accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

Action: Motion carried.

National Incident-Based Reporting System Offenses

APB Approved Offense	APB Approved Offense Code	Recommended Offense Code	APB Approved Definition	Recommended NIBRS Definition	Requested Action
Failure to Register as a Sex Offender	36C	**360**	The failure to register or update a registration as required as a sex offender.	**To fail to register or keep current a registration as required by state and federal laws.**	**Changing code from 36C to 360 and updating the definition.**
Treason	101	**No changes**	The crime of betraying one's country, especially by attempting to kill the sovereign or overthrow the government.	**Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere.**	**Updating the definition only.**
Espionage	103	**No changes**	The practice of spying or using spies, typically by governments to obtain political and military information.	**The act of obtaining, delivering, transmitting, communicating, or receiving national security or national defense information with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation**	**Updating the definition only.**
Illegal Entry into the United States	301	**30A**			**Updating code only.**
False Citizenship	302	**30B**	Whoever falsely and willfully represents themselves to be a citizen of the United States.	**Falsely and willfully representing oneself to be a citizen of the United States.**	**Changing code from 302 to 30B and updating the definition.**
Smuggling Aliens	303	**30C**	When a person knowingly encouraged, induced, assisted, abetted, or aided another person to enter, or try to enter, the United States.	**To knowingly assist, abet, or aid another person to enter, or try to enter, the United States illegally.**	**Changing code from 303 to 30B and updating the definition.**

National Incident-Based Reporting System Offenses

APB Approved Offense	APB Approved Offense Code	Recommended Offense Code	APB Approved Definition	Recommended NIBRS Definition	Requested Action
Re-entry After Deportation	304	**30D**	Individual who enters, attempts to enter, or has been found in the United States after being removed, excluded, deported, or has departed the United States while an order of removal exclusion or deportation is outstanding.	**The act of entering, attempting to enter, or being found in the United States after being removed, excluded, deported, or has departed the United States while an order of removal exclusion or deportation is outstanding.**	**Changing code from 304 to 30B and updating the definition.**
Other Immigration Violations	399	**30E**			**Recommend removing this violation and not including in the NIBRS collection.** **If the offense is not removed completely, recommend changing from 399 to 30E.**
Fugitive (Harboring Escapee/Concealing from Arrest)	490	**49A**	Harboring or concealing any person for whose arrest warrant or process has been issued under the provision of any law of the United States to prevent his/her discovery and arrest. This includes any prisoner after his/her escape from the custody of the AG, or from a federal penal or correctional institution.	**To harbor or conceal any person for whose arrest, a warrant or process has been issued, so as to prevent the fugitive's discovery and arrest, after having notice or knowledge that a warrant or process has been issued for the fugitive's apprehension.**	**Changing code from 490 to 49A and updating the definition.**

National Incident-Based Reporting System Offenses					
APB Approved Offense	**APB Approved Offense Code**	**Recommended Offense Code**	**APB Approved Definition**	**Recommended NIBRS Definition**	**Requested Action**
Fugitive (Flight to Avoid Prosecution)	499A	**49B**	Moving or traveling in interstate or foreign commerce with intent to avoid prosecution, custody, confinement, or to avoid giving testimony in any criminal proceedings.	**To knowingly leave the jurisdiction where charges were filed with intent to avoid prosecution, custody, confinement, or to avoid giving testimony in any criminal proceedings.**	**Changing code from 499A to 49B and updating the definition.**
Fugitive (Flight to Avoid Deportation)	499B	**49C**	Moving or traveling in interstate or foreign commerce with intent to avoid deportation.	**To knowingly leave the jurisdiction with intent to avoid deportation.**	**Changing code from 499B to 49C and updating the definition.**
Perjury	500	**90M**	The offense of willfully telling an untruth in a court after having taken an oath of affirmation.	**To knowingly or intentionally communicate or certify an untruth through testimony, declaration, deposition, or certificate before a competent tribunal, officer, or person in which a law of the United States authorizes an oath to be administered.**	**Go back through the APB Process for updated Group, offense code, and definition.**

National Incident-Based Reporting System Offenses

APB Approved Offense	APB Approved Offense Code	Recommended Offense Code	APB Approved Definition	Recommended NIBRS Definition	Requested Action
Import Violations	580	**58A**	Any individual who knowingly or willfully, with intent to defraud the United States, 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.	**To knowingly or willfully defraud the United States by smuggling, importing, or clandestinely introducing merchandise that should have been invoiced, received, bought, sold, or facilitate the transportation, the concealment, or sale of such merchandise after importation.**	**Changing code from 580 to 48A and updating the definition.**
Export Violations	581	**58B**	Any individual who knowingly or willfully, with intent to defraud the United States, 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.	**To knowingly or willfully defraud the United States by smuggling, exporting, or clandestinely distributing merchandise that should have been invoiced, received, bought, sold, or facilitate the transportation, the concealment, or sale of such merchandise after exportation.**	**Changing code from 581 to 58B and updating the definition.**

National Incident-Based Reporting System Offenses APB Approved Offense	APB Approved Offense Code	Recommended Offense Code	APB Approved Definition	Recommended NIBRS Definition	Requested Action
Federal Liquor Offenses	610A	**61A**	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.	**The unlawful production (using an unregistered still), transportation (without proper bill of lading), receipt, distribution, or smuggling of distilled spirits on which federal tax has not been paid. Acting as a distiller, a winery, or a wholesaler of distilled spirits, wine, or malt beverages without a federal permit.**	**Changing code from 610A to 61A and updating the definition.**
Federal Tobacco Offenses	610B	**61B**	The sale, 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.	**The unlawful possession and/or distribution of contraband tobacco products; including any quantity of cigarettes in excess of 10,000 or other tobacco products if the cigarettes/products bear no evidence of the payment of applicable state taxes in the state where the cigarettes are found. Engaging in interstate commerce in tobacco products without registering with, and reporting to, the federal government and applicable state tax administrators.**	**Changing code from 610B to 61B and updating the definition.**

National Incident-Based Reporting System Offenses

APB Approved Offense	APB Approved Offense Code	Recommended Offense Code	APB Approved Definition	Recommended NIBRS Definition	Requested Action
Wildlife Trafficking	620	**No changes**	Violations of the Conservation on International Trade in Endangered Species of Wild Fauna and Flora (CITES), which regulates exports, imports, and re-exports of wildlife.	**The poaching or other illegal taking of protected or managed species and the illegal trade in wildlife and their related parts and products.**	**Updating the definition.**
Federal Resource Violations	90L	**No changes**	Crimes related to the damage or destruction of the nation’s national 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.	**To unlawfully and intentionally damage or destruct national resources including those protected under any Act intended to preserve or protect the nation's environmental, natural, cultural, or historically significant resources.**	**Updating the definition.**

National Incident-Based Reporting System Offenses					
APB Approved Offense	**APB Approved Offense Code**	**Recommended Offense Code**	**APB Approved Definition**	**Recommended NIBRS Definition**	**Requested Action**
Firearm (violation of the National Firearm Act of 1934)	520A	**521**	The violation of federal laws prohibiting the manufacture, importation, sale, purchase, transfer, possession or interstate transportation of unregistered (non-tax aid) weapons including machine guns, firearm mufflers or silencers, short barreled rifles, short-barreled shotguns, destructive devices, and any other weapons as defined as Title 26 United States Code (U.S.C.) §5854 – Definitions.	**To manufacture, import, sell, purchase, transfer, possess, or transport in interstate commerce, a firearm knowing it has the characteristics or features of a short barreled rifle or shotgun, machinegun, silencer, destructive device, or any other weapon as defined at 26 U.S.C. § 5845(a) in violation of the provisions of the National Firearms Act (generally non-tax paid, unregistered).**	**Changing code from 520A to 521 and updating the definition.**
Weapons of Mass Destruction	520B	**522**	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.C. §2332a – Use of weapons of mass destruction.	**To knowingly violate the federal law 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 by federal law.**	**Changing code from 520B to 522 and updating the definition.**

National Incident-Based Reporting System Offenses					
APB Approved Offense	APB Approved Offense Code	Recommended Offense Code	APB Approved Definition	Recommended NIBRS Definition	Requested Action
Explosives	526	**No changes**	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 U.S.C. § 841 (c).	**To knowingly violate the federal law prohibiting the manufacture, importation, sale, purchase, transfer, possession, unlawful use, intra or interstate transportation, or improper storage of any chemical compound mixture the primary or common purpose of which is to function by explosion including explosive materials or any explosive bomb, rocket, grenade, missile, or similar device, or any incendiary bomb or grenade, fire bomb, or "Molotov cocktail."**	**Updating the definition.**

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING SUBCOMMITTEE (UCR)
NORFOLK, VA
OCTOBER 8, 2019

STAFF PAPER

UCR ISSUE #7

Why Participation Matters in the National Use-of-Force Data Collection

PURPOSE

The purpose of this paper is to provide an informational update on the National Use-of-Force Data Collection, as well as to reiterate why participation in this collection is so important to Law Enforcement and the communities they serve.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to <agmu@leo.gov>

BACKGROUND

On September 5, 2018, the Federal Bureau of Investigation (FBI) CJIS Division received approval from the Office of Management and Budget (OMB) to launch the National Use-of-Force Data Collection. The official launch commenced on January 1, 2019. The FBI established a National Use-of-Force Data Collection at the behest of local, state, tribal, and federal law enforcement partners and major law enforcement organizations. This collection promotes transparency between law enforcement and the communities they serve.

This voluntary program gathers data on law enforcement use-of-force incidents which result in the death or serious bodily injury of a person, as well as the discharge of a firearm at or in the direction of a person. The goal of the resulting statistics is not to offer insight into single use-of-force incidents but to provide an aggregate view of the incidents reported and the circumstances, subjects, and officers involved.

DISCUSSION AND ANALYSIS

What is the National Use-of-Force Data Collection:

The FBI has a long-standing tradition of providing crime statistics on Law Enforcement Officers Killed and Assaulted (LEOKA) and justifiable homicides to facilitate transparency and accountability. To improve the data currently available, the FBI will also collect use of force data. The CJIS Advisory Policy Board (APB) approved the recommendation to develop this collection on December 3, 2015 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 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 Title 18, Section 2246 (4) of the United States Code:

> "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 Use-of-Force 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. The task force met in person on January 27, 2016; March 17, 2016; May 4-5, 2016; August 3, 2016; September 7, 2017; February 22, 2018; September 12, 2018; and June 6, 2019. In addition, a monthly teleconference is held with the task force between in person meetings. The Use-of-Force Task Force identified the following data elements for inclusion and measurement in the National Use-of-Force Data Collection:

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 the following 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."

Participation Metrics:

Participating agencies are defined as agencies that have released use-of-force data to the FBI at least one time from January 1 to December 31 of the current year. Participating agencies may contribute use-of-force data via the use-of-force portal application housed on LEEP, or via bulk submission using a JavaScript Object Notation or Extensible Markup Language file format.

As of May 20, 2019, 1,724 (9.37 percent) out of over 18,000 (100 percent) of law enforcement agencies were participating and providing use-of-force data to the FBI. These agencies represent 143,305 (17.91 percent) out of 800,000 (100 percent) of sworn law enforcement officers nationwide. One hundred and six out of over 500 target agencies that employ 200 or more sworn law enforcement officers were participating and providing use-of-force data to the FBI. Federal agencies are excluded from this target list at this time until the universe of applicable federal agencies and the associated number of sworn law enforcement officers are determined. If all target agencies (currently excluding federal agencies) begin participating and providing use-of-force data to the FBI, the participation percentage would be greater than 50 percent.

The largest ten participation agencies included:

- Chicago Police Department

- Los Angeles Metropolitan Police Department
- Washington D.C. Metropolitan Police Department
- Las Vegas Metropolitan Police Department
- San Diego County Sheriff's Office
- Detroit Police Department
- San Francisco Police Department
- San Antonio Police Department
- Memphis Police Department
- Orange County Sheriff's Office

The largest participating tribal law enforcement agency was:

- Tohono O'Odham Nation

The largest participating college/university was:

- Georgia State University

The largest participating federal agency was:

- FBI

Use-of-Force Data Publication:

National use-of-force data will be published on Crime Data Explorer (CDE) for future publicly available publications. This decision was previously approved by the former CJIS Division Assistant Director on December 17, 2018 and was supported by the Use-of-Force Task Force.

As the collection grows toward the minimum 40 percent participation threshold, a status report was provided to CJIS Systems Officers (CSOs) and State Program Managers (SPMs), and participating federal centralized data managers. The intent of this status report was to provide a narrative status concerning agency and police employment counts, as well as a downloadable list of enrolled/participating agencies for the United States, as well as individual states and federal agencies in order to strategize engagement throughout the nation and encourage more participation in this collection.

The nature of working in an environment dependent on external participation requires an organization to be agile and open to potential change. The FBI is required by OMB to achieve minimum participation thresholds by sworn law enforcement officers before any use-of-force data can be released to the public, in order to maintain a nationally representative and accurate message. The minimum participation thresholds were not met to publish use-of-force data publicly; however, the FBI did provide a status report to CSOs, SPMs, and federal centralized data managers.

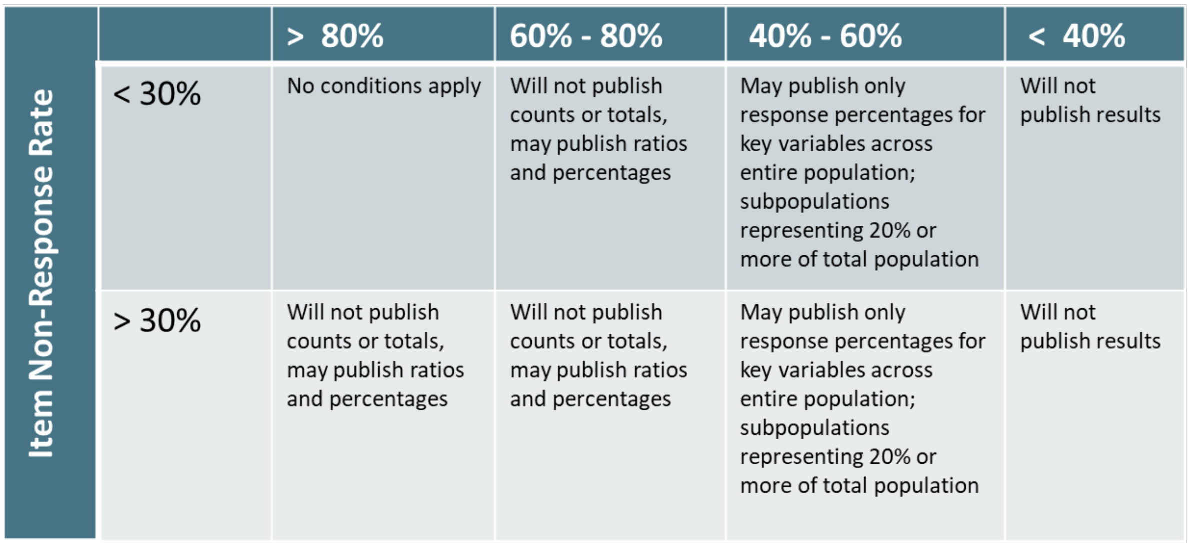
Why is Participation in this Collection Important:

The FBI was requested by the major law enforcement organizations to manage the National Use-of-Force Data Collection as a trusted law enforcement partner. Law enforcement agencies nationwide expressed the need for a national collection that would provide context and control of the narrative in place of independent collections managed by national news media outlets. In addition, data derived from this collection can be used to enhance law enforcement training regarding de-escalation techniques, as well as aid law enforcement leaders in determining how and where to appropriately staff personnel to improve community safety, while providing transparency and accountability.

The success of this collection will be measured according to coverage rate, which refers to the total sworn law enforcement officer population covered by the National Use-of-Force Data Collection. **A minimum coverage rate of 40 percent of sworn law enforcement officers participating and releasing data to the FBI is required by January 1, 2020 to provide minimal metrics to the general public.** To ensure the continuation of the collection, a 60 percent coverage rate of participation is needed by January 1, 2021, and a coverage rate of participation greater than 60 percent is needed by January 1, 2022. If these participation thresholds are not achieved, OMB has recommended disbanding the collection, and revisiting previous options with separate statistical entities. If law enforcement agencies do not take action and proactively begin releasing data to the FBI, we will fail our partners who have specifically requested the FBI's trusted leadership and assistance.

As of May 20, 2019, the percentage of law enforcement officers who participated in this collection and released data to the FBI since January 1, 2019, was 17.91 percent. This was a significant percentage achieved in just four months. However, minimal participation thresholds must be achieved before the FBI will publicly release use-of-force data to ensure the data is nationally representative and not misleading. See Table 1 below to reference the coverage and item non-response rates.

Table 1: Coverage and Item Non-Response Rates



		> 80%	60% - 80%	40% - 60%	< 40%
Item Non-Response Rate	< 30%	No conditions apply	Will not publish counts or totals, may publish ratios and percentages	May publish only response percentages for key variables across entire population; subpopulations representing 20% or more of total population	Will not publish results
	> 30%	Will not publish counts or totals, may publish ratios and percentages	Will not publish counts or totals, may publish ratios and percentages	May publish only response percentages for key variables across entire population; subpopulations representing 20% or more of total population	Will not publish results

The FBI discovered many state Uniform Crime Reporting (UCR) programs plan to incorporate a use-of-force module within their new records management systems during the National Incident-Based Reporting System transition. Therefore, the ability for agencies to participate and release data to this collection via their new records management systems may be slightly delayed due to funding and technical builds, which accounts for the 8.58 percent gap between law enforcement officer enrollment and preparation to release data and their actual participation and release of data to the FBI. However, as of May 20, 2019, most state UCR programs have agreed agencies within their state may use the use-of-force portal application if they choose to in the interim.

By providing status reports to CSOs, SPMs, and federal centralized data managers, the FBI provided current participation metrics to key stakeholders to encourage marketing and messaging, as well as allow these stakeholders to provide actionable plans and commitment dates for future participation. The FBI is asking SPMs who are experiencing a delay in participation due to funding and technical builds to encourage their local agencies to use the use-of-force portal application housed on LEEP in the interim.

The FBI will not release use-of-force data publicly until all data quality standards are met to ensure nationally representative data is provided. These thresholds are in line with federal statistical program standards. This includes the coverage and item non-response rates described in Table 1 above. Once data quality standards are met, use-of-force data will be aggregated and published at the state and federal levels, as well as regionally and nationally. No use-of-force data will be published at the individual agency level.

Engagement Strategies:

The FBI is working to execute engagement strategies targeting law enforcement agencies, major law enforcement organizations, legislative bodies, advocacy groups, criminologists, criminal justice students, media outlets, and the general public utilizing publications, conferences, training events, and social media to successfully achieve participation thresholds.

The FBI participated in the following 28 speaking engagements since January 1, 2019:

- Michigan Chiefs of Police Association, February 2019
- Michigan Sheriffs' Association, March 2019
- 2019 International Association of Chiefs of Police (IACP) Indian County Law Enforcement Section Mid-Year Meeting, March 2019
- Alaska Joint FBI Civil Rights/UCR Hate Crime Training, April 2019
- Georgia Sheriffs' Association, April 2019
- Virginia Sheriffs' Association, April 2019
- Spring 2019 UCR Subcommittee Meeting, April 2019
- West Virginia Webinar Use-of-Force Portal Demo, April 2019
- California Joint FBI Civil Rights/UCR Hate Crime Training, May 2019
- FBI National Academy Associates, May 2019
- Colorado State Program Manager Event, May 2019
- Washington Association of Sheriffs and Police Chiefs, May 2019
- Association of State Criminal Investigative Agencies 2019 Spring Conference, May 2019
- 2019 Major Cities Chiefs Association, Police Executive Research Forum, and FBI National Executive Institute Associates Joint Meeting, May 2019
- 2019 IACP Technology Conference, May 2019
- Texas Webinar Use-of-Force Portal Demo, May 2019

- Florida Webinar Use-of-Force Portal Demo, May 2019
- Kansas CJIS Conference, June 2019
- Spring 2019 APB Meeting, June 2019
- 14th Annual Tribal Leader/Scholar Forum at the National Congress of American Indians, June 2019
- National Sheriffs' Association Annual Education and Technology Exposition, June 2019
- 2019 International Association of Campus Law Enforcement Annual Conference, June 2019
- Florida Department of Law Enforcement's 2019 CJIS Annual Training Symposium, July 2019
- Alabama Sheriff's Association, July 2019
- Oregon Annual CJIS Training, August 2019
- Oregon Sheriff's Association, August 2019
- National Organization of Black Law Enforcement Executives Summer Conference, August 2019
- 27th Annual National Native American Law Enforcement Association National Collaborative Training Event, August 2019

Marketing and Outreach:

To market the National Use-of-Force Data Collection, the FBI developed the following webpage which law enforcement agencies and the general public may use to obtain answers to frequently asked questions and access resources and support information: <http://www.fbi.gov/useofforce>. Additionally, the National Use-of-Force Data Collection 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 use-of-force portal application, such as "How to Create an 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 Quick Guides to supplement training components regarding the use of the use-of-force portal application. These resources are housed on the use-of-force portal application itself. Furthermore, the FBI is amending the National Use-of-Force Data Collection marketing video to include interviews with The International Association of Chiefs of Police, Major County Sheriffs of America, and Washington State Patrol.

The FBI is working with both internal and external entities to publish articles highlighting the National Use-of-Force Data Collection. The following two articles have been published:

- The National Use-of-Force Data Collection: Now Enrolling Agencies and Accepting Data, *Police Chief Magazine*, June 2019
- The National Use-of-Force Data Collection: International Association of Campus Law Enforcement Administrators Campus *Law Enforcement Journal*, June 2019

In addition, one article is being considered for publication by the *Law Enforcement Bulletin*.

For more information, the Use-of-Force Help Desk may be reached by telephone: 304-625-9998 or e-mail: <useofforce@fbi.gov>.

FALL 2019 WORKING GROUP ACTIONS:
This topic was accepted as information only by all five working groups.

FALL 2019 UCR SUBCOMMITTEE ACTION:
Accepted as information only.

CJIS ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING SUBCOMMITTEE (UCR)
NORFOLK, VA
OCTOBER 8, 2019

STAFF PAPER

UCR ISSUE #9

Status of the National Incident-Based Reporting System (NIBRS) Transition

PURPOSE

To provide an update on the Federal Bureau of Investigation (FBI) efforts to transition to NIBRS

POINT OF CONTACT

Crime Data Modernization—NIBRS Transition

Questions regarding this topic should be directed to <agmu@leo.gov>

BACKGROUND

The FBI's established date to discontinue the acceptance of Summary Reporting System (SRS) data remains set for January 1, 2021, in accordance with the CJIS Advisory Policy Board (APB) recommendation from 2015 which states:

> "The FBI Uniform Crime Reporting (UCR) Program will transition to a NIBRS-only data collection by January 1, 2021, and will evaluate the probability of achieving that goal on an annual basis. Federal, state, local, and tribal agencies unable to meet the five-year transition and who have committed to transitioning to NIBRS will collaborate with the FBI CJIS Division to develop a transition plan and timeline for conversion."

As previously reported, 2018 was a pivotal year for NIBRS Transition. The FBI implemented activities of engagement and marketing, and accomplished the following:

- Completed direct communications with the CJIS Systems Officers (CSO) and UCR Program Managers from all 50 states about agency commitments
- Presented 49 NIBRS Transition briefings at conferences/meetings (Calendar Year 2018)
- Published 12 articles
- Provided approximately 46 training sessions to roughly 3,100 attendees representing 1,520 agencies [Fiscal Year (FY) 2018]
- Redesigned the UCR and NIBRS webpages
- Developed a NIBRS Toolbox of marketing resources

Great progress was made by agencies transitioning to NIBRS. For instance, the 2017 *Crime in the United States* publication reflected there were 6,998 law enforcement agencies who submitted NIBRS data. Additionally, the FBI's work with state and local law enforcement agencies has identified over 3,500 other agencies committed to transitioning to NIBRS by 2021.

As of summer 2019, 38 state UCR Programs are NIBRS certified. Hawaii and Wyoming were the most recent to attain NIBRS certification. The 12 remaining states to be NIBRS certified are: Alabama (currently testing for certification), Alaska, California, Florida, Illinois, Maryland, Mississippi, Nevada, New Jersey, New Mexico, New York, and North Carolina.

Once certified the state UCR Program is able to better assist local agencies with NIBRS transition, and they will be responsible for certifying agencies to submit NIBRS-only data. One federal agency, the Pentagon Force Protection Agency, also attained NIBRS certification.

Marketing
The FBI continues to work to make agencies aware of the benefits of transitioning to NIBRS, the steps for an agency to transition, and training opportunities available to agencies. Marketing resources such as the new and robust UCR and NIBRS Web pages leverage public platforms to contact and educate stakeholders about changes with UCR data and NIBRS transition. With the focused theme of transition, agencies considering transition, or who are in the process of transitioning to NIBRS, will find a wealth of information about the January 1, 2021 deadline and other related topics such as:

- Benefits of NIBRS;
- "30 Questions and Answers about NIBRS Transition";
- Interactive Map linked to the Crime Data Explorer website;
- Steps on how to get to NIBRS;
- NIBRS Toolbox for Law Enforcement;
- Links to relevant publications;
- NIBRS 101 video; and,
- Other NIBRS resources.

The "NIBRS Toolbox" of transition resources includes: a "NIBRS Readiness Assessment"; a playbook/guide for implementing an IBR system; "NIBRS Quick Facts"; and, a two-page informational flyer.

Additionally, the FBI continues to publish articles recognizing agencies that have already transitioned and the benefits of NIBRS, as well as offering scenarios from different types of law enforcement agencies, to further promote NIBRS transition. Recent articles published, as well as articles scheduled for publication throughout 2019, include:

- 2018 publication
  - December—"30 Frequently Asked Questions about NIBRS" for *the NIBRS webpage and CJIS Link.*

- 2019 publications
    - February—"Why Agencies Should Transition to NIBRS" for *Criminal Intelligence Coordinating Council's (CICC) Five in 5*
    - March—"The FBI's Transition to NIBRS" for *Campus Law Enforcement Journal [March/April 2019 Edition]*
- 2019 planned publications
    - Pending—"Crime Data Explorer: UCR Data with a Focus on NIBRS" for *The Police Chief*
    - Pending—"Benefits of NIBRS for Colleges and Universities" for *Campus Law Enforcement Journal*
    - Pending—"How the Norman, Oklahoma Police Department Uses NIBRS" for *The Police Chief*

Training events about NIBRS also continue to be a priority for the FBI throughout 2019. With a dedicated staff of trainers and subject matter experts, the CJIS Training and Advisory Process (CTAP) Unit provides nationwide and onsite training services at conferences and training hosted by state UCR Programs and other law enforcement organizations/associations. Each event is usually two-full days of comprehensive, "A-Z" training about NIBRS data elements, definitions, and reporting categories. Through coordination with the FBI's UCR Program, the trainers begin these events by emphasizing the January 1, 2021 deadline and highlighting the benefits of richer crime data with NIBRS.

As of April 23, 2019, the CTAP Unit has completed approximately 13 NIBRS training sessions with approximately 700 attendees and nearly 400 agencies. Additional FY 2019 NIBRS trainings are scheduled for the following states/agencies:

<u>May 2019</u>

- 6-7 Savannah, GA
- 9-10 Augusta, GA
- 13-14 Calhoun, GA
- 16-17 Conyers, GA
- 13-14 Loveland, OH
- 15-16 Fairview, OH

<u>June 2019</u>

- 18-19 Clarksburg, WV (CJIS)
- 24-25 Oxford, MS
- 27-28 Long Beach, MS
- 24-25 Michigan City, IN
- 27-28 French Lick, IN

July 2019

- 16-18 Guam
- 11-12 Orlando, FL
- 15-16 Boca Raton, FL
- 18-19 Sarasota, FL
- 22-23 Tallahassee, FL
- 25-26 Jacksonville, FL

August 2019

- 5-6 Kennewick, WA
- 8-9 Seattle, WA
- 20-21 Clarksburg, WV (CJIS)
- 26-27 St. Louis, MO
- 29-30 Kansas City, MO

September 2019

- 16-17 Cambridge, MD
- 18-19 Anne Arundel Co, MD
- 23-24 Baltimore Co, MD
- 25-26 Hagerstown, MD
- 23-24 Wells, ME
- 26-27 Hampden, ME

Besides training, more information about NIBRS is available within computer-based modules via the LEEP, or on digital versatile disk upon request at <ucrtrainers@leo.gov>. The 14 tutorials are as follows:

- MODULE 1, Introduction to NIBRS
- MODULE 2, The Benefits of NIBRS
- MODULE 3, The Rules of NIBRS
- MODULE 4, Crimes Against Persons
- MODULE 5, Crimes Against Property 1
- MODULE 6, Crimes Against Property 2
- MODULE 7, Crimes Against Society
- MODULE 8, Group B Offenses
- MODULE 9, Administrative Segment
- MODULE 10, Offense Segment
- MODULE 11, Property Segment
- MODULE 12, Victim Segment
- MODULE 13, Offender Segment
- MODULE 14, Arrestee Segment

With these marketing tools, the FBI continues to urge all local, state, tribal, federal, and other agencies who have not yet started preparing for the implementation of NIBRS, to make a commitment in 2019.

Stakeholder Engagement

Direct engagement with stakeholders continues to be the primary activity of the FBI's goal for the nationwide transition to NIBRS. With more than 18,000 stakeholders, engagement activities throughout 2019 continue to focus on local, state, tribal and federal law enforcement agencies for increased communication about NIBRS transition. Moreover, the outreach follows a tiered approach, which leverages previous engagements, as well as engagement with state UCR Program Managers, CSOs, peer groups, and the Special Agent in Charge at specific FBI Field Offices.

Stakeholder Engagement: State and Local Agencies

The FBI's communication with the CSOs and the state UCR Program Managers has given states more opportunities to ask questions about the NIBRS transition, request resources, and share concerns, challenges, and lessons learned. It has also been the primary method for the states to provide status updates of agencies' efforts to transition. As a result, the FBI has been able to more accurately track commitments and gauge how many agencies plan to transition to NIBRS by 2021, as requested by the APB in the aforementioned 2015 motion.

Additionally, the NIBRS Transition Task Force continues to support the FBI's engagement activities. These representatives from the law enforcement community met again via teleconference on February 11, 2019, and have provided outstanding stakeholder support by serving as advocates, sharing the importance and benefits of transitioning to NIBRS, and focusing on making agencies and associations aware of the NIBRS transition date.

Stakeholder Engagement: Federal Agencies

The FBI continues to encourage NIBRS participation by seeking commitments from federal agencies. For those federal agencies committed, the FBI provides assistance with planning and implementation, where necessary, to bridge existing technical gaps. The FBI is developing a NIBRS Reporting Application, which will provide agencies a mechanism for submitting NIBRS data to the FBI's UCR Program.

Stakeholder Engagement: Tribal Agencies

The FBI's NIBRS transition efforts also focused on engagement with tribal law enforcement agencies. Tribal engagement activities in 2019 and 2020, will consist of continued work with the Department of Interior and the Bureau of India Affairs on a solution for tribal agencies to report NIBRS data. Going forward, the plan is to allow tribal agencies to submit through the state programs. If a tribal agency is unable or unwilling to submit via a state program, the FBI is working to allow tribal agencies to utilize the NIBRS Reporting Application.

Stakeholder Engagement: **Higher Education Law Enforcement**

The FBI continues to work with the Department of Education (ED) and university law enforcement associations to promote NIBRS transition through informational articles and briefings. The ED has agreed to work with the FBI as opportunities to change definitions used in the Clery Act become available. The ED has also suggested use of a “Dear Colleague” letter to engage higher education institutions about NIBRS for their respective campus law enforcement agencies to transition from SRS to NIBRS.

Challenges

Throughout the engagement activities, law enforcement agencies have shared challenges and learning experiences with the NIBRS transition. As expected, the biggest obstacles are resources and funding for making the necessary technical changes to records management systems to transition from SRS to NIBRS. Additionally, some law enforcement agencies have training challenges. Other states lack the necessary resources to enable transition for all of the agencies within their state. Overall, many agencies find educating decision makers and the public of how NIBRS data does not increase crime but is a better reflection of the true picture of crime, as a challenge.

Looking Ahead

The FBI remains steadfast in transition efforts and encourages all agencies to study the benefits of NIBRS data. Having more accurate and meaningful crime statistics to help improve policing and community safety is a common goal.

The transition to NIBRS will allow the FBI and its contributing agencies to have a data collection capable of identifying and addressing evolving crime issues, gaining context at the national level, and providing facts to inform perception and planning.

The FBI’s UCR Program continues to assist agencies in achieving transition to NIBRS. FBI resources are available without charge and include programmatic and technical support, NIBRS training, outreach, and subject matter expertise. Contact the FBI’s UCR Program Office for information or assistance as follows:

• NIBRS Website:	<https://www.fbi.gov/services/cjis/ucr/nibrs>
• NIBRS E-mail address:	<UCR-NIBRS@fbi.gov>
• NIBRS Contact:	304-625-9999
• NIBRS Training:	ucrtrainers@leo.gov

<u>FALL 2019 WORKING GROUP ACTIONS</u>

This topic was accepted as information only by all five working groups.

<u>FALL 2019 UCR SUBCOMMITTEE ACTION:</u>

Accepted as information only.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA

STAFF PAPER

APB ITEM #18

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

SA ISSUE #1*
Action Item Review
FBI Action Item: The ISO Program Office accepted an action item to obtain the FBI's interpretation of the changes made to *CJIS Security Policy*, Section 4.1 regarding the protection of CJI indirectly released into open judicial proceedings. Specifically, the ISO Program will clarify the timeframe in which CJI remains under the protection of the courts after adjudication.

SA ISSUE #2*
Task Force Update

SA ISSUE #3
Mobile Device Management Requirements in the *CJIS Security Policy*

SA ISSUE #4
CJIS Security Policy Advanced Password Standards

SA ISSUE #5*
CJIS Cloud Implementation

SA ISSUE #6*
Clarifying *CJIS Security Policy* Language

SA ISSUE #7
Audit of Vendor Contracts with Authorized Criminal Justice Agencies

SA ISSUE #8*
Information Security Officer Training Symposium Review

SA ISSUE #9*
Risk Based Information Assurance

SA ISSUE #10* **(see APB Item #2, NCIC Issue #2 for staff paper)**
Law Enforcement Enterprise Portal Status Report

Ad Hoc Issues*
1. National Association of State Chief Information Officers (NASCIO)

*No staff paper

Intentionally Left Blank

CJIS ADVISORY POLICY BOARD (APB)
SECURITY AND ACCESS (SA) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

SA ISSUE #3

Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*

PURPOSE

To demonstrate consistency with other CJIS Security Policy requirements placing responsibility for compliance with the MDM requirement with the user agency.

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 options outlined in this topic paper.

BACKGROUND

The FBI CJIS Designated Federal Officer (DFO) received an external topic request form concerning the responsibility of ensuring compliance with the current MDM requirement when directly accessing criminal justice information (CJI). The requestor believes the requirement, as written, places the onus of compliance on the service provider allowing direct access to CJI. Additionally, the requestor believes this is inconsistent with other requirements which place the responsibility for compliance with the user agency. The topic was assigned to the FBI CJIS Information Security Officer (ISO) for staffing and presentation of the topic paper.

While briefing the topic to the Security and Access (SA) Subcommittee during the Spring 2019 APB Subcommittee meetings, the FBI CJIS ISO staff pointed out the current MDM requirements and that the *CJIS Security Policy* (Policy) clearly states that "…agencies shall implement the following controls when allowing CJI access from devices running a limited-feature operating system:". This does not infer the responsibility lies with the service provider but rather the user's agency allowing the access to information from the service provider. The FBI CJIS IT Audit staff confirmed the current audit questionnaire validates compliance at the agency level rather than the service provider and that they interpret the Policy, as written, puts the responsibility for an MDM on the agency providing the access point. Therefore if the user agency allows direct access to CJI from an agency controlled device, regardless of the source of the information accessed (local agency or a service provider), the agency is responsible to enforce the MDM requirement(s).

Further discussion amongst the subcommittee brought to light if CJI is directly accessed through internet-based means, there should be additional security controls or considerations in-place that are not currently found in the Policy. The subcommittee's consensus was that policy modernization is needed and that new requirement options to be considered should include containerization, application virtualization, and secure web servers.

The ISO Program Office agreed to prepare a topic paper for the Fall 2019 Working Groups.

DISCUSSION AND ANALYSIS

As pointed out during discussion at the most recent SA Subcommittee meeting, the MDM requirement as found in Section 5.13.2 clearly places the responsibility for compliance with the agency allowing access to CJI. Furthermore, the FBI CJIS Audit IT staff concurred and stated their audit questionnaire validates compliance against the agency and not the service provider.

Although the CJIS Security Policy is clear on the responsibility for the MDM requirement, there is room for improvement concerning the security of CJI for internet and application-based access. The SA Subcommittee has supported a policy modernization effort and new requirements in this area can be addressed during that process.

OPTIONS

1. Change the *CJIS Security Policy* as indicated (deletions in ~~**bold strikethrough**~~ and additions in ***red bold italics***):

5.13.2 Mobile Device Management
User ~~**A**~~***a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** ~~**allowing**~~ CJI access from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

2. Make no changes to the *CJIS Security Policy*

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

RECOMMENDATION

The CJIS ISO Program Office recommends Option 1.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1: Change the *CJIS Security Policy* as indicated (deletions in ~~**bold strikethrough**~~ and additions in ***red bold italics***):

5.13.2 Mobile Device Management
User ~~**A**~~***a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** ~~**allowing**~~ CJI ~~**access**~~ from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 1: Change the *CJIS Security Policy* as indicated (deletions in ~~**bold strikethrough**~~ and additions in ***red bold italics***):

5.13.2 Mobile Device Management
User ~~**A**~~***a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** ~~**allowing**~~ CJI ~~**access**~~ from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Change the *CJIS Security Policy* as indicated (deletions in ~~**bold strikethrough**~~ and additions in ***red bold italics***):

5.13.2 Mobile Device Management
User ~~**A**~~***a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** ~~**allowing**~~ CJI ~~**access**~~ from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Action: Motion carried

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt Option 1: Change the *CJIS Security Policy* as indicated (deletions in **~~bold strikethrough~~** and additions in ***red bold italics***):

5.13.2 Mobile Device Management
User **~~A~~*a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** **~~allowing~~** CJI **~~access~~** from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Action: Motion carried

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 1: Change the *CJIS Security Policy* as indicated (deletions in
~~bold strikethrough~~ and additions in ***red bold italics***):

5.13.2 Mobile Device Management
User **~~A~~*a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** **~~allowing~~** CJI **~~access~~** from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Action: Motion carried

FALL 2019 SA SUBCOMMITTEE ACTION:

Motion: To accept Option 3:
5.13.2 Mobile Device Management

User **~~A~~*a***gencies shall implement the following controls when ***directly accessing*** **~~allowing~~** CJI **~~access~~** from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Action: Motion carried with a vote of 7 yay and 2 nay

CJIS ADVISORY POLICY BOARD (APB)
SECURITY AND ACCESS (SA) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

SA ISSUE #4

CJIS Security Policy Advanced Password Standards

PURPOSE

Propose modifications to *CJIS Security Policy* Section 5.6.2.1.1.2 to align the *Advanced Password Standards* with National Institute of Standards and Technology (NIST) 800-63B.

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 options outlined in this topic paper.

BACKGROUND

The latest version of NIST SP 800-63 was released in June 2017. Following the release of these new password guidelines, the FBI CJIS APB Designated Federal Officer (DFO) received external topic paper submissions requesting the *CJIS Security Policy* adopt the new NIST SP 800-63B requirements for *Memorized Secrets* (i.e., passwords) and modify *CJIS Security Policy* Section 5.6.2.1.1 to reflect the new requirements. In the fall of 2018, the CJIS APB approved *CJIS Security Policy* Section 5.6.2.1.1.2 *Advanced Password Standards*, but made modifications to the length and expiration of passwords. This topic paper seeks to align the length and expiration of passwords back to the NIST recommended values.

DISCUSSION AND ANALYSIS

Currently, the *CJIS Security Policy*, Section 5.6.2.1.1.2 *Advanced Password Standards* states that agencies adopting the new password requirements shall have passwords that are “a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).” Additionally, 5.6.2.1.1.7 requires verifiers to “force a password change if there is evidence of authenticator compromise or every 365 days from the last password change." These variants of the NIST policy were introduced by the Fall 2018 APB Security Access Subcommittee; however, in doing so, the Security Access Subcommittee made the *CJIS Security Policy* more stringent than national information assurance requirements. The modification for a minimum of twenty (20) character password was created because a member of the committee "could not think of an eight character passphrase." These modifications were also discussed during the discussion and voting on adding advanced password standards to the *CJIS Security Policy*, but the motion passed as the topic was written (i.e., minimum twenty characters and 365 day expiration).

Another shall statement included in the newest version of the CJIS Security Policy is the maintenance of a banned password list. NIST recommends that passwords "obtained from previous breach corpuses" should not be used and the service should "advise the subscriber that they need to select a different secret". Discussions with NIST Security Engineers revealed a NIST-recommended website with a listing of passwords from "previous breach[ed] corpuses. Another NIST recommendation is that agencies maintain a list of around one thousand (1,000) passwords within a local repository. To this end, it is recommended the current requirements be modified and aligned with the original NIST recommended requirements.

With regard to the expiration of the password, the recommendation states "[agencies] MAY issue authenticators that expire. If and when an authenticator expires, it SHALL NOT be usable for authentication. When an authentication is attempted using an expired authenticator, the [agency] SHOULD give an indication to the subscriber that the authentication failure is due to expiration rather than some other cause." The *CJIS Security Policy* states in 5.6.2.1.1.2 (7), "Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change." While non-expiring passwords were ultimately not selected, the decision made by the Security Access Subcommittee lessens the burden on users while maintaining an acceptable risk appetite.

OPTIONS

1. Modify the *CJIS Security Policy* as follows:

> 5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~**twenty (20)**~~ *eight (8)* characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
>
> 5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:
>
> 1. Passwords obtained from previous breach corpuses
>   - **a.** ***Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.***
> 2. Dictionary words
> 3. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')

4. Context-specific words, such as the name of the service, the username, and derivatives thereof

2. Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~**twenty (20)**~~ ***eight (8)*** characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses
    a. ***Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.****
2. Dictionary words
3. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
4. Context-specific words, such as the name of the service, the username, and derivatives thereof

5.6.2.1.1.2 (4): When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list. ***Agencies shall reconcile their directory service against the "banned password" list at least every 90 days. If a "banned password" is discovered, the Agency shall notify affected user to execute a password change***.

5.6.2.1.1.2 (7): Verifiers shall force a password change if there is evidence of authenticator compromise. ~~**or every 365 days from the last password change**~~

3. Make no changes to the *CJIS Security Policy*

Please note, this staff paper was updated for the SA Subcommittee meeting, "or the latest version" in bullet 1a was left off in Option 2 of the topic paper sent to working group members.

RECOMMENDATION

The CJIS ISO Program Office recommends Option 2.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 2: Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~**twenty (20)**~~ *eight (8)* characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses

   a. Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.

2. Dictionary words
3. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
4. Context-specific words, such as the name of the service, the username, and derivatives thereof

5.6.2.1.1.2 (4): When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list. ***Agencies shall reconcile their directory service against the "banned password" list at least every 90 days. If a "banned password" is discovered, the Agency shall notify affected user to execute a password change***.

5.6.2.1.1.2 (7): Verifiers shall force a password change if there is evidence of authenticator compromise.~~**or every 365 days from the last password change**.~~

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion: To accept Option 2: Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~**twenty (20)**~~ *eight (8)* characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses
   - ***a. Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.***
2. Dictionary words
3. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
4. Context-specific words, such as the name of the service, the username, and derivatives thereof

5.6.2.1.1.2 (4): When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list. ***Agencies shall reconcile their directory service against the "banned password" list at least every 90 days. If a "banned password" is discovered, the Agency shall notify affected user to execute a password change***.

5.6.2.1.1.2 (7): Verifiers shall force a password change if there is evidence of authenticator compromise. ~~**or every 365 days from the last password change**~~

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 2: Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~**twenty (20)**~~ ***eight (8)*** characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses
   - ***a. Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.***
2. Dictionary words
3. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
4. Context-specific words, such as the name of the service, the username, and derivatives thereof

5.6.2.1.1.2 (4): When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list. ***Agencies shall reconcile their directory service against the "banned password" list at least every 90 days. If a "banned password" is***

discovered, the Agency shall notify affected user to execute a password change.

5.6.2.1.1.2 (7): Verifiers shall force a password change if there is evidence of authenticator compromise. ~~**or every 365 days from the last password change**~~

Action: Motion carried

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt revised Option 2: Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~**twenty (20)**~~ ***eight (8)*** characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses
    a. ***Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.***
2. Dictionary words
3. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
4. Context-specific words, such as the name of the service, the username, and derivatives thereof

5.6.2.1.1.2 (4): When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list. ***Agencies shall reconcile their ~~directory service~~ passwords against the "banned password" list at least every 90 days. If a "banned password" is discovered, the Agency shall notify affected user to execute a password change***.

5.6.2.1.1.2 (7): Verifiers shall force a password change if there is evidence of authenticator compromise. ~~or every 365 days from the last password change.~~

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion: To accept Option 3: Make no changes to the *CJIS Security Policy.*

Action: Motion carried.

FALL 2019 SA SUBCOMMITTEE ACTION:

Motion: To accept Option 3: Make no changes to the *CJIS Security Policy*

Action: Motion carried.

CJIS ADVISORY POLICY BOARD (APB)
SECURITY AND ACCESS (SA) SUBCOMMITTEE
NORFOLK, VA
OCTOBER 9, 2019

STAFF PAPER

SA ISSUE #7

Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs)

PURPOSE

To inform the Subcommittees of the Criminal Justice Information Services (CJIS) Division's plan to include vendor contracts as part of the Criminal Justice Information Technology Security (ITS) audit.

POINT OF CONTACT

Resources Management Section, CJIS Audit Unit (CAU).

Questions regarding this topic should be directed to <agmu@leo.gov>

BACKGROUND

The FBI CJIS Designated Federal Officer (DFO) received an external topic request from the Colorado Bureau of Investigation (CBI) requesting that the CAU review vendor contracts for appropriate *CJIS Security Policy* language during the ITS audit.

During an ITS audit, the CAU requests a signed CJIS Security Addendum for each unescorted contractor performing a criminal justice function on behalf of an authorized CJA. Although the CAU requests the signed certificate page of the CJIS Security Addendum, a copy of the contract initiated between the CJA and the vendor providing criminal justice services has not been requested to verify the incorporation of the CJIS Security Addendum or the *CJIS Security Policy*. The CBI is asking that the CAU request a current agreement between the CJA and all private contractors to ensure the protection of the CJA if a noncompliance issue is found.

During the process of creating a statewide CJIS vendor program, CBI discovered many large national corporations providing CJIS services nationwide could not produce a single contract with any customer (nationwide) that mentioned the CJIS Security Addendum or the *CJIS Security Policy*. The argument the CBI is presenting is that when an issue of noncompliance is found, the CJA does not have the ability to resolve the issue because the original agreement does not include mention of the *CJIS Security Policy* nor includes the CJIS Security Addendum and therefore, the vendor is not bound to meet compliance requirements. In order to resolve audit findings, this often means additional costs that exceed resources available to the local CJA.

Because the CAU does not look at private contractor agreements as part of the ITS audit, the requirement is left to each CJIS Systems Agency (CSA) to ensure appropriate language is included within the agreements enacted by local CJAs within their jurisdiction. The CBI feels that if included in the FBI ITS audit, the requirement would be taken more seriously by CJIS industry partners and would increase the credibility of state auditors seeking to ensure this *CJIS Security Policy* requirements is met.

DISCUSSION AND ANALYSIS

The *CJIS Security Policy* states in Section 5.1.1.5, “All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.” The Section goes on to say, “Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to criminal justice information (CJI). Access shall be permitted pursuant to an agreement which specifically identifies the agency’s purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).”

The CJIS Security Addendum further clarifies its purpose by stating “The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the *CJIS Security Policy* in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).” When the CJIS Security Addendum is incorporated into the private contractor agreement, it then ties the private contractor to abide the *CJIS Security Policy*.

The CAU already reviews all other agreements during the ITS audit (including: user agreements [CSA to Local CJA], information exchange agreements [CJA to CJA], and management control agreements [CJA to Noncriminal Justice Governmental Agency]), and therefore, has agreed to add the already existing requirement to the current ITS audit. The CAU will assess that an agreement is in place between the CJA and private contractor that stipulates the purpose and scope of the criminal justice services provided. Because the *CJIS Security Policy* does not provide additional details for “purpose and scope of providing services”, the CAU will only review that a purpose and scope exists within the agreement (e.g. if the agreement says, “shredding CJI” but the contractor is also “storing CJI”, the CAU will advise, but will not mark as out of compliance). The CAU will also assess the incorporation of the CJIS Security Addendum (which stipulates adherence to the *CJIS Security Policy*).

Both the CAU and the CBI have acknowledged that the inclusion of the agreement requirement within the ITS audit will not necessarily resolve the issue of noncompliance between a CJA and its private contractor. Rather, both parties feel that the inclusion will bring focus to the agreement and needed language to not only encourage the private contractor community to ensure their contracts (i.e. products) meet CJIS standards, but also encourage CJAs to include the necessary language to protect their interest for compliance (i.e. save the community money in trying to fix contractual gaps for compliance).

This topic was presented as an Ad Hoc Topic at the Security and Access Subcommittee meeting in Spring 2019. The Subcommittee suggested a zero-cycle for the requirement and an addition to the Appendix with a sample agreement. Traditionally, the CAU does not afford a zero-cycle for a long-standing requirement. A zero-cycle policy is not considered sanctionable (i.e. will not result in a state-wide recommendation during the audit or be presented to the APB's Compliance Evaluation Subcommittee) for the first full fiscal year, and is assessed as informational during this period. If this option is accepted, the requirement for vendor contracts will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.

CAU audit documents (i.e. preaudit questionnaires, questionnaires, policy assessments packets, cheats, policy samples, etc.) are available upon request to any CSA or authorized CJA via email at <cjisaudit@fbi.gov>.

The *CJIS Security Policy* previously included a sample contract addendum for CJAs to use to incorporate the CJIS Security Addendum into their existing contract language. The same language has been provided (Attachment 1) and could be re-added to Appendix H, if requested.

<u>OPTIONS</u>

Option 1: Approve the following:

> 1A: CAU will evaluate the existing contractor agreement requirements as "new policy". (If this option is accepted, the requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)
>
> 1B: CAU will evaluate the existing vendor agreement requirements as existing requirements.

Option 2: Approve the following:

> 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.
>
> 2B: CAU will provide Attachment 1 as requested, but make no changes to the *CJIS Security Policy*.

<u>RECOMMENDATION</u>

The CJIS Division would recommend options 1B and 2A, since this has been an existing requirement since approximately 2002 and would better address the issue identified in the paper request.

FALL 2019 WORKING GROUP ACTIONS:

FEDERAL WORKING GROUP ACTION:

Motion: To accept Option 1A: CAU will evaluate the existing contractor agreement requirements as "new policy". (If this option is accepted, the requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)

Action: Motion carried.

Motion: To accept Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Action: Motion carried.

NORTH CENTRAL WORKING GROUP ACTION:

Motion 1: To accept Option 1B: CAU will evaluate the existing vendor agreement requirements as existing requirements.

Action: Motion carried.

Motion 2: To accept Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Action: Motion carried.

NORTHEASTERN WORKING GROUP ACTION:

Motion: To adopt Option 1B: CAU will evaluate the existing vendor agreement requirements as existing requirements.

Action: Motion carried.

Motion: To adopt Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: To adopt Option 1A: CAU will evaluate the existing contractor agreement requirements as "new policy". (If this option is accepted, the requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)

Action: Motion carried.

Motion: To adopt Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Action: Motion carried.

WESTERN WORKING GROUP ACTION:

Motion 1: To accept Option 1B: CAU will evaluate the existing vendor agreement requirements as existing requirements.

Action: Motion carried.

Motion 2: To accept Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Action: Motion carried.

FALL 2019 SA SUBCOMMITTEE ACTION:

Motion: To accept Option 1A: CAU will evaluate the existing contractor agreement requirements as “new policy”. (If this option is accepted, the requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)

Action: Motion carried.

Motion: To accept Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

Action: Motion carried.

Attachment 1

AMENDMENT NO. ___ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2](), upon notification and pursuant to Paragraph/Section No. ___ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "___"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

a.
b.
c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _________, 201_.

On behalf of [Party No. 1]: ________________________________
[Name]

____
[Title]

____
Date

On behalf of [Party No. 2]: ________________________________
[Name]

____
[Title]

CJIS ADVISORY PROCESS REQUEST FOR TOPIC

Please provide the following information when submitting a request for a topic paper.

1. Clear statement of request:

The Colorado Bureau of Investigation requests the CJIS Audit Unit (CAU) review vendor contracts for appropriate CJIS Security Policy language during Information Technology Security Audits (ITSA).

2. How this is handled now (or description of problem being solved):

Auditors will request CJIS Security Addendum Certifications, however, that certification does not protect the CGA if a noncompliance issue is found. For instance, an agency can contract for Records Management System (RMS) Software, but not realize the vendor contracts with a non-CJIS compliant cloud provider for storage. When the issue is discovered, the agency has no capacity to resolve the issue because the original vendor was not contractually bound to follow the CJIS Security Policy. The security issues cannot be addressed until the contractual issue is resolved. Because CAU does not look at contracts, the question of appropriate language is left to the CSA to raise and does not show up in the FBI Audit. The CBI has discovered many large national corporations providing CJIS services nationwide that could not produce a single contract with any customer that mentioned the CJIS Security Addendum or CJIS Security Policy. Until CBI started the CJIS vendor program these requests were largely ignored. Now CBI has an immediate sanction directly upon the vendor, but the local agencies still face additional costs and other challenges that exceed their resources.

3. Suggested solution:

When CAU performs an ITSA, request the contract for each vendor the agency works with. Check the contract for the incorporation of the CJIS Security Addendum by reference as mandated in Chapter 5.1.1.5 under numbered items 1 and 2.

4. Scenario/example:

Local Police Department is searching for a new Records Management System (RMS). They decide to go with a large national business with hundreds of clients nationwide. The sales representative believes the business and RMS are CJIS compliant, as they have never heard otherwise. During a state audit, it is discovered that the RMS is hosted using a non-CJIS compliant cloud storage. The State levies a finding and the Police Chief contacts their contractor. The business is incredulous as they've had other customers pass FBI audits with the same contract language. The Police Chief contacts the CSA's Chief Executive questioning the reliability of the auditor's findings. The city attorney reviews the contract and finds the contractor has no obligation to comply with CJIS policy.

5. Benefit(s) to the criminal justice community:

This would increase the credibility of the state auditors. It would also increase the push CJIS industry partners to ensure their contracts meet CJIS standards. Contracting is foundational for CJIS compliance, so this change would proactively facilitate easier resolution of other CJIS audit findings because noncompliance becomes clear contractual breach.

6. Impact on state system users, if known. (Time and resources):

This change could increase the cost of contracting CJIS services as it would expose more compliance issues and clarify contractor’s obligations when subcontracting services; especially expansive IT services such as cloud storage.

7. Importance/criticality:

Important but not critical

8. Suggested Topic Name:

Auditing Contracts for CJIS Compliance

9. Contact person: Ted DeRosa, CJIS Systems Officer

Please provide any additional information that may be helpful to understand the topic.

**CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
DECEMBER 4-5, 2019
ATLANTA, GA**

STAFF PAPER

APB ITEM #20

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

NICS ISSUE #1*
Action Item Review

NICS ISSUE #2** ***(See Informational Topic H for staff paper)***
NICS Enhancements

NICS ISSUE #3** ***(See Informational Topic I for staff paper)***
NICS Operational Update

NICS ISSUE #4 ***(See APB Item #4 for staff paper)***
Race Code Standardization across CJIS Division Systems

NICS ISSUE #5 ***(See APB Item #2, NCIC Issue #9 for staff paper)***
Request to Expand the NCIC Protection Order File Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders

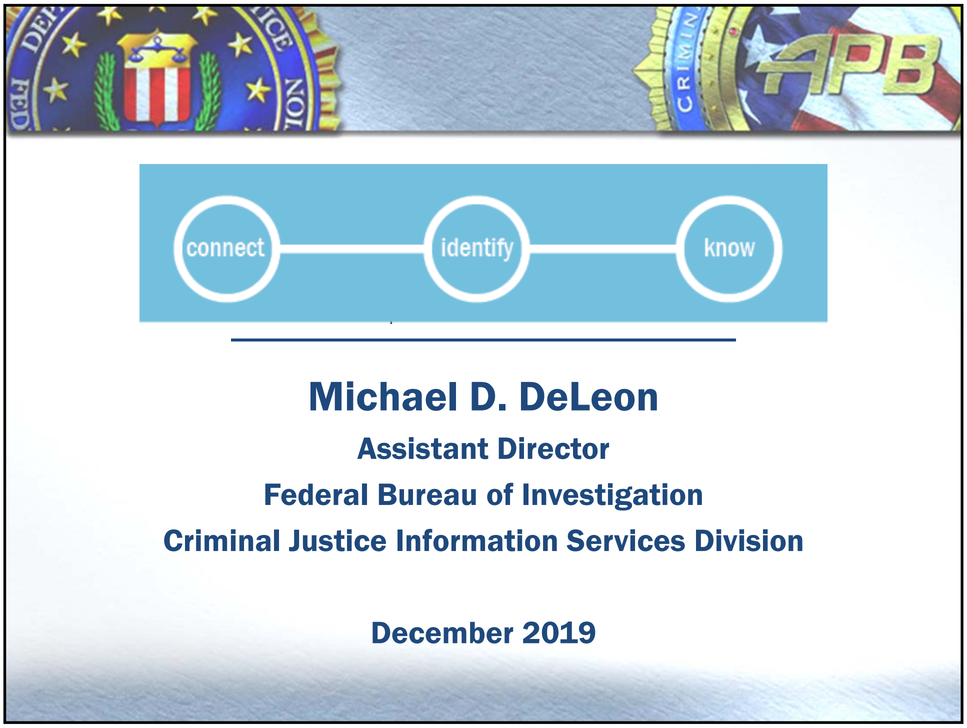
NICS ISSUE #6*
NICS Audit Update

NICS Issue #7 ***(See APB Item #2, NCIC Issue #2 for staff paper)***
Law Enforcement Enterprise Portal Status Report

NICS Issue #8*
Ad Hoc Topics

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

Intentionally Left Blank


connect
identify
know

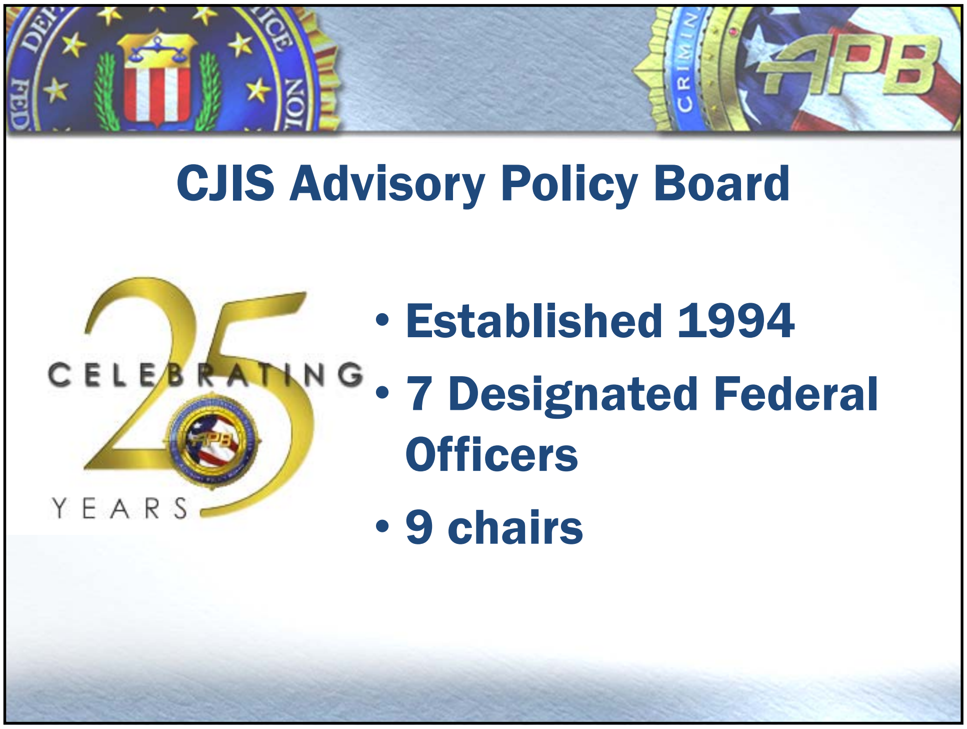
Michael D. DeLeon

Assistant Director

Federal Bureau of Investigation

Criminal Justice Information Services Division

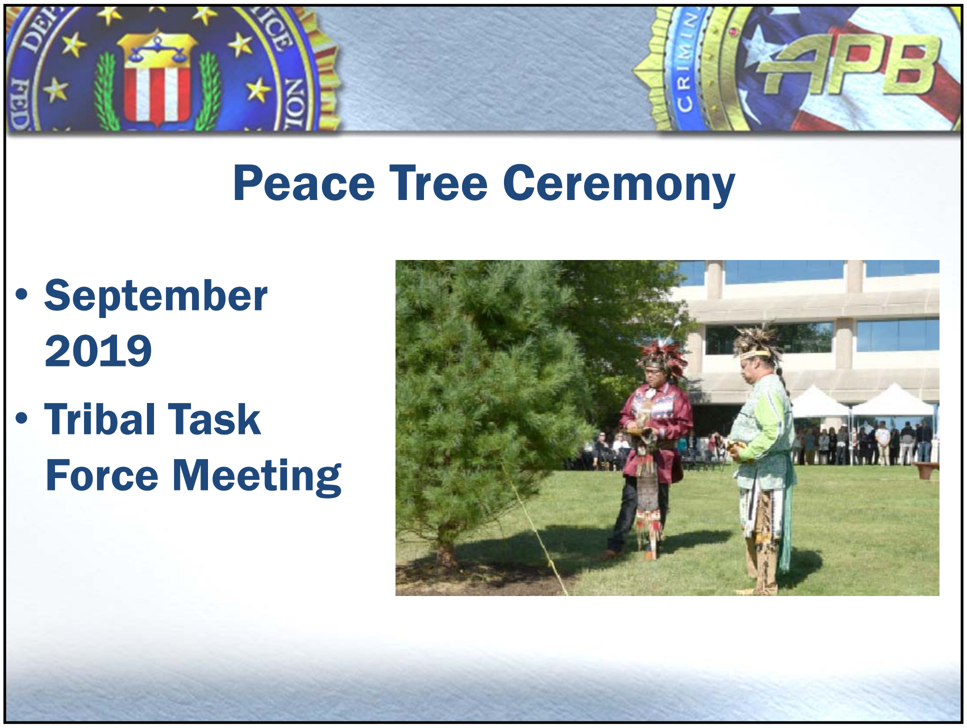
December 2019



CJIS Advisory Policy Board

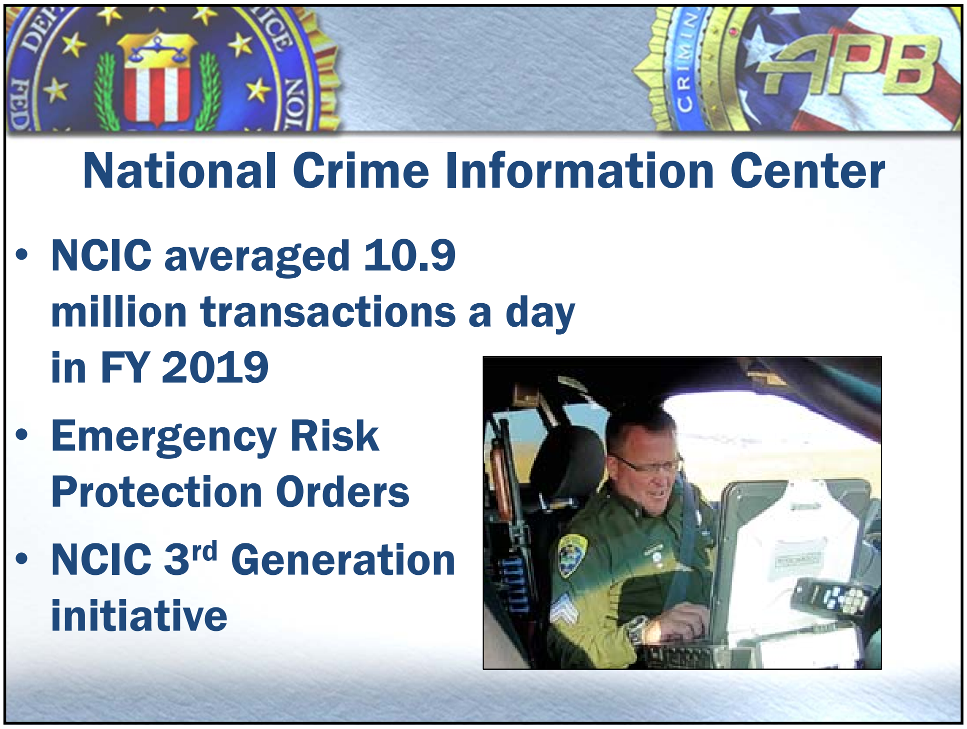
CELEBRATING
25
YEARS

- **Established 1994**
- **7 Designated Federal Officers**
- **9 chairs**



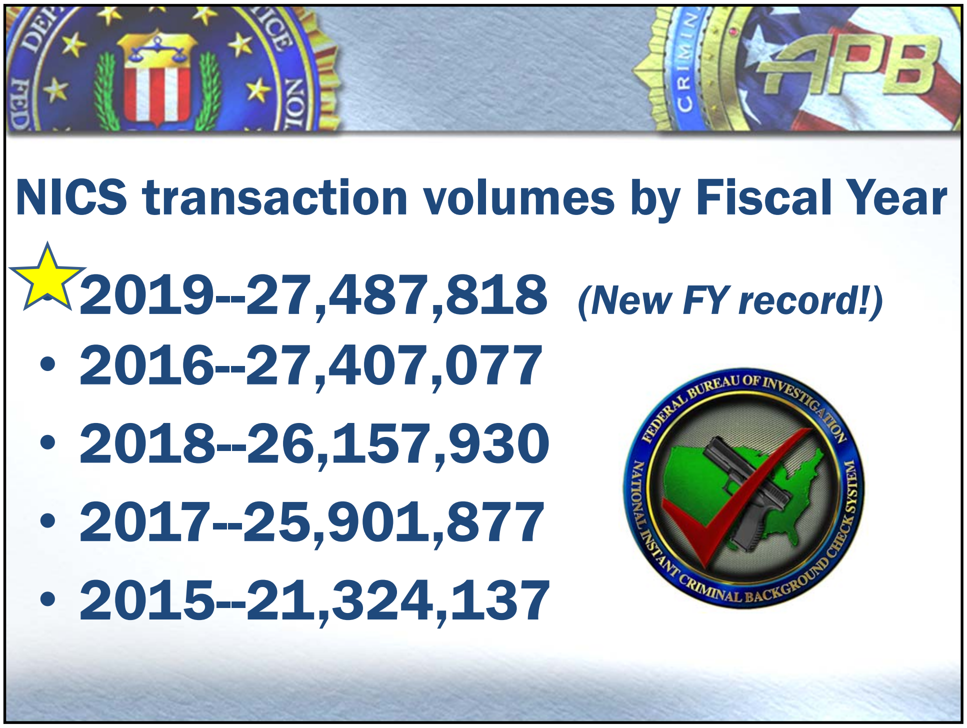
Peace Tree Ceremony

- September 2019
- Tribal Task Force Meeting



National Crime Information Center

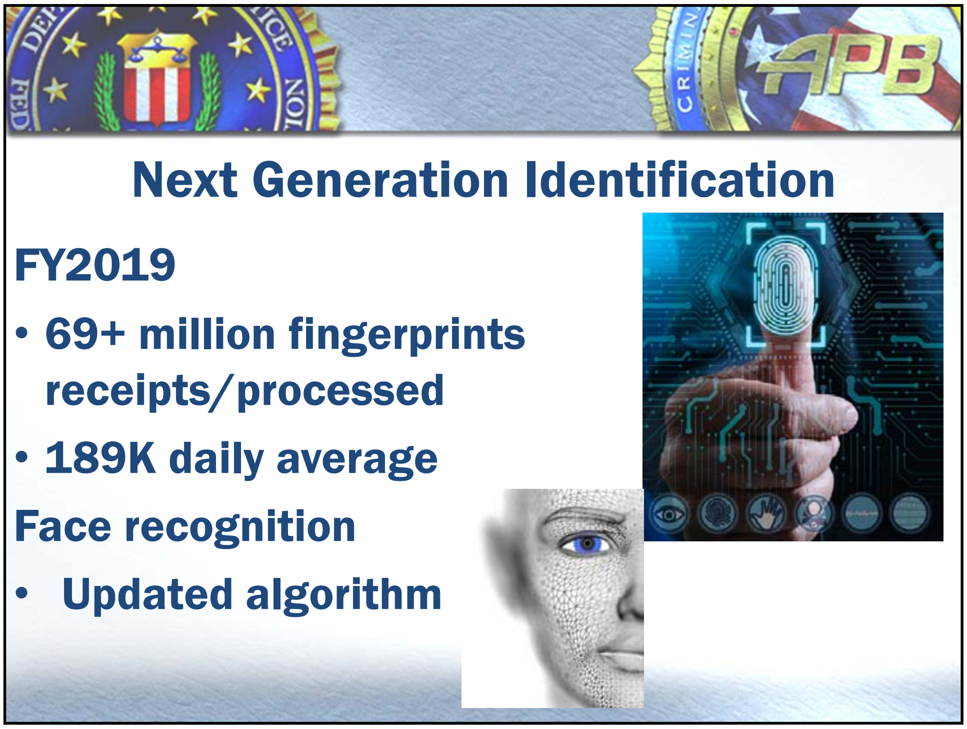
- NCIC averaged 10.9 million transactions a day in FY 2019
- Emergency Risk Protection Orders
- NCIC 3rd Generation initiative



NICS transaction volumes by Fiscal Year

★ 2019--27,487,818 *(New FY record!)*

- 2016--27,407,077
- 2018--26,157,930
- 2017--25,901,877
- 2015--21,324,137



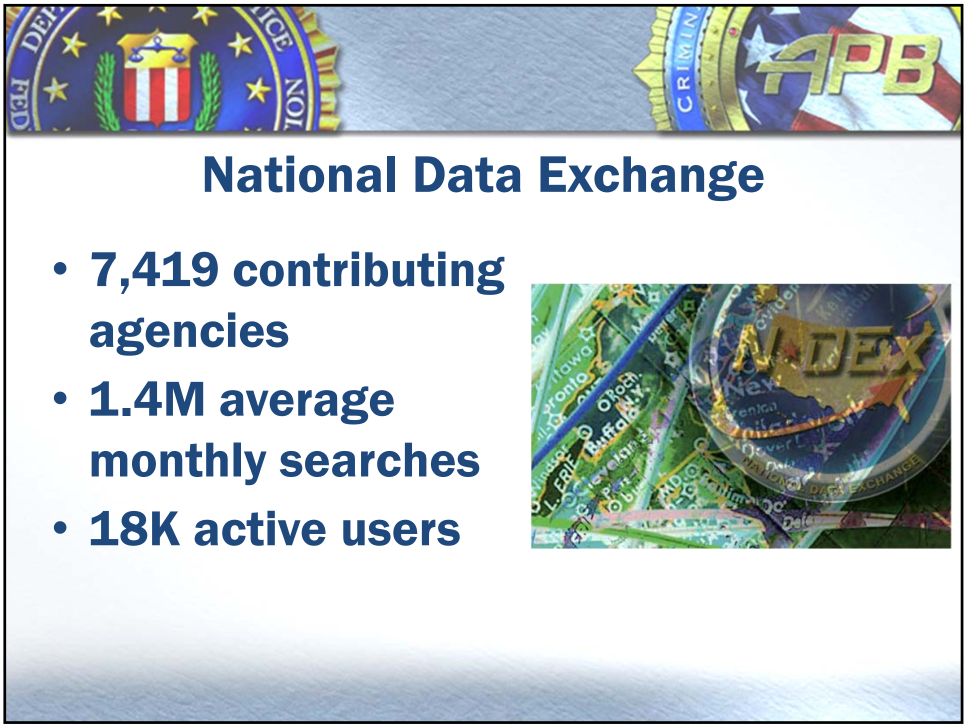
Next Generation Identification

FY2019

- 69+ million fingerprints receipts/processed
- 189K daily average

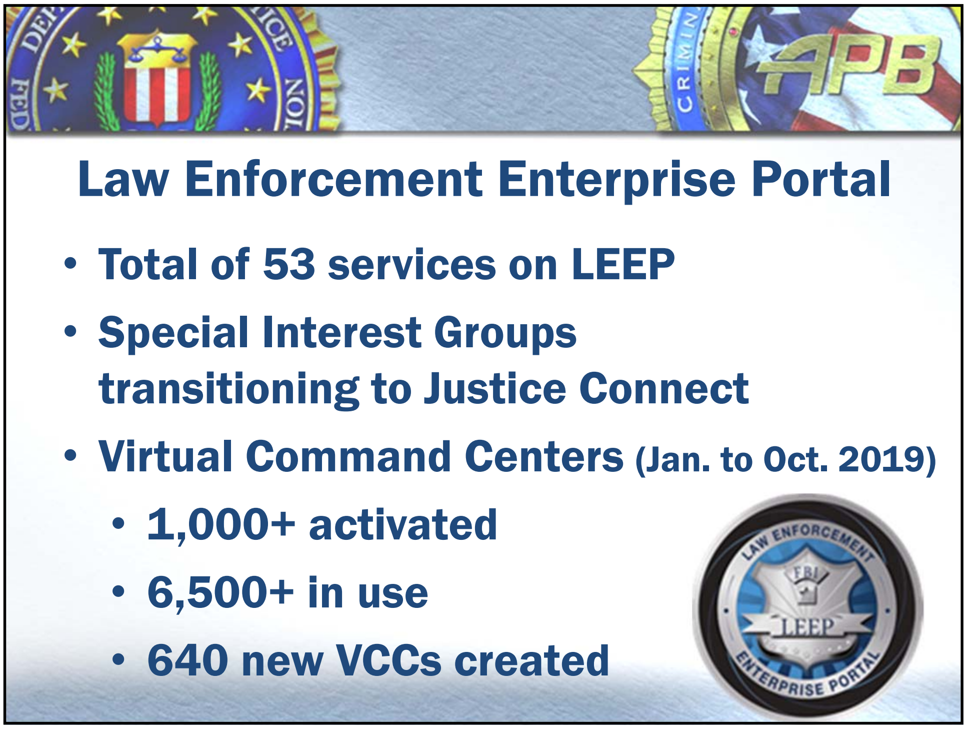
Face recognition

- Updated algorithm



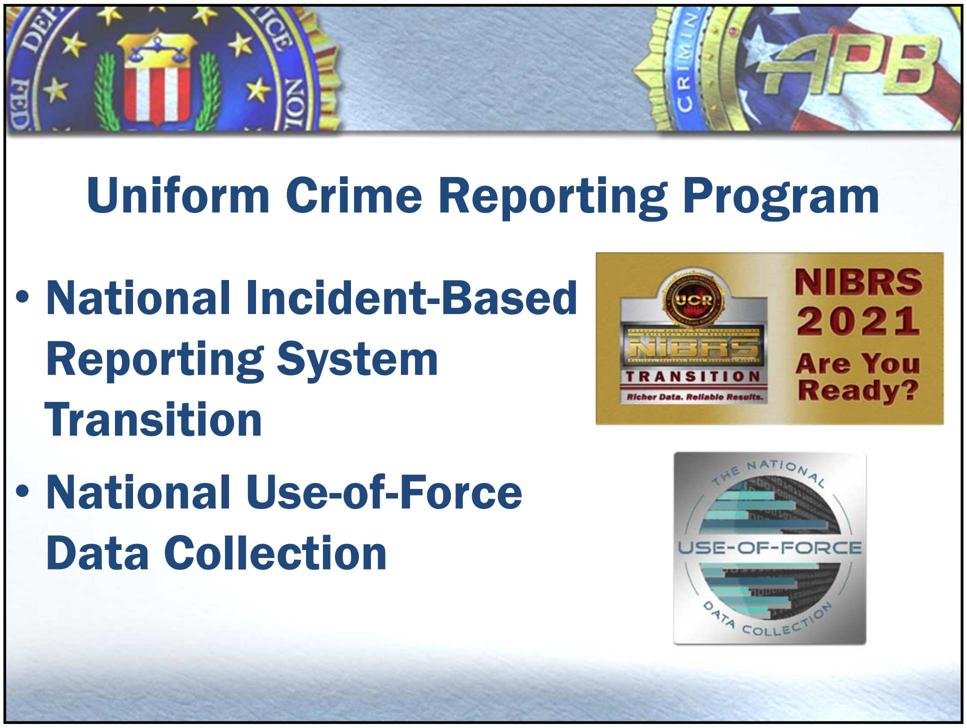
National Data Exchange

- 7,419 contributing agencies
- 1.4M average monthly searches
- 18K active users



Law Enforcement Enterprise Portal

- Total of 53 services on LEEP
- Special Interest Groups transitioning to Justice Connect
- Virtual Command Centers (Jan. to Oct. 2019)
  - 1,000+ activated
  - 6,500+ in use
  - 640 new VCCs created


APB
UCR
NIBRS
TRANSITION
Richer Data. Reliable Results.
NIBRS 2021 Are You Ready?
THE NATIONAL
USE-OF-FORCE
DATA COLLECTION

Uniform Crime Reporting Program

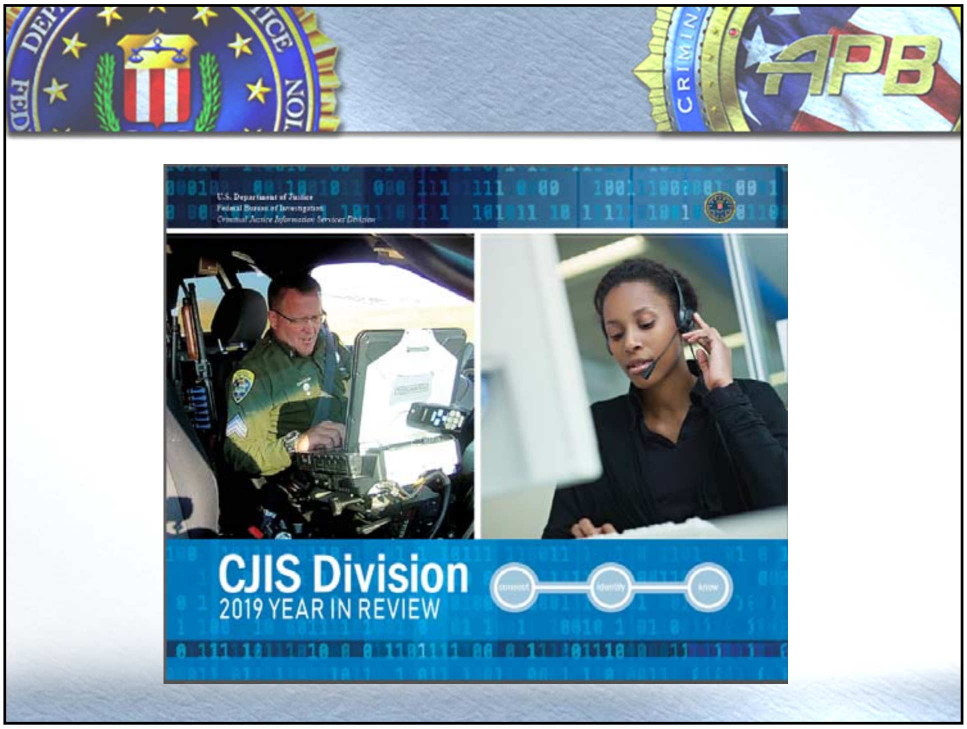
- National Incident-Based Reporting System Transition
- National Use-of-Force Data Collection

National Threat Operations Center

No Average Call

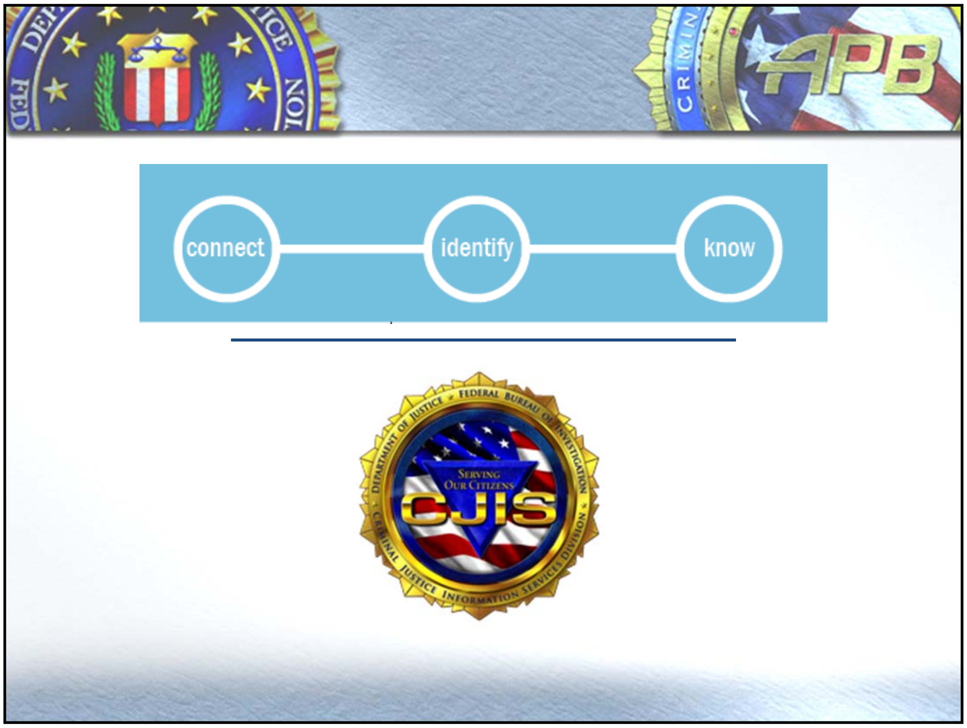
A Look Inside the FBI's National Threat Operations Center

[redacted]



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

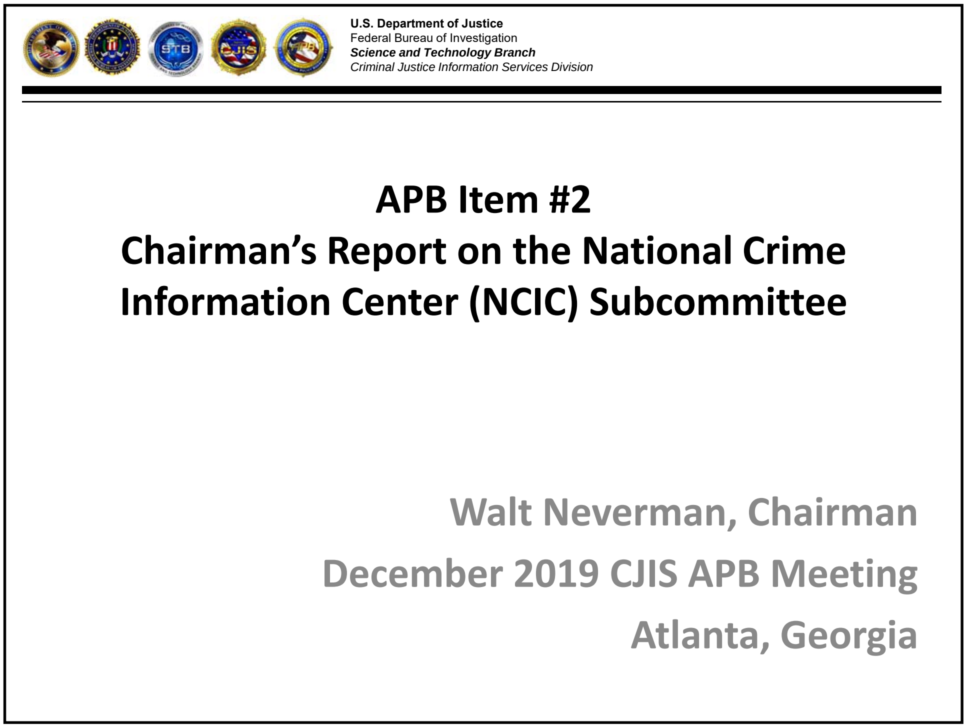
CJIS Division
2019 YEAR IN REVIEW



connect — identify — know

APB
Serving Our Citizens
CJIS
Department of Justice • Federal Bureau of Investigation • Criminal Justice Information Services Division

Intentionally Left Blank



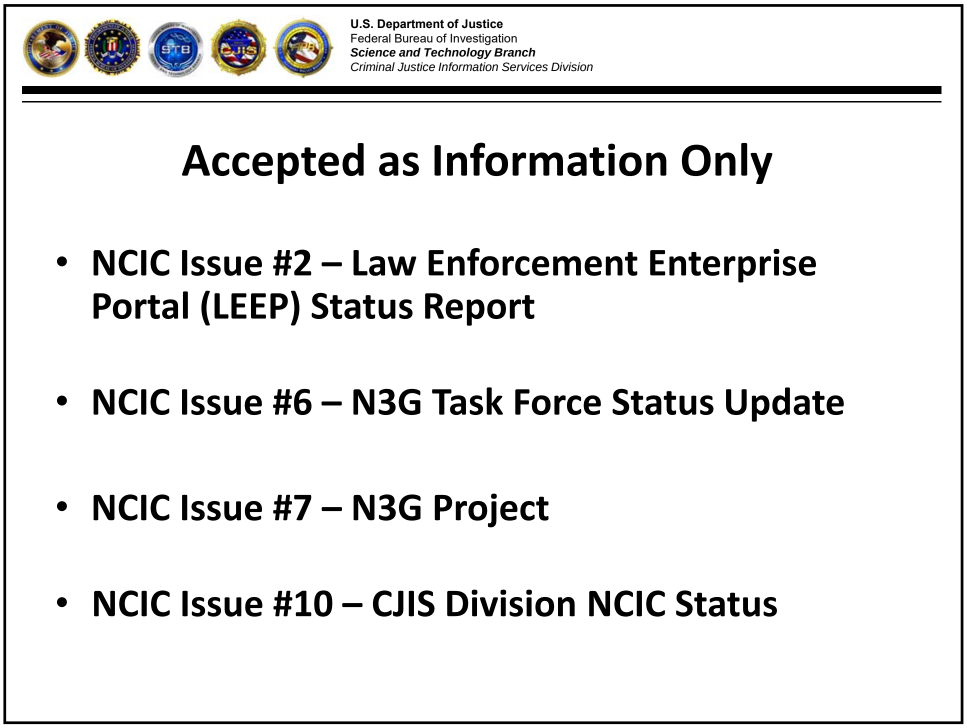
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB Item #2
Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

Walt Neverman, Chairman

December 2019 CJIS APB Meeting

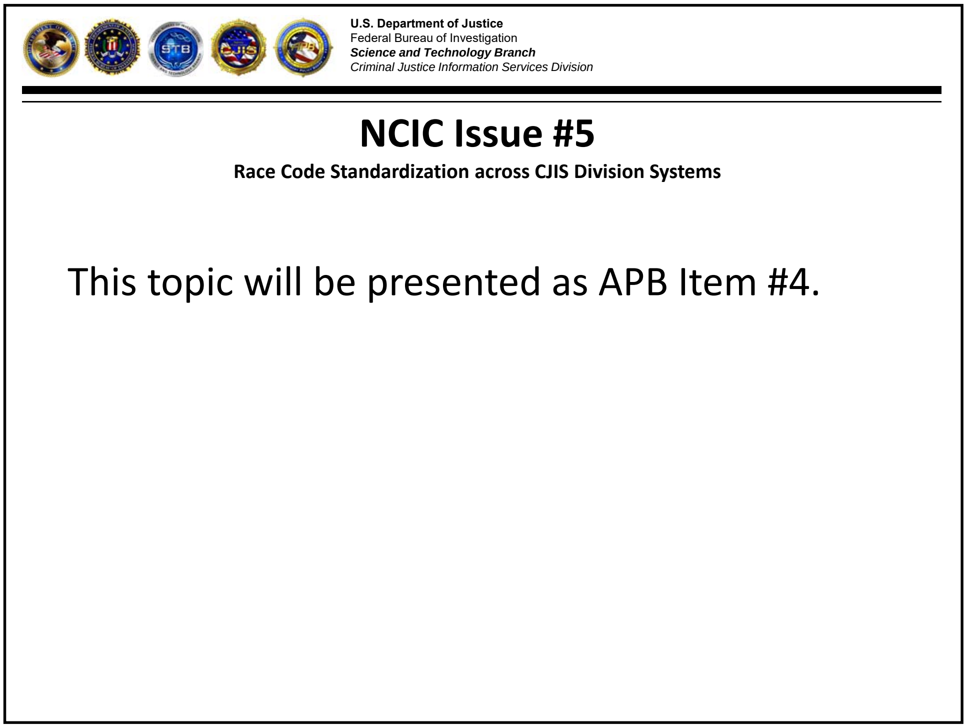
Atlanta, Georgia



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Accepted as Information Only

- NCIC Issue #2 – Law Enforcement Enterprise Portal (LEEP) Status Report
- NCIC Issue #6 – N3G Task Force Status Update
- NCIC Issue #7 – N3G Project
- NCIC Issue #10 – CJIS Division NCIC Status

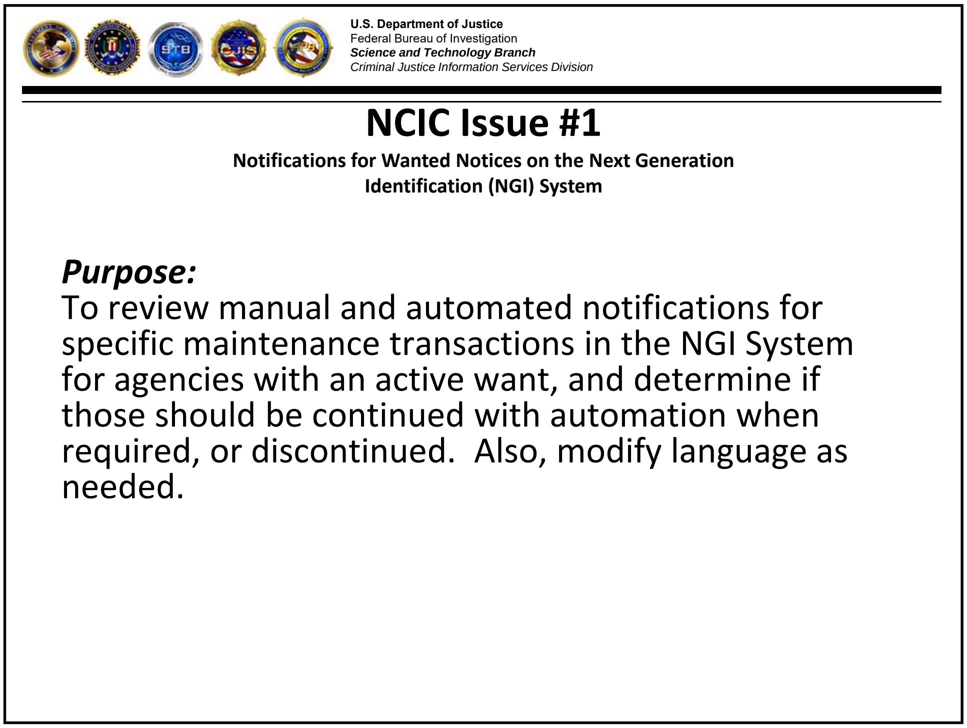


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #5

Race Code Standardization across CJIS Division Systems

This topic will be presented as APB Item #4.

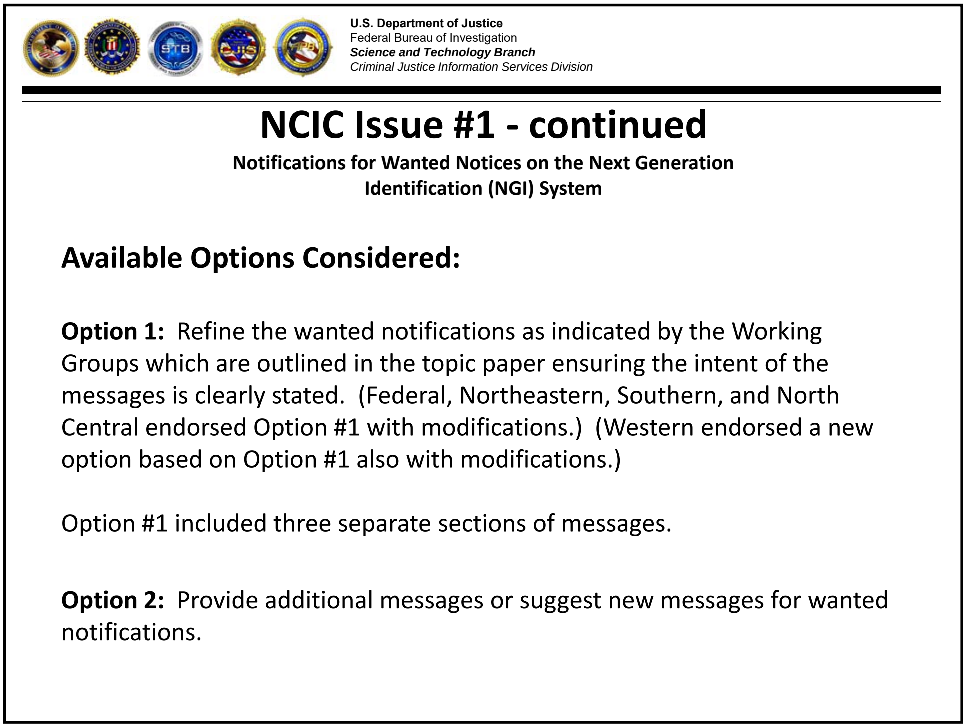


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #1

Notifications for Wanted Notices on the Next Generation Identification (NGI) System

Purpose:
To review manual and automated notifications for specific maintenance transactions in the NGI System for agencies with an active want, and determine if those should be continued with automation when required, or discontinued. Also, modify language as needed.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #1 - continued

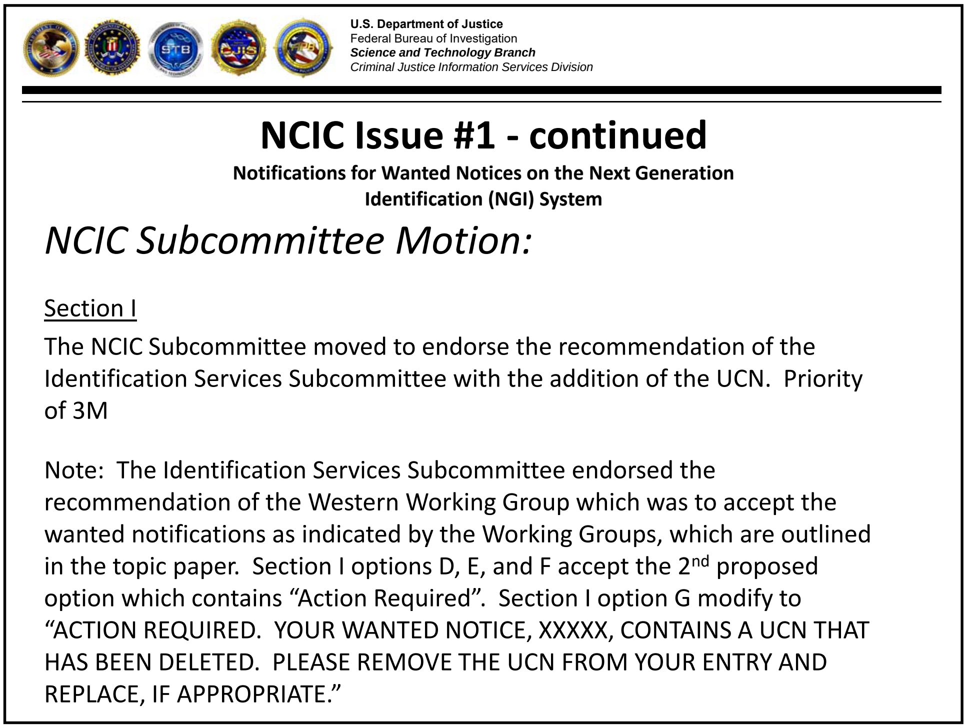
Notifications for Wanted Notices on the Next Generation Identification (NGI) System

Available Options Considered:

Option 1: Refine the wanted notifications as indicated by the Working Groups which are outlined in the topic paper ensuring the intent of the messages is clearly stated. (Federal, Northeastern, Southern, and North Central endorsed Option #1 with modifications.) (Western endorsed a new option based on Option #1 also with modifications.)

Option #1 included three separate sections of messages.

Option 2: Provide additional messages or suggest new messages for wanted notifications.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #1 - continued

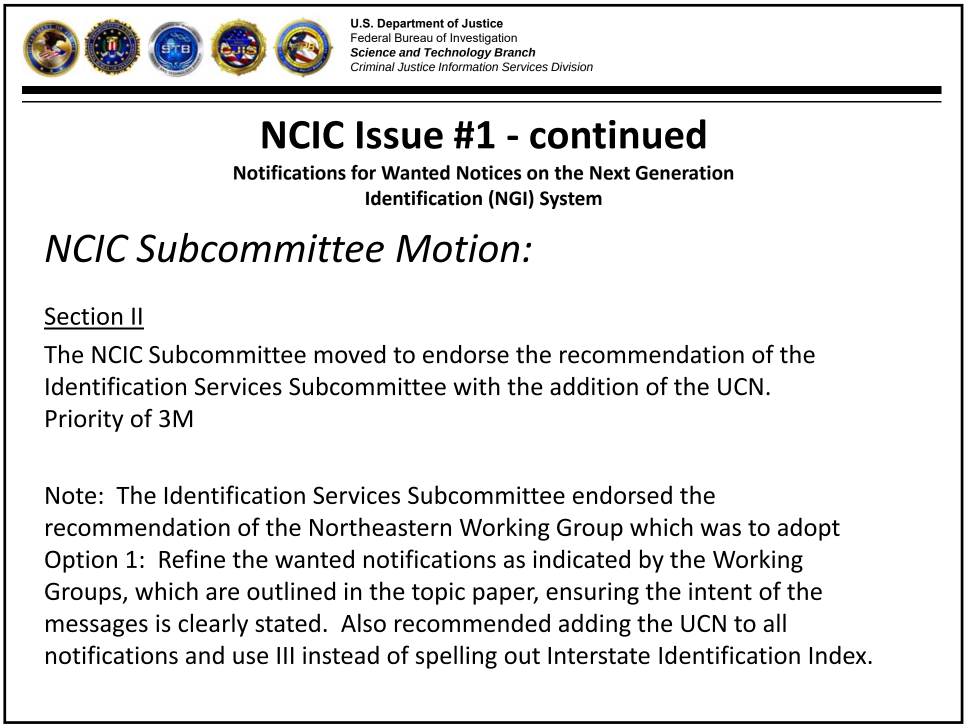
Notifications for Wanted Notices on the Next Generation Identification (NGI) System

NCIC Subcommittee Motion:

<u>Section I</u>

The NCIC Subcommittee moved to endorse the recommendation of the Identification Services Subcommittee with the addition of the UCN. Priority of 3M

Note: The Identification Services Subcommittee endorsed the recommendation of the Western Working Group which was to accept the wanted notifications as indicated by the Working Groups, which are outlined in the topic paper. Section I options D, E, and F accept the 2nd proposed option which contains “Action Required”. Section I option G modify to “ACTION REQUIRED. YOUR WANTED NOTICE, XXXXX, CONTAINS A UCN THAT HAS BEEN DELETED. PLEASE REMOVE THE UCN FROM YOUR ENTRY AND REPLACE, IF APPROPRIATE.”



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #1 - continued

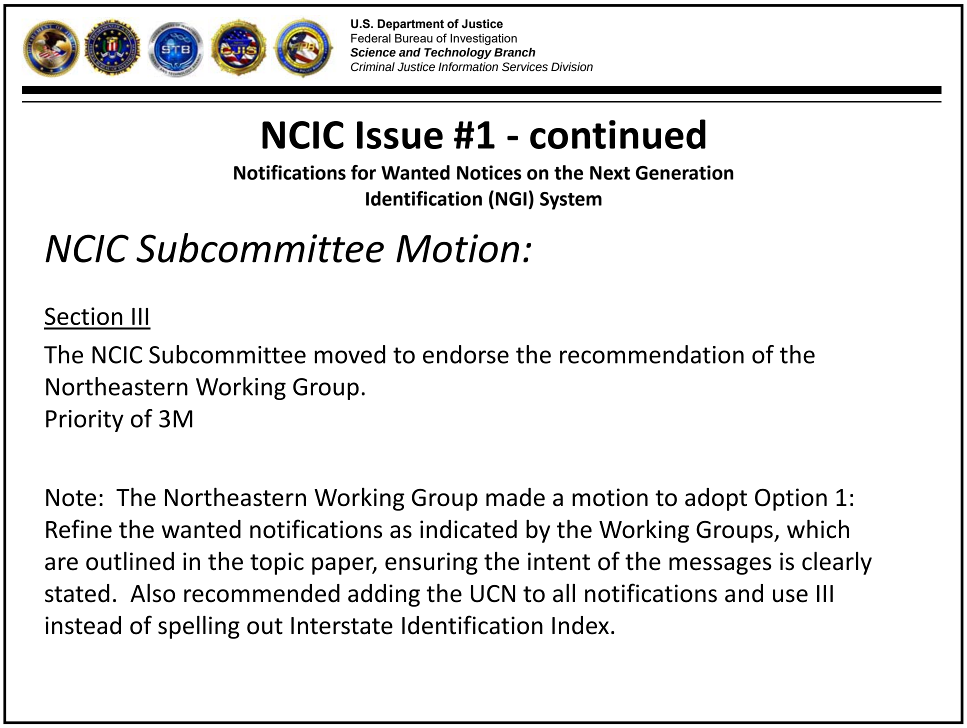
Notifications for Wanted Notices on the Next Generation Identification (NGI) System

NCIC Subcommittee Motion:

Section II

The NCIC Subcommittee moved to endorse the recommendation of the Identification Services Subcommittee with the addition of the UCN.
Priority of 3M

Note: The Identification Services Subcommittee endorsed the recommendation of the Northeastern Working Group which was to adopt Option 1: Refine the wanted notifications as indicated by the Working Groups, which are outlined in the topic paper, ensuring the intent of the messages is clearly stated. Also recommended adding the UCN to all notifications and use III instead of spelling out Interstate Identification Index.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #1 - continued

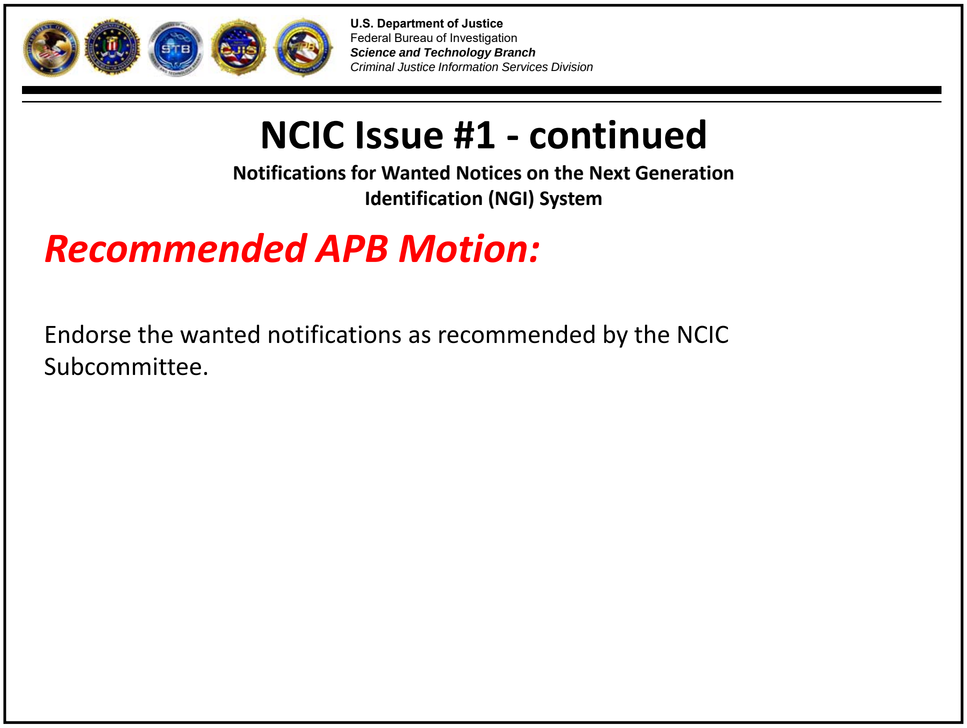
Notifications for Wanted Notices on the Next Generation Identification (NGI) System

NCIC Subcommittee Motion:

Section III

The NCIC Subcommittee moved to endorse the recommendation of the Northeastern Working Group.
Priority of 3M

Note: The Northeastern Working Group made a motion to adopt Option 1: Refine the wanted notifications as indicated by the Working Groups, which are outlined in the topic paper, ensuring the intent of the messages is clearly stated. Also recommended adding the UCN to all notifications and use III instead of spelling out Interstate Identification Index.



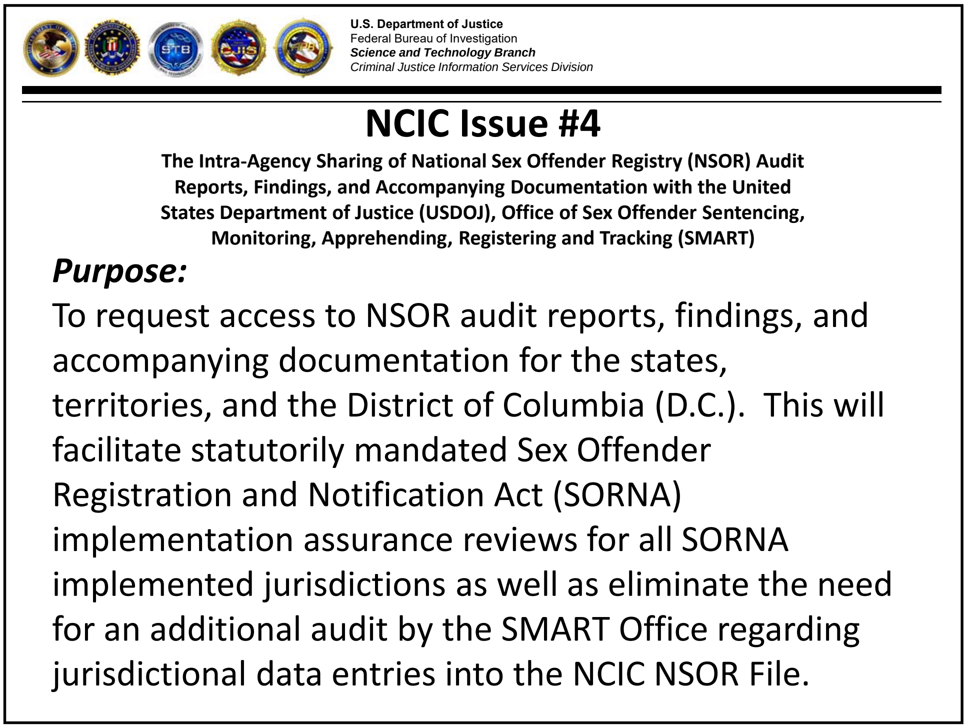
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #1 - continued

Notifications for Wanted Notices on the Next Generation Identification (NGI) System

Recommended APB Motion:

Endorse the wanted notifications as recommended by the NCIC Subcommittee.



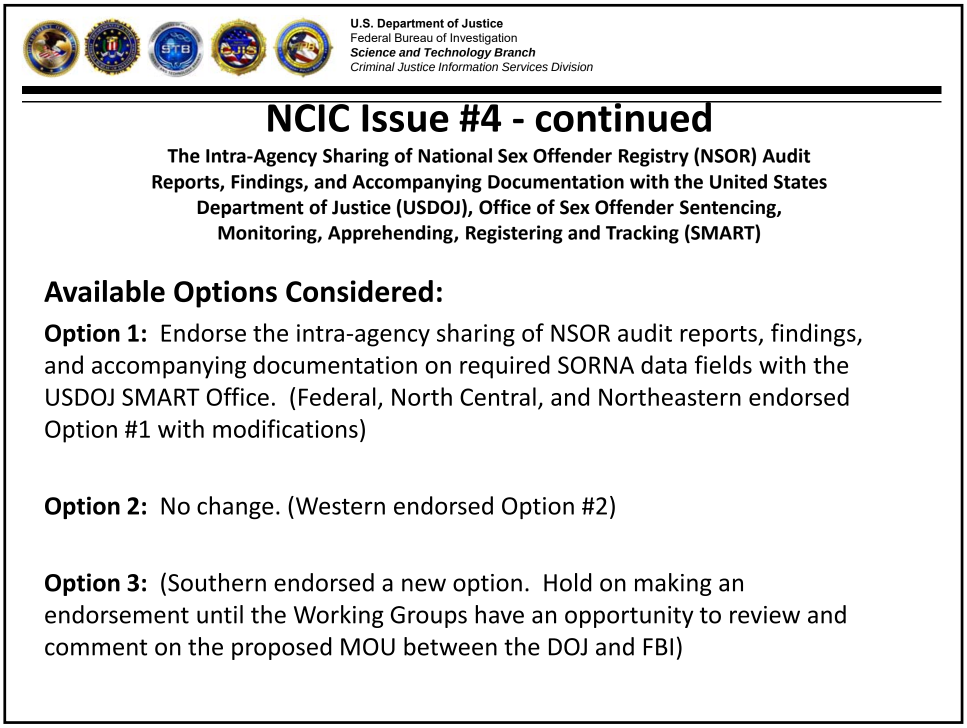
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #4

The Intra-Agency Sharing of National Sex Offender Registry (NSOR) Audit Reports, Findings, and Accompanying Documentation with the United States Department of Justice (USDOJ), Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (SMART)

Purpose:

To request access to NSOR audit reports, findings, and accompanying documentation for the states, territories, and the District of Columbia (D.C.). This will facilitate statutorily mandated Sex Offender Registration and Notification Act (SORNA) implementation assurance reviews for all SORNA implemented jurisdictions as well as eliminate the need for an additional audit by the SMART Office regarding jurisdictional data entries into the NCIC NSOR File.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #4 - continued

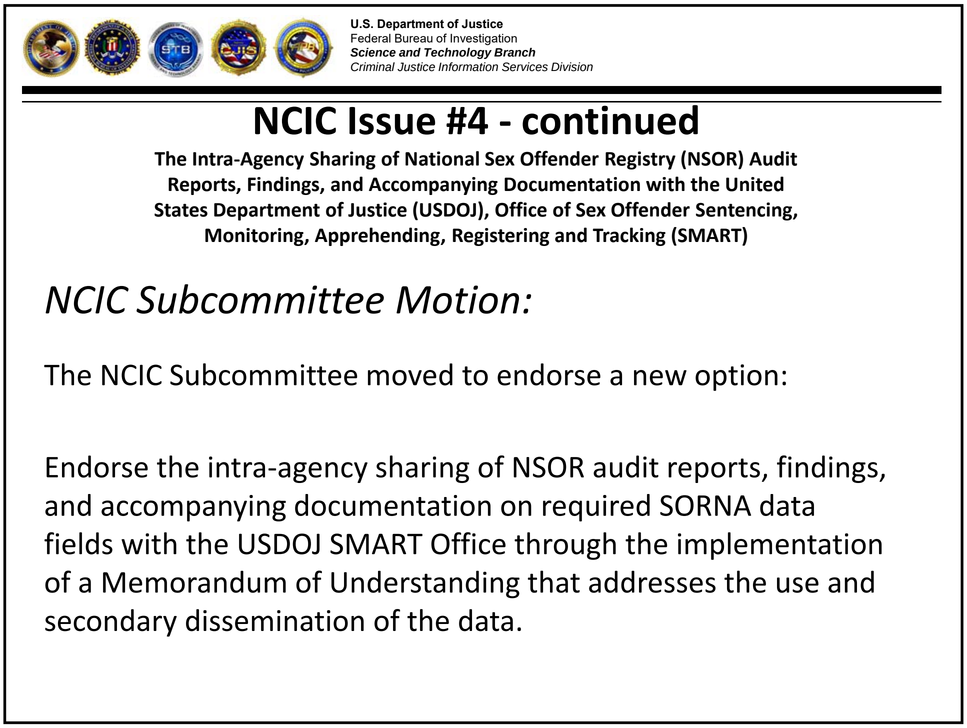
The Intra-Agency Sharing of National Sex Offender Registry (NSOR) Audit Reports, Findings, and Accompanying Documentation with the United States Department of Justice (USDOJ), Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (SMART)

Available Options Considered:

Option 1: Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office. (Federal, North Central, and Northeastern endorsed Option #1 with modifications)

Option 2: No change. (Western endorsed Option #2)

Option 3: (Southern endorsed a new option. Hold on making an endorsement until the Working Groups have an opportunity to review and comment on the proposed MOU between the DOJ and FBI)



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

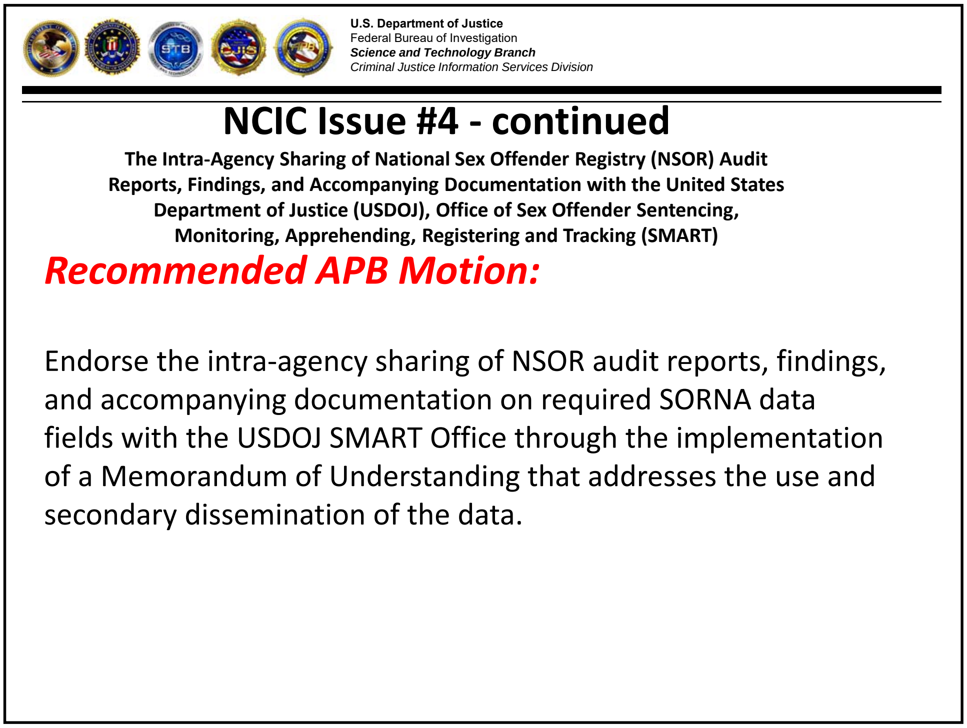
NCIC Issue #4 - continued

The Intra-Agency Sharing of National Sex Offender Registry (NSOR) Audit Reports, Findings, and Accompanying Documentation with the United States Department of Justice (USDOJ), Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (SMART)

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to endorse a new option:

Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office through the implementation of a Memorandum of Understanding that addresses the use and secondary dissemination of the data.



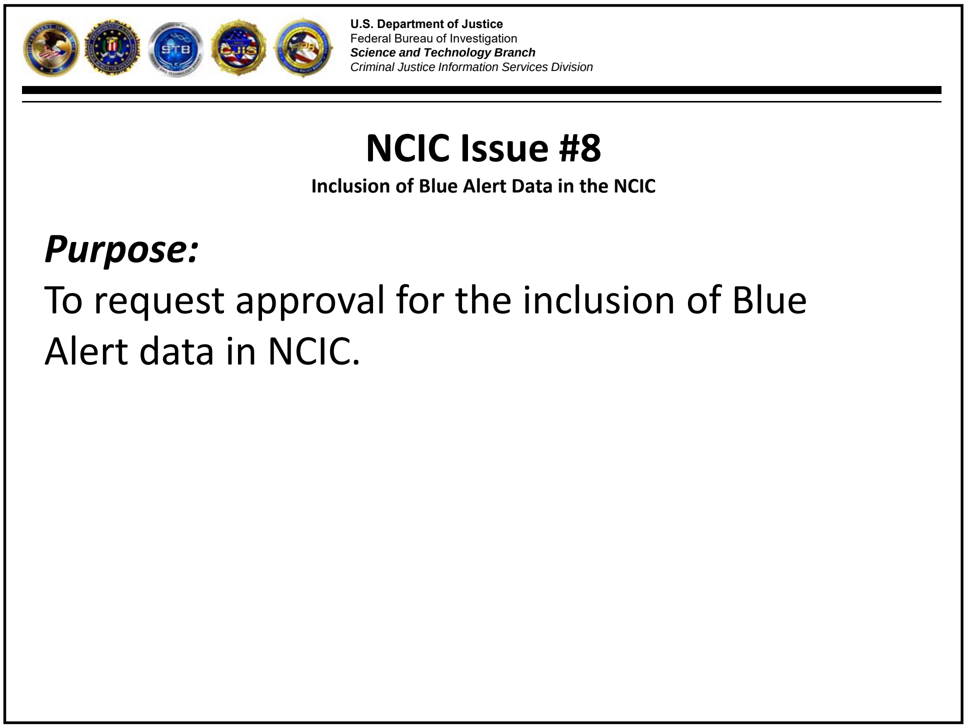
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #4 - continued

The Intra-Agency Sharing of National Sex Offender Registry (NSOR) Audit Reports, Findings, and Accompanying Documentation with the United States Department of Justice (USDOJ), Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (SMART)

Recommended APB Motion:

Endorse the intra-agency sharing of NSOR audit reports, findings, and accompanying documentation on required SORNA data fields with the USDOJ SMART Office through the implementation of a Memorandum of Understanding that addresses the use and secondary dissemination of the data.



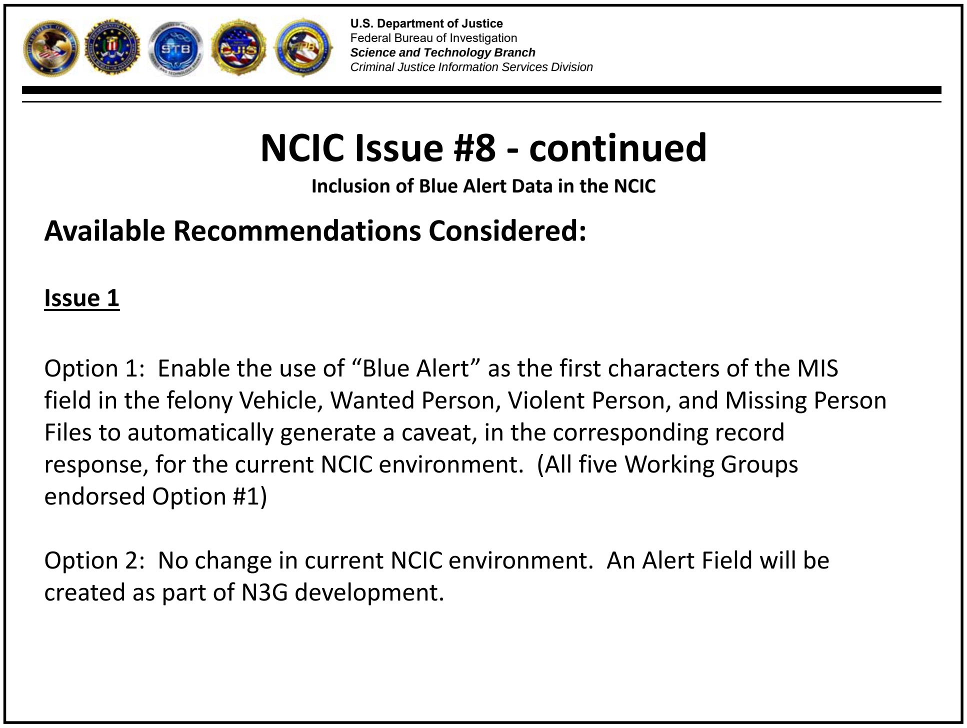
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #8

Inclusion of Blue Alert Data in the NCIC

Purpose:

To request approval for the inclusion of Blue Alert data in NCIC.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #8 - continued

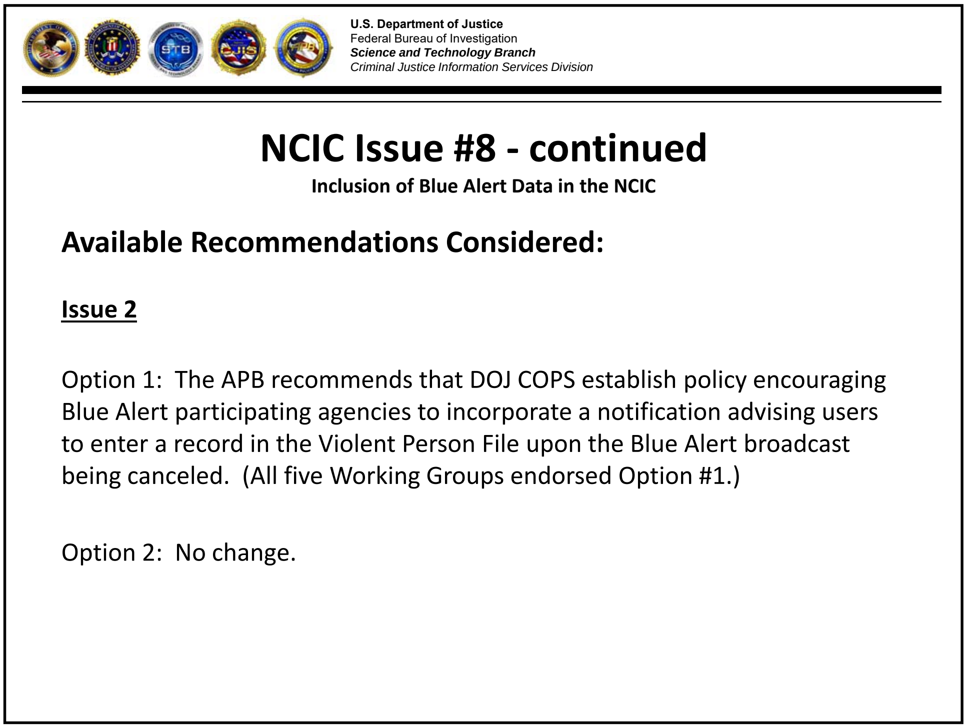
Inclusion of Blue Alert Data in the NCIC

Available Recommendations Considered:

Issue 1

Option 1: Enable the use of “Blue Alert” as the first characters of the MIS field in the felony Vehicle, Wanted Person, Violent Person, and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. (All five Working Groups endorsed Option #1)

Option 2: No change in current NCIC environment. An Alert Field will be created as part of N3G development.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #8 - continued

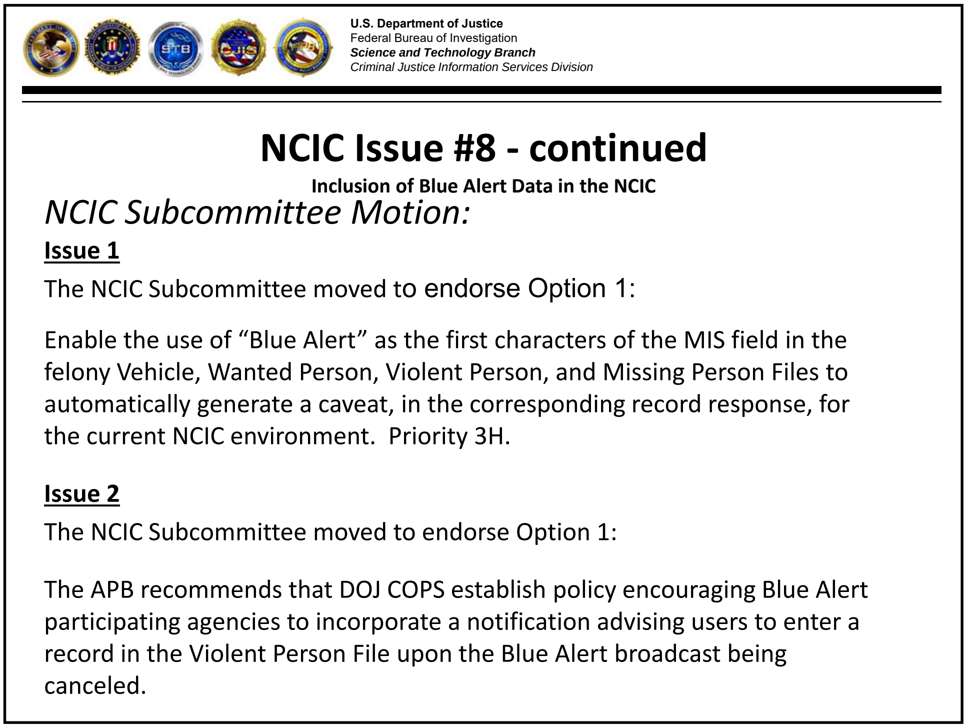
Inclusion of Blue Alert Data in the NCIC

Available Recommendations Considered:

Issue 2

Option 1: The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled. (All five Working Groups endorsed Option #1.)

Option 2: No change.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #8 - continued

Inclusion of Blue Alert Data in the NCIC

NCIC Subcommittee Motion:

Issue 1

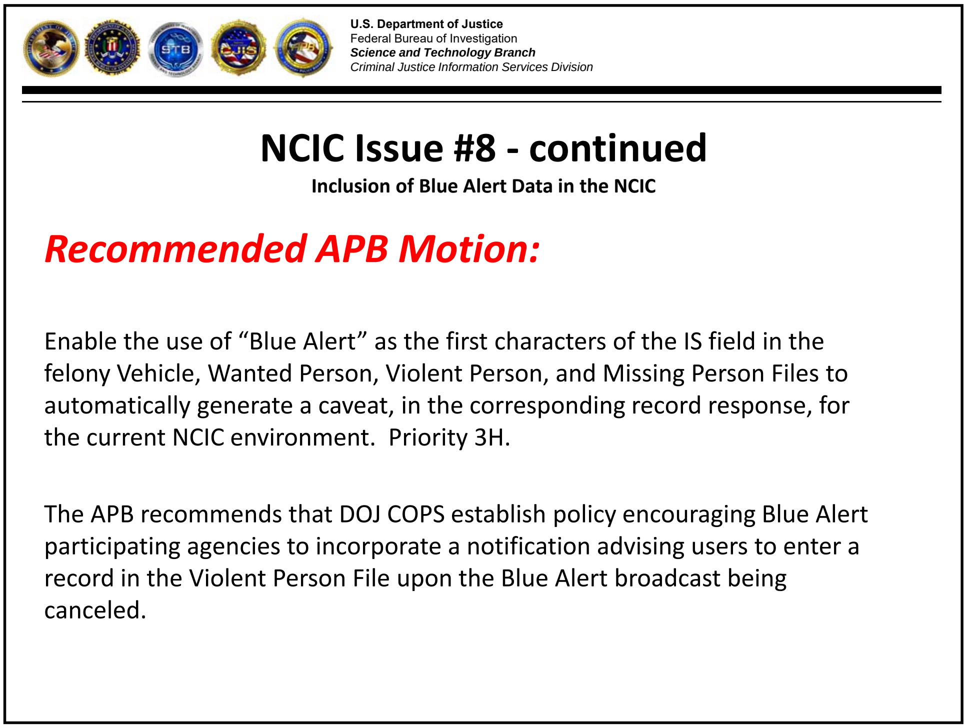
The NCIC Subcommittee moved to endorse Option 1:

Enable the use of “Blue Alert” as the first characters of the MIS field in the felony Vehicle, Wanted Person, Violent Person, and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. Priority 3H.

Issue 2

The NCIC Subcommittee moved to endorse Option 1:

The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

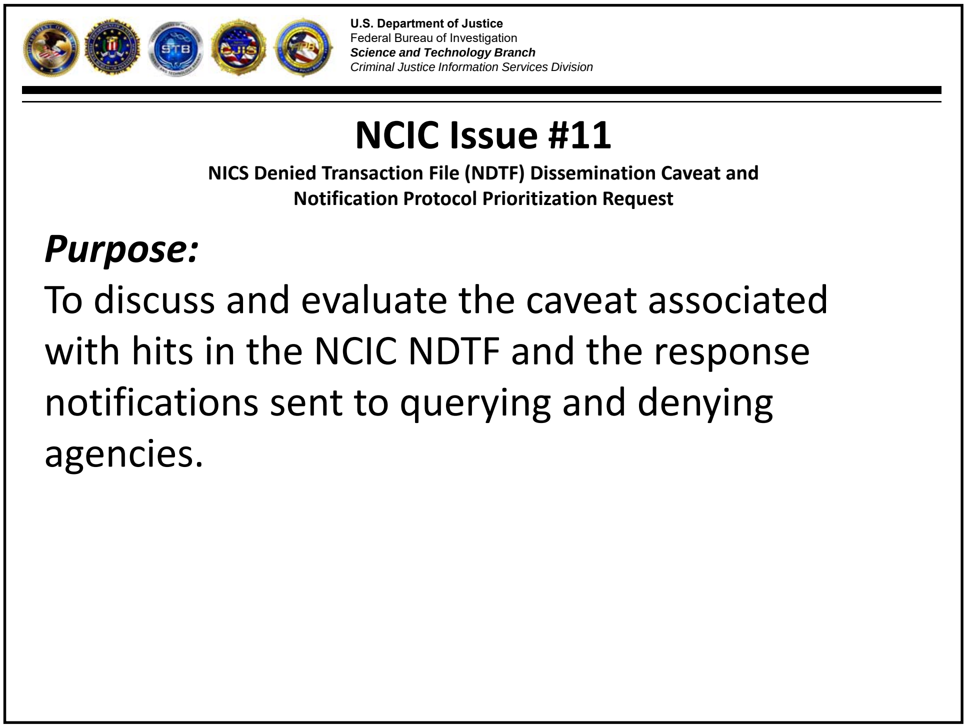
NCIC Issue #8 - continued

Inclusion of Blue Alert Data in the NCIC

Recommended APB Motion:

Enable the use of “Blue Alert” as the first characters of the IS field in the felony Vehicle, Wanted Person, Violent Person, and Missing Person Files to automatically generate a caveat, in the corresponding record response, for the current NCIC environment. Priority 3H.

The APB recommends that DOJ COPS establish policy encouraging Blue Alert participating agencies to incorporate a notification advising users to enter a record in the Violent Person File upon the Blue Alert broadcast being canceled.



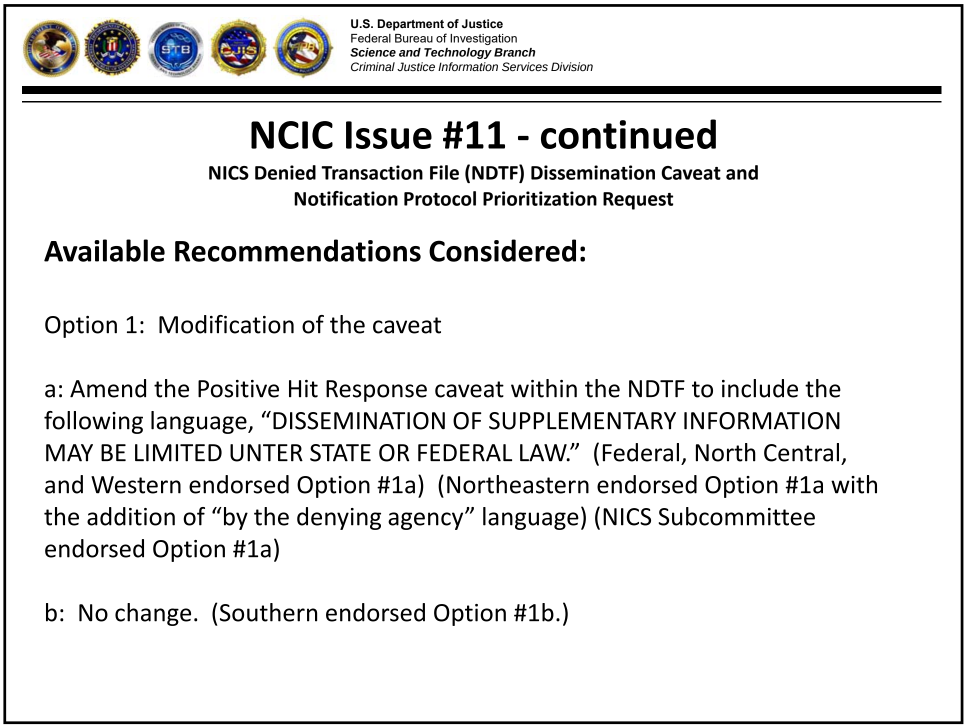
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #11

NICS Denied Transaction File (NDTF) Dissemination Caveat and Notification Protocol Prioritization Request

Purpose:

To discuss and evaluate the caveat associated with hits in the NCIC NDTF and the response notifications sent to querying and denying agencies.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #11 - continued

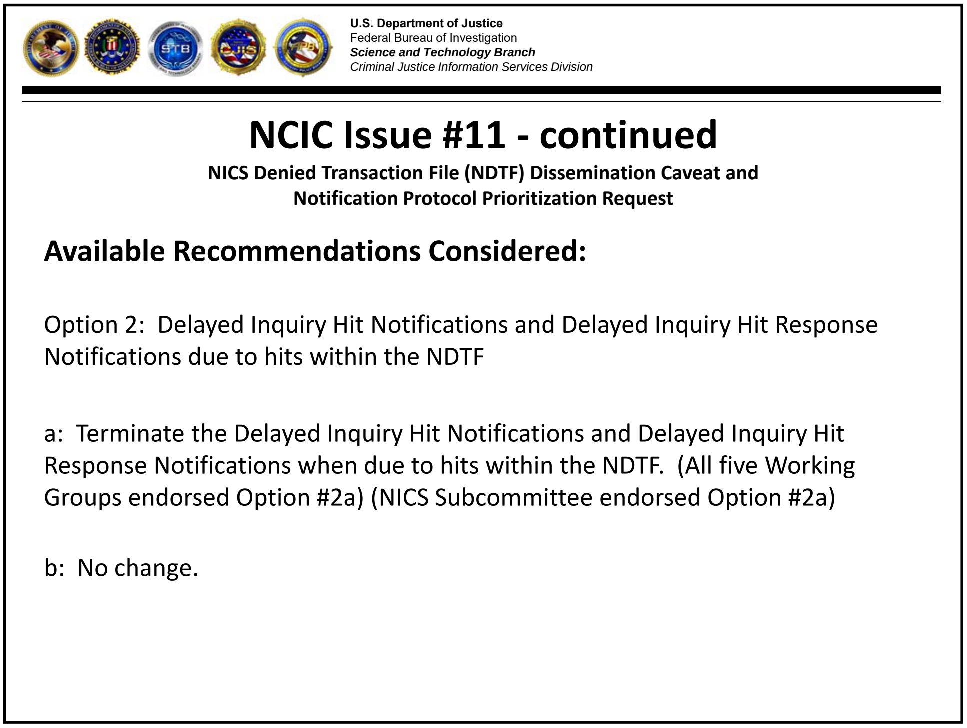
NICS Denied Transaction File (NDTF) Dissemination Caveat and Notification Protocol Prioritization Request

Available Recommendations Considered:

Option 1: Modification of the caveat

a: Amend the Positive Hit Response caveat within the NDTF to include the following language, “DISSEMINATION OF SUPPLEMENTARY INFORMATION MAY BE LIMITED UNTER STATE OR FEDERAL LAW.” (Federal, North Central, and Western endorsed Option #1a) (Northeastern endorsed Option #1a with the addition of “by the denying agency” language) (NICS Subcommittee endorsed Option #1a)

b: No change. (Southern endorsed Option #1b.)



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #11 - continued

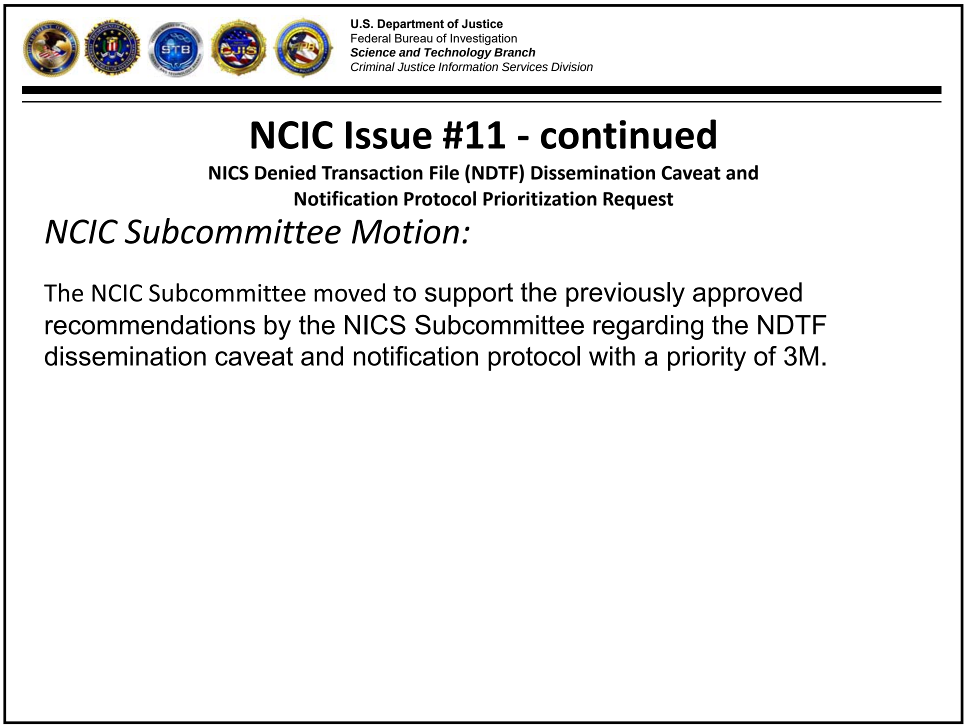
NICS Denied Transaction File (NDTF) Dissemination Caveat and Notification Protocol Prioritization Request

Available Recommendations Considered:

Option 2: Delayed Inquiry Hit Notifications and Delayed Inquiry Hit Response Notifications due to hits within the NDTF

a: Terminate the Delayed Inquiry Hit Notifications and Delayed Inquiry Hit Response Notifications when due to hits within the NDTF. (All five Working Groups endorsed Option #2a) (NICS Subcommittee endorsed Option #2a)

b: No change.



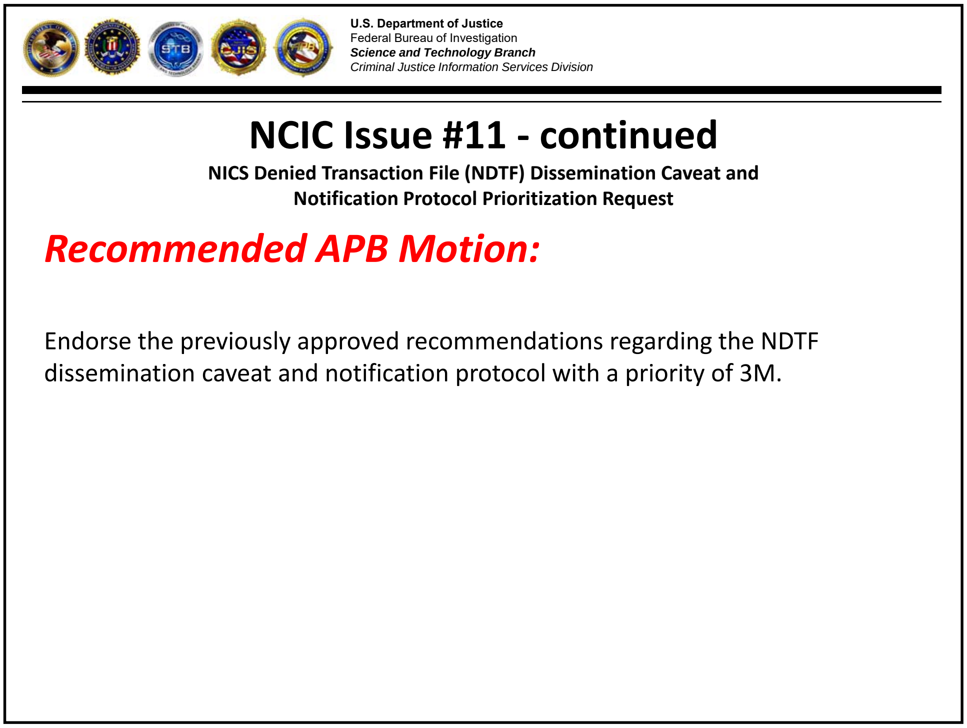
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #11 - continued

NICS Denied Transaction File (NDTF) Dissemination Caveat and Notification Protocol Prioritization Request

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to support the previously approved recommendations by the NICS Subcommittee regarding the NDTF dissemination caveat and notification protocol with a priority of 3M.



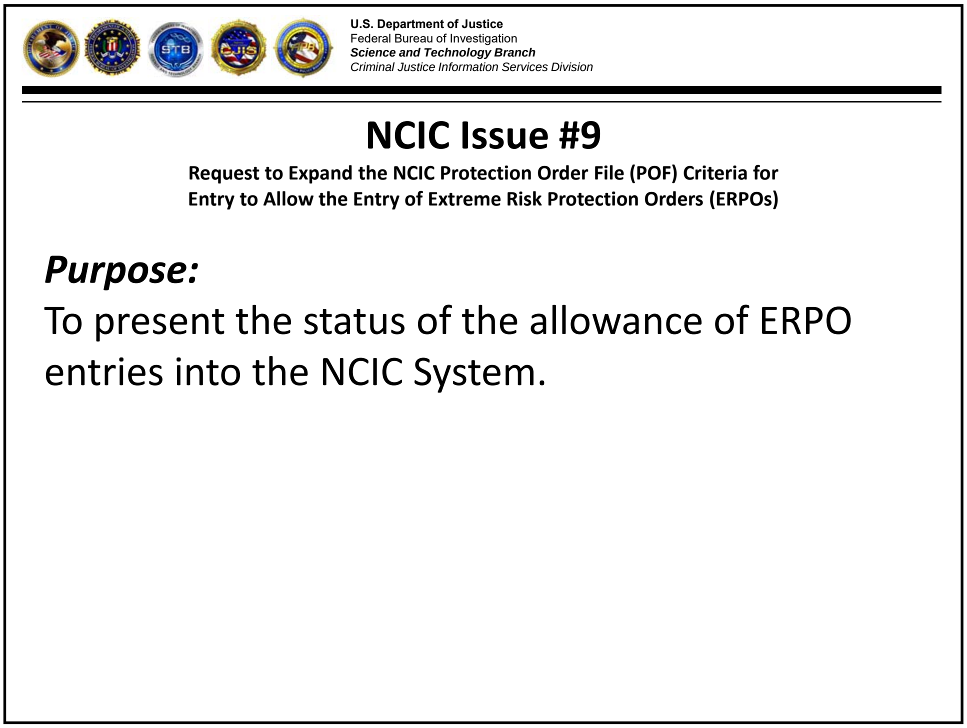
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #11 - continued

NICS Denied Transaction File (NDTF) Dissemination Caveat and Notification Protocol Prioritization Request

Recommended APB Motion:

Endorse the previously approved recommendations regarding the NDTF dissemination caveat and notification protocol with a priority of 3M.



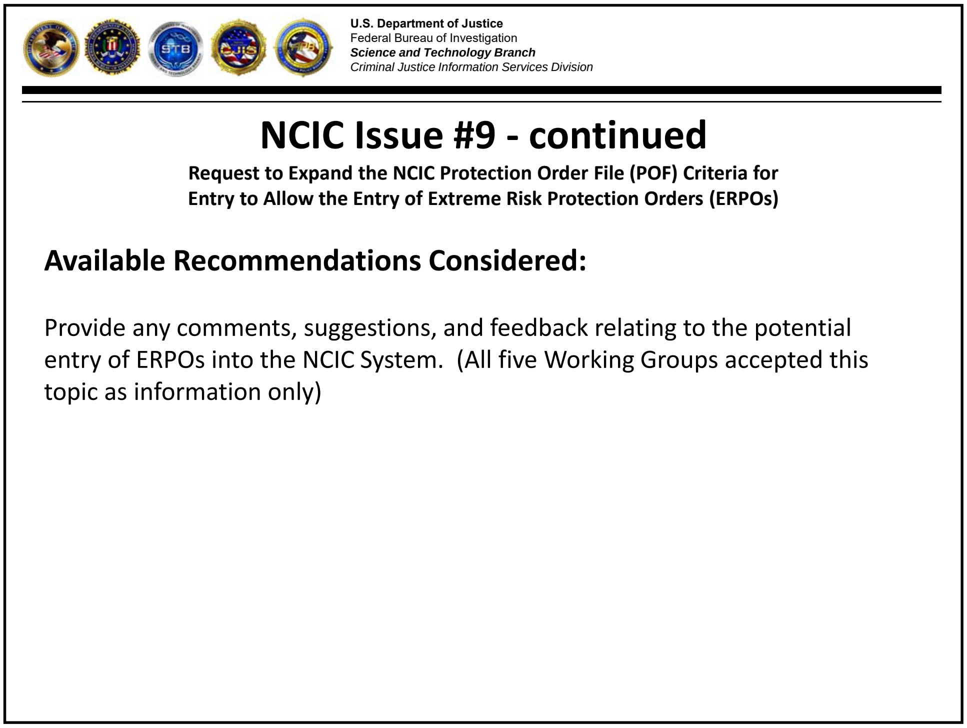
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #9

Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPOs)

Purpose:

To present the status of the allowance of ERPO entries into the NCIC System.



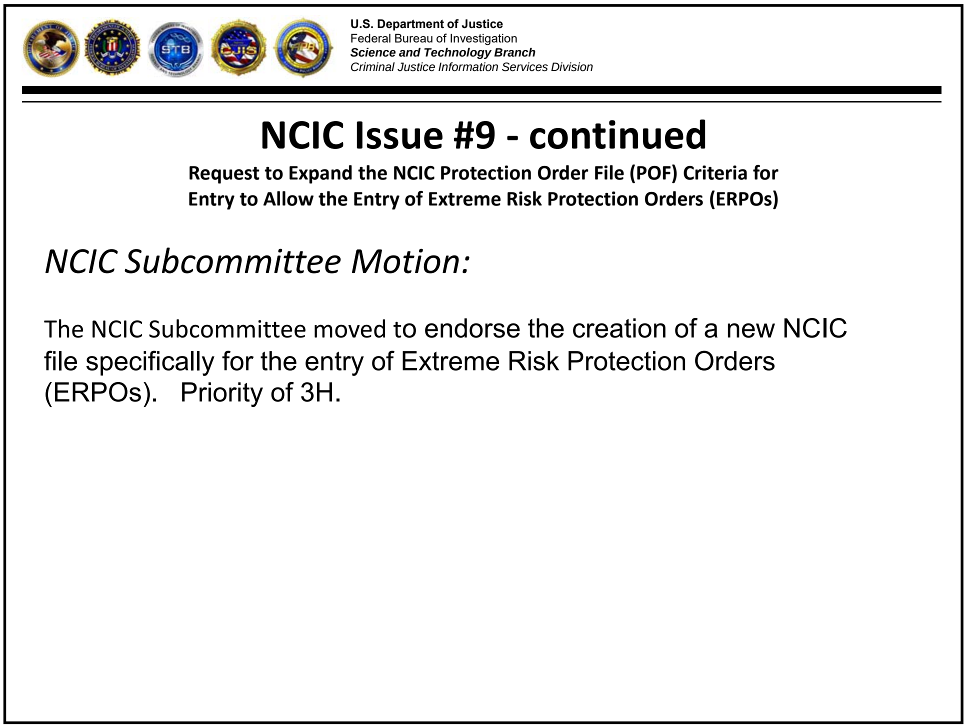
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #9 - continued

Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPOs)

Available Recommendations Considered:

Provide any comments, suggestions, and feedback relating to the potential entry of ERPOs into the NCIC System. (All five Working Groups accepted this topic as information only)



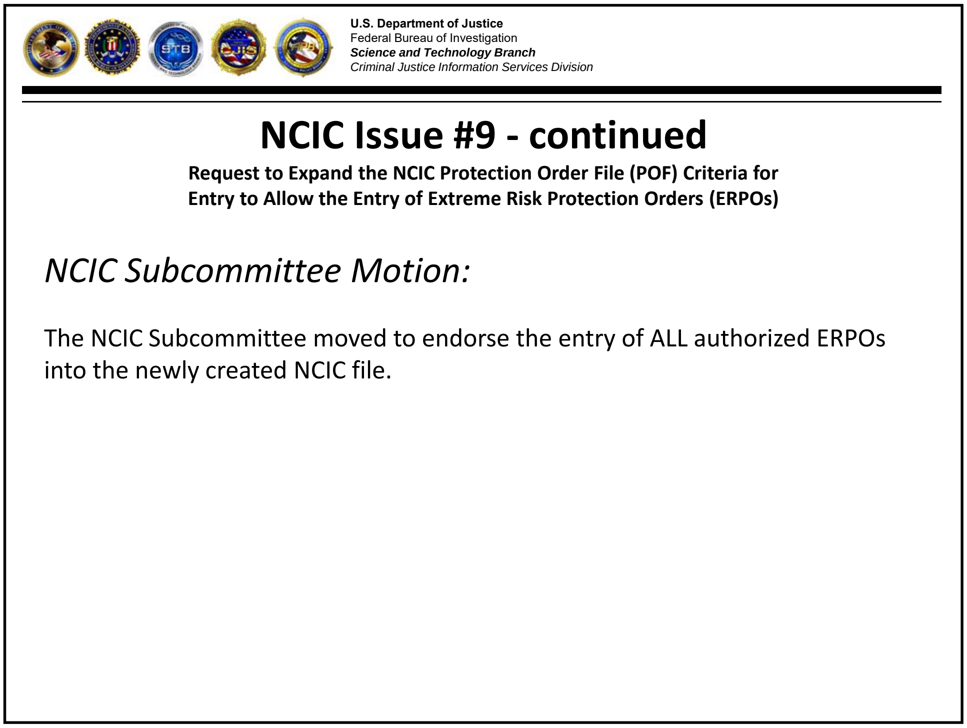
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #9 - continued

Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPOs)

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to endorse the creation of a new NCIC file specifically for the entry of Extreme Risk Protection Orders (ERPOs). Priority of 3H.



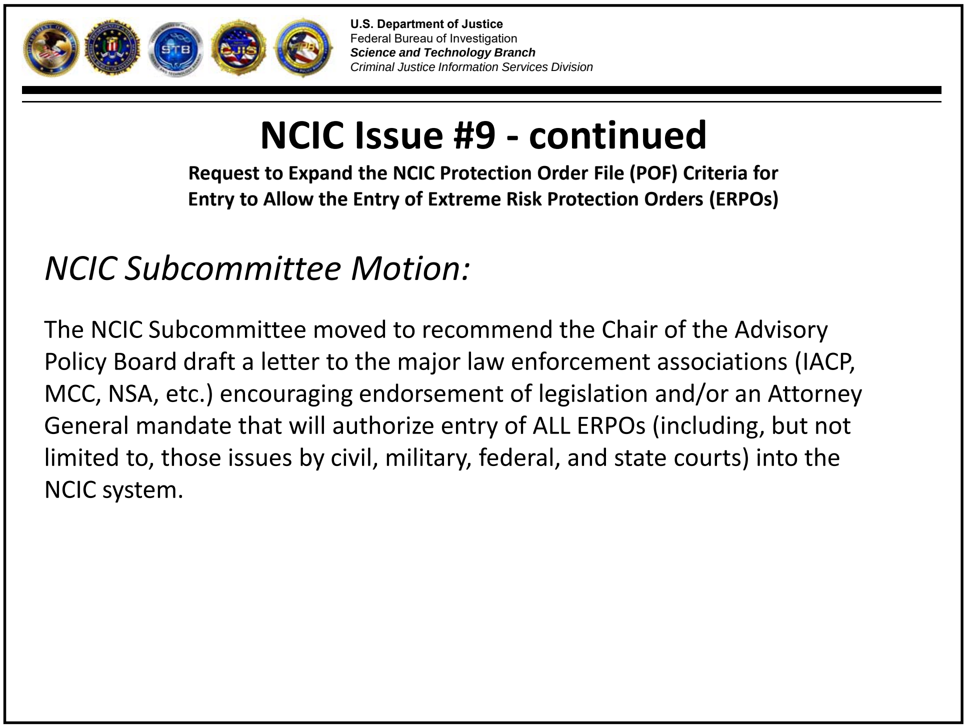
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #9 - continued

Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPOs)

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to endorse the entry of ALL authorized ERPOs into the newly created NCIC file.



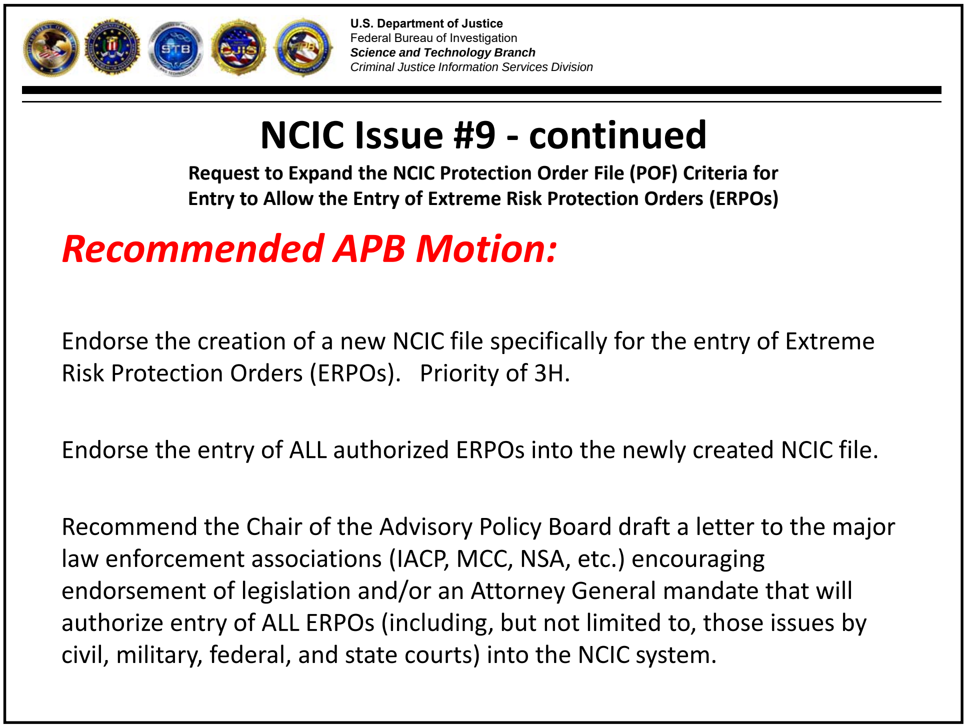
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #9 - continued

Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPOs)

NCIC Subcommittee Motion:

The NCIC Subcommittee moved to recommend the Chair of the Advisory Policy Board draft a letter to the major law enforcement associations (IACP, MCC, NSA, etc.) encouraging endorsement of legislation and/or an Attorney General mandate that will authorize entry of ALL ERPOs (including, but not limited to, those issues by civil, military, federal, and state courts) into the NCIC system.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC Issue #9 - continued

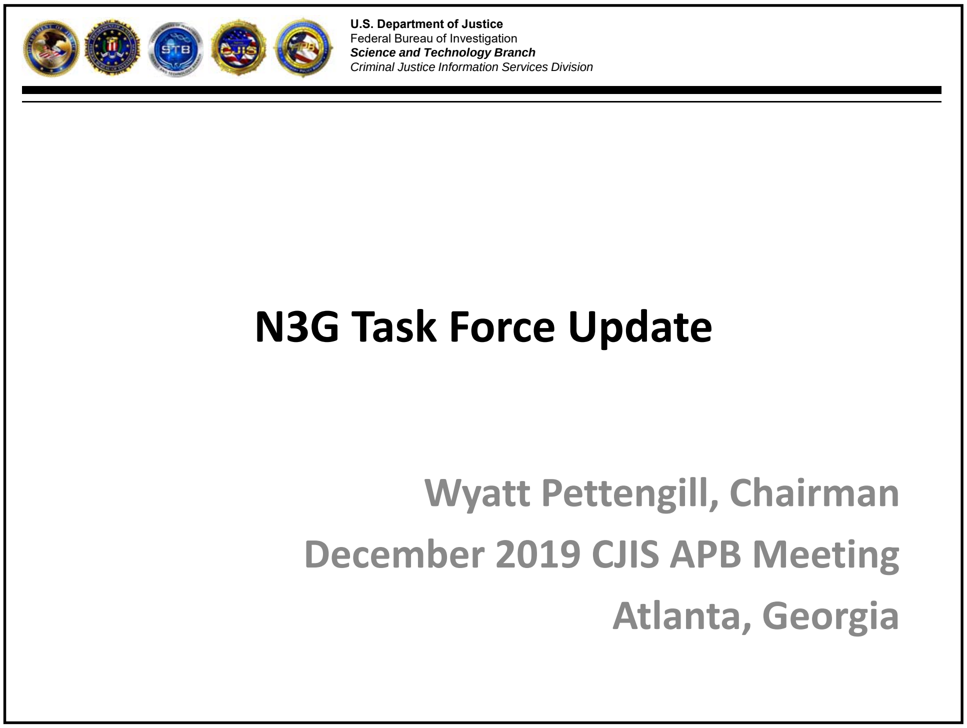
Request to Expand the NCIC Protection Order File (POF) Criteria for Entry to Allow the Entry of Extreme Risk Protection Orders (ERPOs)

Recommended APB Motion:

Endorse the creation of a new NCIC file specifically for the entry of Extreme Risk Protection Orders (ERPOs). Priority of 3H.

Endorse the entry of ALL authorized ERPOs into the newly created NCIC file.

Recommend the Chair of the Advisory Policy Board draft a letter to the major law enforcement associations (IACP, MCC, NSA, etc.) encouraging endorsement of legislation and/or an Attorney General mandate that will authorize entry of ALL ERPOs (including, but not limited to, those issues by civil, military, federal, and state courts) into the NCIC system.



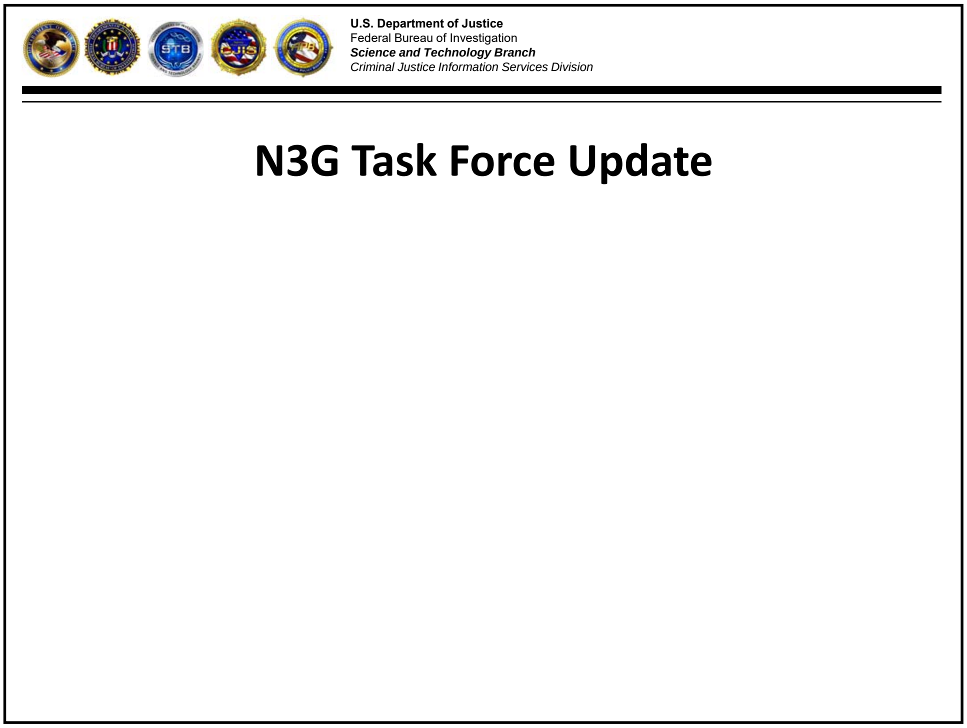
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N3G Task Force Update

Wyatt Pettengill, Chairman

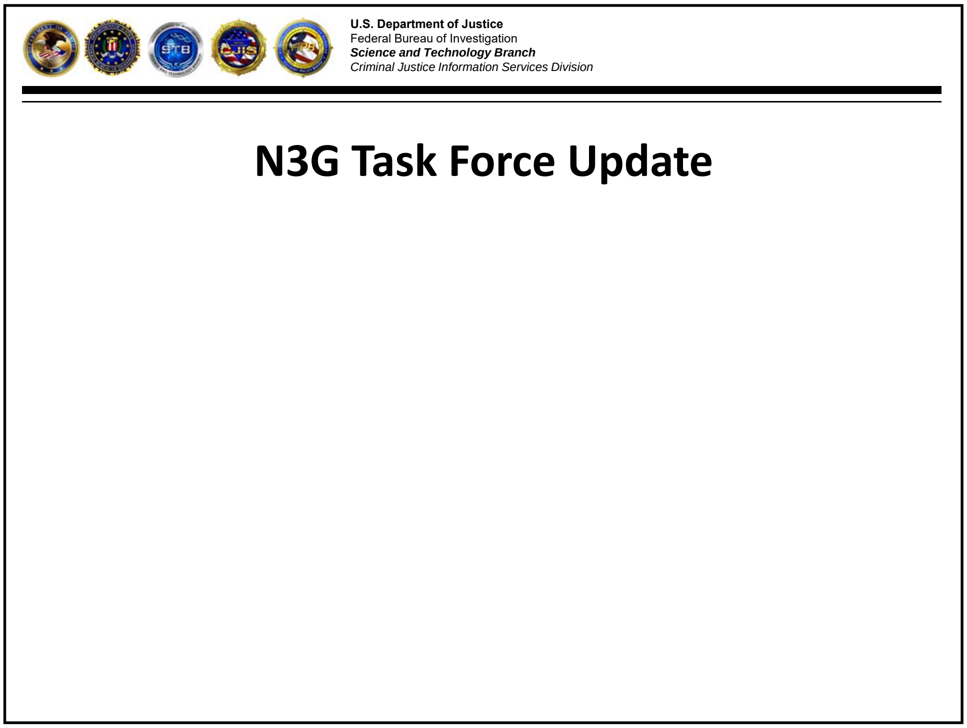
December 2019 CJIS APB Meeting

Atlanta, Georgia



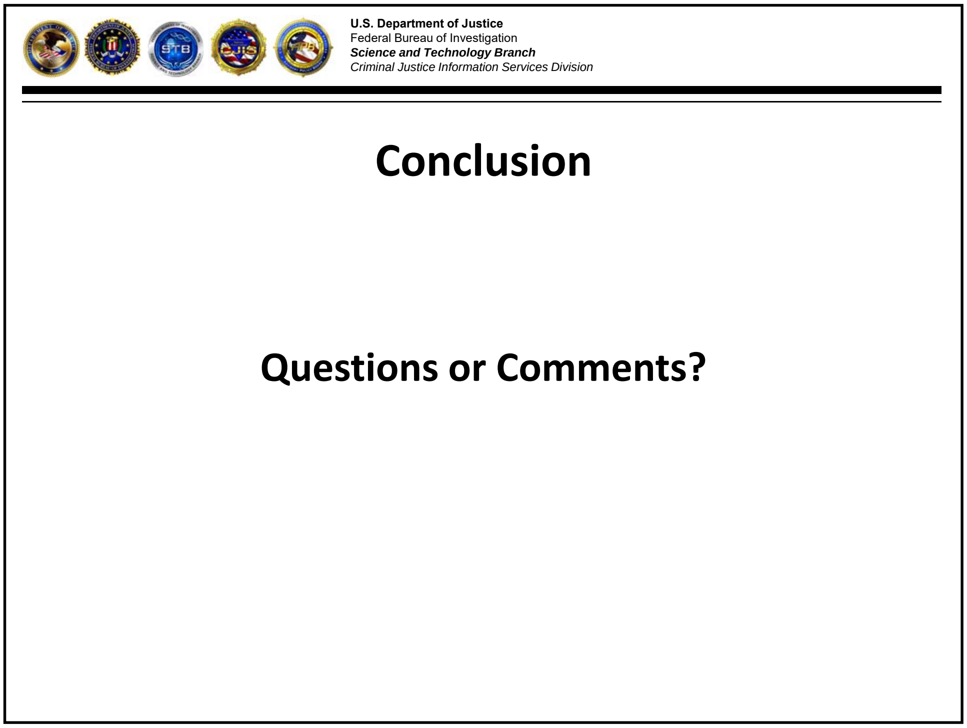
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N3G Task Force Update



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

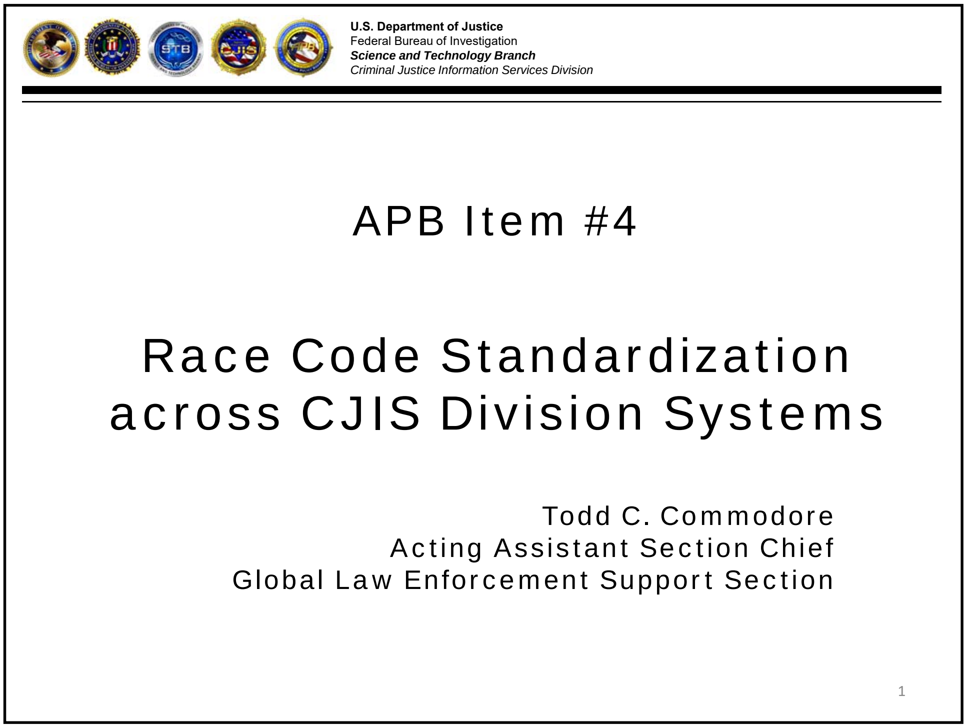
N3G Task Force Update



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Conclusion

Questions or Comments?



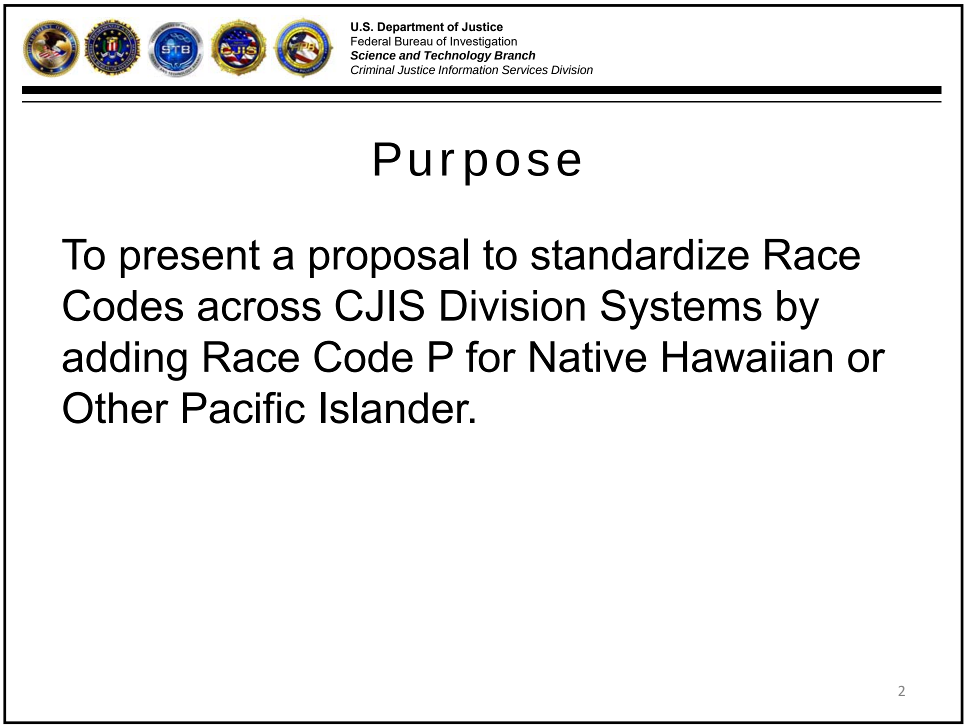
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB Item #4

Race Code Standardization across CJIS Division Systems

Todd C. Commodore
Acting Assistant Section Chief
Global Law Enforcement Support Section

1

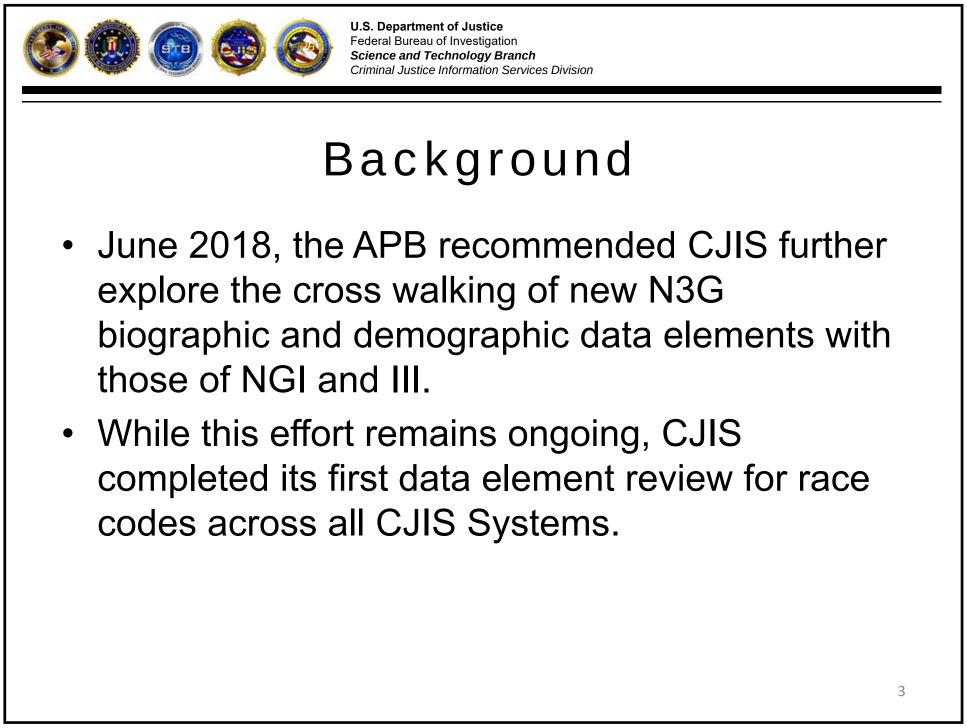


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Purpose

To present a proposal to standardize Race Codes across CJIS Division Systems by adding Race Code P for Native Hawaiian or Other Pacific Islander.

2

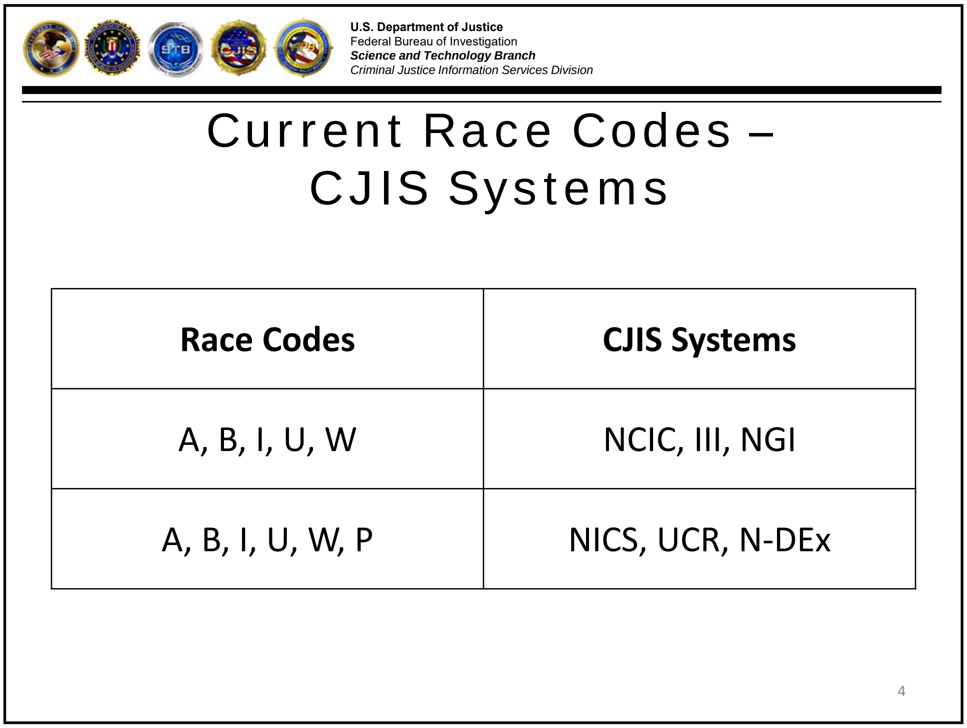


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Background

- June 2018, the APB recommended CJIS further explore the cross walking of new N3G biographic and demographic data elements with those of NGI and III.
- While this effort remains ongoing, CJIS completed its first data element review for race codes across all CJIS Systems.

3

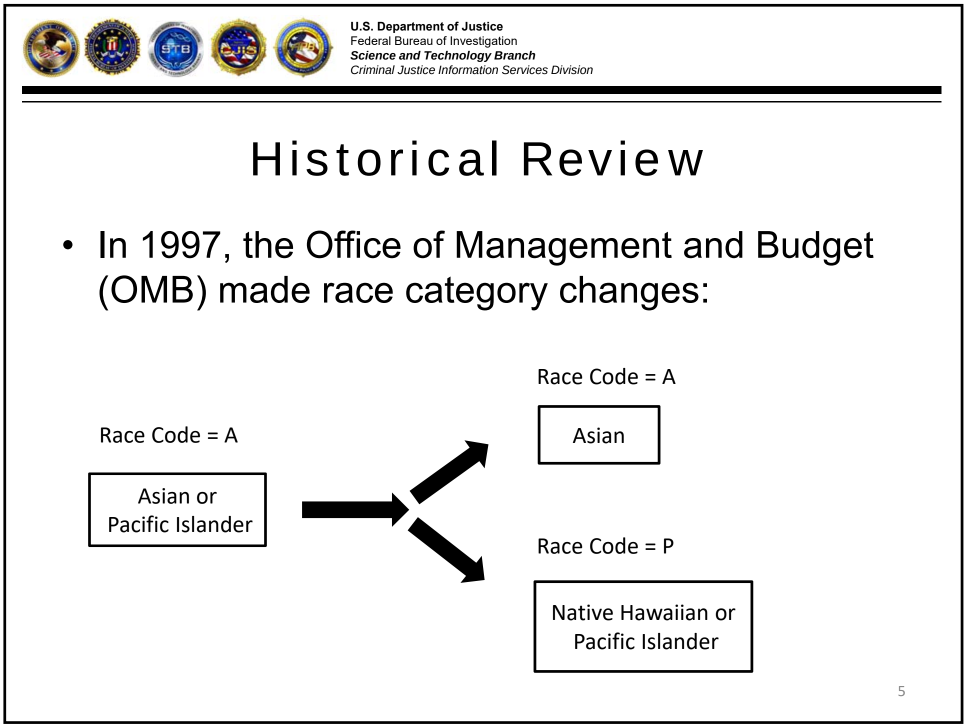


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Current Race Codes – CJIS Systems

Race Codes	CJIS Systems
A, B, I, U, W	NCIC, III, NGI
A, B, I, U, W, P	NICS, UCR, N-DEx

4



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Historical Review

- In 1997, the Office of Management and Budget (OMB) made race category changes:

Race Code = A

Asian or Pacific Islander

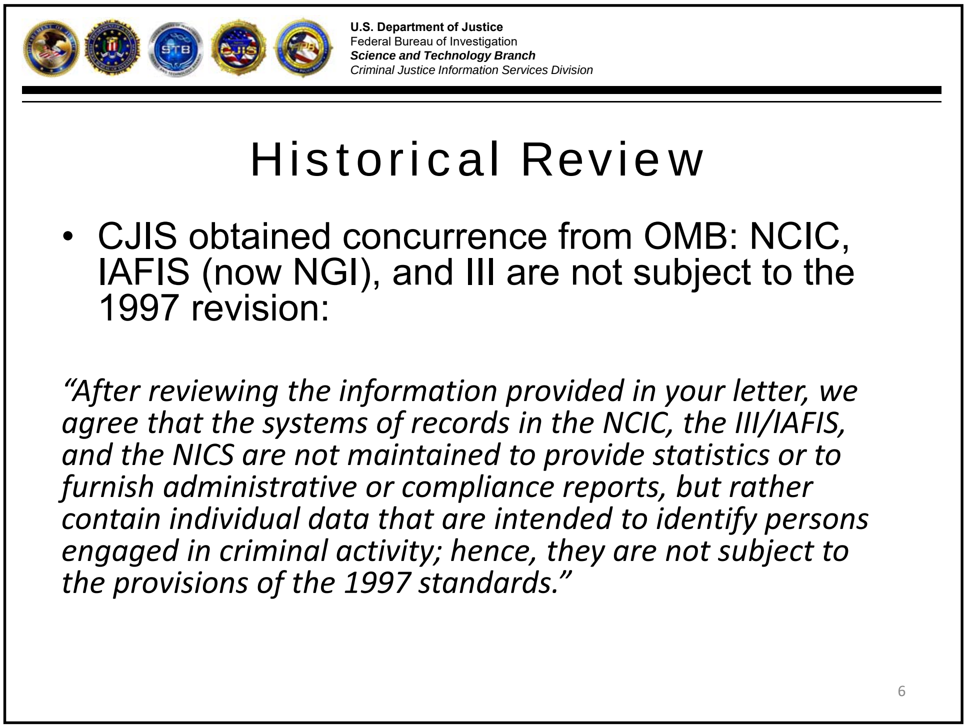
Race Code = A

Asian

Race Code = P

Native Hawaiian or Pacific Islander

5



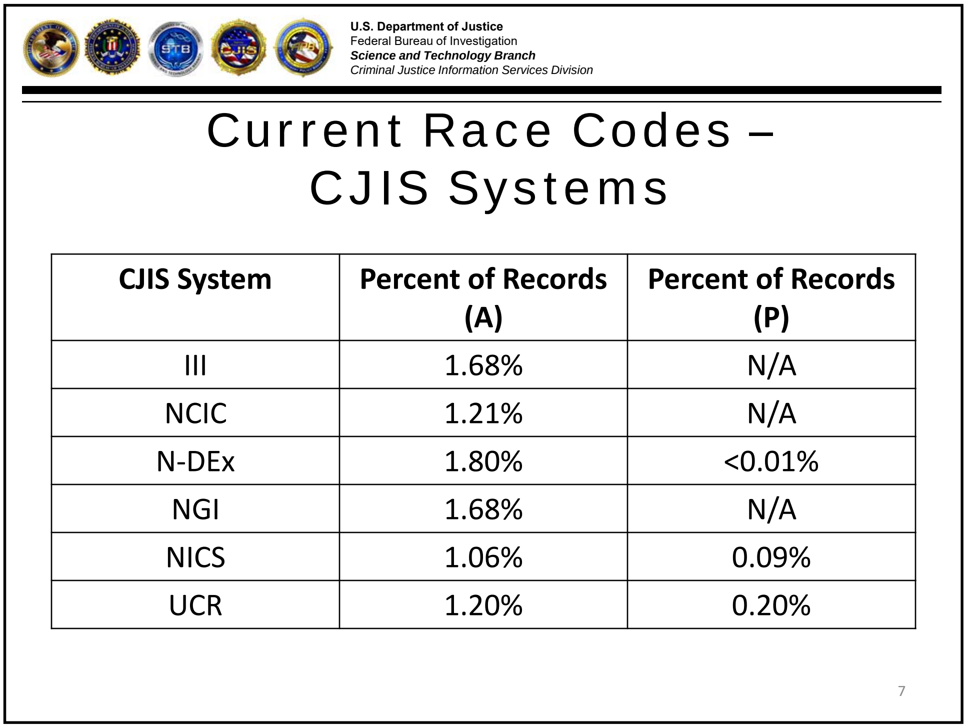
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Historical Review

- CJIS obtained concurrence from OMB: NCIC, IAFIS (now NGI), and III are not subject to the 1997 revision:

"After reviewing the information provided in your letter, we agree that the systems of records in the NCIC, the III/IAFIS, and the NICS are not maintained to provide statistics or to furnish administrative or compliance reports, but rather contain individual data that are intended to identify persons engaged in criminal activity; hence, they are not subject to the provisions of the 1997 standards."

6

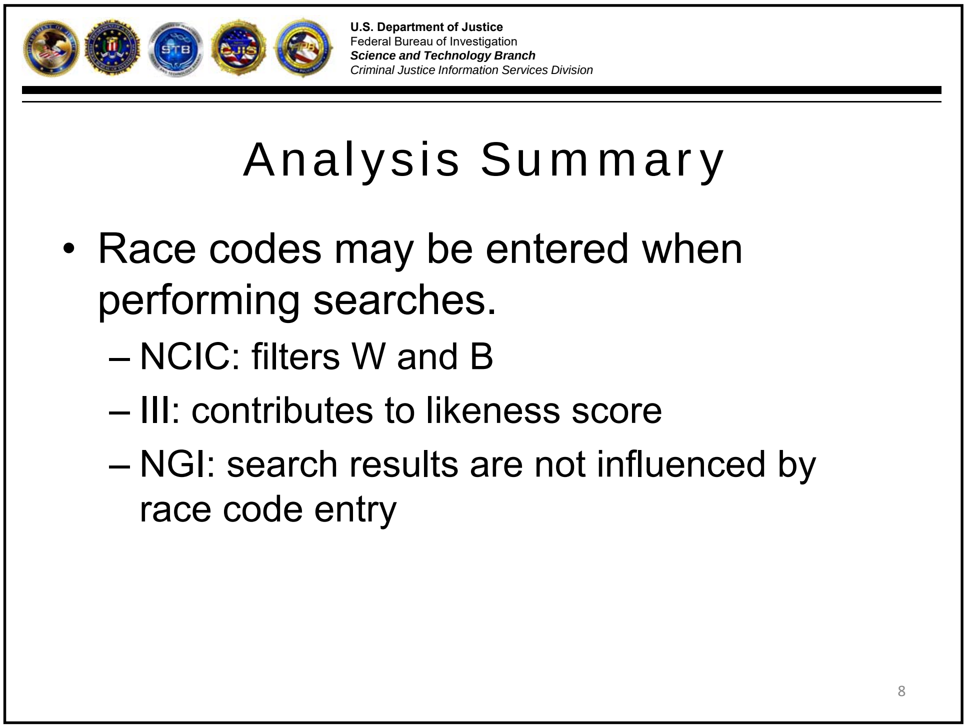


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Current Race Codes – CJIS Systems

CJIS System	Percent of Records (A)	Percent of Records (P)
III	1.68%	N/A
NCIC	1.21%	N/A
N-DEx	1.80%	<0.01%
NGI	1.68%	N/A
NICS	1.06%	0.09%
UCR	1.20%	0.20%

7

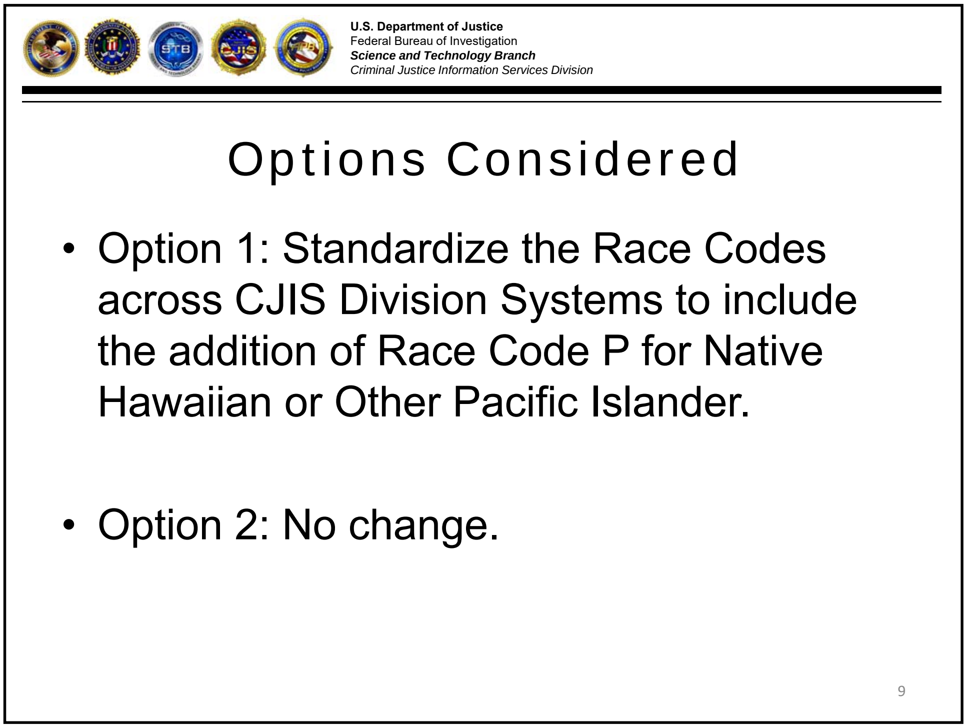


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Analysis Summary

- Race codes may be entered when performing searches.
  - NCIC: filters W and B
  - III: contributes to likeness score
  - NGI: search results are not influenced by race code entry

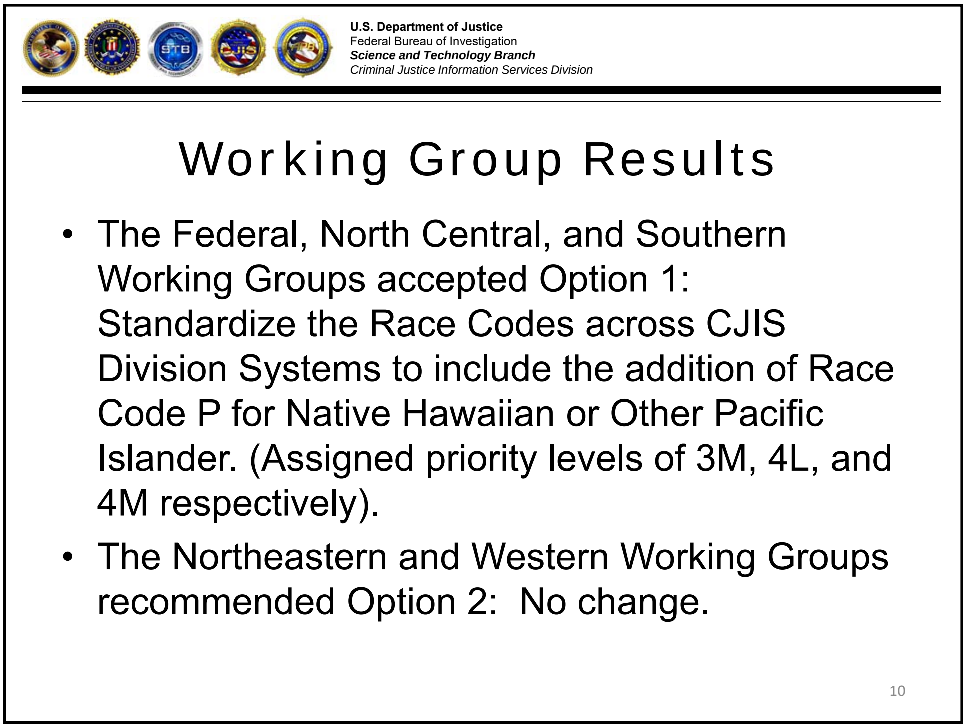
8



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Options Considered

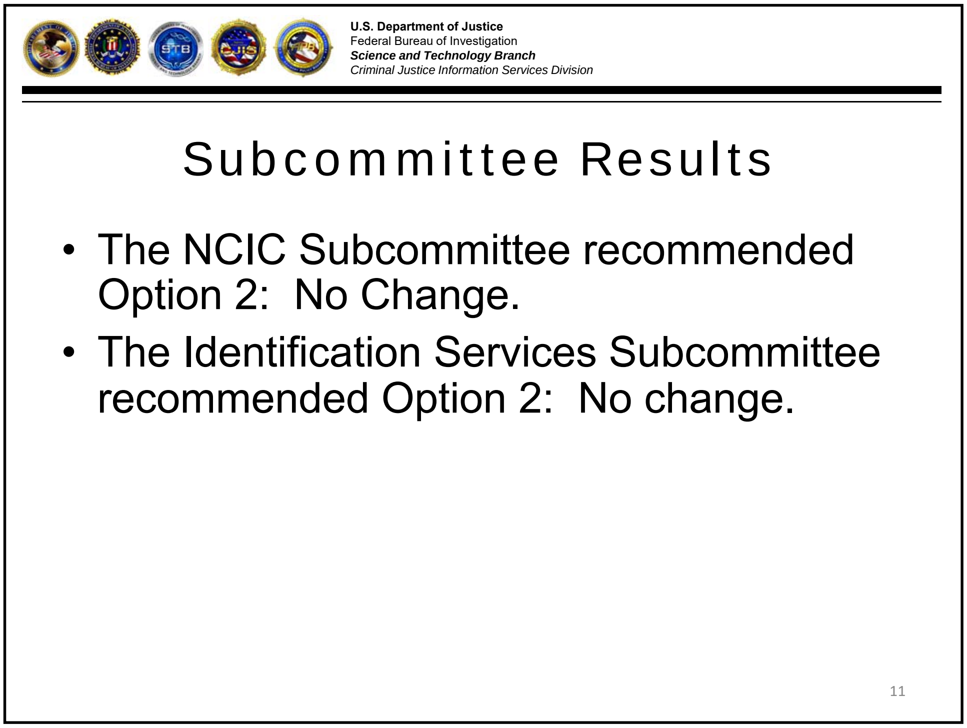
- Option 1: Standardize the Race Codes across CJIS Division Systems to include the addition of Race Code P for Native Hawaiian or Other Pacific Islander.
- Option 2: No change.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Working Group Results

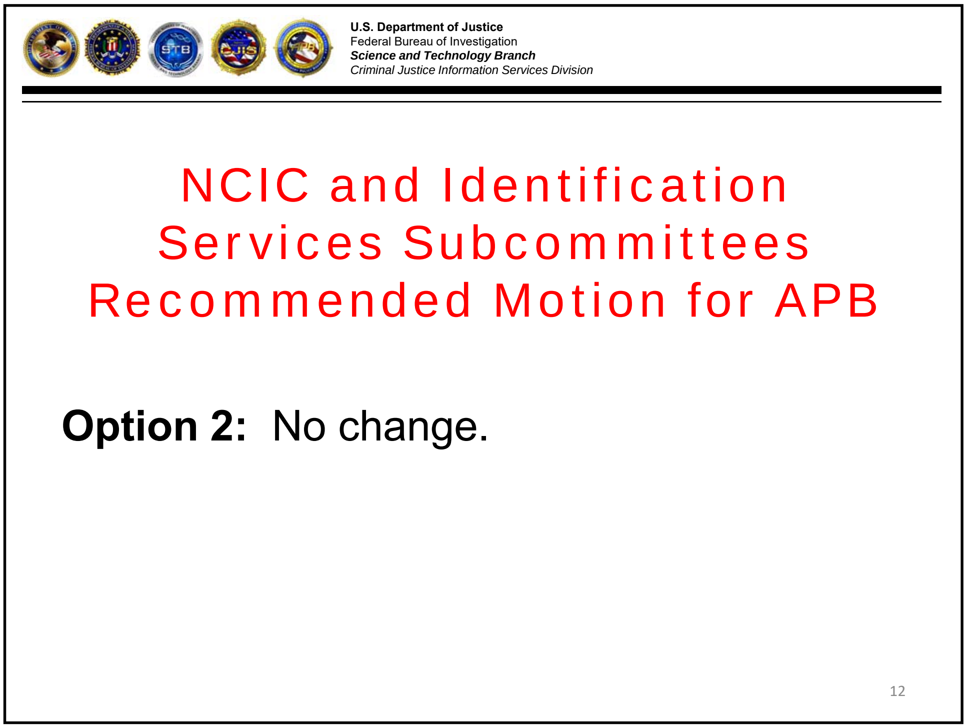
- The Federal, North Central, and Southern Working Groups accepted Option 1: Standardize the Race Codes across CJIS Division Systems to include the addition of Race Code P for Native Hawaiian or Other Pacific Islander. (Assigned priority levels of 3M, 4L, and 4M respectively).
- The Northeastern and Western Working Groups recommended Option 2: No change.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Subcommittee Results

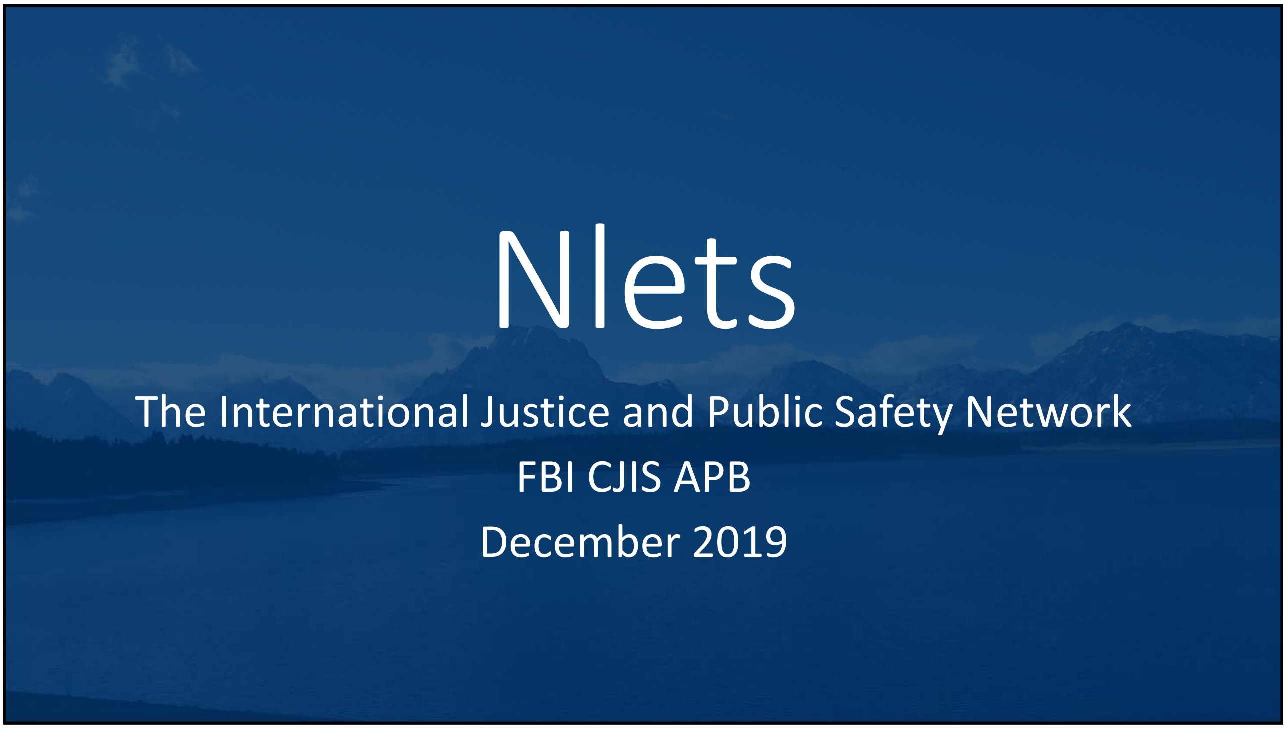
- The NCIC Subcommittee recommended Option 2: No Change.
- The Identification Services Subcommittee recommended Option 2: No change.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NCIC and Identification Services Subcommittees Recommended Motion for APB

Option 2: No change.



Nlets

The International Justice and Public Safety Network

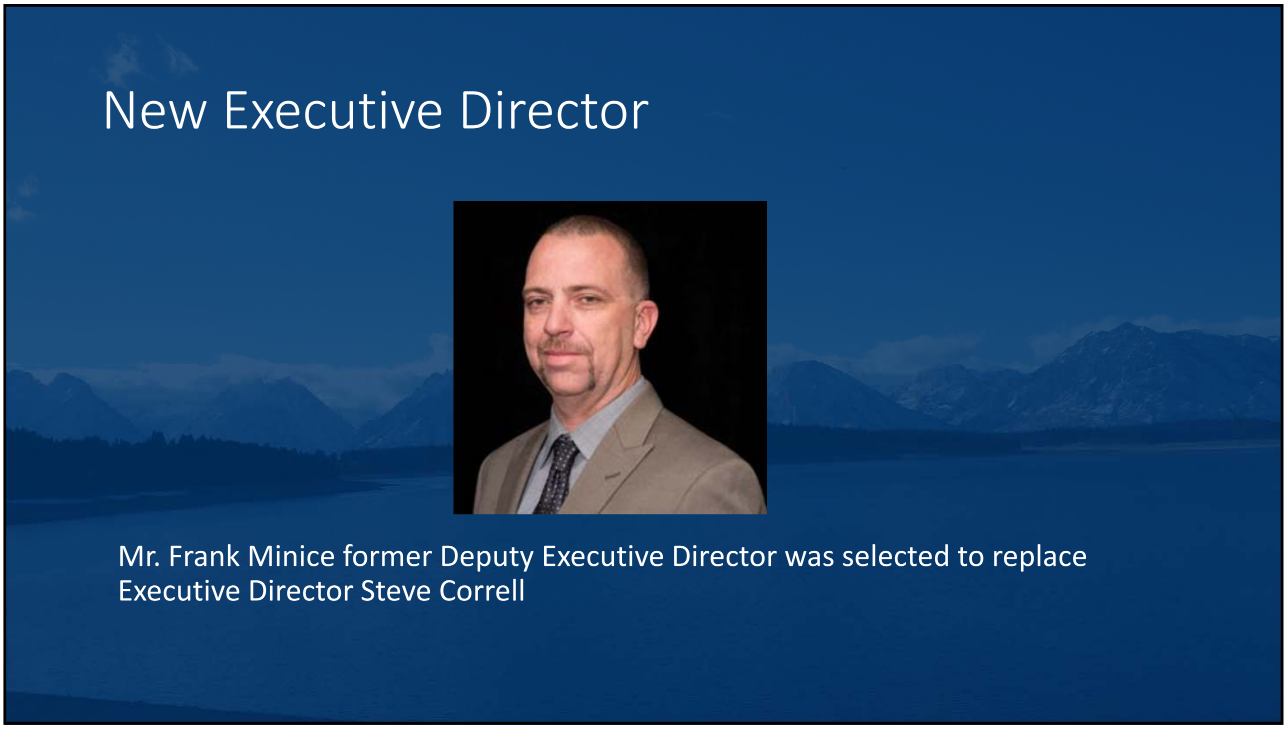
FBI CJIS APB

December 2019

Nlets – a 501(c)(3) corporation, owned by the States and Territories; Board of Directors:

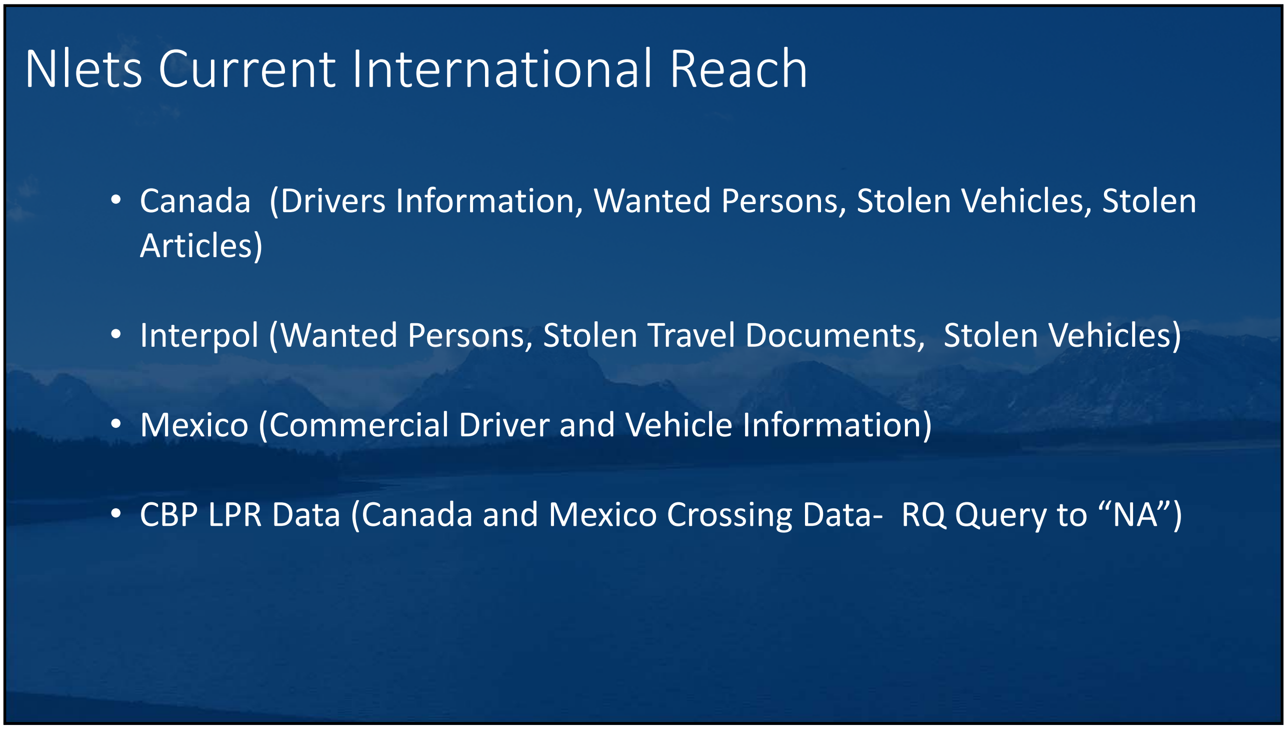
- Officers
  - Charles Schaeffer, Florida
    President
  - Wyatt Pettengill, North Carolina
    1st Vice President
  - Tim Struck, New Mexico
    2nd Vice President

- Board
  - Bill Guy, Rhode Island
  - Rachel VanDeusen, New York
  - Greg Meetze, South Carolina
  - Terri Fisher, Georgia
  - Dawn Brinningstaull, Michigan
  - Tom Prevo, Nebraska
  - Ted DeRosa, Colorado
  - Joe Guerrero, Guam
  - Frank Dubiel, USDOS



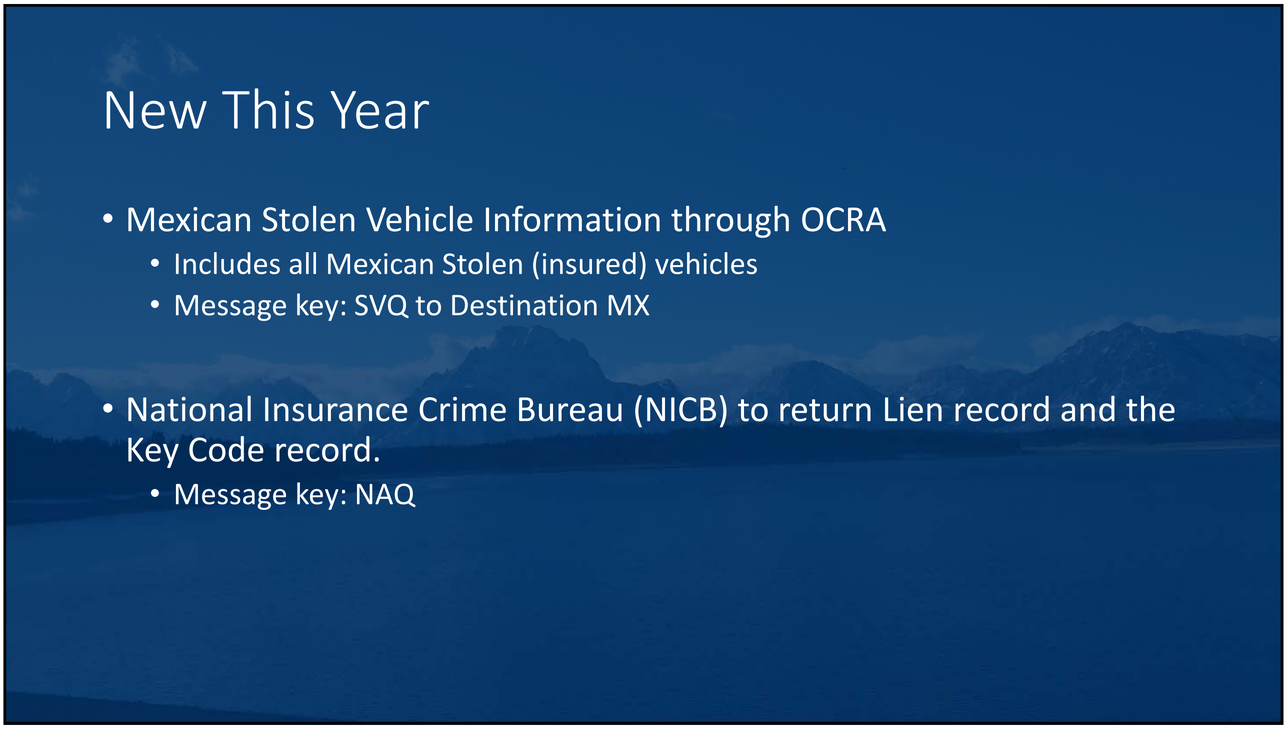
New Executive Director

Mr. Frank Minice former Deputy Executive Director was selected to replace Executive Director Steve Correll



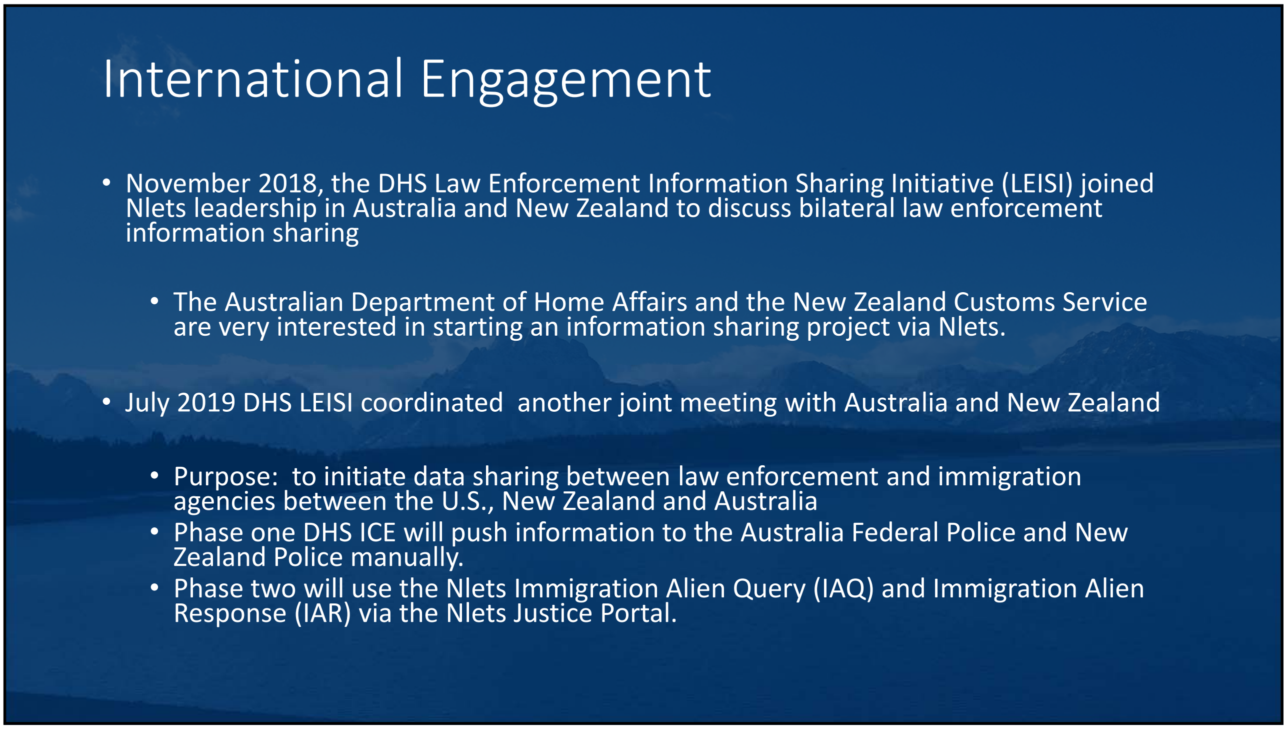
Nlets Current International Reach

- Canada (Drivers Information, Wanted Persons, Stolen Vehicles, Stolen Articles)
- Interpol (Wanted Persons, Stolen Travel Documents, Stolen Vehicles)
- Mexico (Commercial Driver and Vehicle Information)
- CBP LPR Data (Canada and Mexico Crossing Data- RQ Query to “NA”)



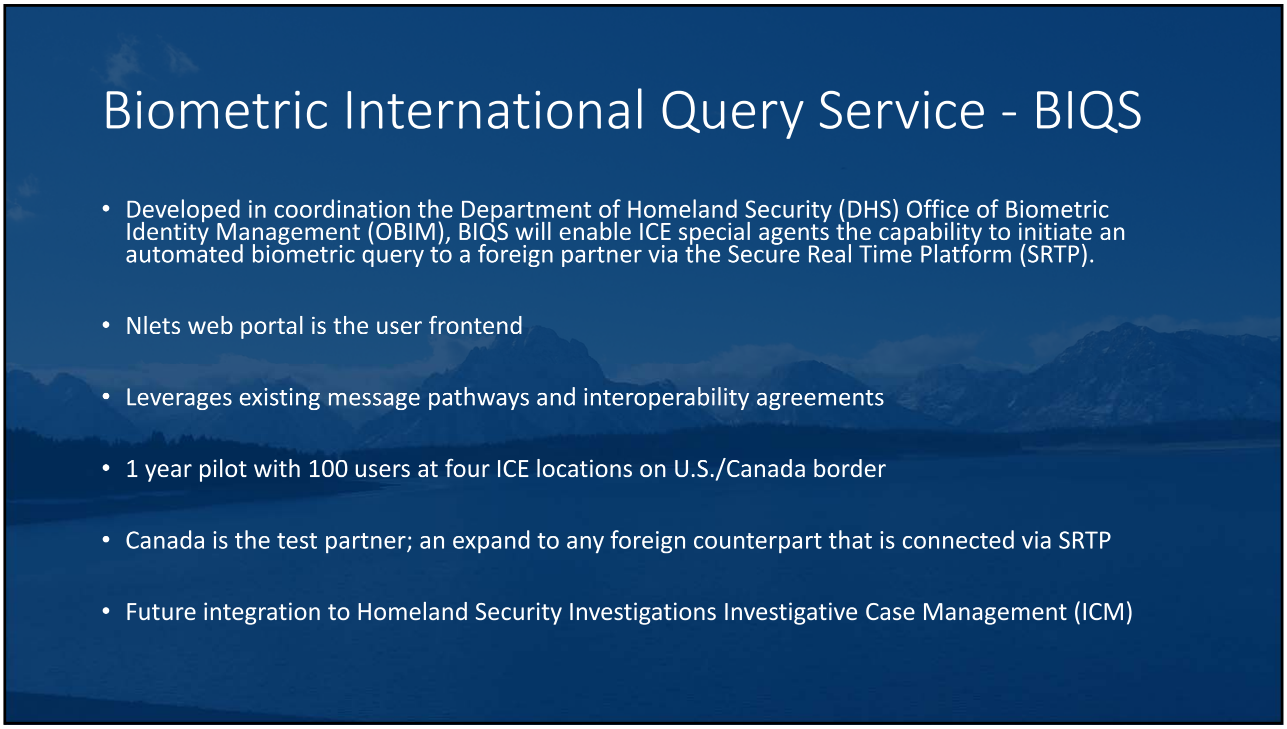
New This Year

- Mexican Stolen Vehicle Information through OCRA
  - Includes all Mexican Stolen (insured) vehicles
  - Message key: SVQ to Destination MX
- National Insurance Crime Bureau (NICB) to return Lien record and the Key Code record.
  - Message key: NAQ



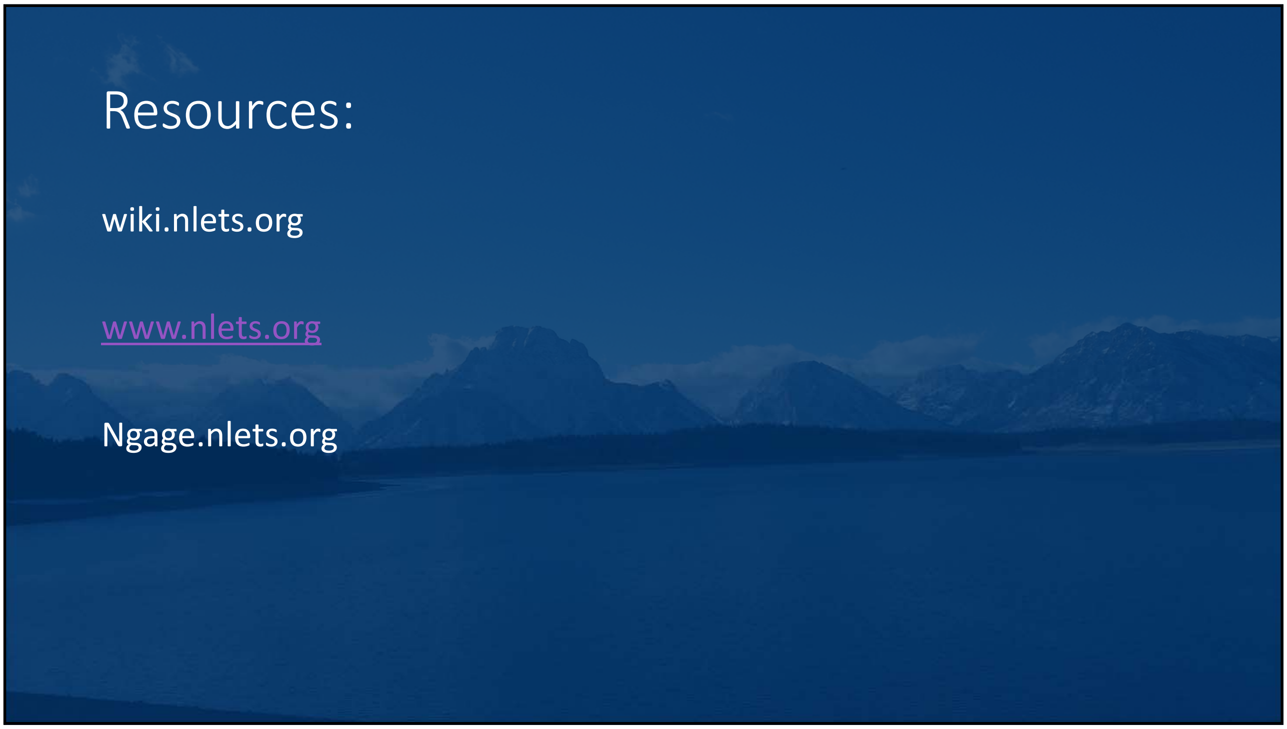
International Engagement

- November 2018, the DHS Law Enforcement Information Sharing Initiative (LEISI) joined Nlets leadership in Australia and New Zealand to discuss bilateral law enforcement information sharing
  - The Australian Department of Home Affairs and the New Zealand Customs Service are very interested in starting an information sharing project via Nlets.
- July 2019 DHS LEISI coordinated another joint meeting with Australia and New Zealand
  - Purpose: to initiate data sharing between law enforcement and immigration agencies between the U.S., New Zealand and Australia
  - Phase one DHS ICE will push information to the Australia Federal Police and New Zealand Police manually.
  - Phase two will use the Nlets Immigration Alien Query (IAQ) and Immigration Alien Response (IAR) via the Nlets Justice Portal.



Biometric International Query Service - BIQS

- Developed in coordination the Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM), BIQS will enable ICE special agents the capability to initiate an automated biometric query to a foreign partner via the Secure Real Time Platform (SRTP).
- Nlets web portal is the user frontend
- Leverages existing message pathways and interoperability agreements
- 1 year pilot with 100 users at four ICE locations on U.S./Canada border
- Canada is the test partner; an expand to any foreign counterpart that is connected via SRTP
- Future integration to Homeland Security Investigations Investigative Case Management (ICM)



Resources:

wiki.nlets.org

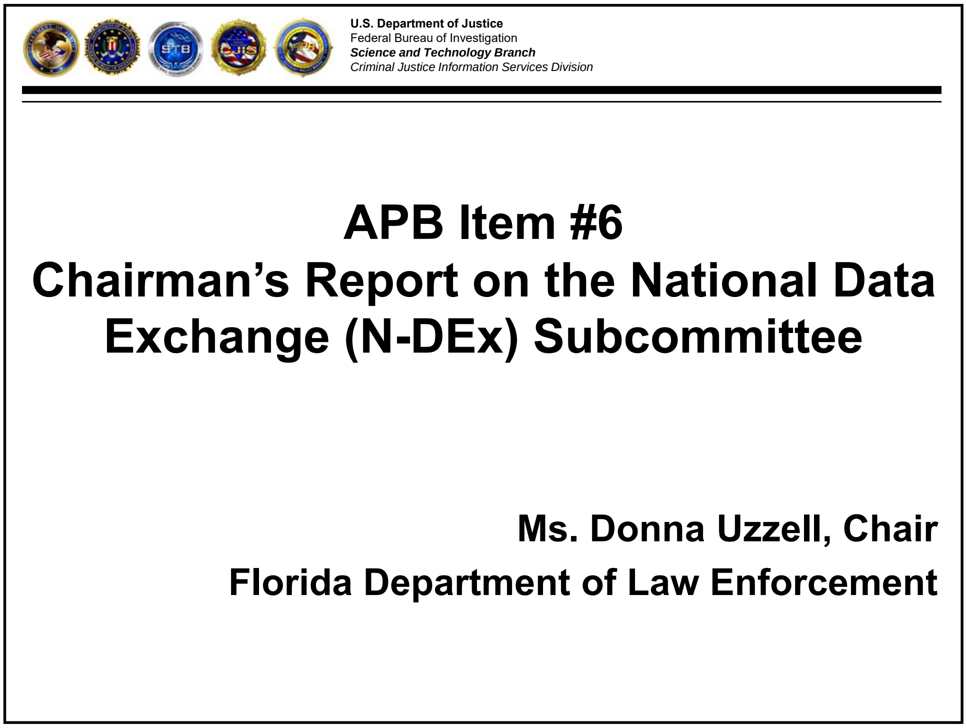
www.nlets.org

Ngage.nlets.org

Contact:

Charles.Schaeffer@nlets.org

Intentionally Left Blank

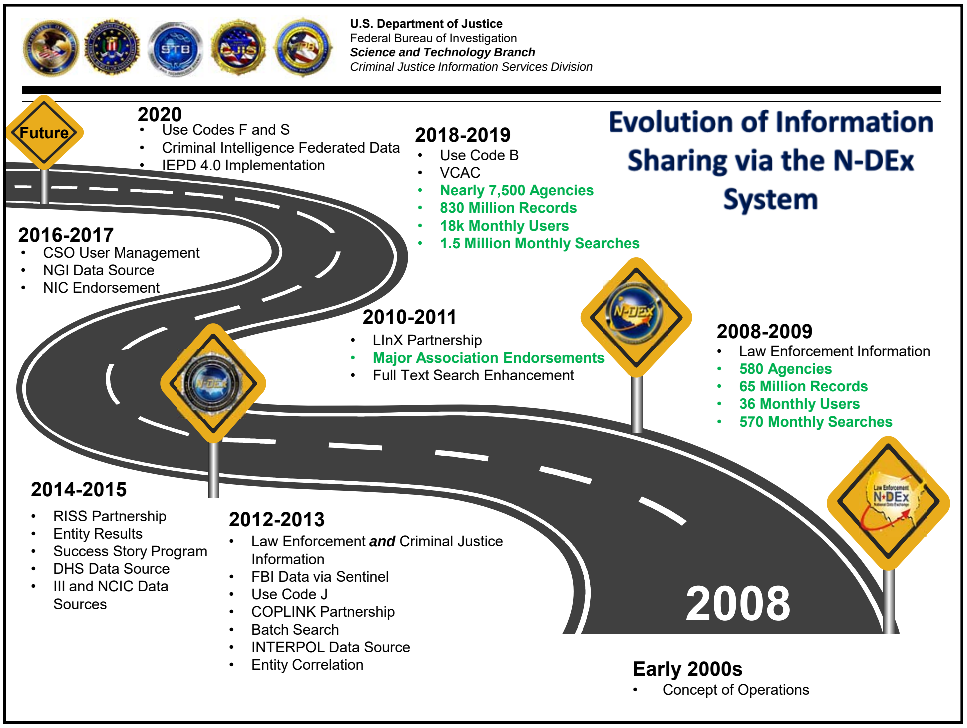


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB Item #6
Chairman's Report on the National Data Exchange (N-DEx) Subcommittee

Ms. Donna Uzzell, Chair

Florida Department of Law Enforcement



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Evolution of Information Sharing via the N-DEx System

2020
- Use Codes F and S
- Criminal Intelligence Federated Data
- IEPD 4.0 Implementation

2018-2019
- Use Code B
- VCAC
- **Nearly 7,500 Agencies**
- **830 Million Records**
- **18k Monthly Users**
- **1.5 Million Monthly Searches**

2016-2017
- CSO User Management
- NGI Data Source
- NIC Endorsement

2010-2011
- LInX Partnership
- **Major Association Endorsements**
- Full Text Search Enhancement

2008-2009
- Law Enforcement Information
- **580 Agencies**
- **65 Million Records**
- **36 Monthly Users**
- **570 Monthly Searches**

2014-2015
- RISS Partnership
- Entity Results
- Success Story Program
- DHS Data Source
- III and NCIC Data Sources

2012-2013
- Law Enforcement ***and*** Criminal Justice Information
- FBI Data via Sentinel
- Use Code J
- COPLINK Partnership
- Batch Search
- INTERPOL Data Source
- Entity Correlation

Early 2000s
- Concept of Operations

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N-DEx Issue # 1

N-DEx Program Status

Purpose:

The N-DEx Program Office presented an update on Program activities.

- N-DEx System Participation
- N-DEx System Technical Updates and Enhancements
- Brand Management
- 2019 Success Stories

Subcommittee Action:

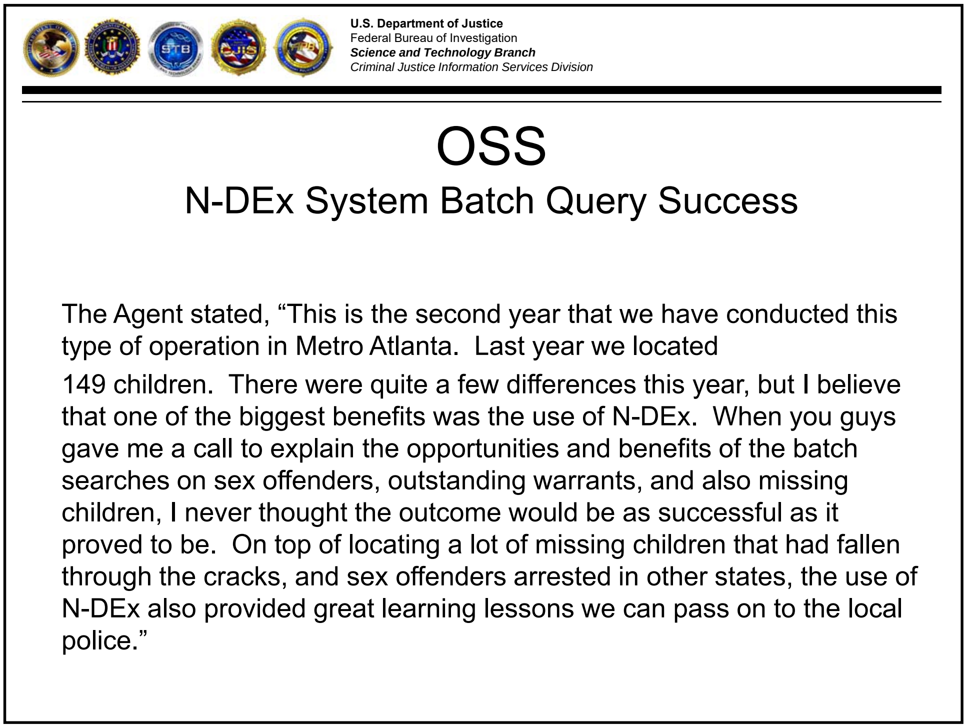
This issue was accepted for information only.

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Operation Safe Summer (OSS)

N-DEx System Batch Query Success

- FBI’s Metro Atlanta Child Exploitation and Human Trafficking (MATCH) task force.
- 27 federal, state, and local law enforcement agencies.
- The operation’s goal was to combat all forms of child exploitation and make the community safer for children heading into the summer months.
- 231 missing and/or exploited children located.
  - 14 missing children, as well as multiple sex offenders, were located due to information in the N-DEx System.



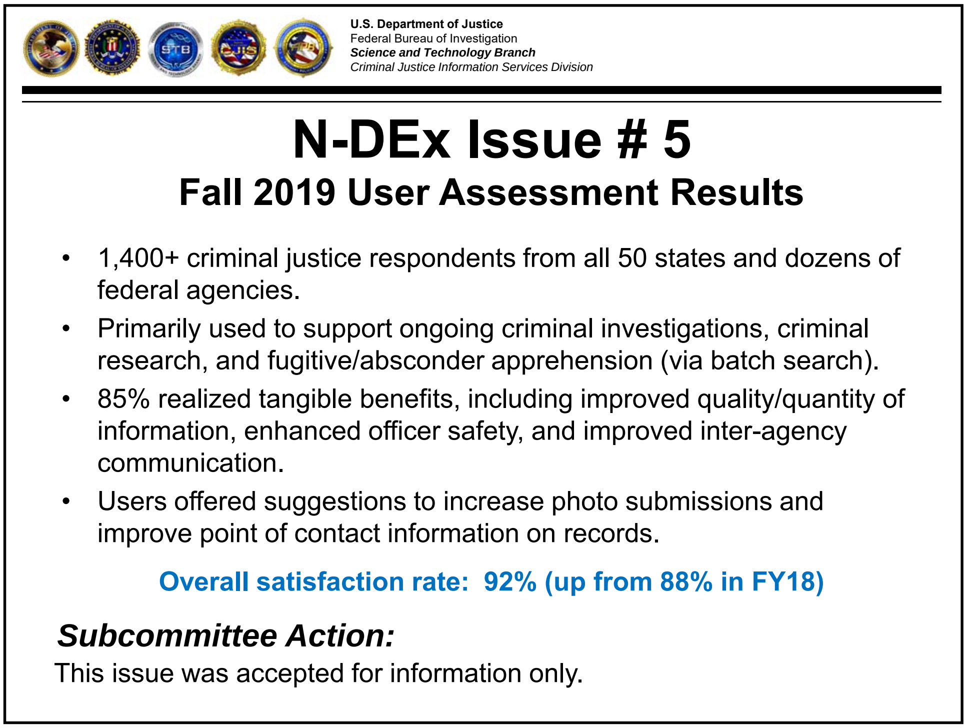
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

OSS

N-DEx System Batch Query Success

The Agent stated, “This is the second year that we have conducted this type of operation in Metro Atlanta. Last year we located

149 children. There were quite a few differences this year, but I believe that one of the biggest benefits was the use of N-DEx. When you guys gave me a call to explain the opportunities and benefits of the batch searches on sex offenders, outstanding warrants, and also missing children, I never thought the outcome would be as successful as it proved to be. On top of locating a lot of missing children that had fallen through the cracks, and sex offenders arrested in other states, the use of N-DEx also provided great learning lessons we can pass on to the local police.”



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N-DEx Issue # 5

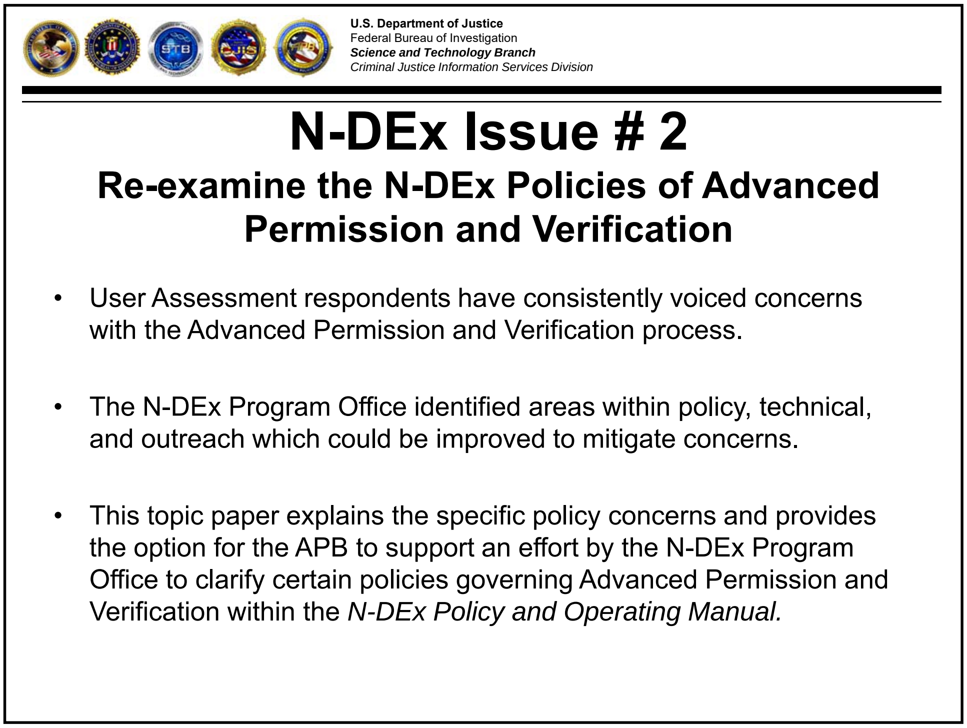
Fall 2019 User Assessment Results

- 1,400+ criminal justice respondents from all 50 states and dozens of federal agencies.
- Primarily used to support ongoing criminal investigations, criminal research, and fugitive/absconder apprehension (via batch search).
- 85% realized tangible benefits, including improved quality/quantity of information, enhanced officer safety, and improved inter-agency communication.
- Users offered suggestions to increase photo submissions and improve point of contact information on records.

Overall satisfaction rate: 92% (up from 88% in FY18)

Subcommittee Action:

This issue was accepted for information only.

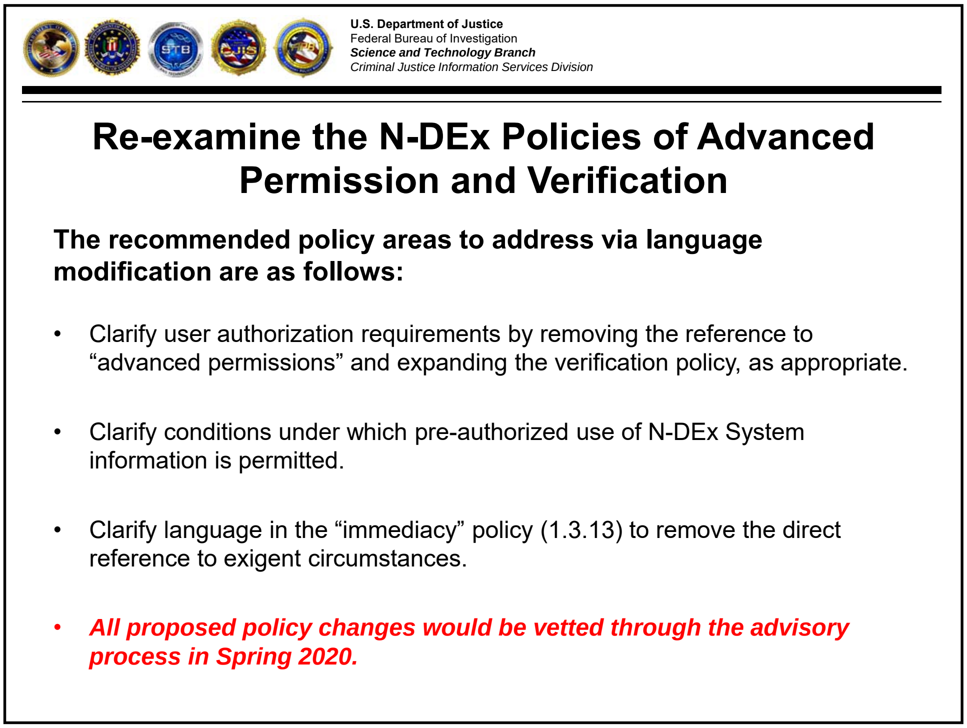


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N-DEx Issue # 2

Re-examine the N-DEx Policies of Advanced Permission and Verification

- User Assessment respondents have consistently voiced concerns with the Advanced Permission and Verification process.
- The N-DEx Program Office identified areas within policy, technical, and outreach which could be improved to mitigate concerns.
- This topic paper explains the specific policy concerns and provides the option for the APB to support an effort by the N-DEx Program Office to clarify certain policies governing Advanced Permission and Verification within the *N-DEx Policy and Operating Manual.*

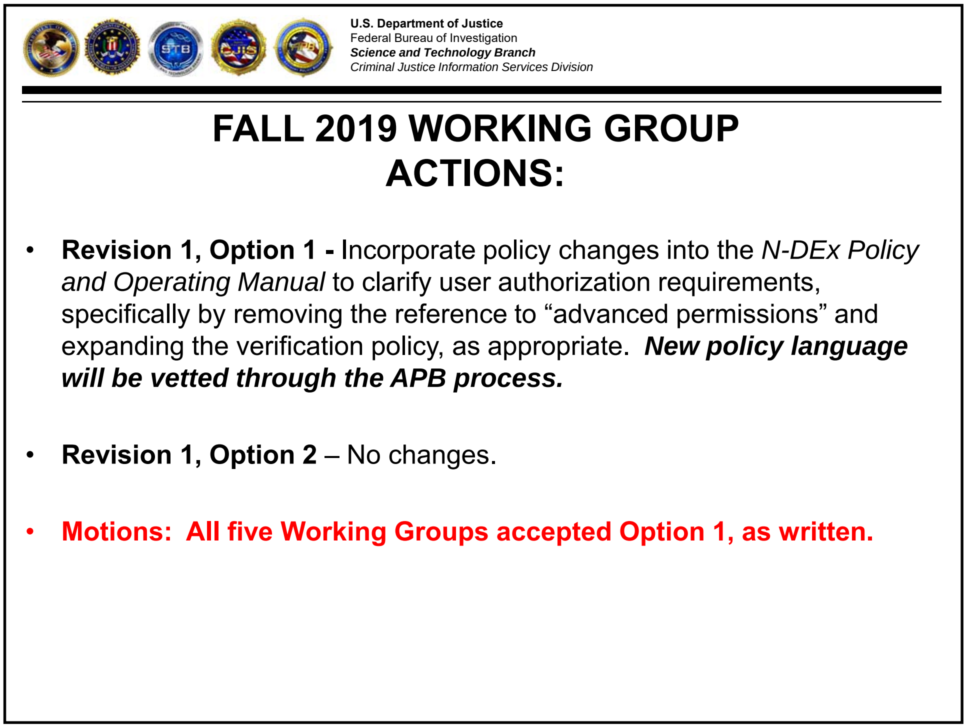


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Re-examine the N-DEx Policies of Advanced Permission and Verification

The recommended policy areas to address via language modification are as follows:

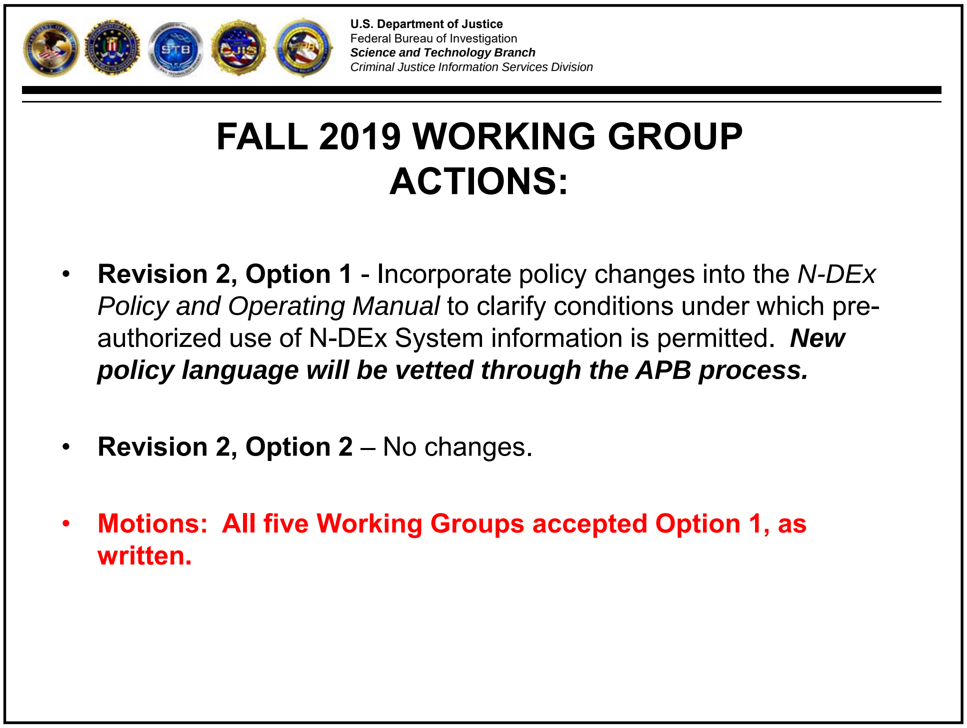
- Clarify user authorization requirements by removing the reference to “advanced permissions” and expanding the verification policy, as appropriate.
- Clarify conditions under which pre-authorized use of N-DEx System information is permitted.
- Clarify language in the “immediacy” policy (1.3.13) to remove the direct reference to exigent circumstances.
- ***All proposed policy changes would be vetted through the advisory process in Spring 2020.***



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

FALL 2019 WORKING GROUP ACTIONS:

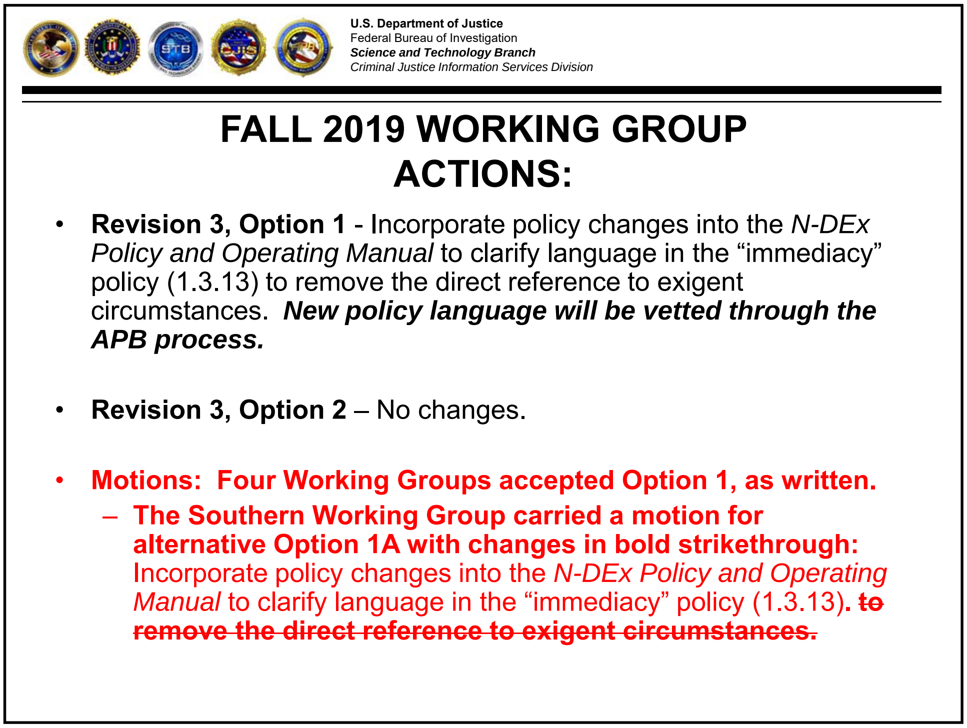
- **Revision 1, Option 1 -** Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate. ***New policy language will be vetted through the APB process.***
- **Revision 1, Option 2** – No changes.
- **Motions: All five Working Groups accepted Option 1, as written.**



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

FALL 2019 WORKING GROUP ACTIONS:

- **Revision 2, Option 1** - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of N-DEx System information is permitted. ***New policy language will be vetted through the APB process.***
- **Revision 2, Option 2** – No changes.
- **Motions: All five Working Groups accepted Option 1, as written.**



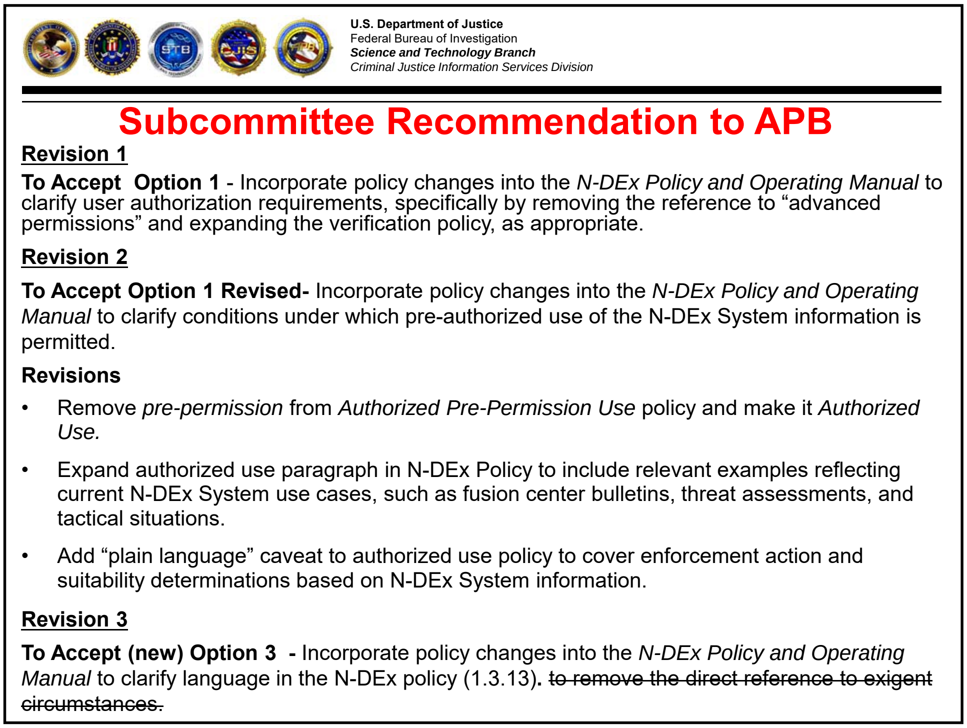
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

FALL 2019 WORKING GROUP ACTIONS:

- **Revision 3, Option 1** - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the "immediacy" policy (1.3.13) to remove the direct reference to exigent circumstances. ***New policy language will be vetted through the APB process.***

- **Revision 3, Option 2** – No changes.

- **Motions: Four Working Groups accepted Option 1, as written.**
  - **The Southern Working Group carried a motion for alternative Option 1A with changes in bold strikethrough:** Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the "immediacy" policy (1.3.13)**.** **~~to remove the direct reference to exigent circumstances.~~**



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Subcommittee Recommendation to APB

Revision 1

To Accept Option 1 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify user authorization requirements, specifically by removing the reference to "advanced permissions" and expanding the verification policy, as appropriate.

Revision 2

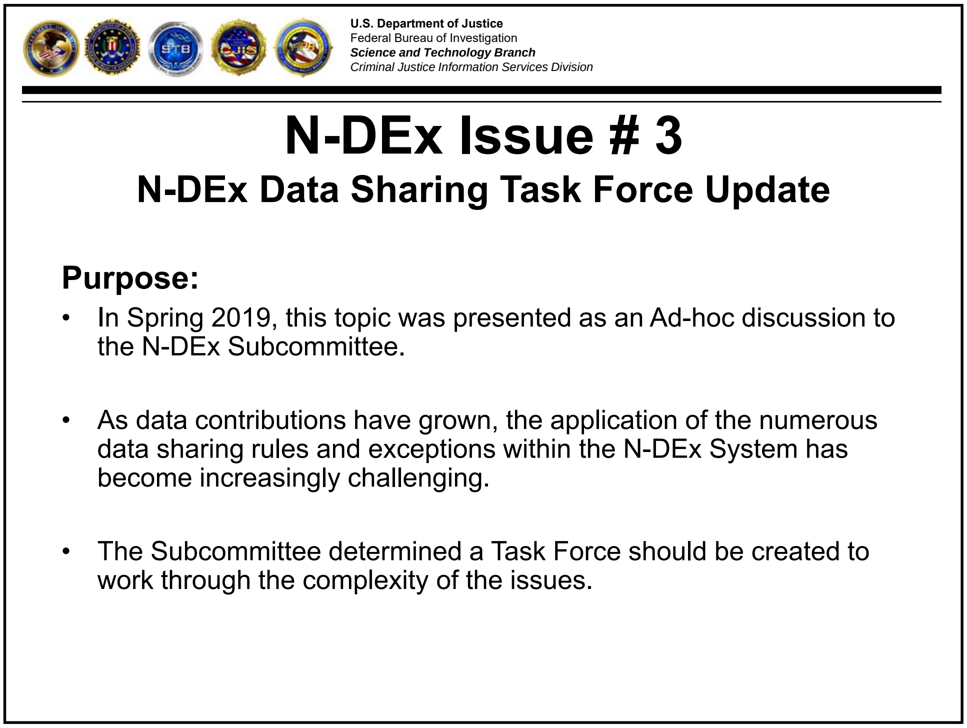
To Accept Option 1 Revised- Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify conditions under which pre-authorized use of the N-DEx System information is permitted.

Revisions

- Remove *pre-permission* from *Authorized Pre-Permission Use* policy and make it *Authorized Use.*
- Expand authorized use paragraph in N-DEx Policy to include relevant examples reflecting current N-DEx System use cases, such as fusion center bulletins, threat assessments, and tactical situations.
- Add "plain language" caveat to authorized use policy to cover enforcement action and suitability determinations based on N-DEx System information.

Revision 3

To Accept (new) Option 3 - Incorporate policy changes into the *N-DEx Policy and Operating Manual* to clarify language in the N-DEx policy (1.3.13)**.** ~~to remove the direct reference to exigent circumstances.~~



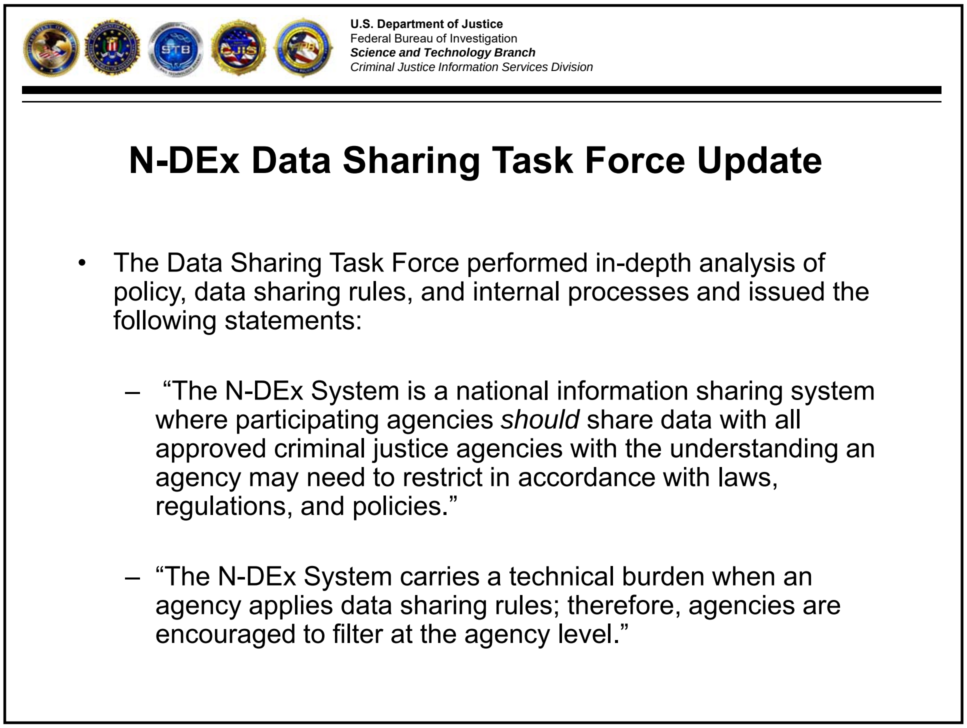
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N-DEx Issue # 3

N-DEx Data Sharing Task Force Update

Purpose:

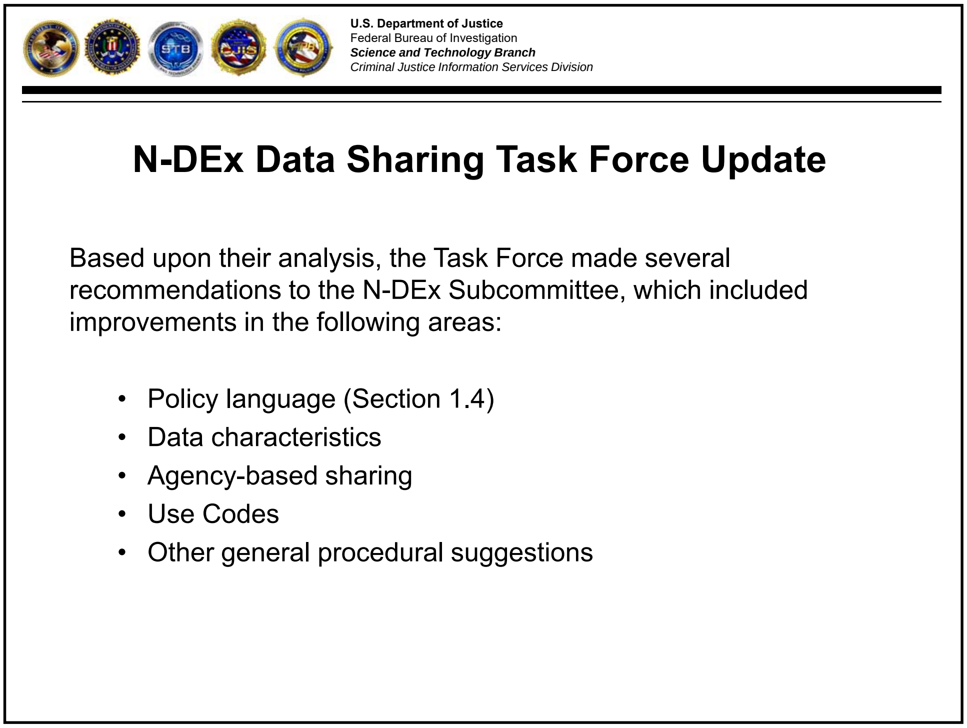
- In Spring 2019, this topic was presented as an Ad-hoc discussion to the N-DEx Subcommittee.
- As data contributions have grown, the application of the numerous data sharing rules and exceptions within the N-DEx System has become increasingly challenging.
- The Subcommittee determined a Task Force should be created to work through the complexity of the issues.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N-DEx Data Sharing Task Force Update

- The Data Sharing Task Force performed in-depth analysis of policy, data sharing rules, and internal processes and issued the following statements:
  - "The N-DEx System is a national information sharing system where participating agencies *should* share data with all approved criminal justice agencies with the understanding an agency may need to restrict in accordance with laws, regulations, and policies."
  - "The N-DEx System carries a technical burden when an agency applies data sharing rules; therefore, agencies are encouraged to filter at the agency level."

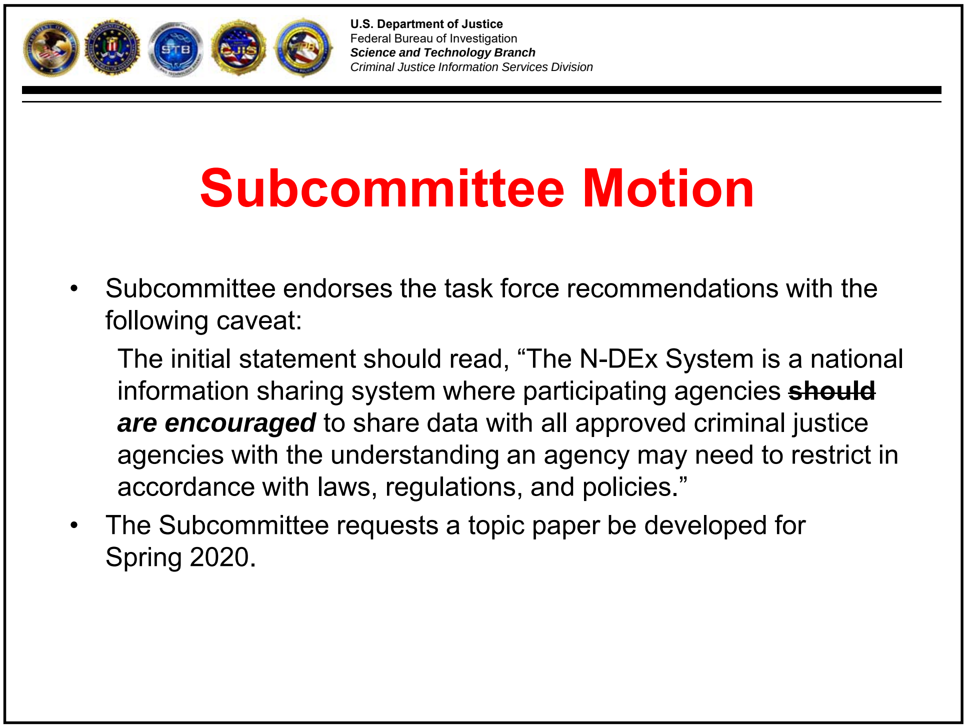


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

N-DEx Data Sharing Task Force Update

Based upon their analysis, the Task Force made several recommendations to the N-DEx Subcommittee, which included improvements in the following areas:

- Policy language (Section 1.4)
- Data characteristics
- Agency-based sharing
- Use Codes
- Other general procedural suggestions

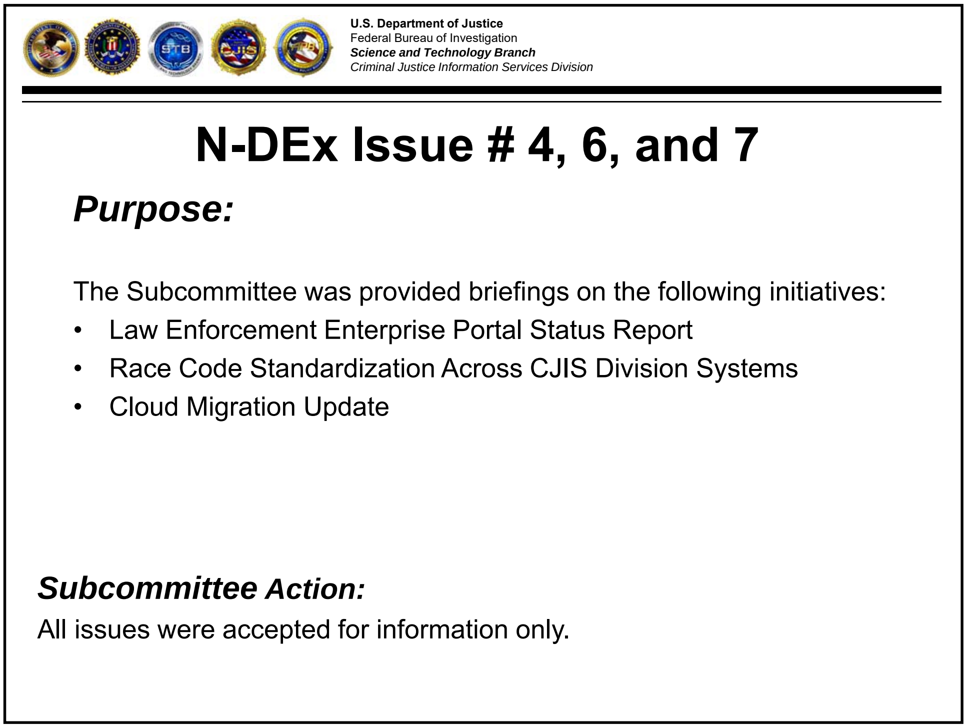


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Subcommittee Motion

- Subcommittee endorses the task force recommendations with the following caveat:

  The initial statement should read, “The N-DEx System is a national information sharing system where participating agencies ~~**should**~~ ***are encouraged*** to share data with all approved criminal justice agencies with the understanding an agency may need to restrict in accordance with laws, regulations, and policies.”
- The Subcommittee requests a topic paper be developed for Spring 2020.



N-DEx Issue # 4, 6, and 7

Purpose:

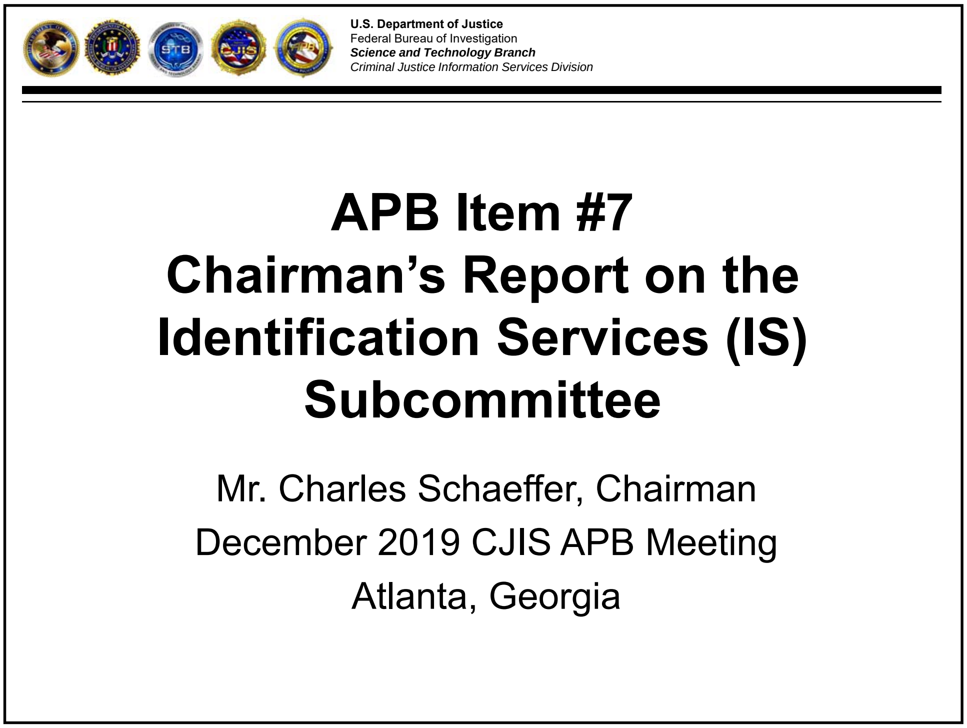
The Subcommittee was provided briefings on the following initiatives:

- Law Enforcement Enterprise Portal Status Report
- Race Code Standardization Across CJIS Division Systems
- Cloud Migration Update

Subcommittee Action:

All issues were accepted for information only.

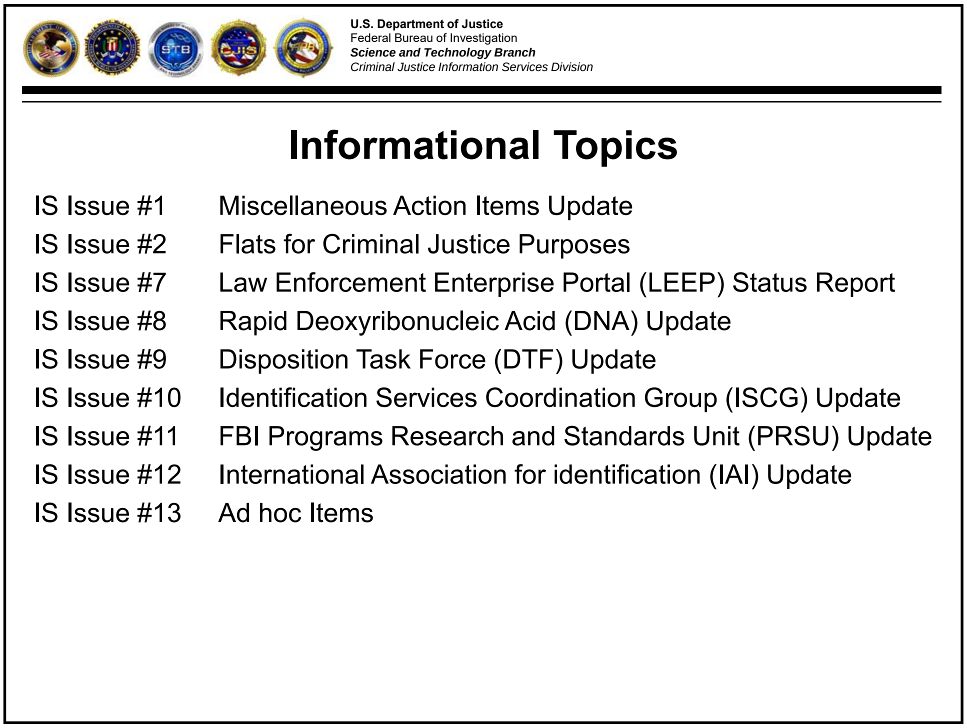
Intentionally Left Blank



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB Item #7 Chairman's Report on the Identification Services (IS) Subcommittee

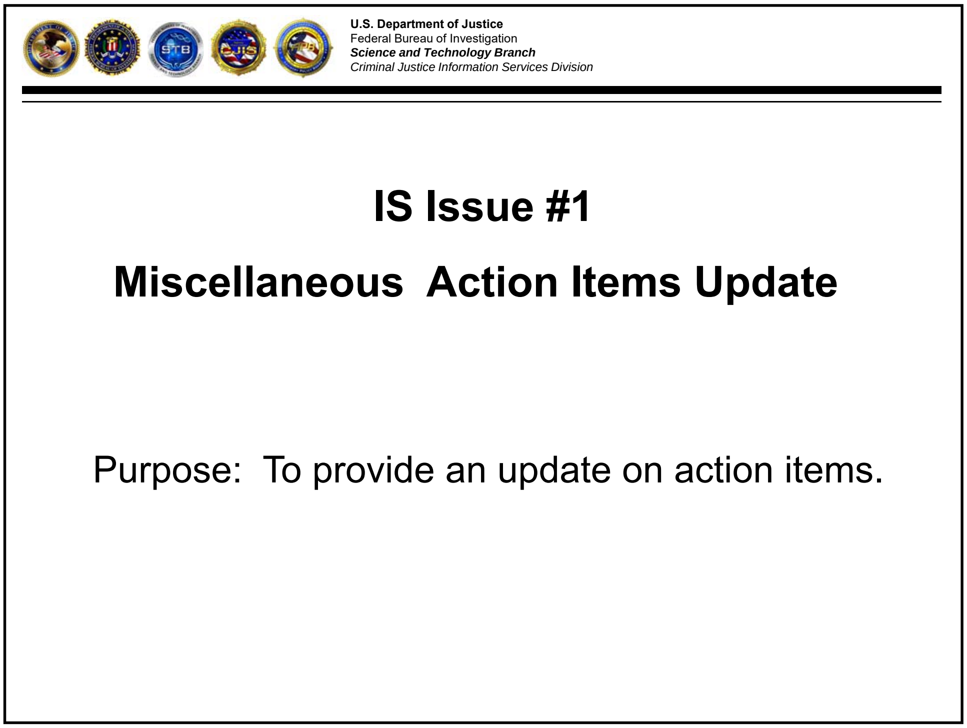
Mr. Charles Schaeffer, Chairman
December 2019 CJIS APB Meeting
Atlanta, Georgia



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Informational Topics

IS Issue #1	Miscellaneous Action Items Update
IS Issue #2	Flats for Criminal Justice Purposes
IS Issue #7	Law Enforcement Enterprise Portal (LEEP) Status Report
IS Issue #8	Rapid Deoxyribonucleic Acid (DNA) Update
IS Issue #9	Disposition Task Force (DTF) Update
IS Issue #10	Identification Services Coordination Group (ISCG) Update
IS Issue #11	FBI Programs Research and Standards Unit (PRSU) Update
IS Issue #12	International Association for identification (IAI) Update
IS Issue #13	Ad hoc Items

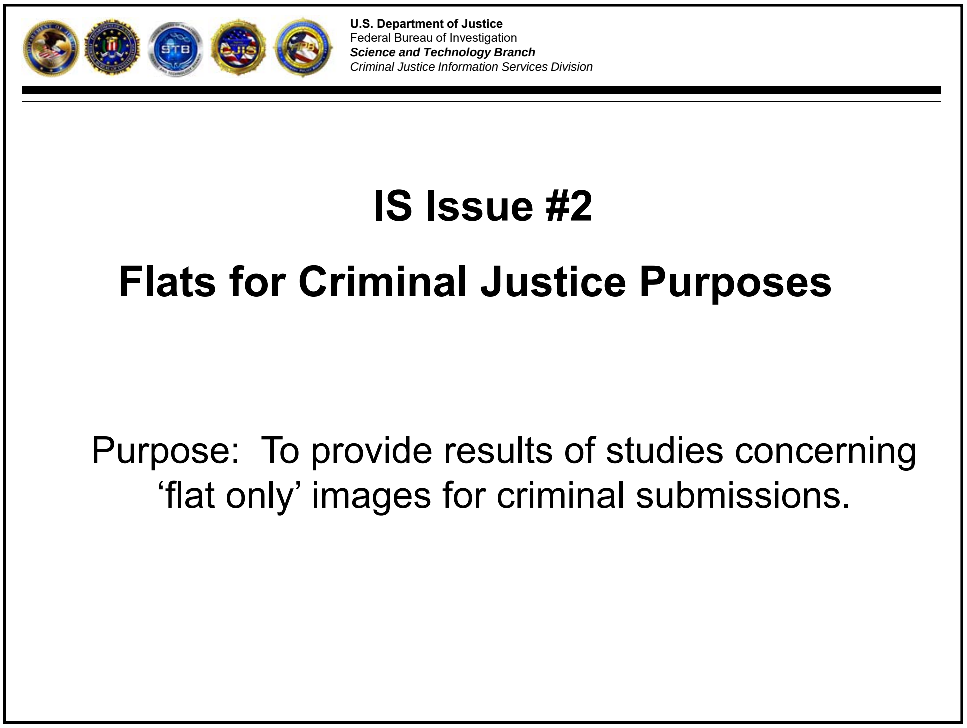


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #1

Miscellaneous Action Items Update

Purpose: To provide an update on action items.

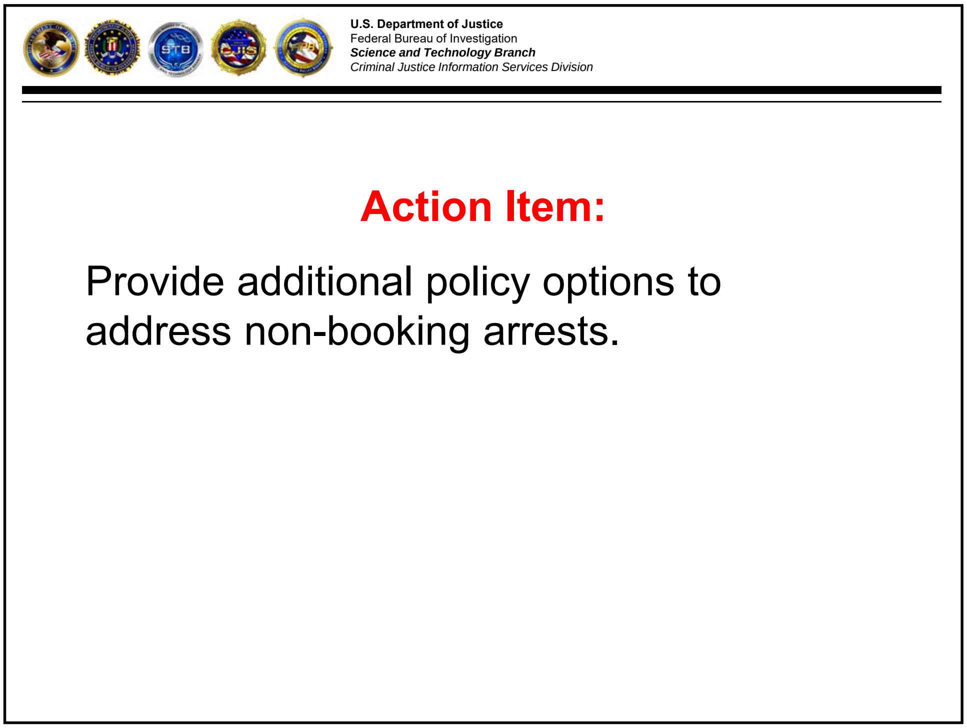


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #2

Flats for Criminal Justice Purposes

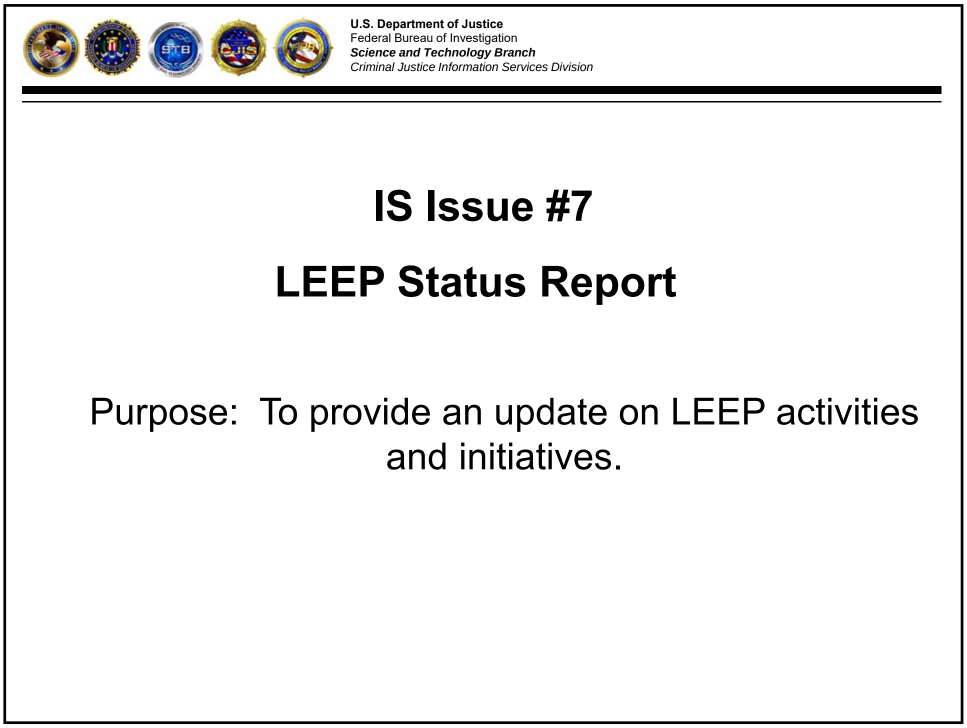
Purpose: To provide results of studies concerning ‘flat only’ images for criminal submissions.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Action Item:

Provide additional policy options to address non-booking arrests.

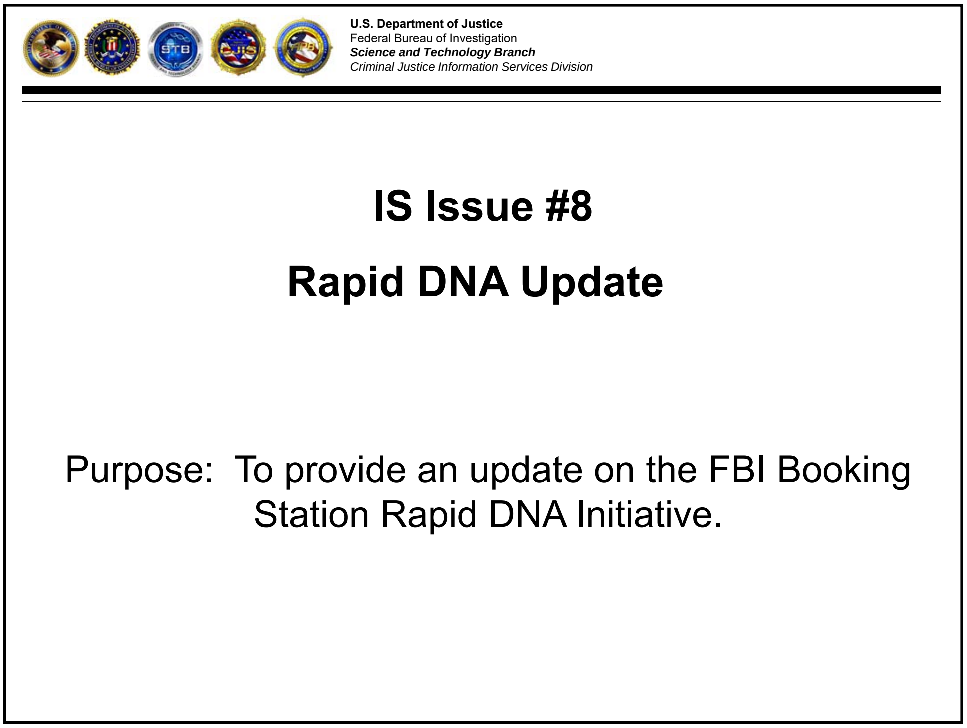


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #7

LEEP Status Report

Purpose: To provide an update on LEEP activities and initiatives.

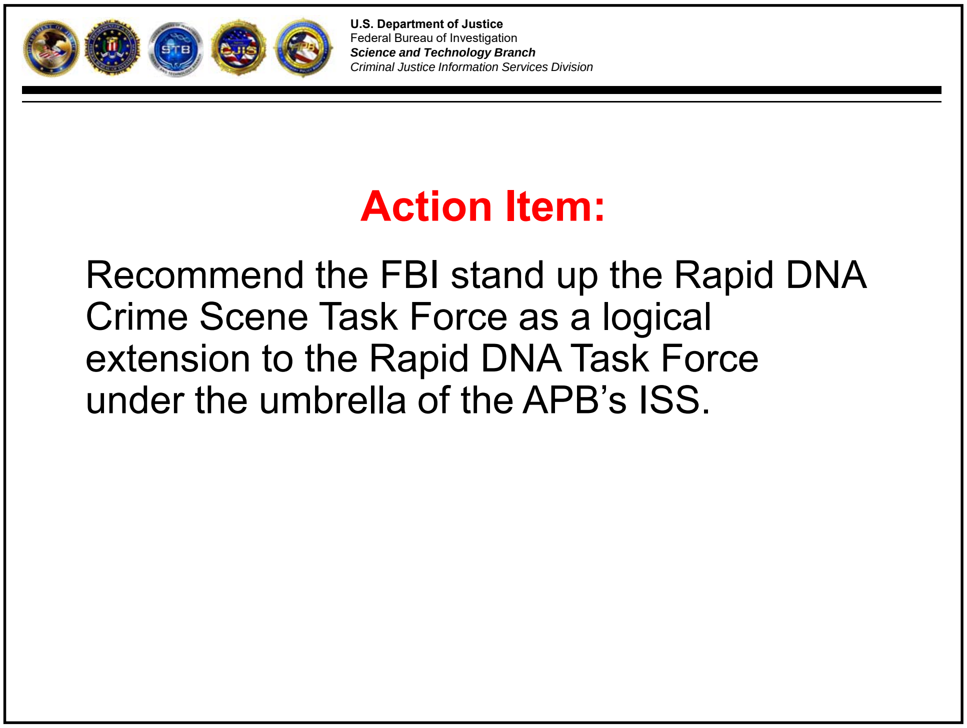


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #8

Rapid DNA Update

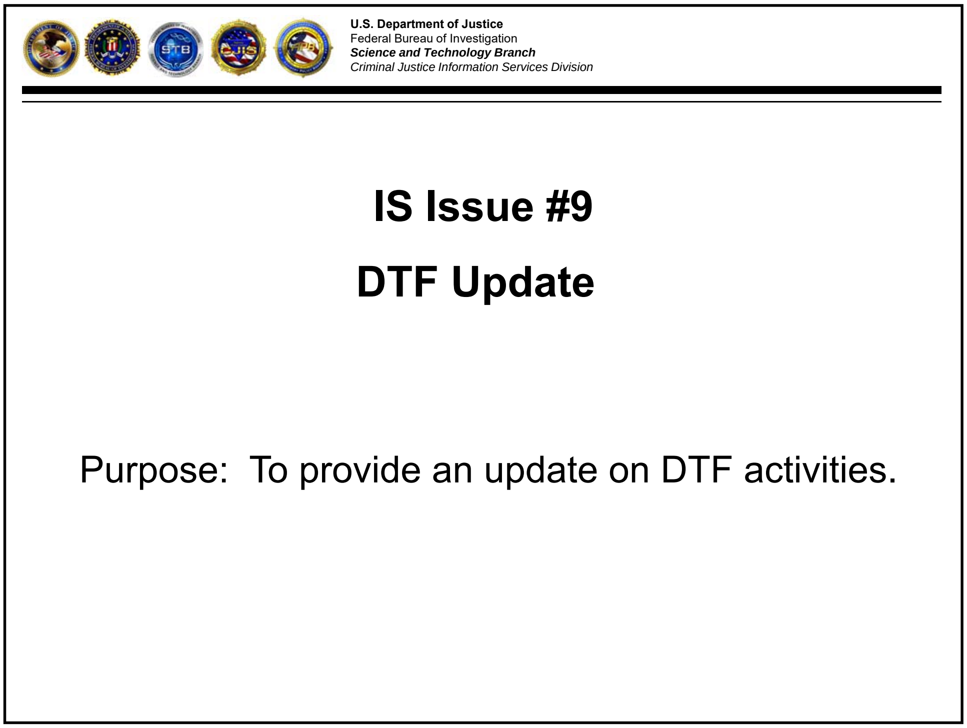
Purpose: To provide an update on the FBI Booking Station Rapid DNA Initiative.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Action Item:

Recommend the FBI stand up the Rapid DNA Crime Scene Task Force as a logical extension to the Rapid DNA Task Force under the umbrella of the APB's ISS.

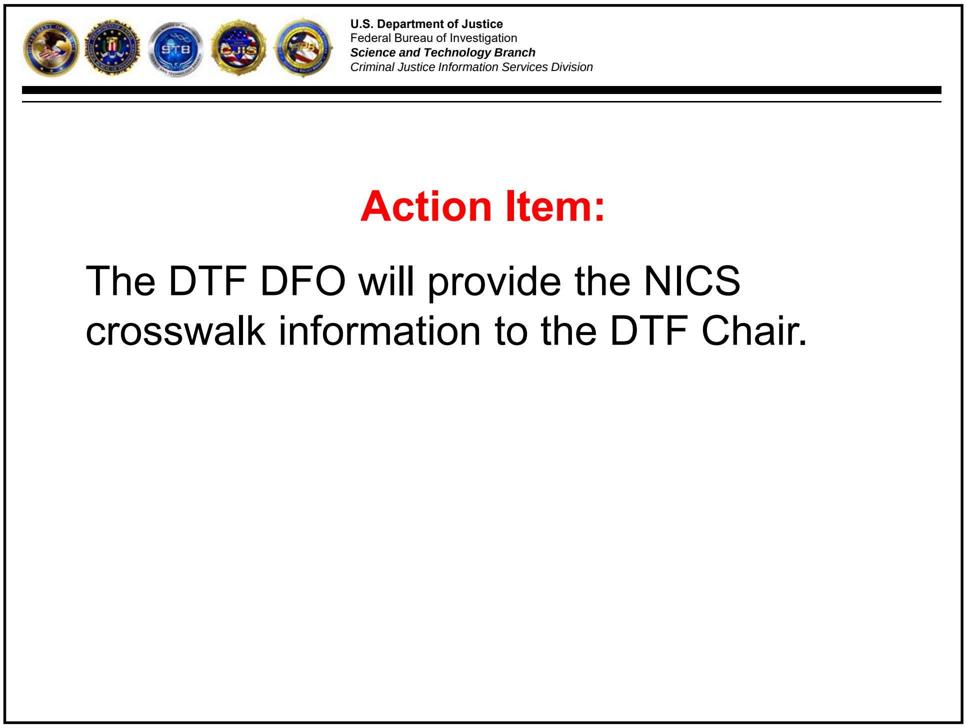


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #9

DTF Update

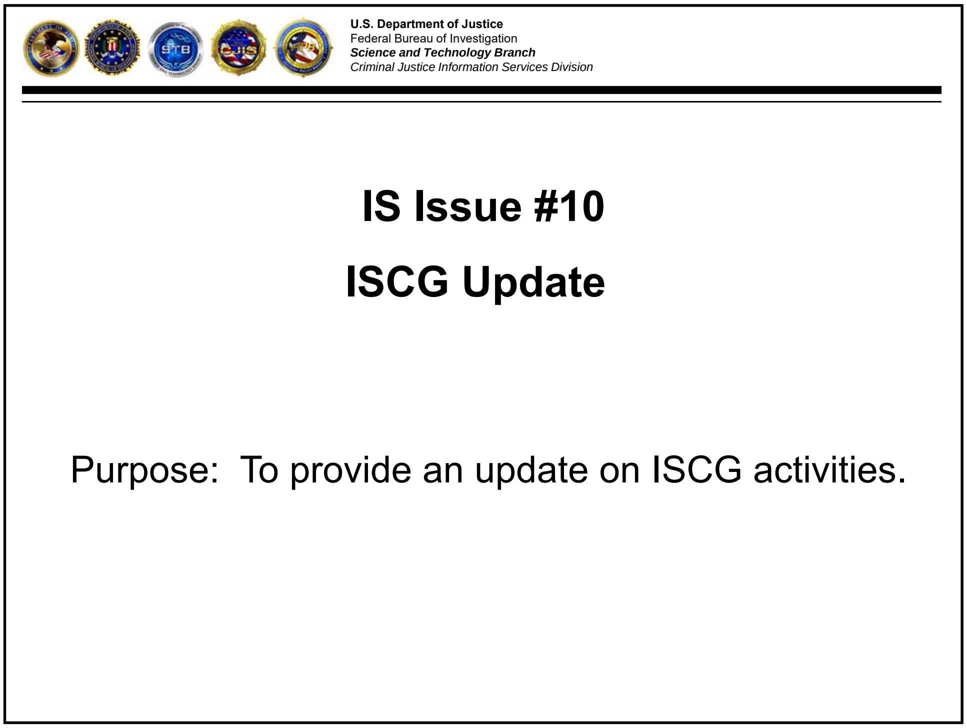
Purpose: To provide an update on DTF activities.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Action Item:

The DTF DFO will provide the NICS crosswalk information to the DTF Chair.

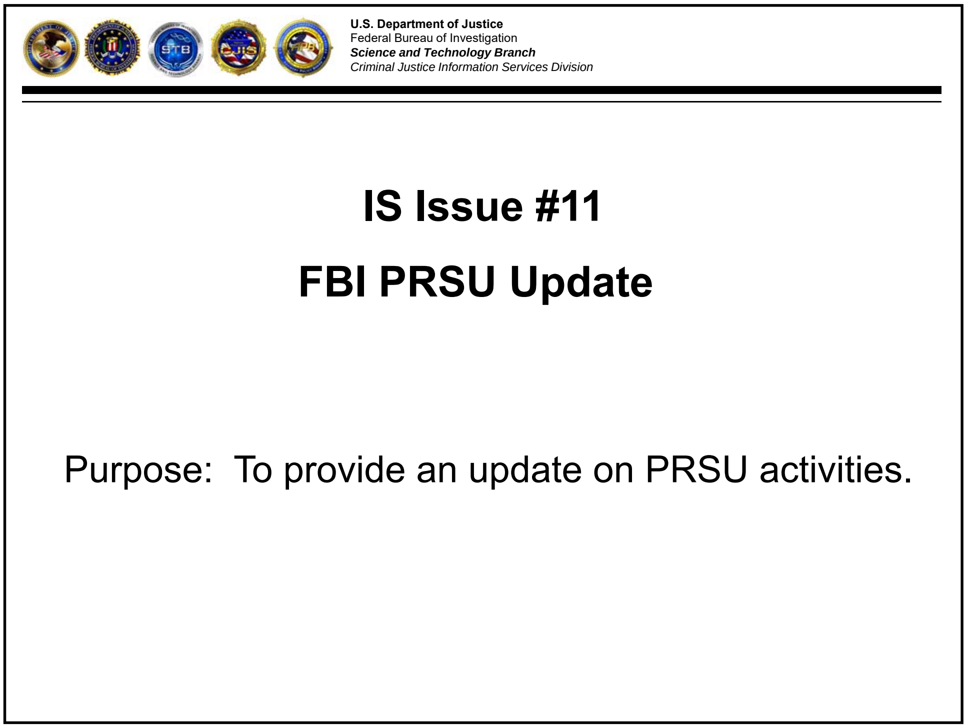


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #10

ISCG Update

Purpose: To provide an update on ISCG activities.

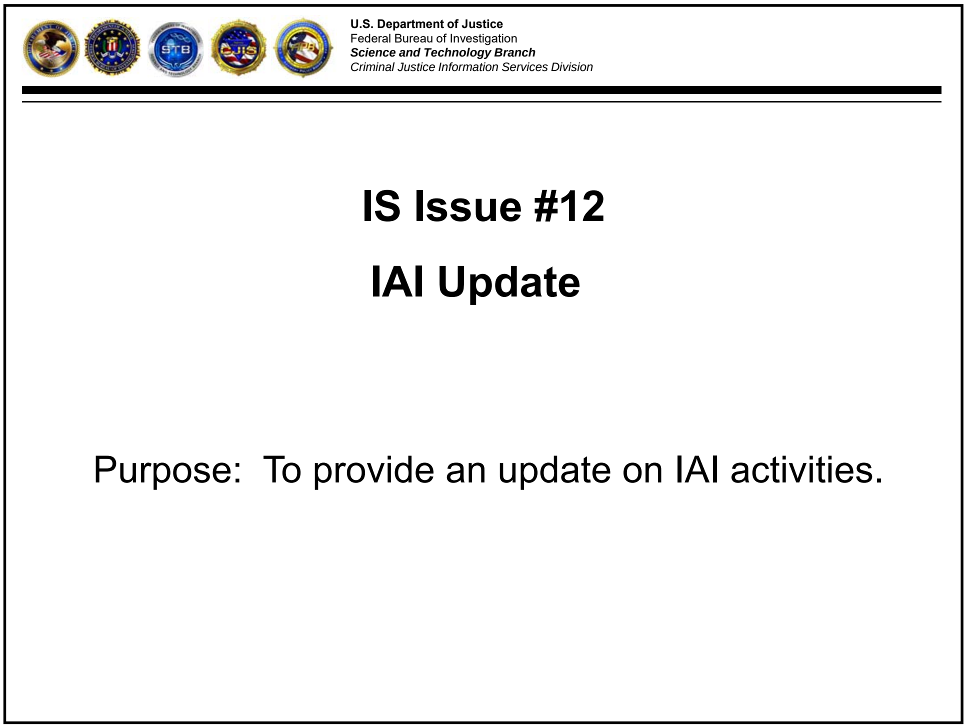


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #11

FBI PRSU Update

Purpose: To provide an update on PRSU activities.

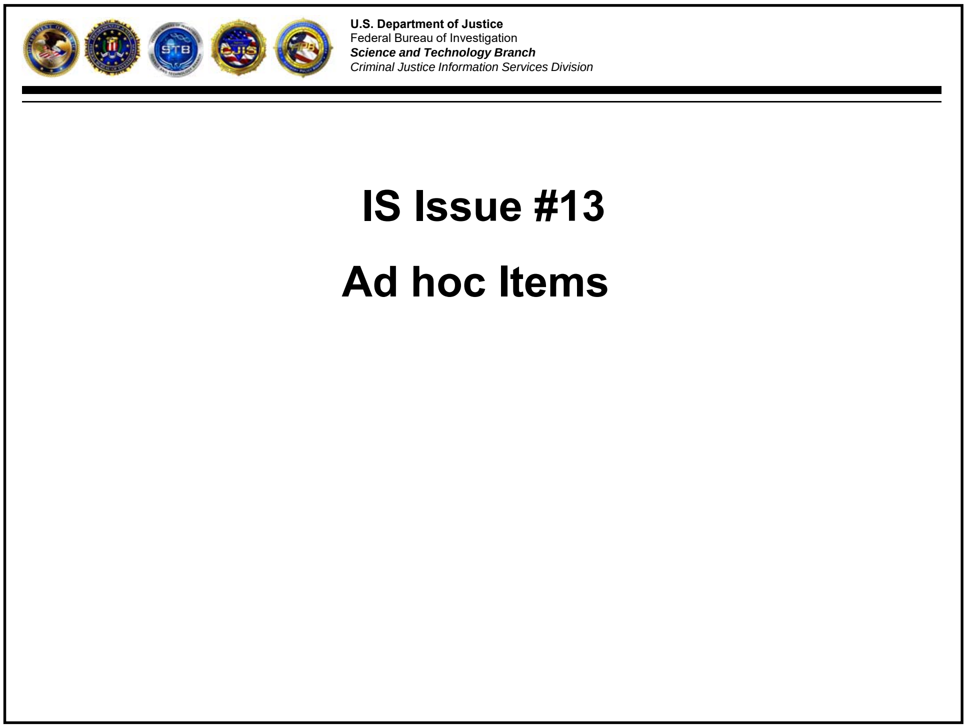


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #12

IAI Update

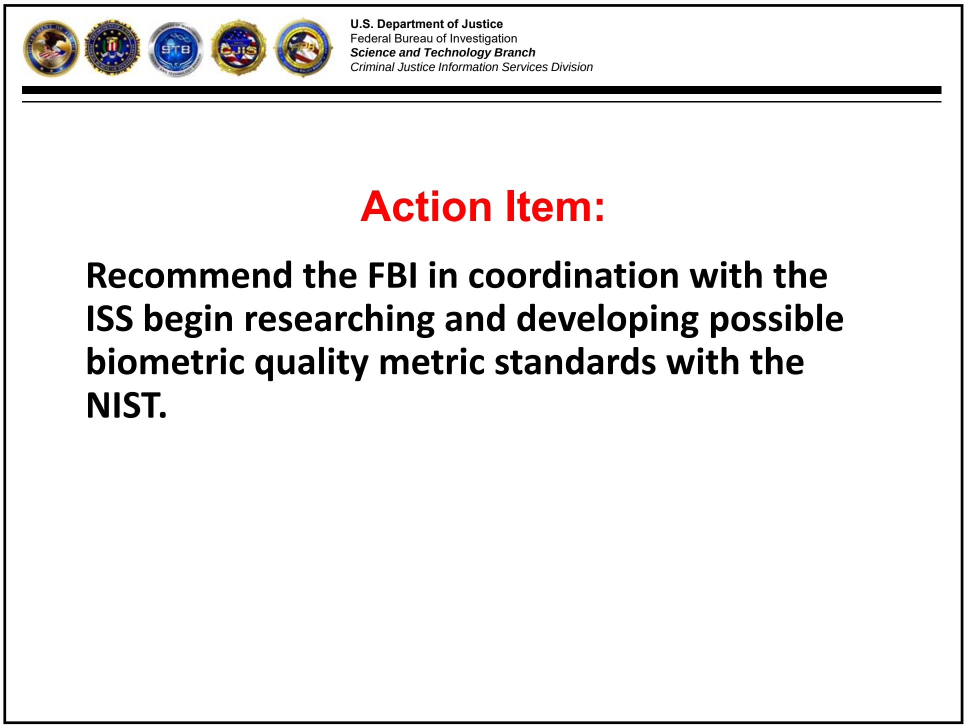
Purpose: To provide an update on IAI activities.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #13

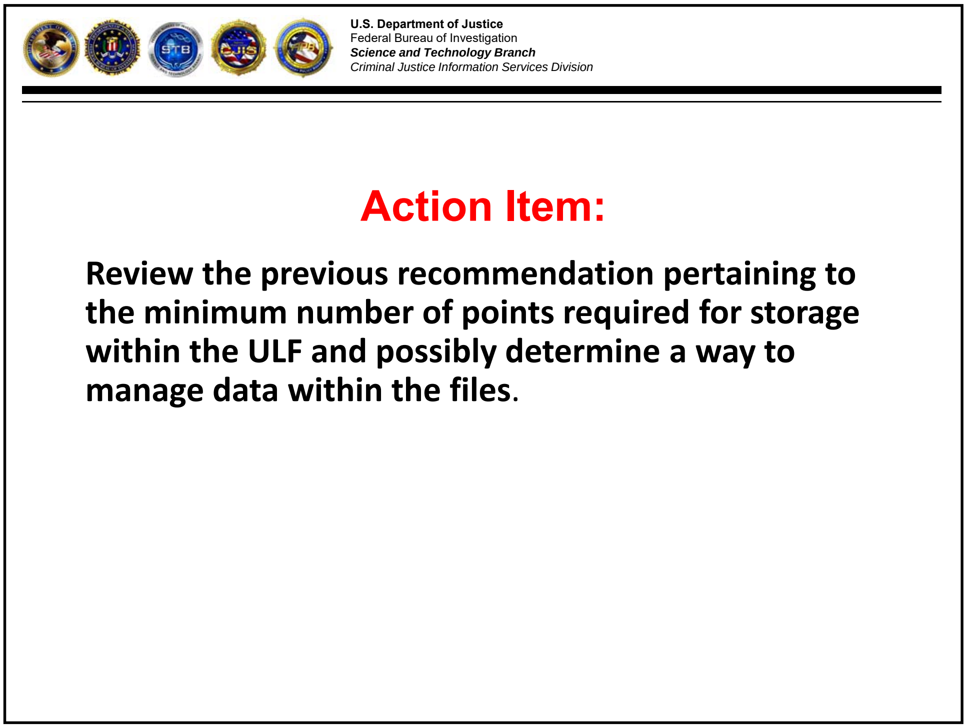
Ad hoc Items



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Action Item:

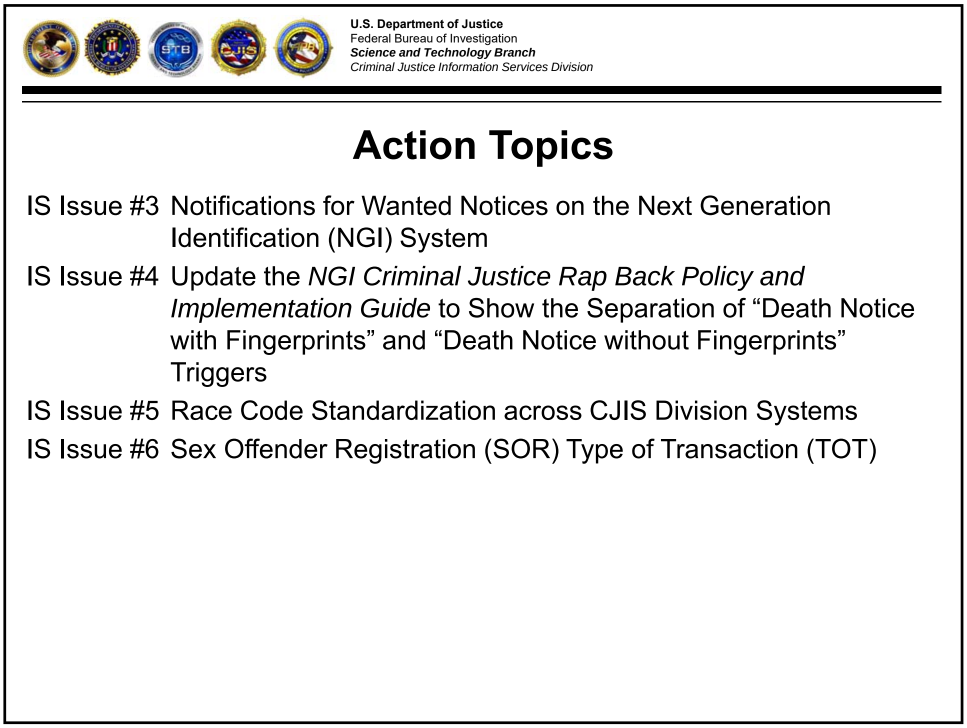
Recommend the FBI in coordination with the ISS begin researching and developing possible biometric quality metric standards with the NIST.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Action Item:

Review the previous recommendation pertaining to the minimum number of points required for storage within the ULF and possibly determine a way to manage data within the files.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

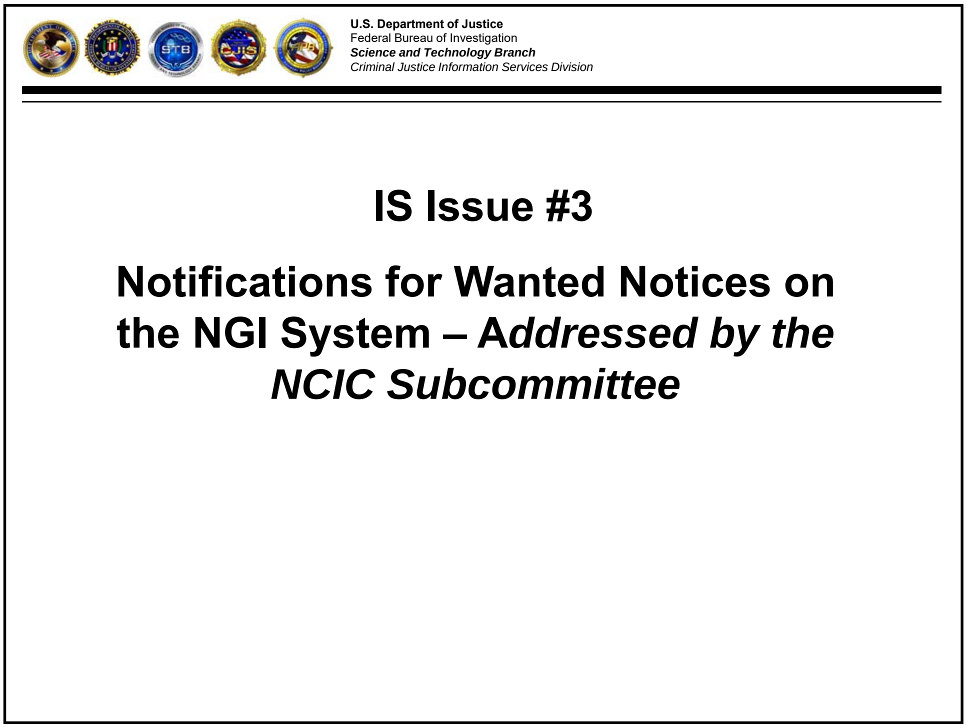
Action Topics

IS Issue #3 Notifications for Wanted Notices on the Next Generation Identification (NGI) System

IS Issue #4 Update the *NGI Criminal Justice Rap Back Policy and Implementation Guide* to Show the Separation of "Death Notice with Fingerprints" and "Death Notice without Fingerprints" Triggers

IS Issue #5 Race Code Standardization across CJIS Division Systems

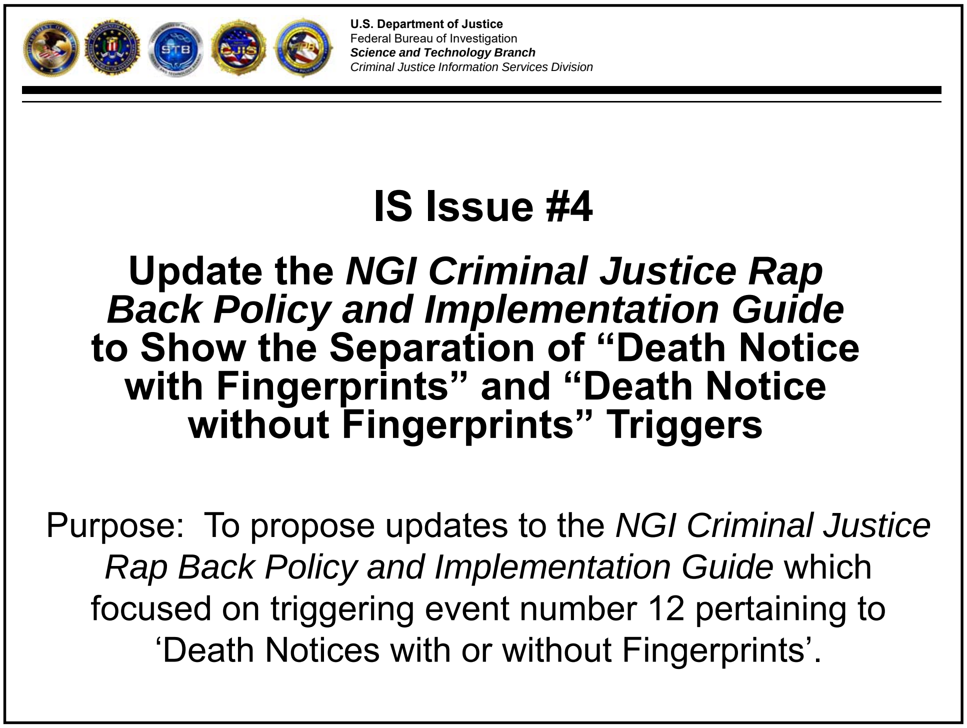
IS Issue #6 Sex Offender Registration (SOR) Type of Transaction (TOT)



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #3

Notifications for Wanted Notices on the NGI System – *Addressed by the NCIC Subcommittee*

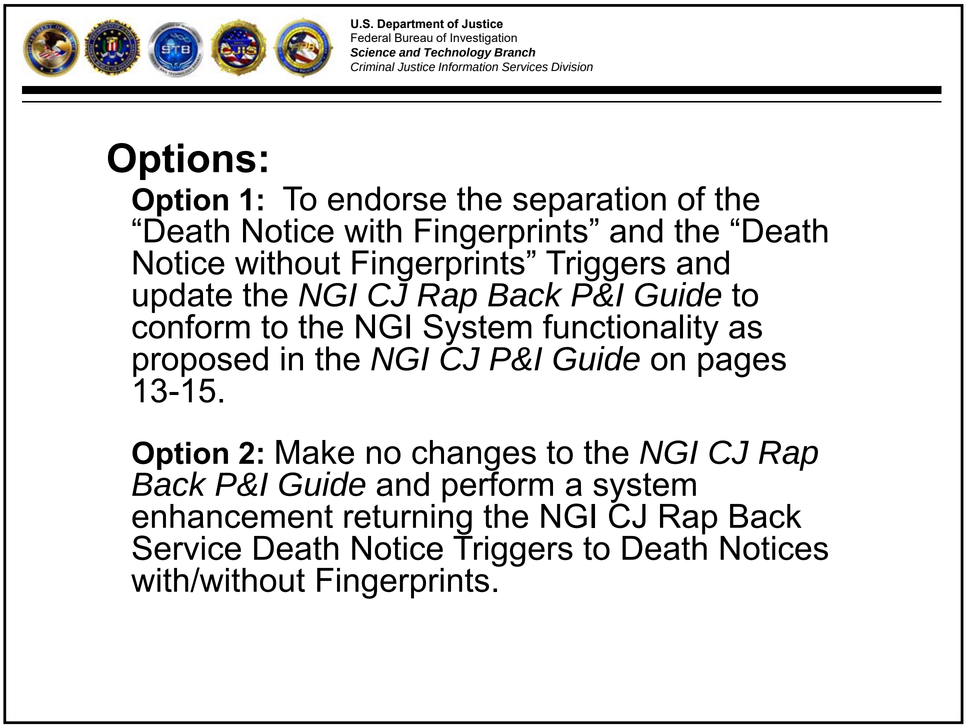


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #4

Update the *NGI Criminal Justice Rap Back Policy and Implementation Guide* to Show the Separation of "Death Notice with Fingerprints" and "Death Notice without Fingerprints" Triggers

Purpose: To propose updates to the *NGI Criminal Justice Rap Back Policy and Implementation Guide* which focused on triggering event number 12 pertaining to 'Death Notices with or without Fingerprints'.

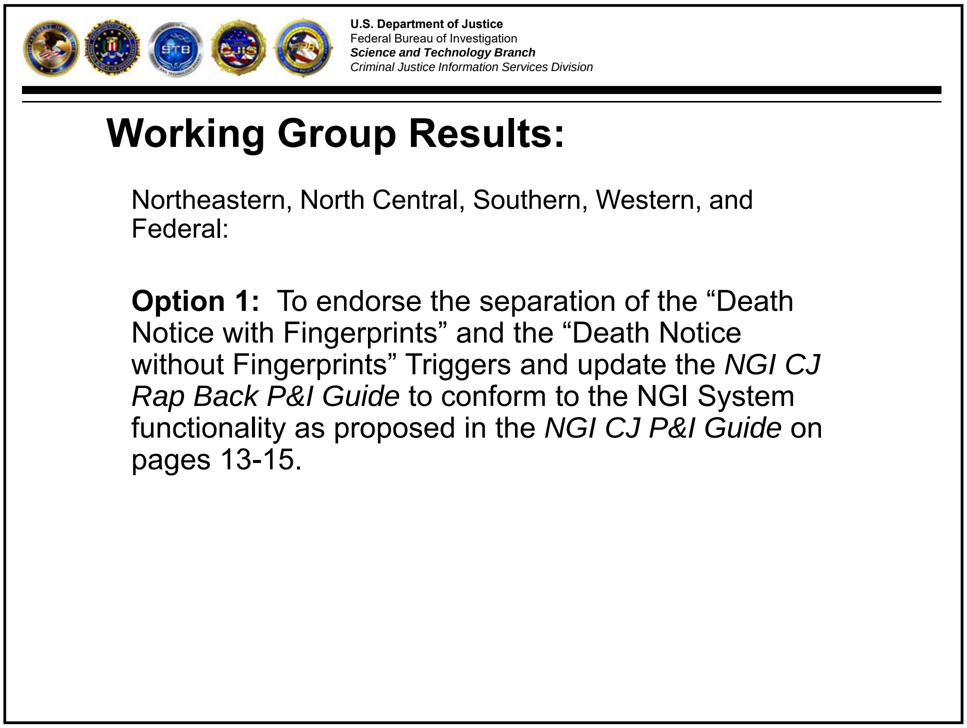


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Options:

Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the *NGI CJ Rap Back P&I Guide* to conform to the NGI System functionality as proposed in the *NGI CJ P&I Guide* on pages 13-15.

Option 2: Make no changes to the *NGI CJ Rap Back P&I Guide* and perform a system enhancement returning the NGI CJ Rap Back Service Death Notice Triggers to Death Notices with/without Fingerprints.

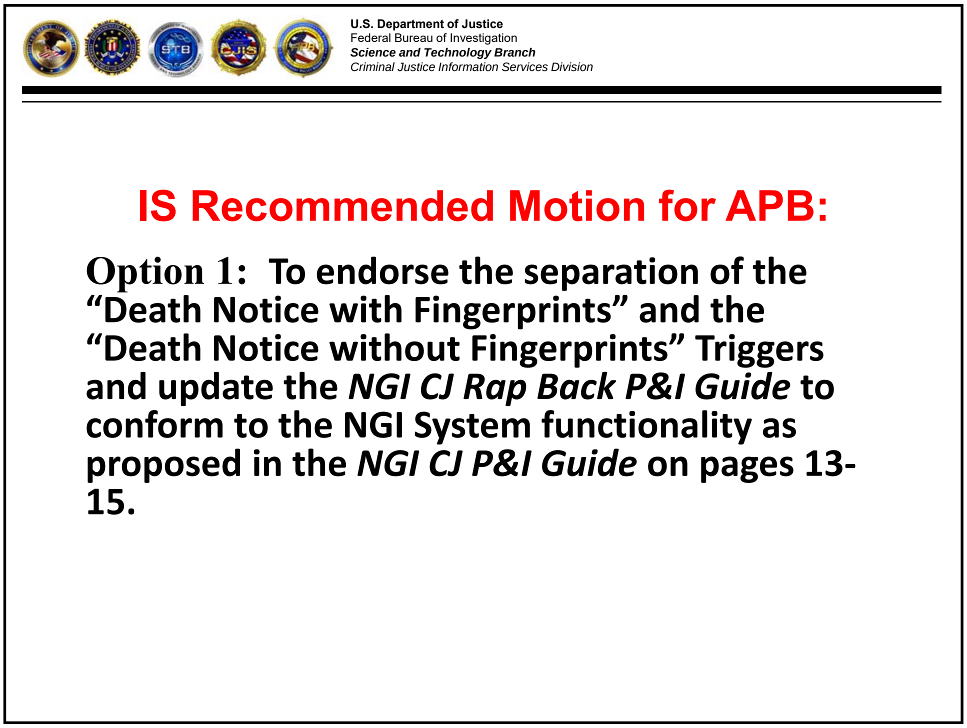


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Working Group Results:

Northeastern, North Central, Southern, Western, and Federal:

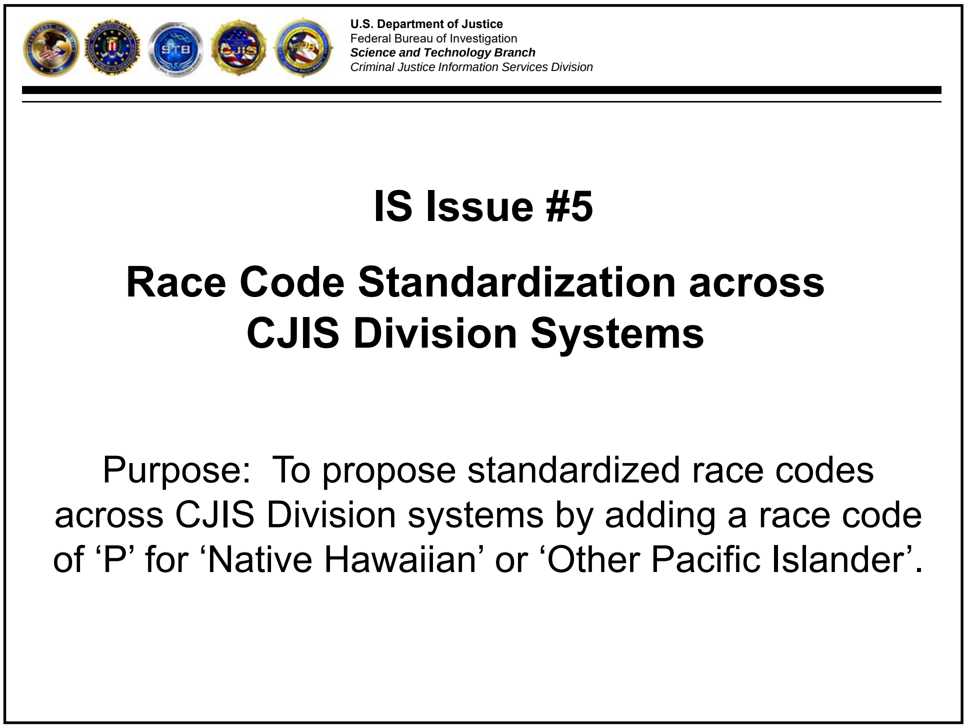
Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the *NGI CJ Rap Back P&I Guide* to conform to the NGI System functionality as proposed in the *NGI CJ P&I Guide* on pages 13-15.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Recommended Motion for APB:

Option 1: To endorse the separation of the "Death Notice with Fingerprints" and the "Death Notice without Fingerprints" Triggers and update the *NGI CJ Rap Back P&I Guide* to conform to the NGI System functionality as proposed in the *NGI CJ P&I Guide* on pages 13-15.

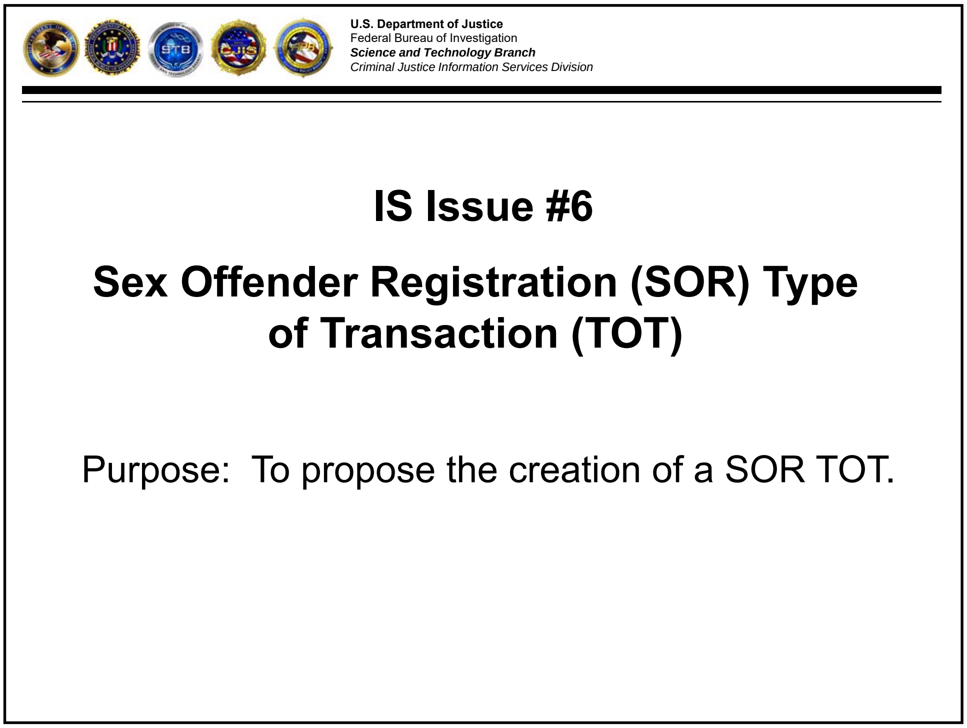


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #5

Race Code Standardization across CJIS Division Systems

Purpose: To propose standardized race codes across CJIS Division systems by adding a race code of ‘P’ for ‘Native Hawaiian’ or ‘Other Pacific Islander’.

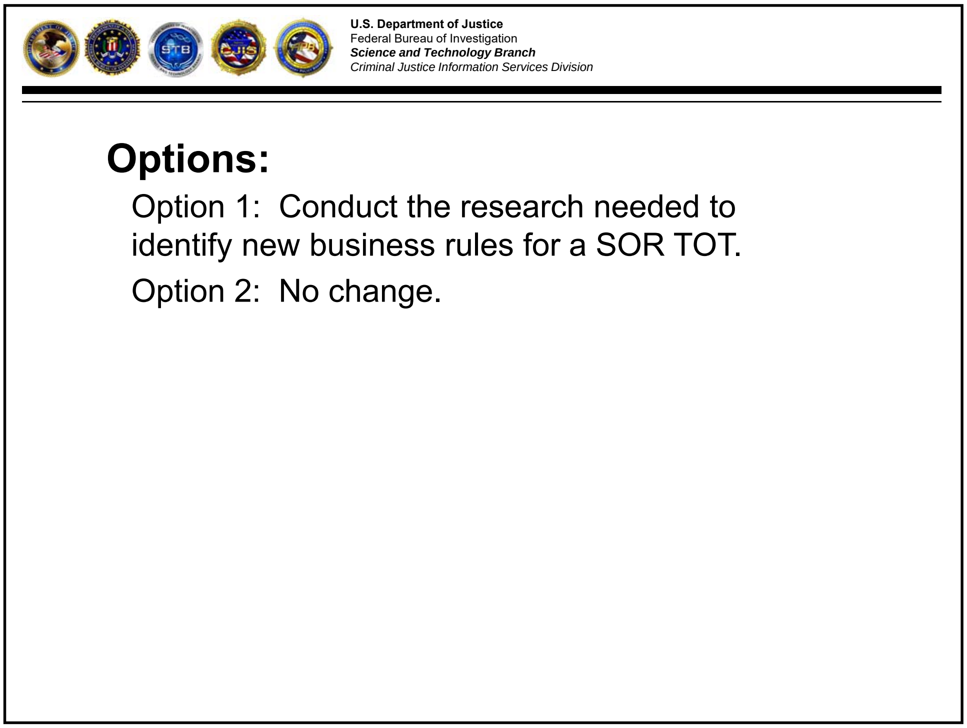


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Issue #6

Sex Offender Registration (SOR) Type of Transaction (TOT)

Purpose: To propose the creation of a SOR TOT.

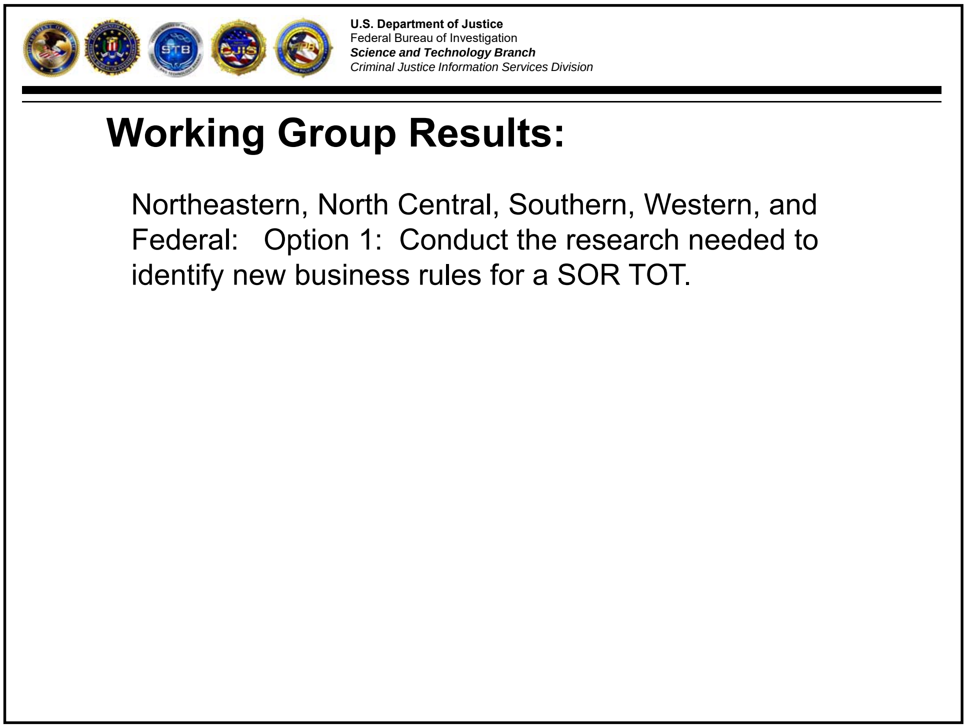


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Options:

Option 1: Conduct the research needed to identify new business rules for a SOR TOT.

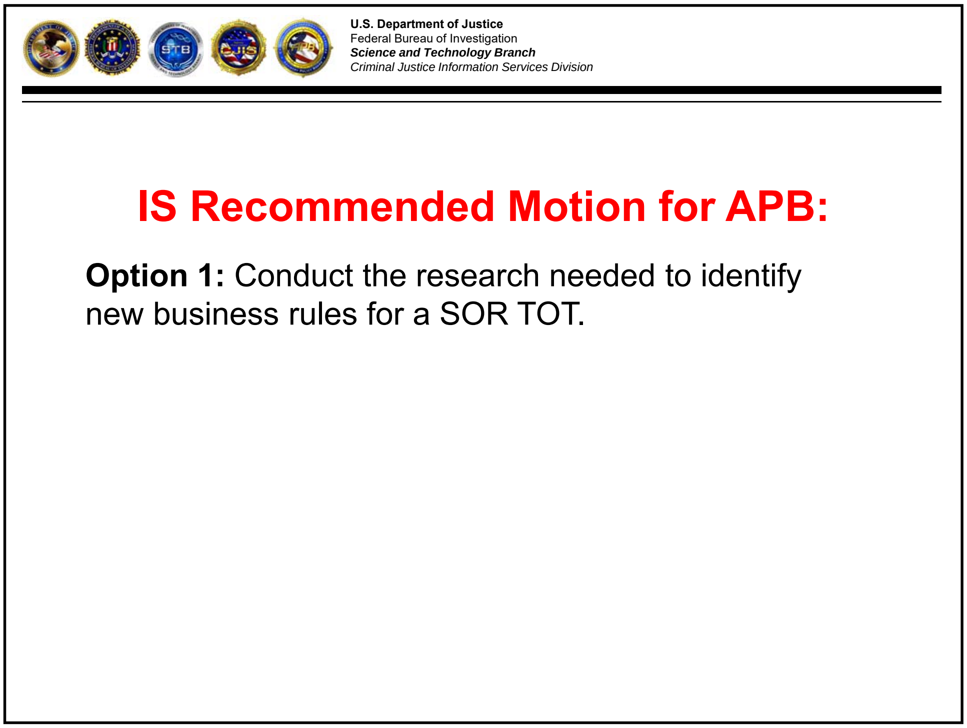
Option 2: No change.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Working Group Results:

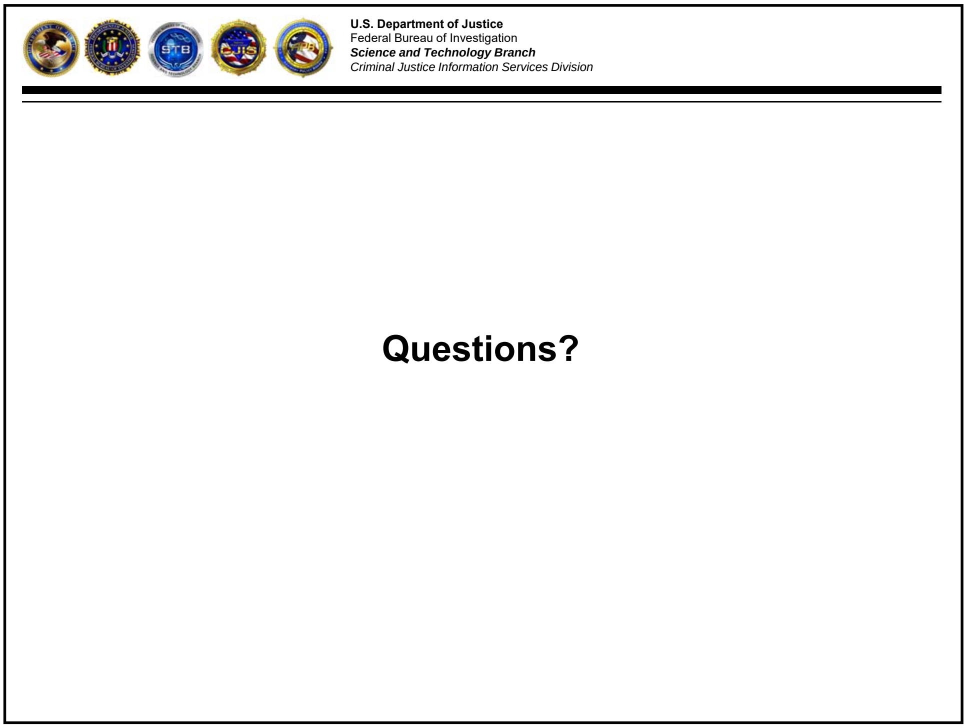
Northeastern, North Central, Southern, Western, and Federal: Option 1: Conduct the research needed to identify new business rules for a SOR TOT.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

IS Recommended Motion for APB:

Option 1: Conduct the research needed to identify new business rules for a SOR TOT.

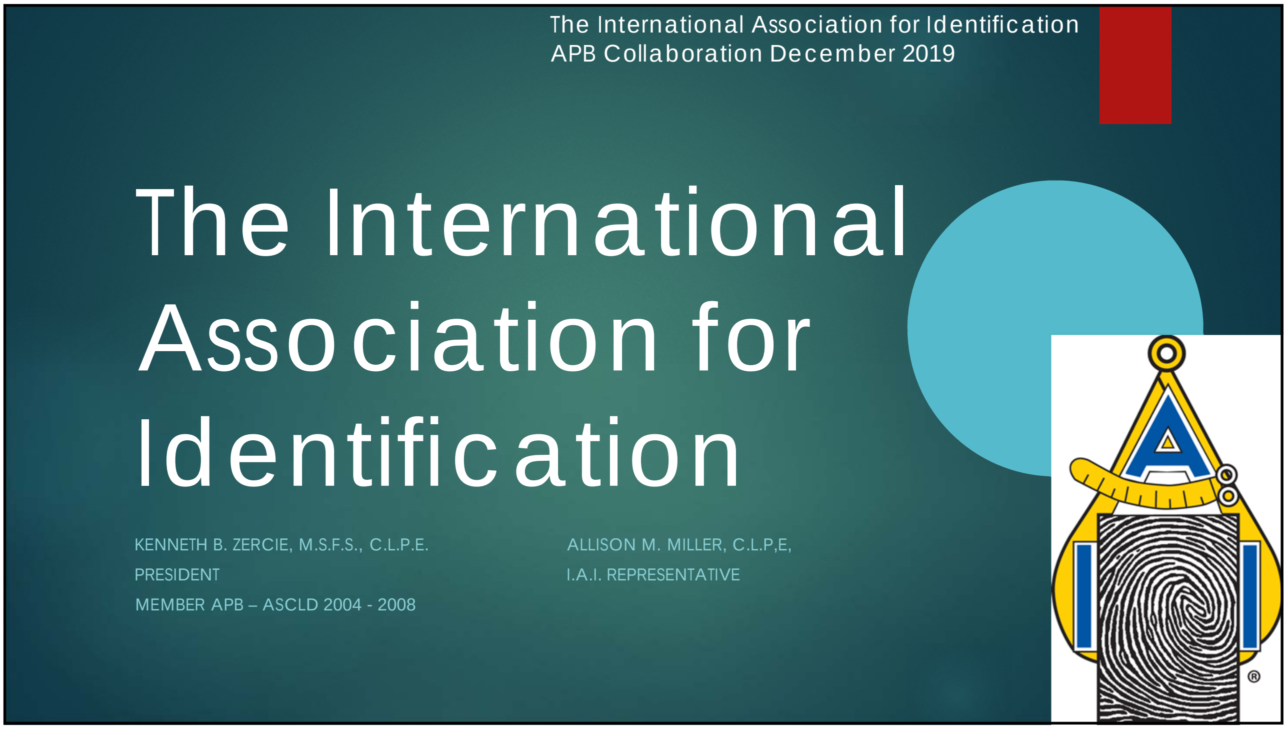


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Questions?

BIOMETRIC
IDENTIFICATION
AWARD
2019

BIOMETRIC
IDENTIFICATION
AWARD
2019
Norfolk Police Department
Norfolk, VA

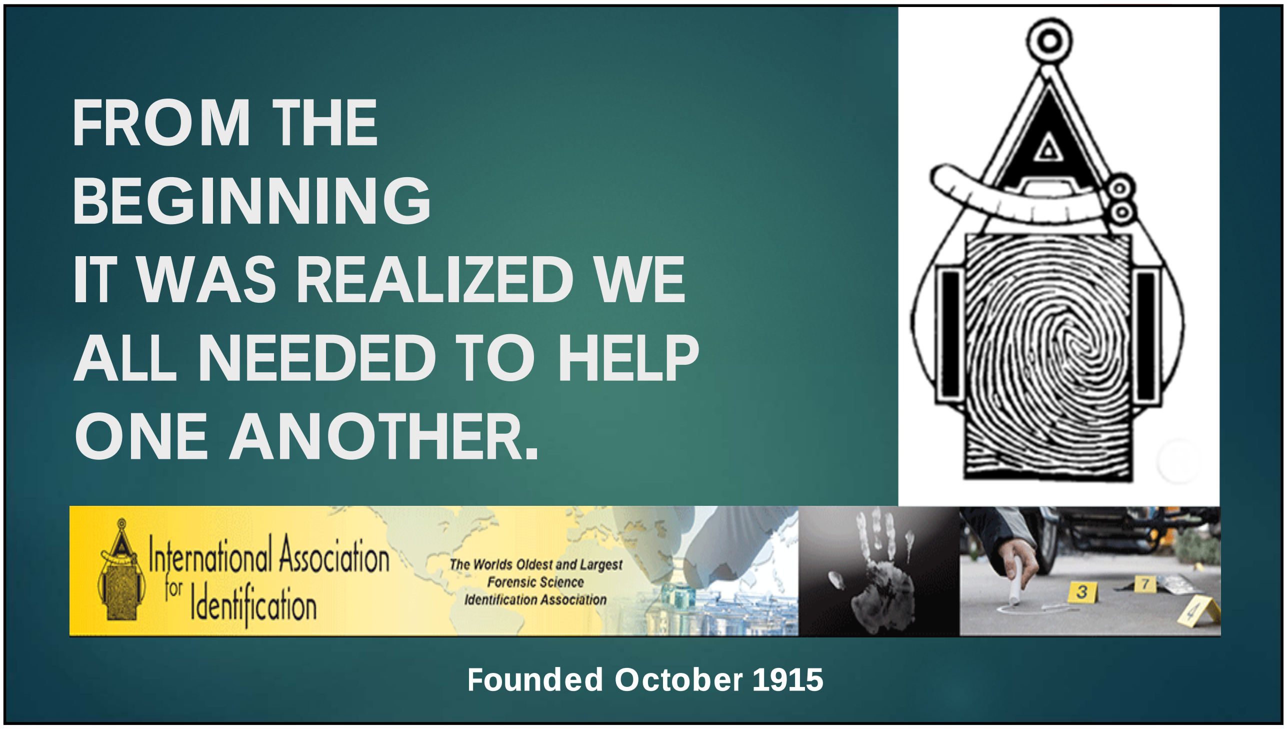


The International Association for Identification
APB Collaboration December 2019

The International Association for Identification

KENNETH B. ZERCIE, M.S.F.S., C.L.P.E.
PRESIDENT
MEMBER APB – ASCLD 2004 - 2008

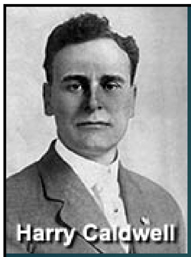
ALLISON M. MILLER, C.L.P,E,
I.A.I. REPRESENTATIVE



FROM THE BEGINNING IT WAS REALIZED WE ALL NEEDED TO HELP ONE ANOTHER.

International Association for Identification
The Worlds Oldest and Largest Forensic Science Identification Association
3
7
4

Founded October 1915



On August 4, 1915, Inspector Harry H. Caldwell of the Oakland (California) Police Department's Bureau of Identification wrote numerous letters to "Criminal Identification Operators" asking them to meet in Oakland for the purpose of forming an organization to further the aims of the identification profession. A group of about twenty-two men met and, as a result, the "International Association for Criminal Identification" was founded in October, 1915, with Inspector Caldwell as the presiding officer.

By 1916, when the second annual conference was held (Leavenworth, KS), the membership had grown to 116 regular members and 13 honorary members. California received the first IAI State Division Charter in 1916. (The Association currently has 44 Divisions representing 48 states and 45 countries).

In 1918, at the fourth annual conference, the word "Criminal" was dropped from the name of the Association, in recognition of the volume of noncriminal work done by identification bureaus.

In 1921, at the seventh annual conference (Washington, DC), the IAI achieved considerable attention from the highest level of the United States government. Members attending the conference were received at the White House, and it was during this meeting that inked fingerprints of President Harding were recorded. This level of influence was maintained for decades, as evidenced by documents revealing communication between the Association and Presidents Roosevelt and Truman, and others in government.

History of the I.A.I.

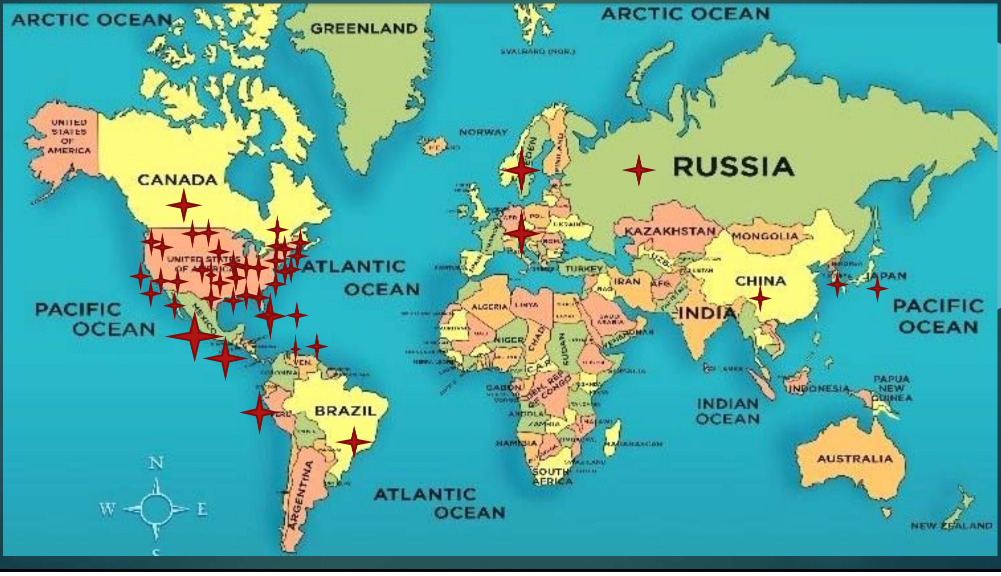
- Founded in 1915
- The I.A.I. celebrated its 100th year in Sacramento, CA in 2015 with a very special Anniversary Meeting
- The I.A.I. represents more then 7,000 active practitioner's in the areas of Forensic Identification from **ALL OVER THE WORLD**
- 44 Chartered Divisions with another 20,000 members
- 10 Areas of the WORLD with "Regional Representatives"

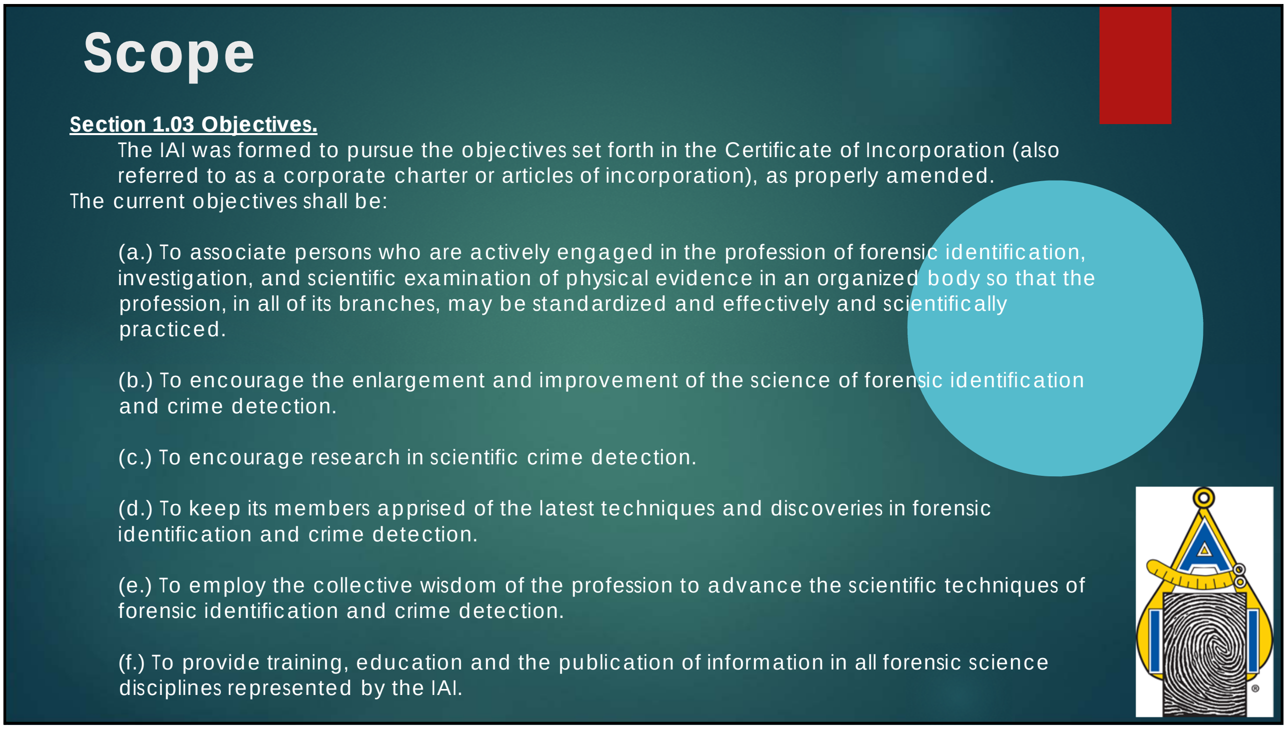
International in Scope - International in Service

theiai.org

Only You Can Make Us All Better

International & Regional Divisions





Scope

Section 1.03 Objectives.

The IAI was formed to pursue the objectives set forth in the Certificate of Incorporation (also referred to as a corporate charter or articles of incorporation), as properly amended.

The current objectives shall be:

(a.) To associate persons who are actively engaged in the profession of forensic identification, investigation, and scientific examination of physical evidence in an organized body so that the profession, in all of its branches, may be standardized and effectively and scientifically practiced.

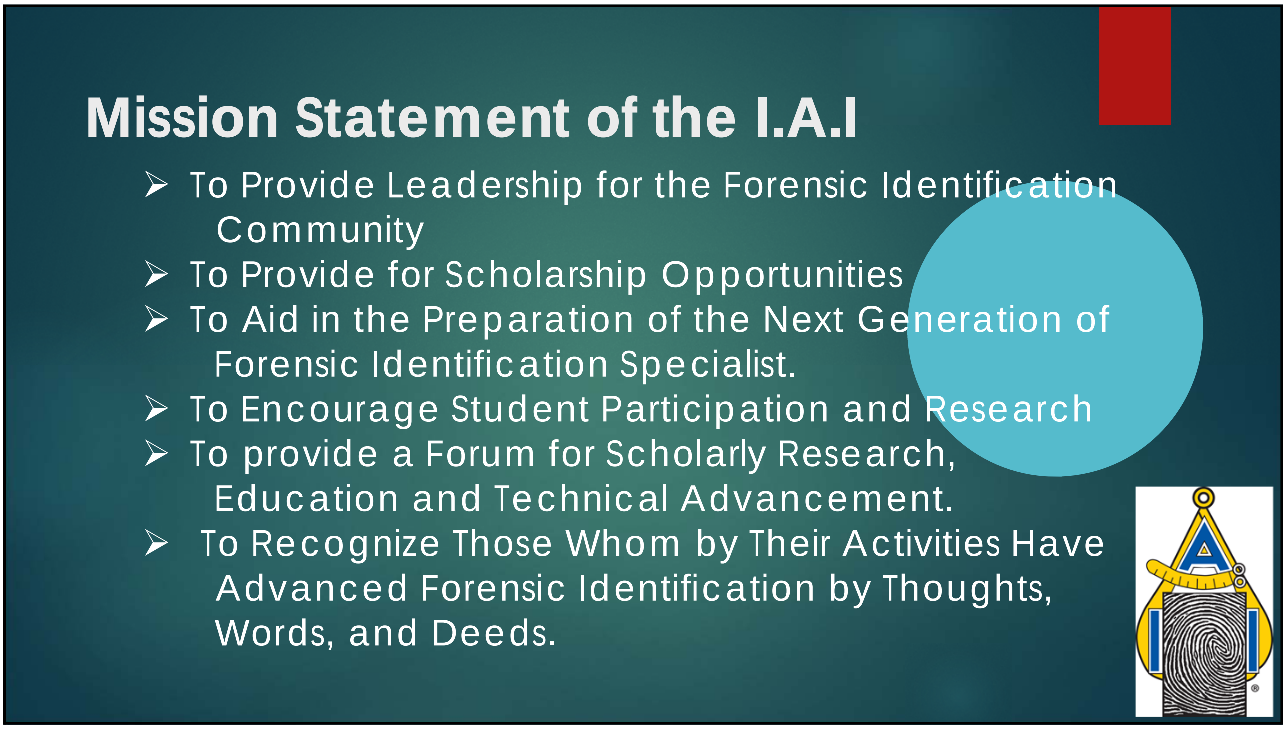
(b.) To encourage the enlargement and improvement of the science of forensic identification and crime detection.

(c.) To encourage research in scientific crime detection.

(d.) To keep its members apprised of the latest techniques and discoveries in forensic identification and crime detection.

(e.) To employ the collective wisdom of the profession to advance the scientific techniques of forensic identification and crime detection.

(f.) To provide training, education and the publication of information in all forensic science disciplines represented by the IAI.



Mission Statement of the I.A.I

- To Provide Leadership for the Forensic Identification Community
- To Provide for Scholarship Opportunities
- To Aid in the Preparation of the Next Generation of Forensic Identification Specialist.
- To Encourage Student Participation and Research
- To provide a Forum for Scholarly Research, Education and Technical Advancement.
- To Recognize Those Whom by Their Activities Have Advanced Forensic Identification by Thoughts, Words, and Deeds.

Objectives and Goals

To advance the Identification Disciplines within the Forensic Sciences in and effort to provide the best processes possible for the user community.

Finding the Truth Through Science

Who Are I.A.I. Members – Many of You

International Association for Identification
INTERNATIONAL ASSOCIATION FOR IDENTIFICATION'S 104th EDUCATIONAL CONFERENCE
AUGUST 11 - 17, 2019 - RENO, NEVADA

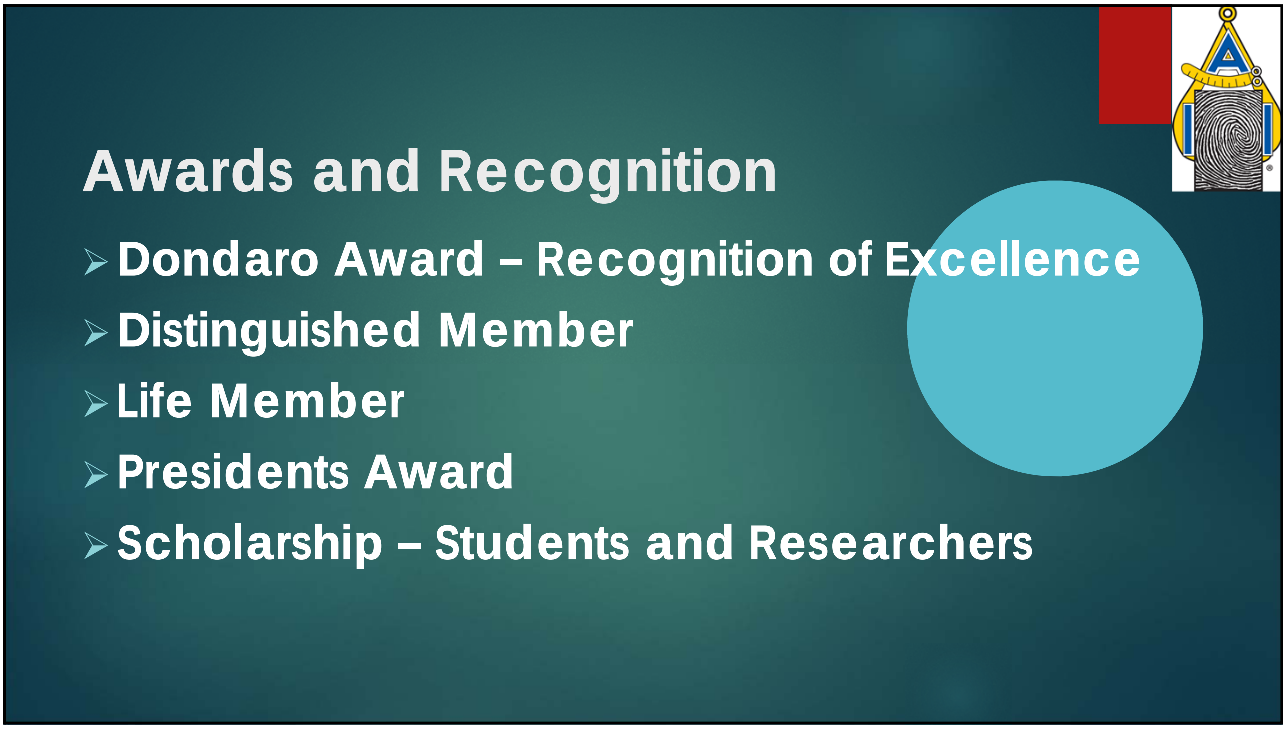
Fourteen Hundred of Your Closest Supporters

Who Are I.A.I. Members - International

Who Are I.A.I. Members

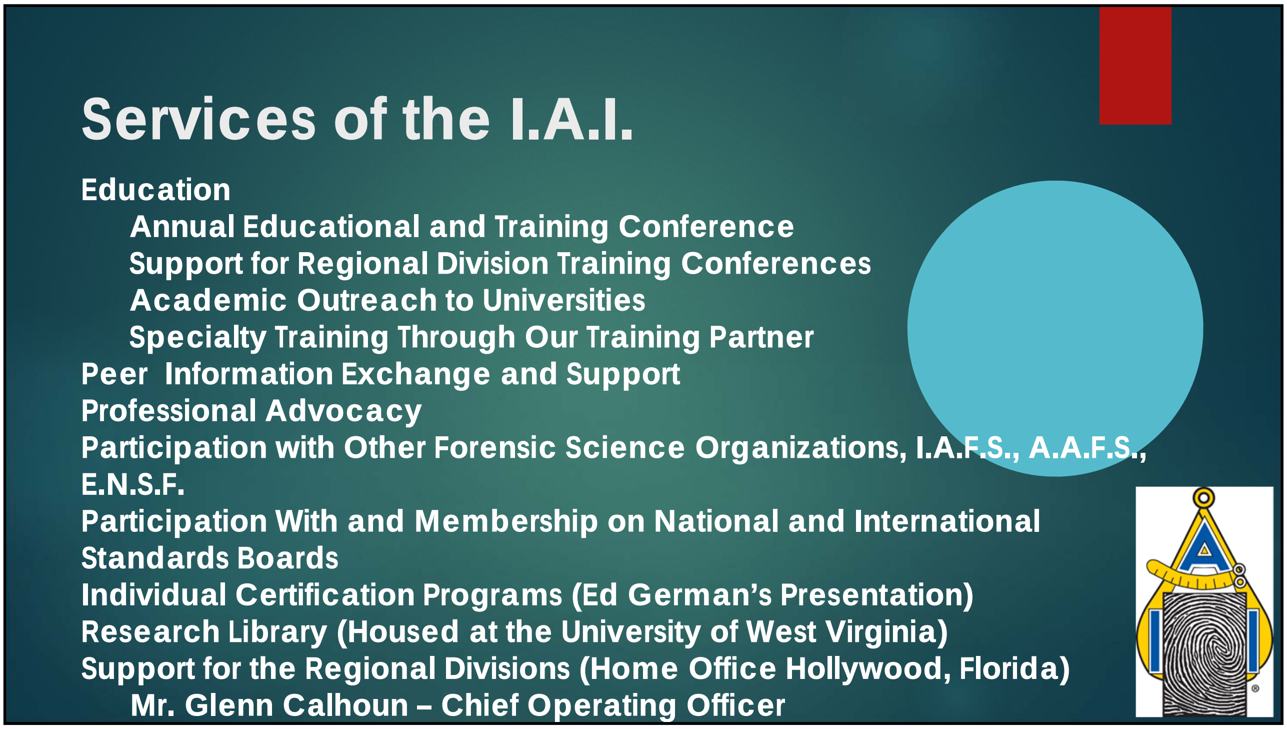
- ➢ Administrators
- ➢ Practitioners
- ➢ Police Officers
- ➢ Crime Scene Specialist
- ➢ Forensic Scientist
- ➢ Professors & Students

➢What About You?



Awards and Recognition

- Dondaro Award – Recognition of Excellence
- Distinguished Member
- Life Member
- Presidents Award
- Scholarship – Students and Researchers



Services of the I.A.I.

Education

Annual Educational and Training Conference

Support for Regional Division Training Conferences

Academic Outreach to Universities

Specialty Training Through Our Training Partner

Peer Information Exchange and Support

Professional Advocacy

Participation with Other Forensic Science Organizations, I.A.F.S., A.A.F.S., E.N.S.F.

Participation With and Membership on National and International Standards Boards

Individual Certification Programs (Ed German's Presentation)

Research Library (Housed at the University of West Virginia)

Support for the Regional Divisions (Home Office Hollywood, Florida)

Mr. Glenn Calhoun – Chief Operating Officer

Journal of Forensic Identification
Read ABSTRACTS Here
The Official Publication of the International Association for Identification

J&W Fund
Scholarship and Funding Opportunities
Your contribution will benefit the field of forensic identification for years to come.

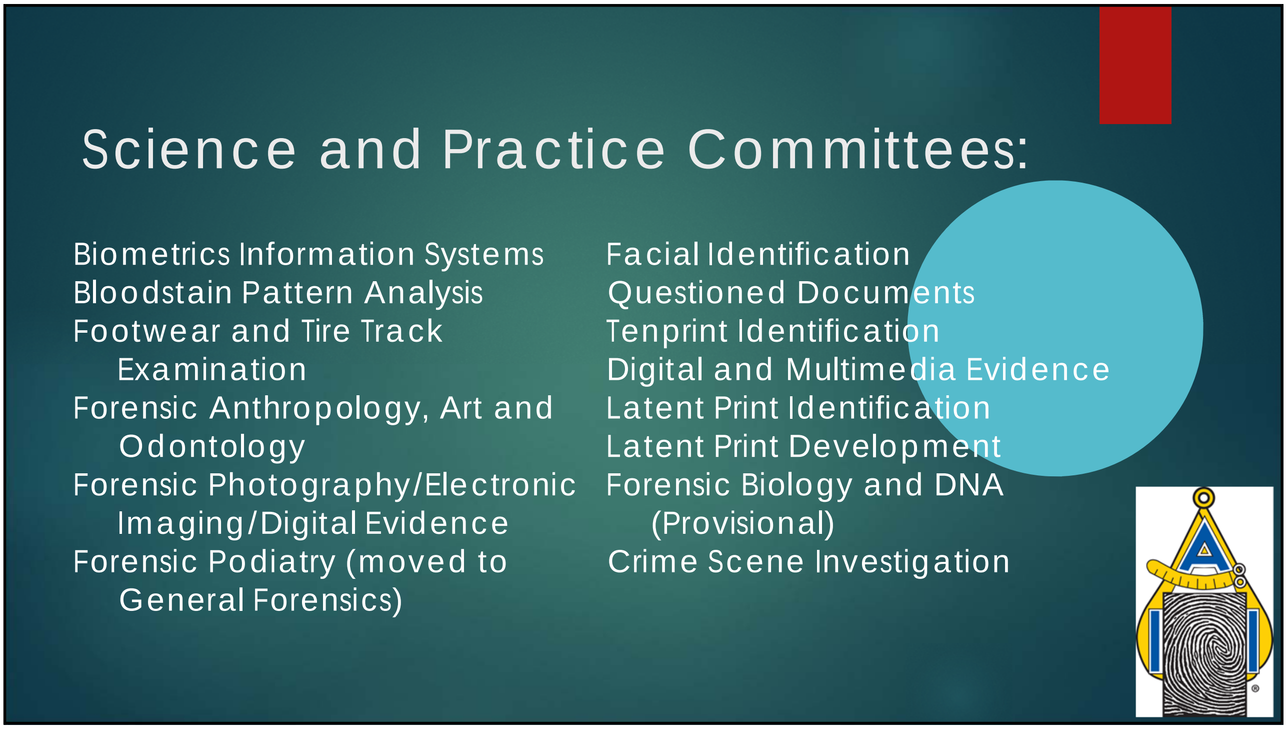
103RD INTERNATIONAL EDUCATIONAL CONFERENCE
IAI
THEIAI.ORG
SAN ANTONIO TEXAS
YOU'RE NOT A LONE STAR WITH THE IAI BEHIND YOU
JULY 29 · AUGUST 4, 2018

The I.A.I. Library and Archive

In 2005, the IAI selected the WVU Libraries to house its priceless research library due in part to WVU's pioneering program in the field of Forensic and Investigative Sciences education.

Consisting of more than 100 linear feet of material, including archives and manuscripts, books, periodicals, and a wide assortment of ephemeral publications, the IAI Collection is the most comprehensive forensics information resource in existence. Included are materials dating back to late 19th century when the field of scientific criminal investigation was in its infancy.

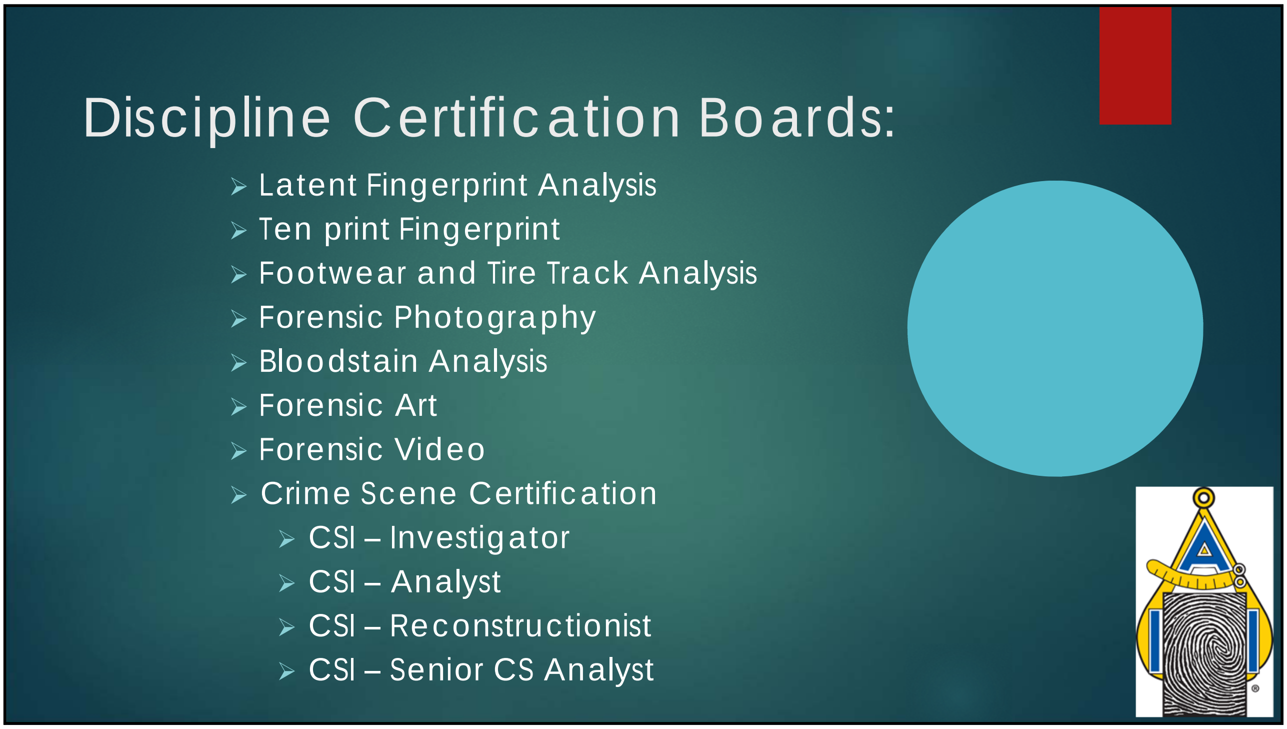
Read more about it, "Desperately Seeking Sherlock Holmes" from the West Virginia & Regional History Center Newsletter, Vol. 21: no. 1, Fall 2005, pages 1-3.



Science and Practice Committees:

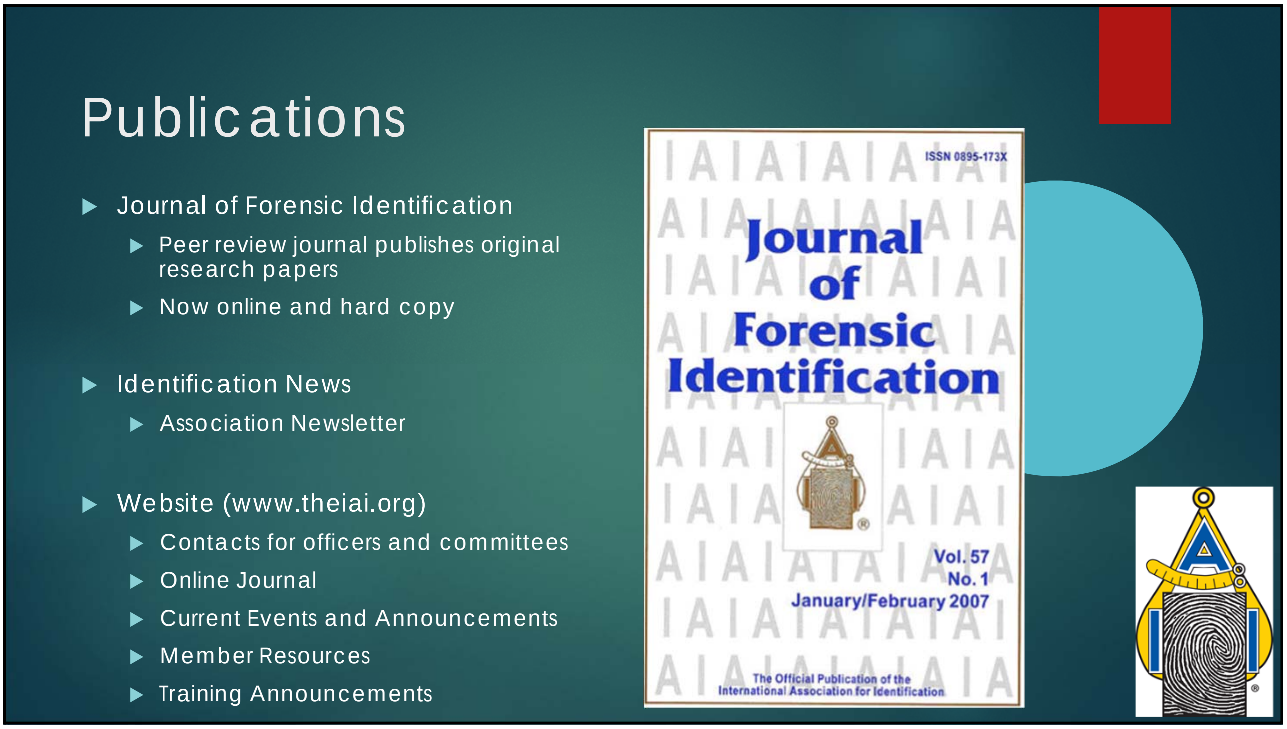
Biometrics Information Systems
Bloodstain Pattern Analysis
Footwear and Tire Track Examination
Forensic Anthropology, Art and Odontology
Forensic Photography/Electronic Imaging/Digital Evidence
Forensic Podiatry (moved to General Forensics)

Facial Identification
Questioned Documents
Tenprint Identification
Digital and Multimedia Evidence
Latent Print Identification
Latent Print Development
Forensic Biology and DNA (Provisional)
Crime Scene Investigation



Discipline Certification Boards:

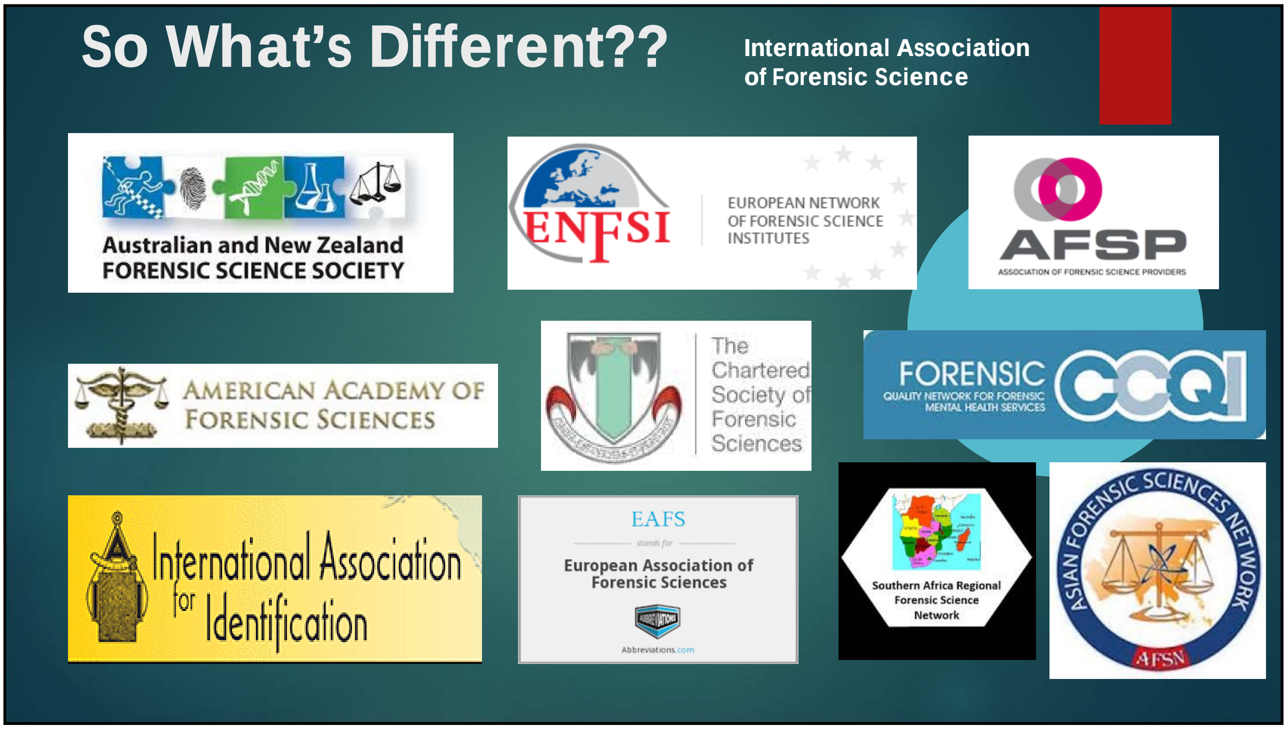
- Latent Fingerprint Analysis
- Ten print Fingerprint
- Footwear and Tire Track Analysis
- Forensic Photography
- Bloodstain Analysis
- Forensic Art
- Forensic Video
- Crime Scene Certification
  - CSI – Investigator
  - CSI – Analyst
  - CSI – Reconstructionist
  - CSI – Senior CS Analyst



Publications

- Journal of Forensic Identification
  - Peer review journal publishes original research papers
  - Now online and hard copy
- Identification News
  - Association Newsletter
- Website (www.theiai.org)
  - Contacts for officers and committees
  - Online Journal
  - Current Events and Announcements
  - Member Resources
  - Training Announcements

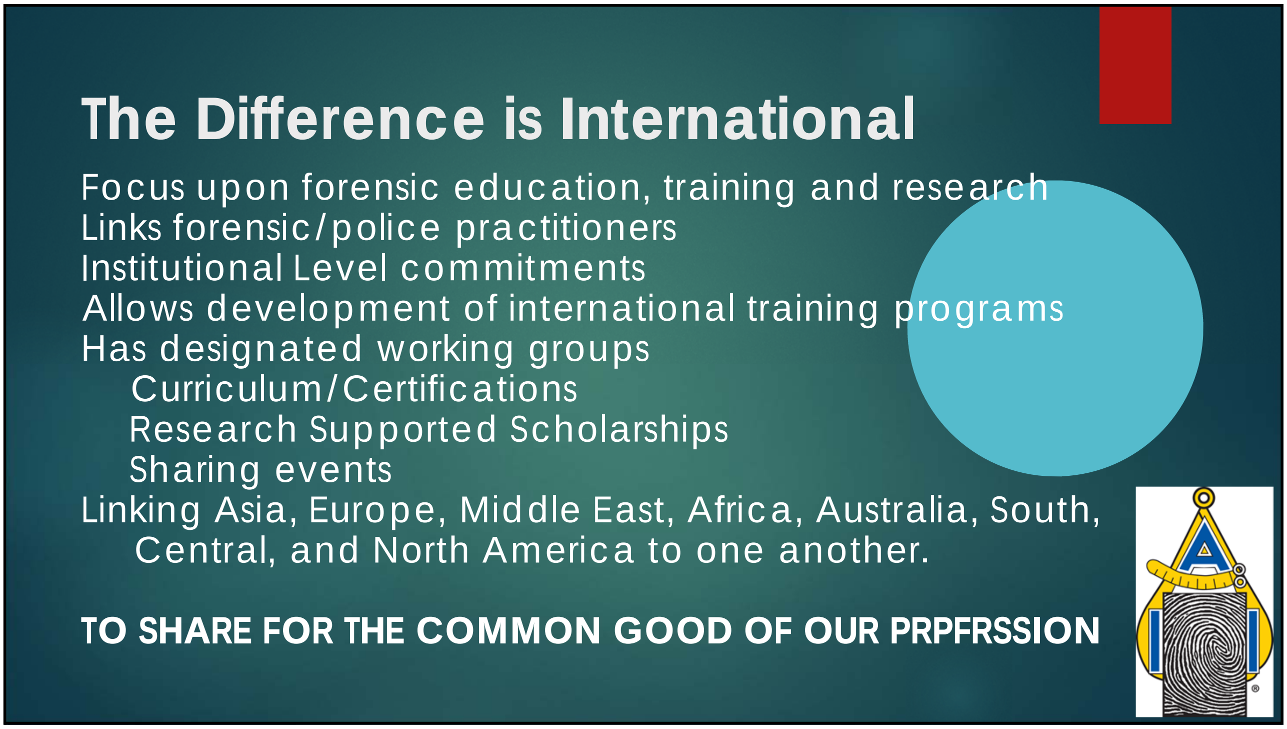
ISSN 0895-173X
Journal of Forensic Identification
Vol. 57
No. 1
January/February 2007
The Official Publication of the International Association for Identification



So What's Different??

International Association of Forensic Science

Australian and New Zealand FORENSIC SCIENCE SOCIETY
ENFSI
EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES
AFSP
ASSOCIATION OF FORENSIC SCIENCE PROVIDERS
AMERICAN ACADEMY OF FORENSIC SCIENCES
The Chartered Society of Forensic Sciences
FORENSIC
QUALITY NETWORK FOR FORENSIC MENTAL HEALTH SERVICES
CCQI
International Association for Identification
EAFS
stands for
European Association of Forensic Sciences
Abbreviations.com
Southern Africa Regional Forensic Science Network
ASIAN FORENSIC SCIENCES NETWORK
AFSN



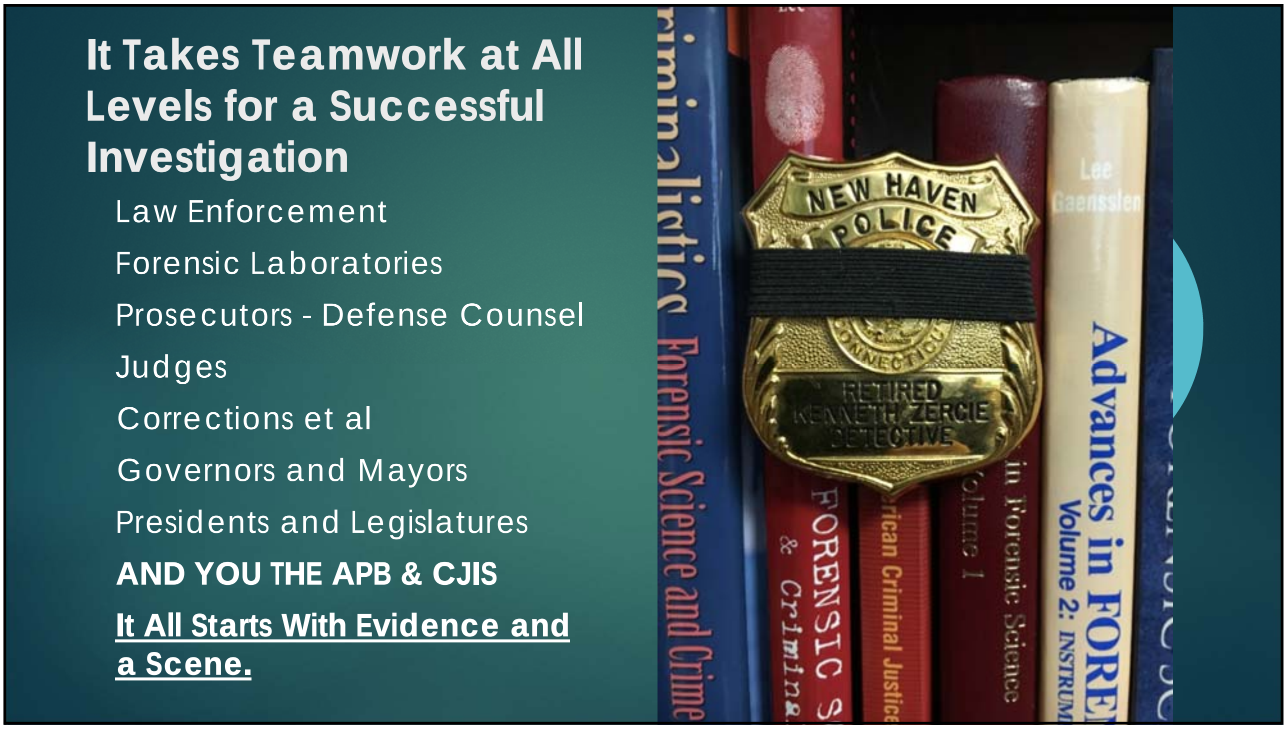
The Difference is International

Focus upon forensic education, training and research
Links forensic/police practitioners
Institutional Level commitments
Allows development of international training programs
Has designated working groups
- Curriculum/Certifications
- Research Supported Scholarships
- Sharing events

Linking Asia, Europe, Middle East, Africa, Australia, South, Central, and North America to one another.

TO SHARE FOR THE COMMON GOOD OF OUR PRPFRSSION

Our Members Have Provided Training All Over the World.



It Takes Teamwork at All Levels for a Successful Investigation

Law Enforcement

Forensic Laboratories

Prosecutors - Defense Counsel

Judges

Corrections et al

Governors and Mayors

Presidents and Legislatures

AND YOU THE APB & CJIS

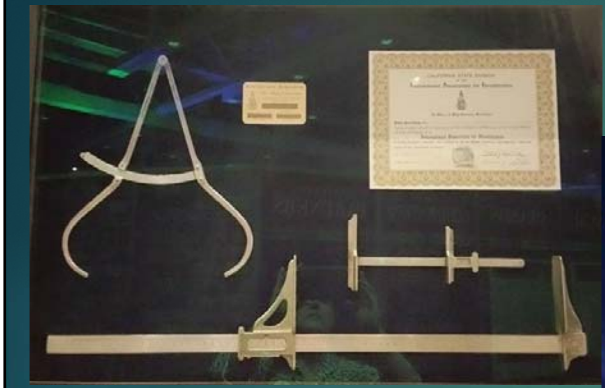
It All Starts With Evidence and a Scene.

The I.A.I. Has Student Scholarships

Groups from Mexico

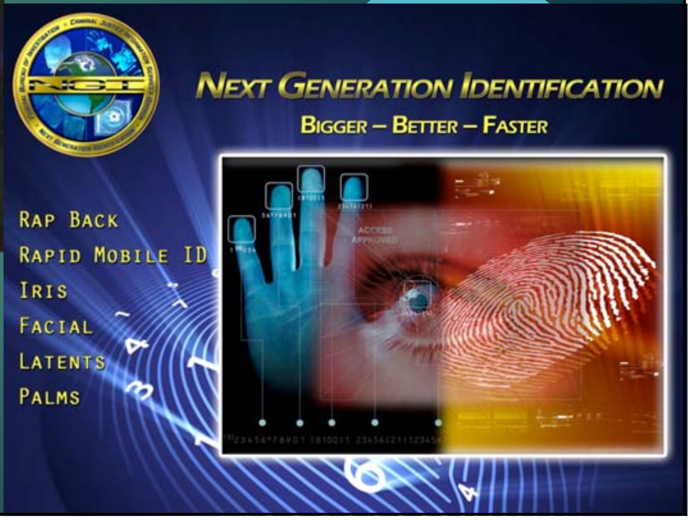
Various Universities in the US

Original Bertillion



We must join together to be the Agents of Change and Advancement Within Our Sciences.

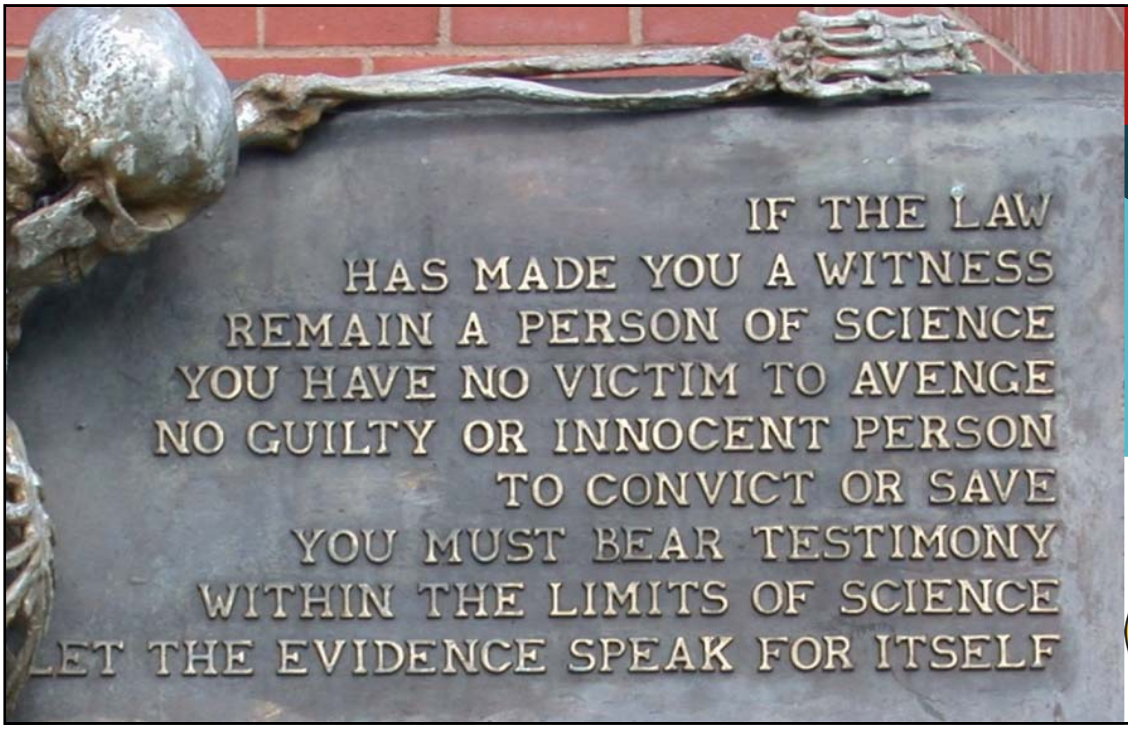
The Next Generation of Bio-Metrics is Here!!



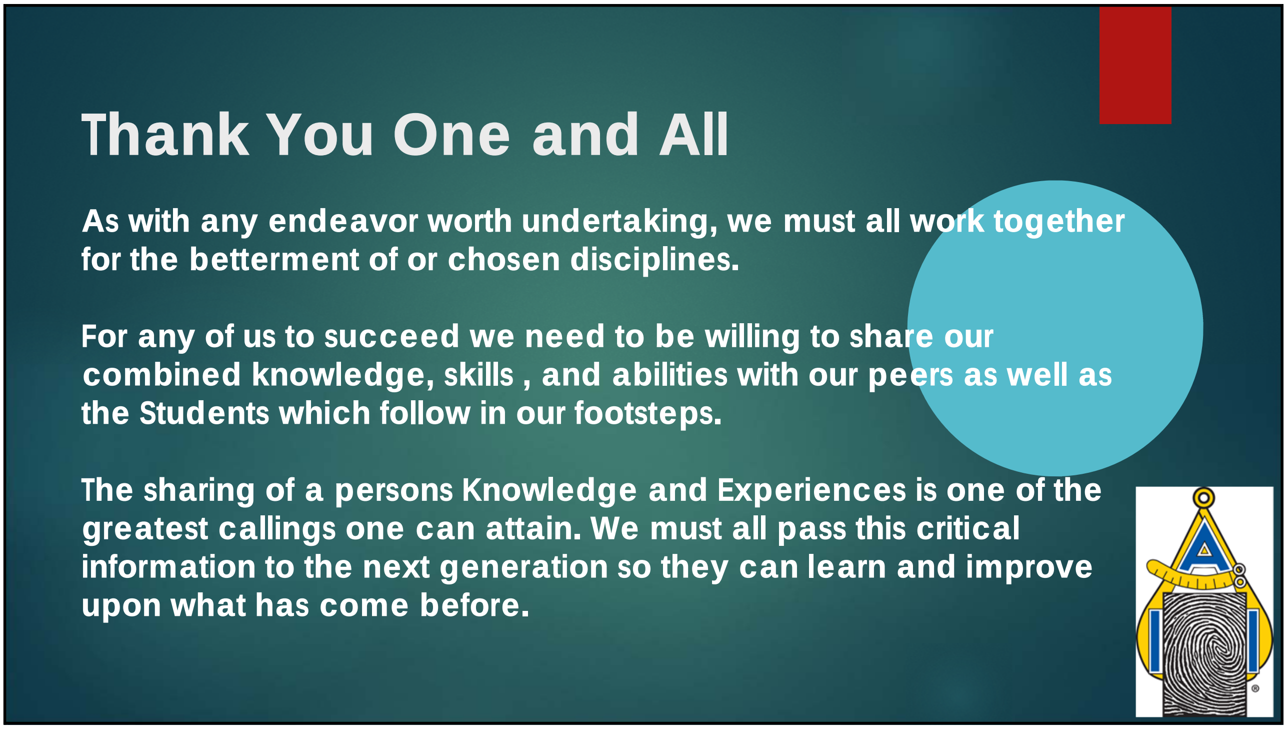
The current Officers, Board of Directors, and Members of the IAI are very pleased and supportive of the work of the APB and CJIS. For Without You We Could Not Accomplish Our Goals of Serving Justice

Parting Thoughts

IF THE LAW
HAS MADE YOU A WITNESS
REMAIN A PERSON OF SCIENCE
YOU HAVE NO VICTIM TO AVENGE
NO GUILTY OR INNOCENT PERSON
TO CONVICT OR SAVE
YOU MUST BEAR TESTIMONY
WITHIN THE LIMITS OF SCIENCE
LET THE EVIDENCE SPEAK FOR ITSELF



IF THE LAW
HAS MADE YOU A WITNESS
REMAIN A PERSON OF SCIENCE
YOU HAVE NO VICTIM TO AVENGE
NO GUILTY OR INNOCENT PERSON
TO CONVICT OR SAVE
YOU MUST BEAR TESTIMONY
WITHIN THE LIMITS OF SCIENCE
LET THE EVIDENCE SPEAK FOR ITSELF

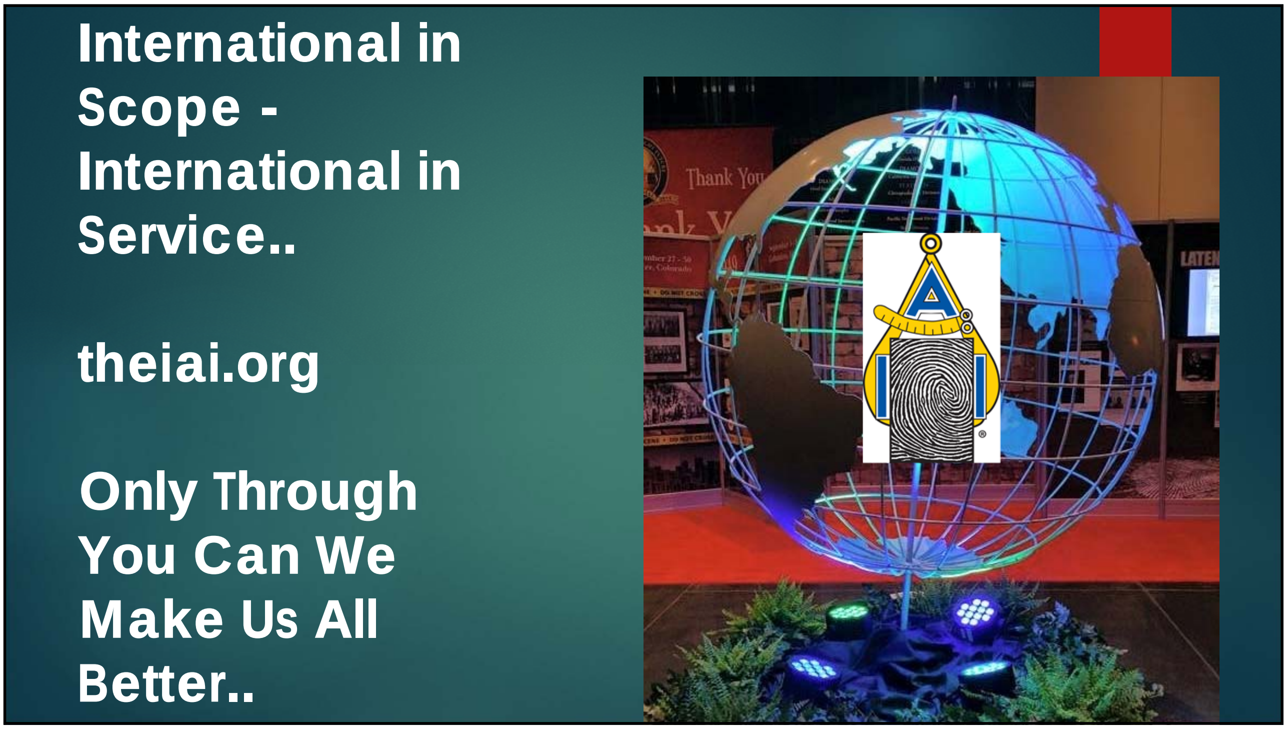


Thank You One and All

As with any endeavor worth undertaking, we must all work together for the betterment of or chosen disciplines.

For any of us to succeed we need to be willing to share our combined knowledge, skills , and abilities with our peers as well as the Students which follow in our footsteps.

The sharing of a persons Knowledge and Experiences is one of the greatest callings one can attain. We must all pass this critical information to the next generation so they can learn and improve upon what has come before.



International in Scope - International in Service..

theiai.org

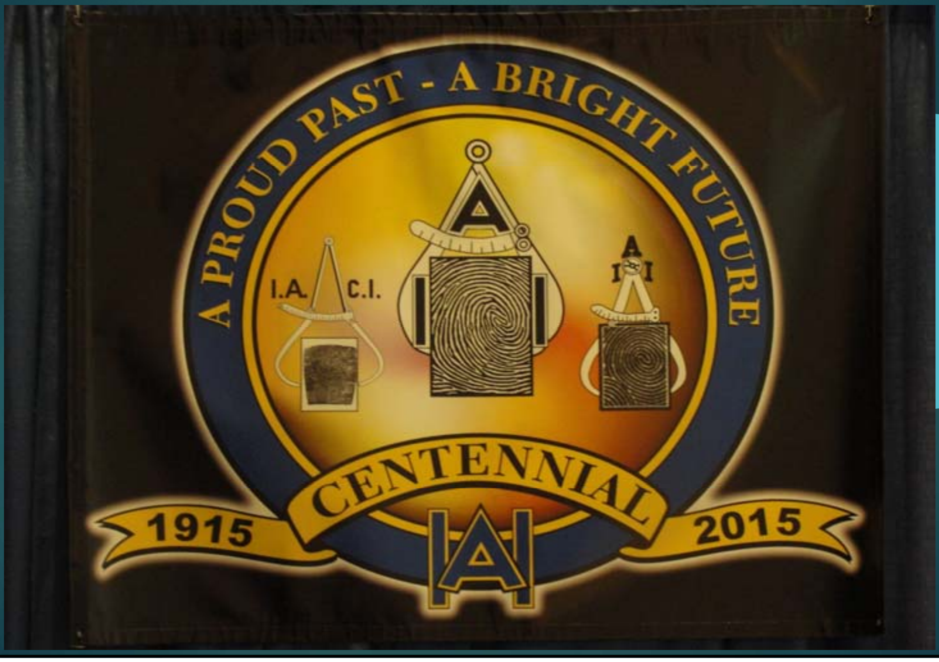
Only Through You Can We Make Us All Better..

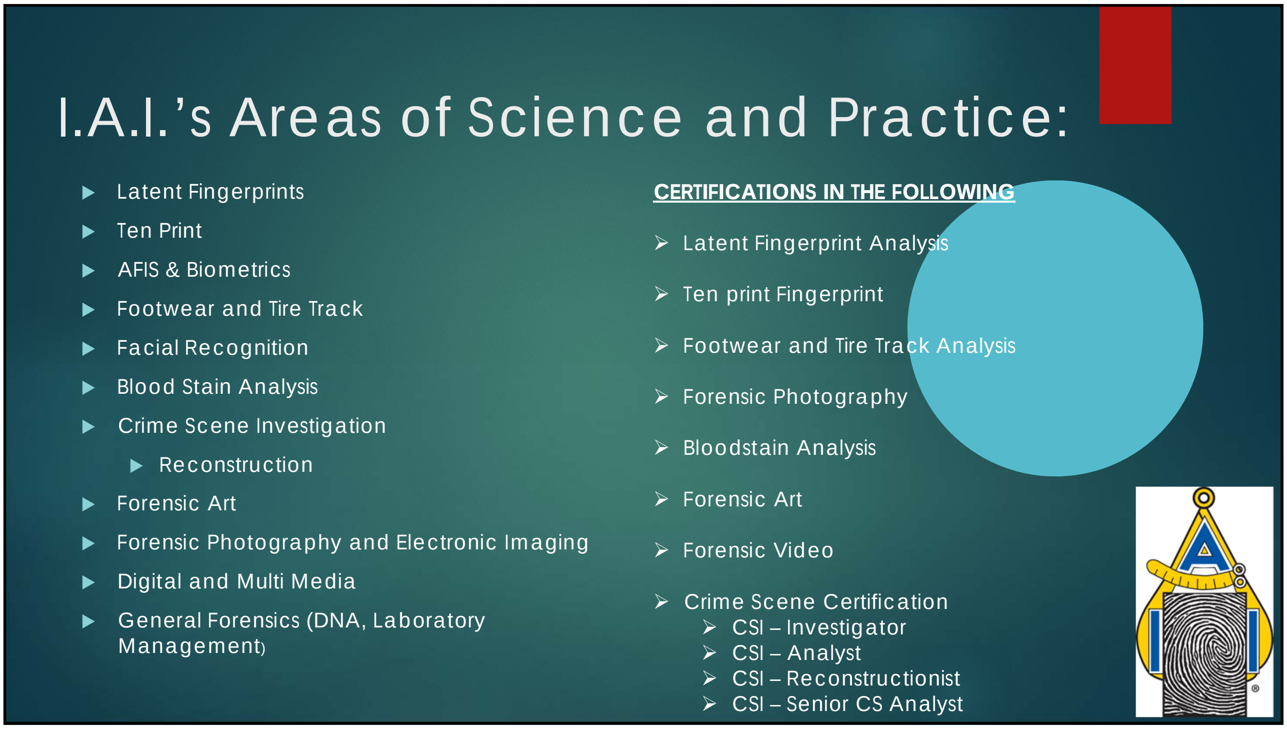
Please Join Us In 2020 In Orlando, FL

Y'all Come!!

The 102nd Annual Training and Educational Conference
San Antonio, Texas – July 29, 2018 through August 04, 2018

Thank You All for the Work That You Do…And on the lighter side:


A PROUD PAST - A BRIGHT FUTURE
I.A.
C.I.
CENTENNIAL
1915
2015

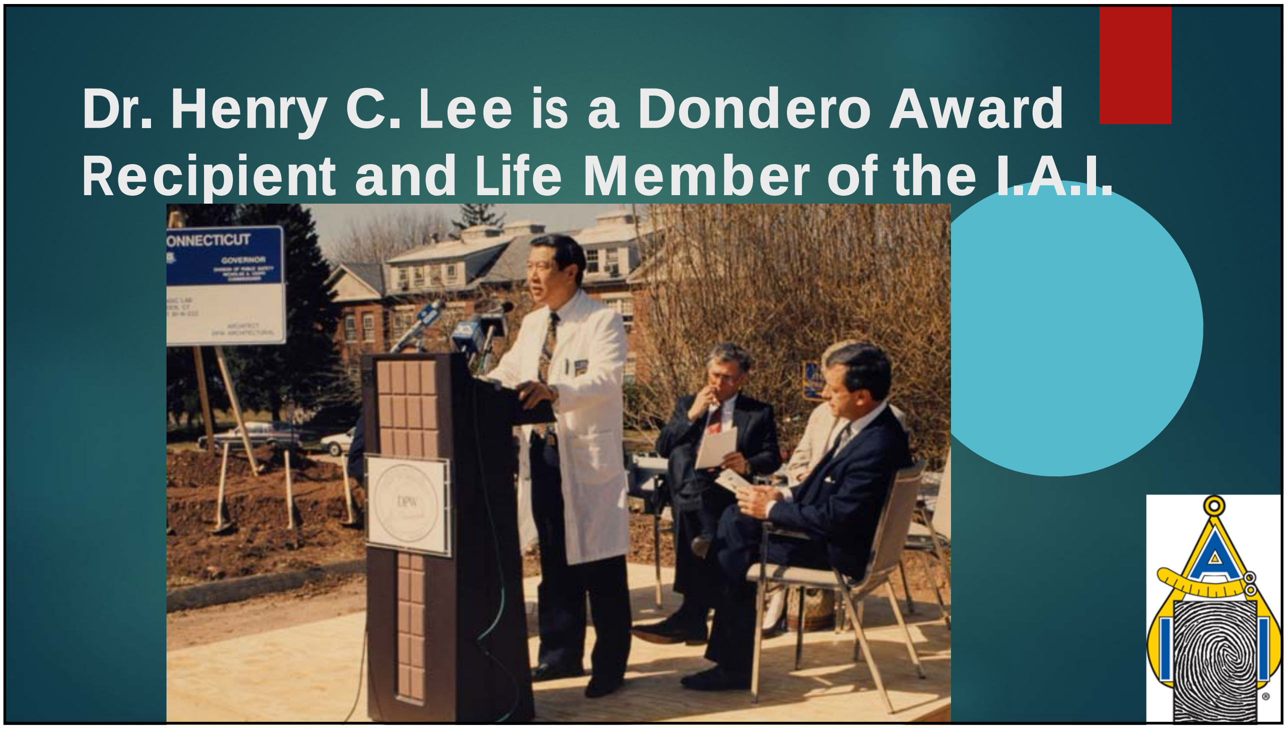


I.A.I.'s Areas of Science and Practice:

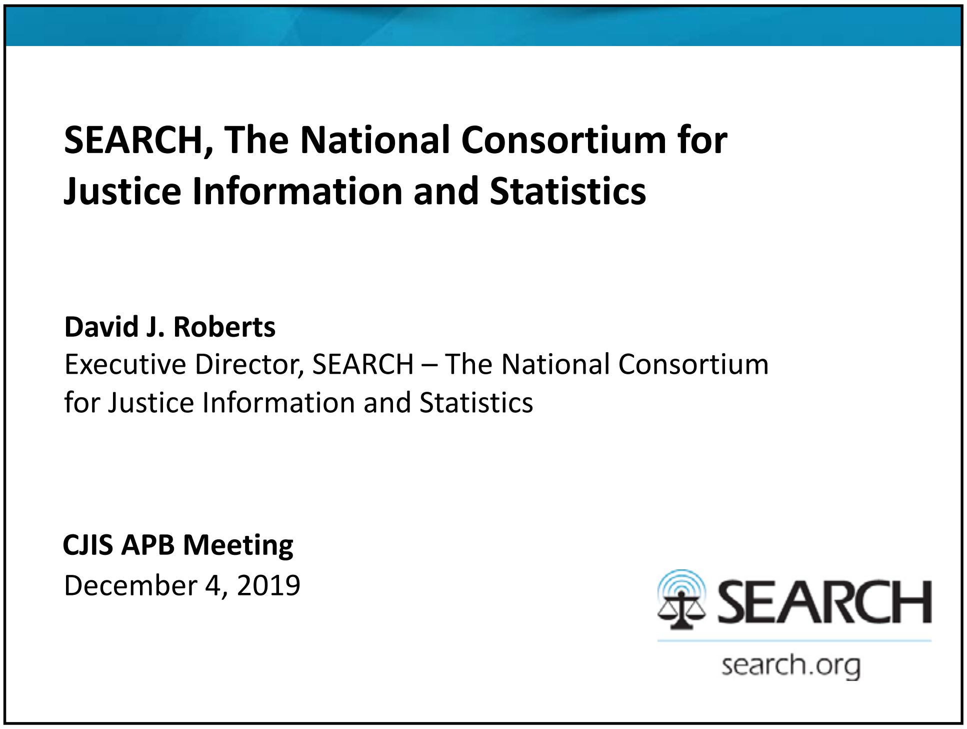
- Latent Fingerprints
- Ten Print
- AFIS & Biometrics
- Footwear and Tire Track
- Facial Recognition
- Blood Stain Analysis
- Crime Scene Investigation
  - Reconstruction
- Forensic Art
- Forensic Photography and Electronic Imaging
- Digital and Multi Media
- General Forensics (DNA, Laboratory Management)

CERTIFICATIONS IN THE FOLLOWING

- Latent Fingerprint Analysis
- Ten print Fingerprint
- Footwear and Tire Track Analysis
- Forensic Photography
- Bloodstain Analysis
- Forensic Art
- Forensic Video
- Crime Scene Certification
  - CSI – Investigator
  - CSI – Analyst
  - CSI – Reconstructionist
  - CSI – Senior CS Analyst



Dr. Henry C. Lee is a Dondero Award Recipient and Life Member of the I.A.I.

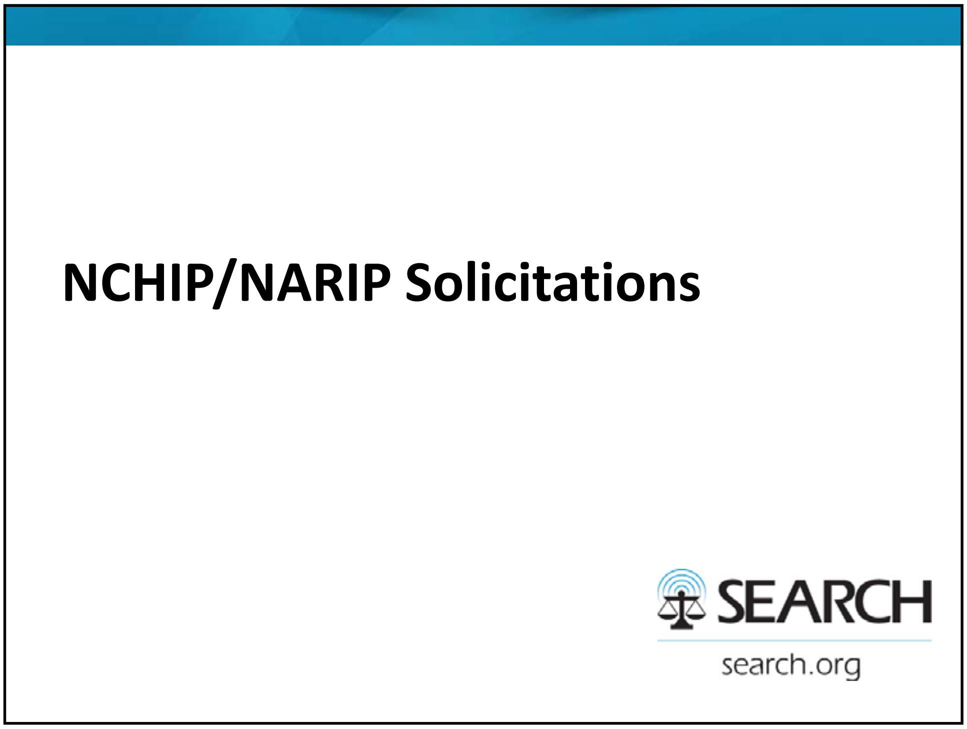


SEARCH, The National Consortium for Justice Information and Statistics

David J. Roberts
Executive Director, SEARCH – The National Consortium
for Justice Information and Statistics

CJIS APB Meeting
December 4, 2019

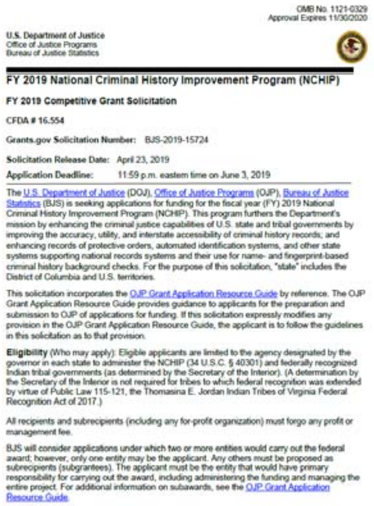
SEARCH
search.org



NCHIP/NARIP Solicitations

SEARCH
search.org

NCHIP/NARIP Solicitations



OMB No. 1121-0329
Approval Expires 11/30/2020

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Statistics

FY 2019 National Criminal History Improvement Program (NCHIP)

FY 2019 Competitive Grant Solicitation

CFDA # 16.554

Grants.gov Solicitation Number: BJS-2019-15724

Solicitation Release Date: April 23, 2019

Application Deadline: 11:59 p.m. eastern time on June 3, 2019

The U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Statistics (BJS) is seeking applications for funding for the fiscal year (FY) 2019 National Criminal History Improvement Program (NCHIP). This program furthers the Department's mission by enhancing the criminal justice capabilities of U.S. state and tribal governments by improving the accuracy, utility, and interstate accessibility of criminal history records; and enhancing records of protective orders, automated identification systems, and other state systems supporting national records systems and their use for name- and fingerprint-based criminal history background checks. For the purpose of this solicitation, "state" includes the District of Columbia and U.S. territories.

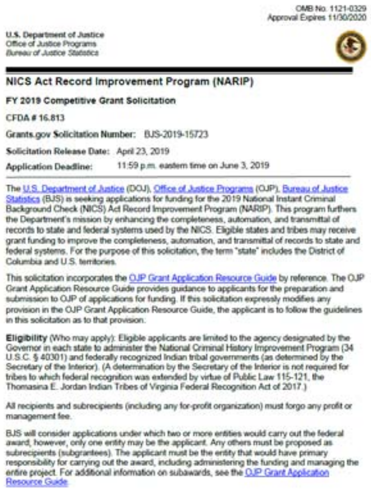
This solicitation incorporates the OJP Grant Application Resource Guide by reference. The OJP Grant Application Resource Guide provides guidance to applicants for the preparation and submission to OJP of applications for funding. If this solicitation expressly modifies any provision in the OJP Grant Application Resource Guide, the applicant is to follow the guidelines in this solicitation as to that provision.

Eligibility (Who may apply): Eligible applicants are limited to the agency designated by the governor in each state to administer the NCHIP (34 U.S.C. § 40301) and federally recognized Indian tribal governments (as determined by the Secretary of the Interior). (A determination by the Secretary of the Interior is not required for tribes to which federal recognition was extended by virtue of Public Law 115-121, the Thomasina E. Jordan Indian Tribes of Virginia Federal Recognition Act of 2017.)

All recipients and subrecipients (including any for-profit organization) must forgo any profit or management fee.

BJS will consider applications under which two or more entities would carry out the federal award; however, only one entity may be the applicant. Any others must be proposed as subrecipients (subgrantees). The applicant must be the entity that would have primary responsibility for carrying out the award, including administering the funding and managing the entire project. For additional information on subawards, see the OJP Grant Application Resource Guide.

39 Awards / $49,359,637



OMB No. 1121-0329
Approval Expires 11/30/2020

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Statistics

NICS Act Record Improvement Program (NARIP)

FY 2019 Competitive Grant Solicitation

CFDA # 16.813

Grants.gov Solicitation Number: BJS-2019-15723

Solicitation Release Date: April 23, 2019

Application Deadline: 11:59 p.m. eastern time on June 3, 2019

The U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Statistics (BJS) is seeking applications for funding for the 2019 National Instant Criminal Background Check (NICS) Act Record Improvement Program (NARIP). This program furthers the Department's mission by enhancing the completeness, automation, and transmittal of records to state and federal systems used by the NICS. Eligible states and tribes may receive grant funding to improve the completeness, automation, and transmittal of records to state and federal systems. For the purpose of this solicitation, the term "state" includes the District of Columbia and U.S. territories.

This solicitation incorporates the OJP Grant Application Resource Guide by reference. The OJP Grant Application Resource Guide provides guidance to applicants for the preparation and submission to OJP of applications for funding. If this solicitation expressly modifies any provision in the OJP Grant Application Resource Guide, the applicant is to follow the guidelines in this solicitation as to that provision.

Eligibility (Who may apply): Eligible applicants are limited to the agency designated by the Governor in each state to administer the National Criminal History Improvement Program (34 U.S.C. § 40301) and federally recognized Indian tribal governments (as determined by the Secretary of the Interior). (A determination by the Secretary of the Interior is not required for tribes to which federal recognition was extended by virtue of Public Law 115-121, the Thomasina E. Jordan Indian Tribes of Virginia Federal Recognition Act of 2017.)

All recipients and subrecipients (including any for-profit organization) must forgo any profit or management fee.

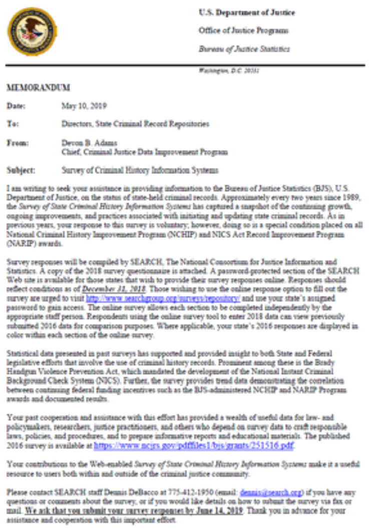
BJS will consider applications under which two or more entities would carry out the federal award; however, only one entity may be the applicant. Any others must be proposed as subrecipients (subgrantees). The applicant must be the entity that would have primary responsibility for carrying out the award, including administering the funding and managing the entire project. For additional information on subawards, see the OJP Grant Application Resource Guide.

19 Awards / $13,541,946

2018 Survey of State Criminal History Information Systems (SSCHIS)

SEARCH
search.org

2018 Survey of State CHIS



U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Statistics

Washington, D.C. 20531

MEMORANDUM

Date: May 10, 2019

To: Directors, State Criminal Record Repositories

From: Devon B. Adams
Chief, Criminal Justice Data Improvement Program

Subject: Survey of Criminal History Information Systems

I am writing to seek your assistance in providing information to the Bureau of Justice Statistics (BJS), U.S. Department of Justice, on the status of state-held criminal records. Approximately every two years since 1989, the *Survey of State Criminal History Information Systems* has captured a snapshot of the continuing growth, ongoing improvements, and practices associated with initiating and updating state criminal records. As in previous years, your response to this survey is voluntary; however, doing so is a special condition placed on all National Criminal History Improvement Program (NCHIP) and NICS Act Record Improvement Program (NARIP) awards.

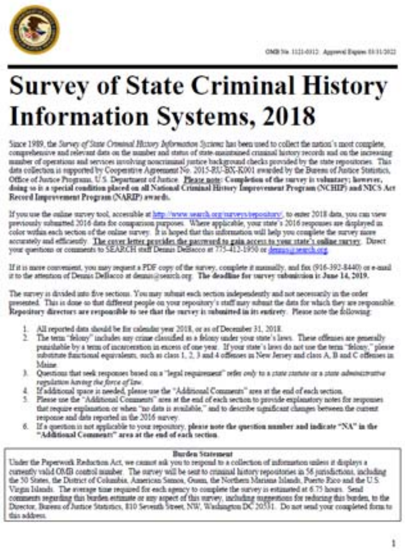
Survey responses will be compiled by SEARCH, The National Consortium for Justice Information and Statistics. A copy of the 2018 survey questionnaire is attached. A password-protected section of the SEARCH Web site is available for those states that wish to provide their survey responses online. Responses should reflect conditions as of *December 31, 2018*. Those wishing to use the online response option to fill out the survey are urged to visit http://www.searchgroup.org/surveys/repository/ and use your state's assigned password to gain access. The online survey allows each section to be completed independently by the appropriate staff person. Respondents using the online survey tool to enter 2018 data can view previously submitted 2016 data for comparison purposes. Where applicable, your state's 2016 responses are displayed in color within each section of the online survey.

Statistical data presented in past surveys has supported and provided insight to both State and Federal legislative efforts that involve the use of criminal history records. Prominent among these is the Brady Handgun Violence Prevention Act, which mandated the development of the National Instant Criminal Background Check System (NICS). Further, the survey provides trend data demonstrating the correlation between continuing federal funding incentives such as the BJS-administered NCHIP and NARIP Program awards and documented results.

Your past cooperation and assistance with this effort has provided a wealth of useful data for law- and policymakers, researchers, justice practitioners, and others who depend on survey data to craft responsible laws, policies, and procedures, and to prepare informative reports and educational materials. The published 2016 survey is available at https://www.ncjrs.gov/pdffiles1/bjs/grants/251516.pdf.

Your contributions to the Web-enabled *Survey of State Criminal History Information Systems* make it a useful resource to users both within and outside of the criminal justice community.

Please contact SEARCH staff Dennis DeBacco at 775-412-1950 (email: dennis@search.org) if you have any questions or comments about the survey, or if you would like details on how to submit the survey via fax or mail. **We ask that you submit your survey responses by June 14, 2019**. Thank you in advance for your assistance and cooperation with this important effort.



OMB No. 1121-0312: Approval Expires 03/31/2022

Survey of State Criminal History Information Systems, 2018

Since 1989, the *Survey of State Criminal History Information Systems* has been used to collect the nation's most complete, comprehensive and relevant data on the number and status of state-maintained criminal history records and on the increasing number of operations and services involving noncriminal justice background checks provided by the state repositories. This data collection is supported by Cooperative Agreement No. 2015-RU-BX-K001 awarded by the Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice. Please note: **Completion of the survey is voluntary; however, doing so is a special condition placed on all National Criminal History Improvement Program (NCHIP) and NICS Act Record Improvement Program (NARIP) awards.**

If you use the online survey tool, accessible at http://www.search.org/surveys/repository/, to enter 2018 data, you can view previously submitted 2016 data for comparison purposes. Where applicable, your state's 2016 responses are displayed in color within each section of the online survey. It is hoped that this information will help you complete the survey more accurately and efficiently. **The cover letter provides the password to gain access to your state's online survey.** Direct your questions or comments to SEARCH staff Dennis DeBacco at 775-412-1950 or dennis@search.org.

If it is more convenient, you may request a PDF copy of the survey, complete it manually, and fax (916-392-8440) or e-mail it to the attention of Dennis DeBacco at dennis@search.org. **The deadline for survey submission is June 14, 2019.**

The survey is divided into five sections. You may submit each section independently and not necessarily in the order presented. This is done so that different people on your repository's staff may submit the data for which they are responsible. **Repository directors are responsible to see that the survey is submitted in its entirety.** Please note the following:

1. All reported data should be for calendar year 2018, or as of December 31, 2018.
2. The term "felony" includes any crime classified as a felony under your state's laws. These offenses are generally punishable by a term of incarceration in excess of one year. If your state's laws do not use the term "felony," please substitute functional equivalents, such as class 1, 2, 3 and 4 offenses in New Jersey and class A, B and C offenses in Maine.
3. Questions that seek responses based on a "legal requirement" refer *only* to a *state statute* or a *state administrative regulation having the force of law*.
4. If additional space is needed, please use the "Additional Comments" area at the end of each section.
5. Please use the "Additional Comments" area at the end of each section to provide explanatory notes for responses that require explanation or when "no data is available," and to describe significant changes between the current response and data reported in the 2016 survey.
6. If a question is not applicable to your repository, **please note the question number and indicate "NA" in the "Additional Comments" area at the end of each section.**

Burden Statement
Under the Paperwork Reduction Act, we cannot ask you to respond to a collection of information unless it displays a currently valid OMB control number. The survey will be sent to criminal history repositories in 56 jurisdictions, including the 50 States, the District of Columbia, American Samoa, Guam, the Northern Mariana Islands, Puerto Rico and the U.S. Virgin Islands. The average time required for each agency to complete the survey is estimated at 6.75 hours. Send comments regarding this burden estimate or any aspect of this survey, including suggestions for reducing this burden, to the Director, Bureau of Justice Statistics, 810 Seventh Street, NW, Washington DC 20531. Do not send your completed form to this address.

1

Survey Status Update

- 100% of States have completed their surveys
- Survey tables are 98% complete
- Final internal quality assurance review will be completed by the end of November
- Will be submitted to BJS for final approval by first week of December
- Publication is anticipated in early 2020

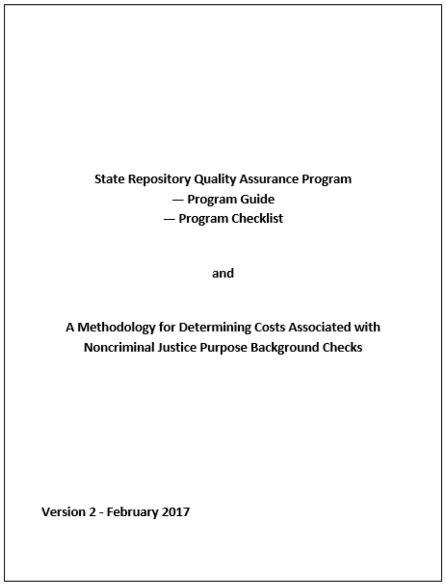
Quality Assurance Program (QAP) and Criminal History Records Improvement Workshops

SEARCH

search.org

SEARCH Quality Assurance Program

- QAP Checklist – developed in 2012 and revised in 2017
- Voluntary performance standards for criminal history information maintenance and reporting requirements
- Includes methodology to estimate CCH repository operations costs



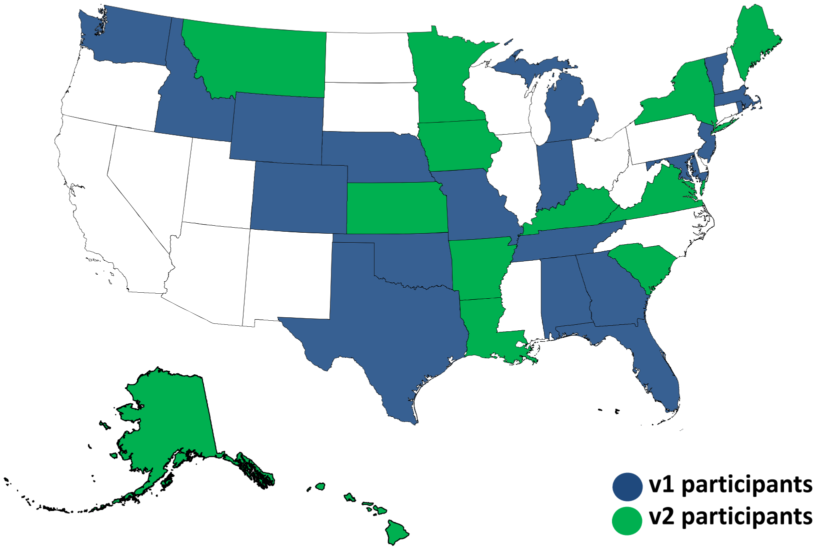
State Repository Quality Assurance Program
— Program Guide
— Program Checklist

and

A Methodology for Determining Costs Associated with
Noncriminal Justice Purpose Background Checks

Version 2 - February 2017

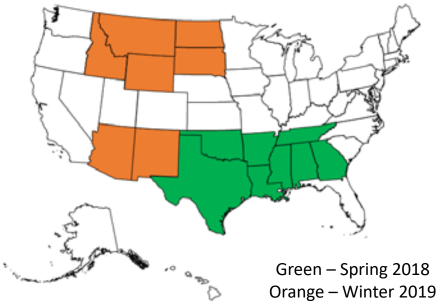
QAP Participation Map



Criminal History Record Improvement Workshops

- Facilitators – Bureau of Justice Statistics, Federal Bureau of Investigation, National Center for State Courts and SEARCH
- Participants – Teams from each state - criminal history repository staff, law enforcement, courts, prosecutors, judicial college staff
- Topics covered:
  - Creation, use and maintenance of criminal history records
  - Disposition reporting
  - NICS prohibitors
  - National Criminal History Improvement Program (NCHP)
  - NICS Act Record Improvement Program (NARIP)

Participating States



Green – Spring 2018
Orange – Winter 2019

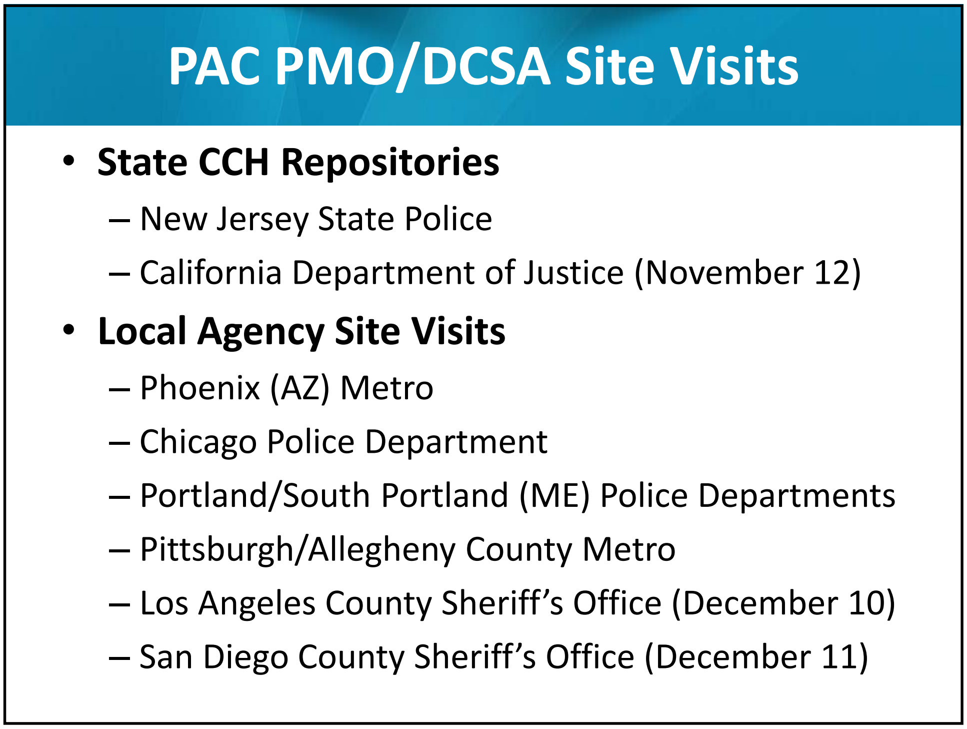
Criminal History Record Gap Analysis

OPM Performance Accountability Council Project Management Office (PAC PMO)
Defense Counterintelligence and Security Agency (DCSA) ***[formerly NBIB]***

SEARCH
search.org

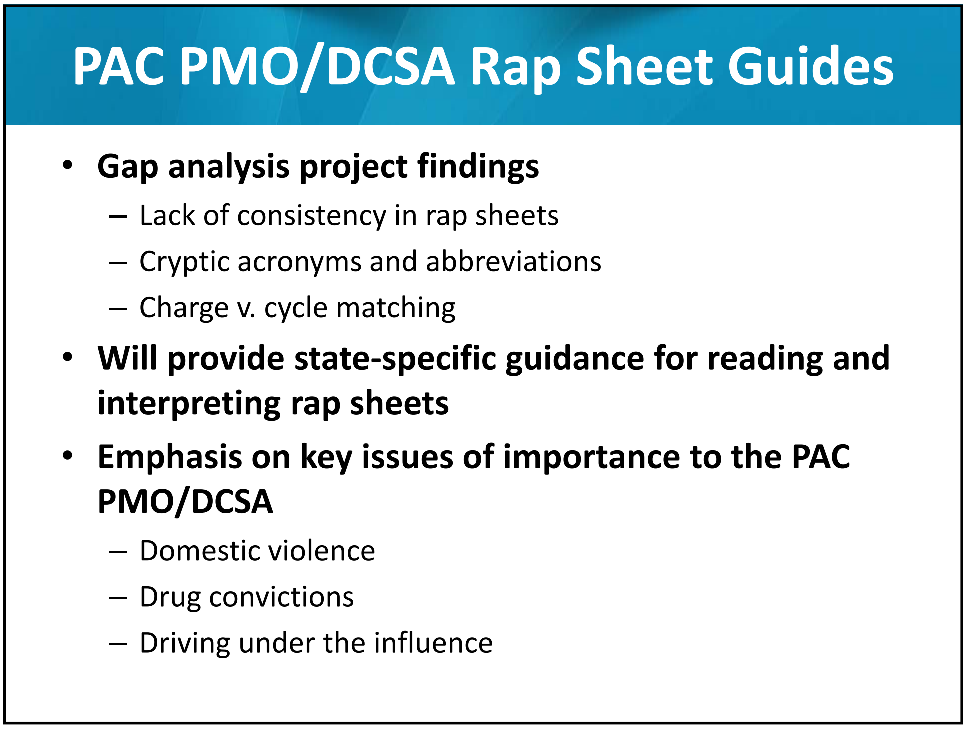
PAC PMO/DCSA Gap Analysis

- **Detailed profiles of CCH Repositories**
- **Inventory/mapping of state CHR to the JTF Standardized XML Rapsheet 4.1**
  - ✓ 37 states completed
- **Cite and release practices**
- **Assessing costs for non-criminal queries**
- **Implications of "Clean Slate" laws on criminal history records made available for civil background checks**
- **On-site detailed review w/2 states and 6 local agencies**



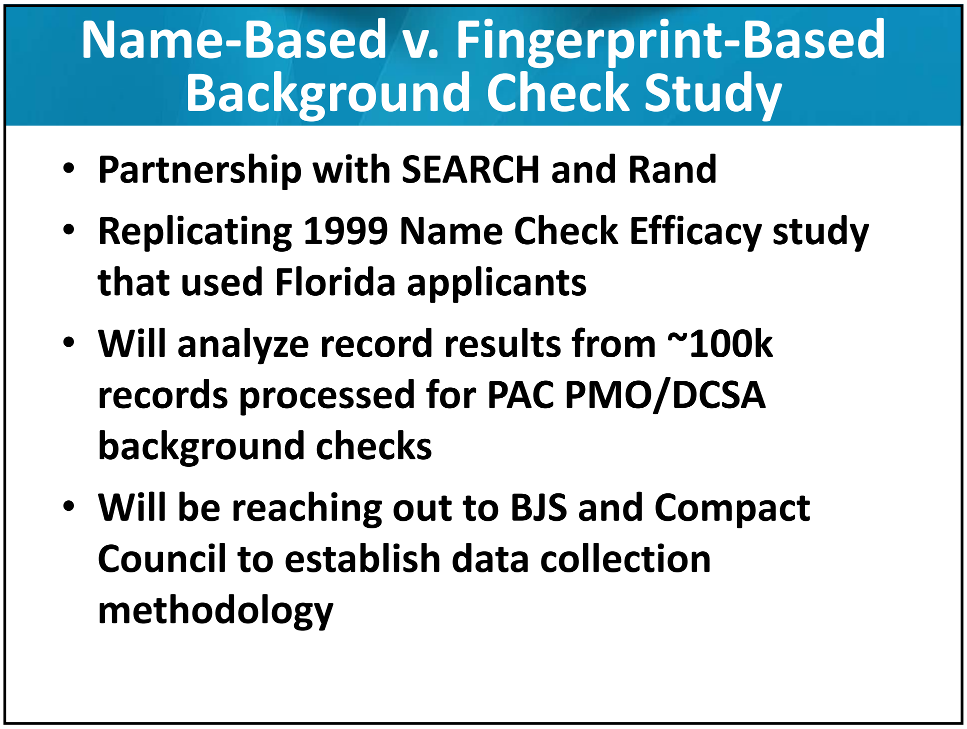
PAC PMO/DCSA Site Visits

- **State CCH Repositories**
  - – New Jersey State Police
  - – California Department of Justice (November 12)
- **Local Agency Site Visits**
  - – Phoenix (AZ) Metro
  - – Chicago Police Department
  - – Portland/South Portland (ME) Police Departments
  - – Pittsburgh/Allegheny County Metro
  - – Los Angeles County Sheriff’s Office (December 10)
  - – San Diego County Sheriff’s Office (December 11)



PAC PMO/DCSA Rap Sheet Guides

- **Gap analysis project findings**
  - – Lack of consistency in rap sheets
  - – Cryptic acronyms and abbreviations
  - – Charge v. cycle matching
- **Will provide state-specific guidance for reading and interpreting rap sheets**
- **Emphasis on key issues of importance to the PAC PMO/DCSA**
  - – Domestic violence
  - – Drug convictions
  - – Driving under the influence

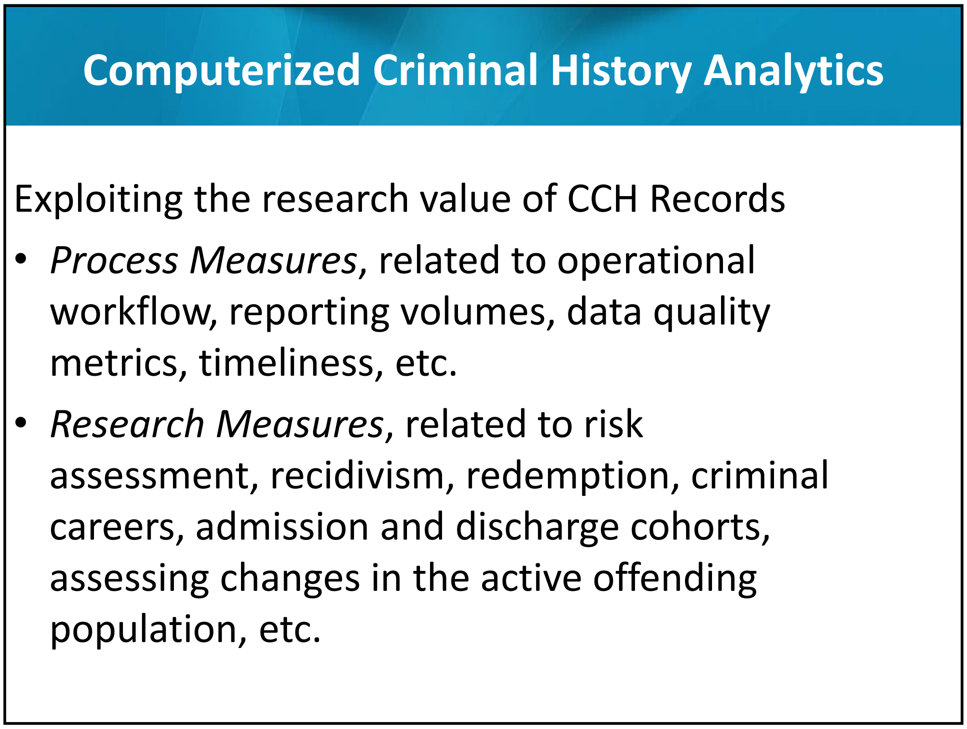


Name-Based v. Fingerprint-Based Background Check Study

- Partnership with SEARCH and Rand
- Replicating 1999 Name Check Efficacy study that used Florida applicants
- Will analyze record results from ~100k records processed for PAC PMO/DCSA background checks
- Will be reaching out to BJS and Compact Council to establish data collection methodology

Developing Criminal History Metrics and Research Measures

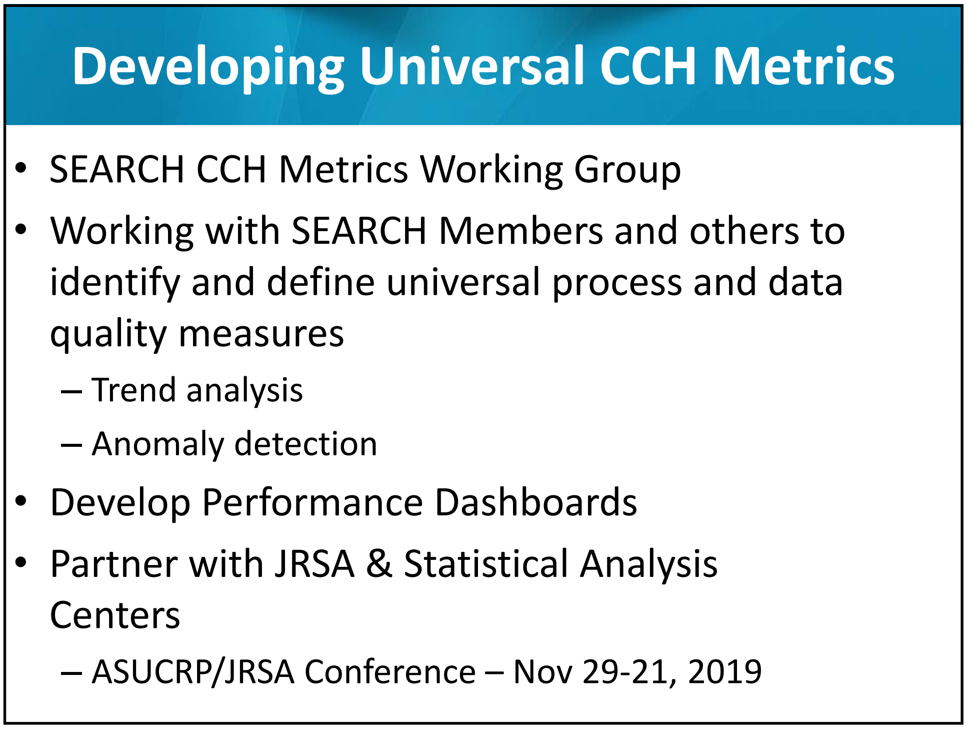
SEARCH
search.org



Computerized Criminal History Analytics

Exploiting the research value of CCH Records

- *Process Measures*, related to operational workflow, reporting volumes, data quality metrics, timeliness, etc.
- *Research Measures*, related to risk assessment, recidivism, redemption, criminal careers, admission and discharge cohorts, assessing changes in the active offending population, etc.



Developing Universal CCH Metrics

- SEARCH CCH Metrics Working Group
- Working with SEARCH Members and others to identify and define universal process and data quality measures
  - Trend analysis
  - Anomaly detection
- Develop Performance Dashboards
- Partner with JRSA & Statistical Analysis Centers
  - ASUCRP/JRSA Conference – Nov 29-21, 2019

CCH Metrics Working Group

Chair: Mr. Matthew R. Ruel, Maine State Police

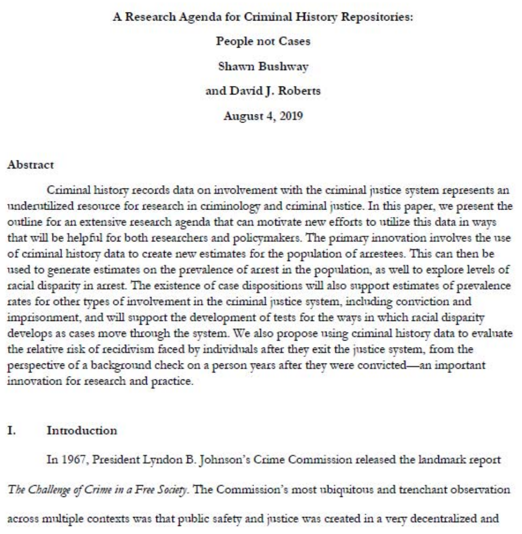
- SEARCH Members
  - Major Brandon Gray (NJ)
  - Ms. Debbie McKinney (OK)
  - Capt. Monty Coates (SC)
  - Dr. Alfred Blumstein (At-Large)
  - Dr. James Lynch (At-Large)
- Will be reaching out to:
  - Arkansas
  - Iowa
  - Tennessee
- Justice Research and Statistics Association
  - Mr. Roger Przybylski, Director of Research
- Statistical Analysis Centers
  - Derrick Veitenheimer, Wisconsin Department of Justice
  - Dr. Kiminori Nakamura, University of Maryland/MD SAC

Ex Officio

- Bureau of Justice Statistics
- Arnold Ventures

Developed a CCH Research Agenda

1. Arrests and Arrestees
2. Understanding Recidivism Using Arrest Cohorts
3. Prevalence of Criminal History Records
4. Understanding the Impact of Race in Justice Decisionmaking



A Research Agenda for Criminal History Repositories:

People not Cases

Shawn Bushway

and David J. Roberts

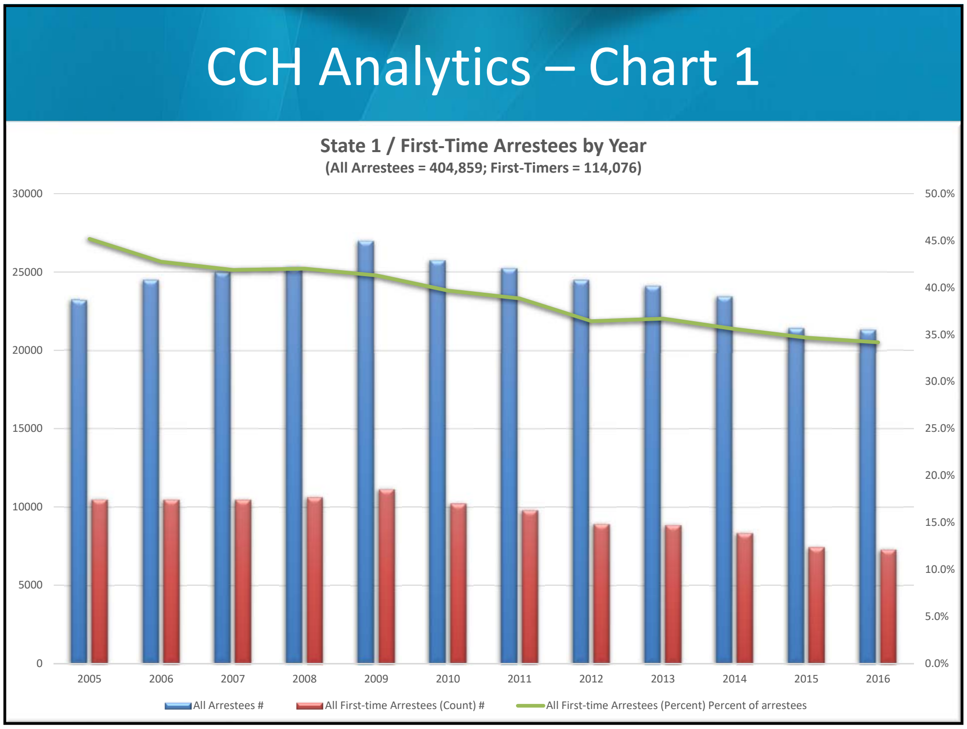
August 4, 2019

Abstract

Criminal history records data on involvement with the criminal justice system represents an underutilized resource for research in criminology and criminal justice. In this paper, we present the outline for an extensive research agenda that can motivate new efforts to utilize this data in ways that will be helpful for both researchers and policymakers. The primary innovation involves the use of criminal history data to create new estimates for the population of arrestees. This can then be used to generate estimates on the prevalence of arrest in the population, as well to explore levels of racial disparity in arrest. The existence of case dispositions will also support estimates of prevalence rates for other types of involvement in the criminal justice system, including conviction and imprisonment, and will support the development of tests for the ways in which racial disparity develops as cases move through the system. We also propose using criminal history data to evaluate the relative risk of recidivism faced by individuals after they exit the justice system, from the perspective of a background check on a person years after they were convicted—an important innovation for research and practice.

I. Introduction

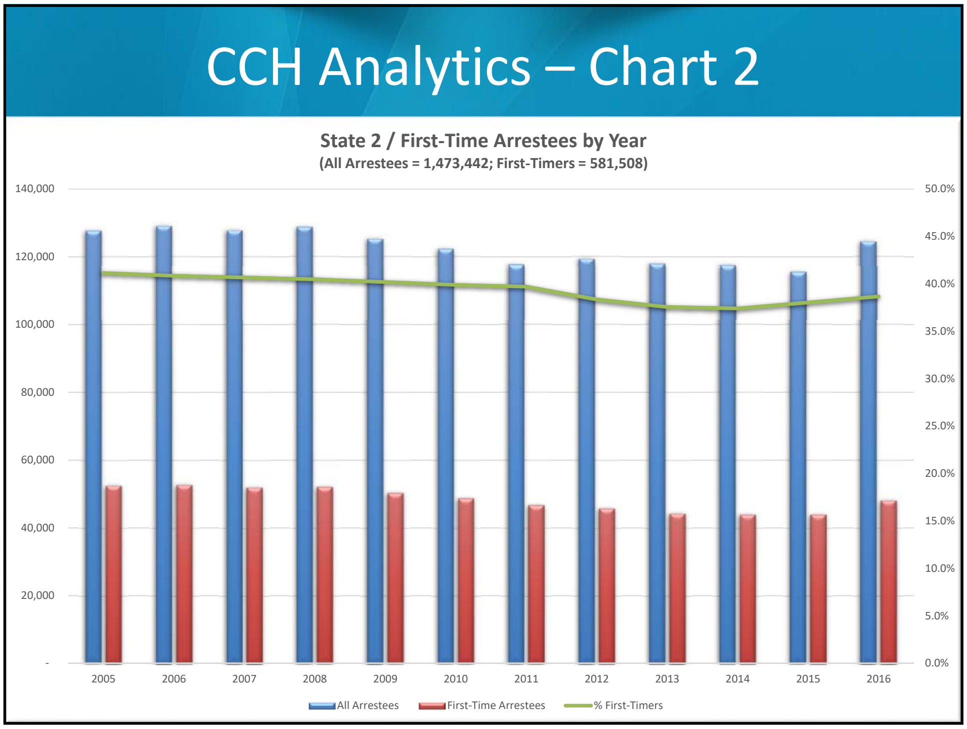
In 1967, President Lyndon B. Johnson's Crime Commission released the landmark report *The Challenge of Crime in a Free Society*. The Commission's most ubiquitous and trenchant observation across multiple contexts was that public safety and justice was created in a very decentralized and



CCH Analytics – Chart 1

State 1 / First-Time Arrestees by Year

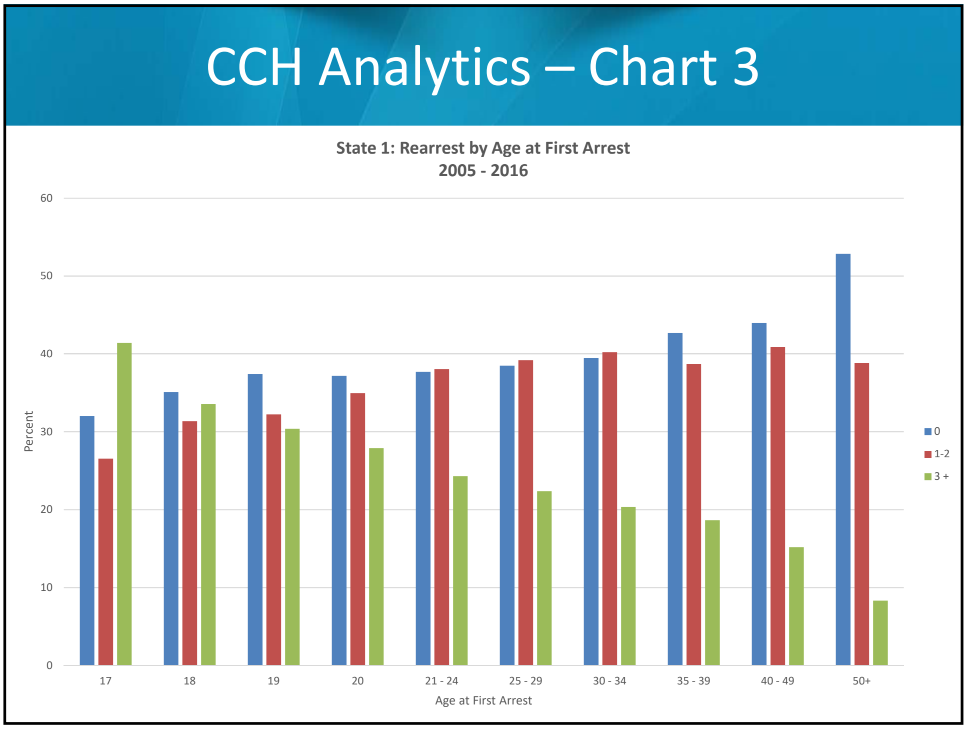
(All Arrestees = 404,859; First-Timers = 114,076)



CCH Analytics – Chart 2

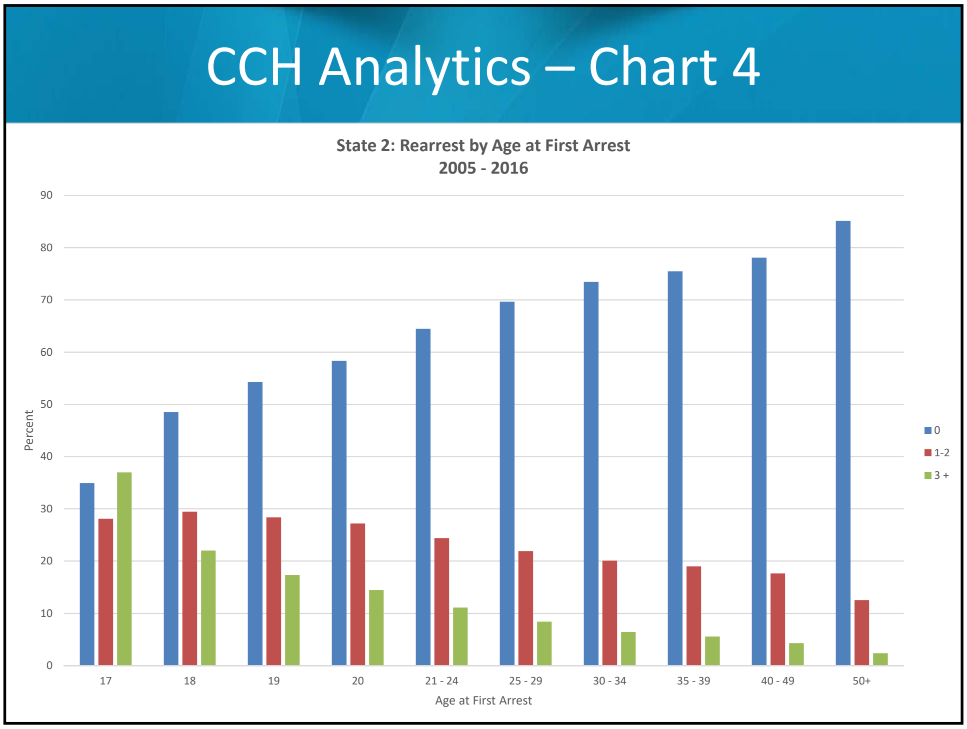
State 2 / First-Time Arrestees by Year

(All Arrestees = 1,473,442; First-Timers = 581,508)



CCH Analytics – Chart 3

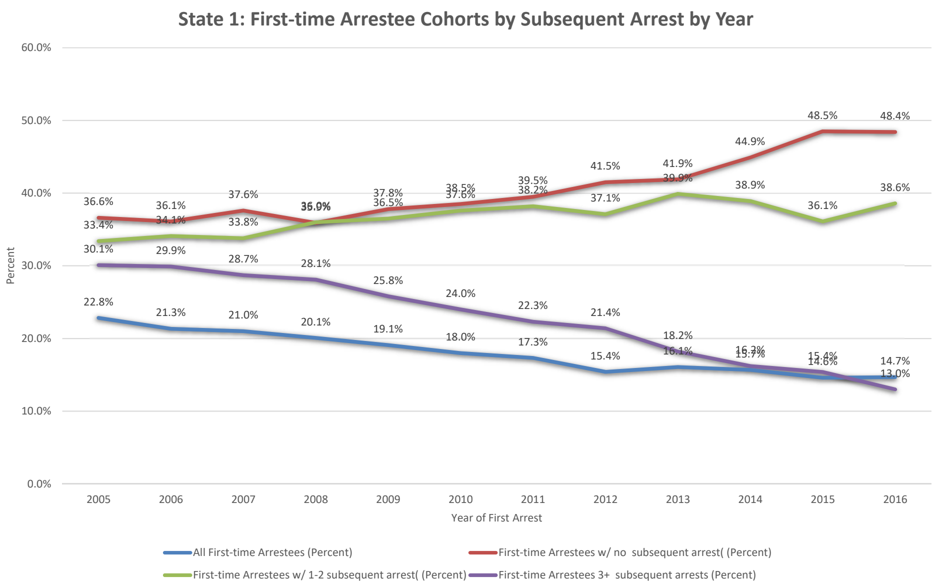
State 1: Rearrest by Age at First Arrest
2005 - 2016



CCH Analytics – Chart 4

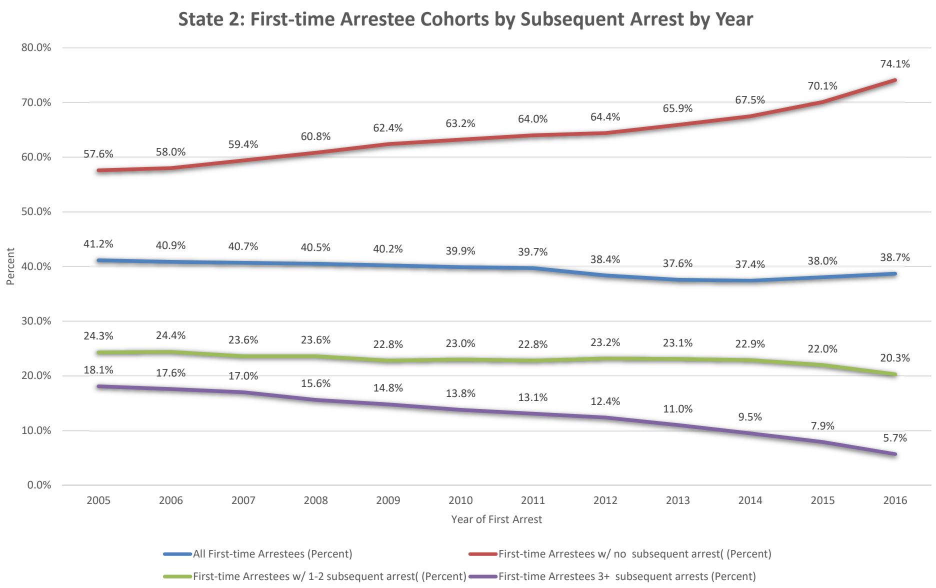
State 2: Rearrest by Age at First Arrest
2005 - 2016

CCH Analytics – Chart 5

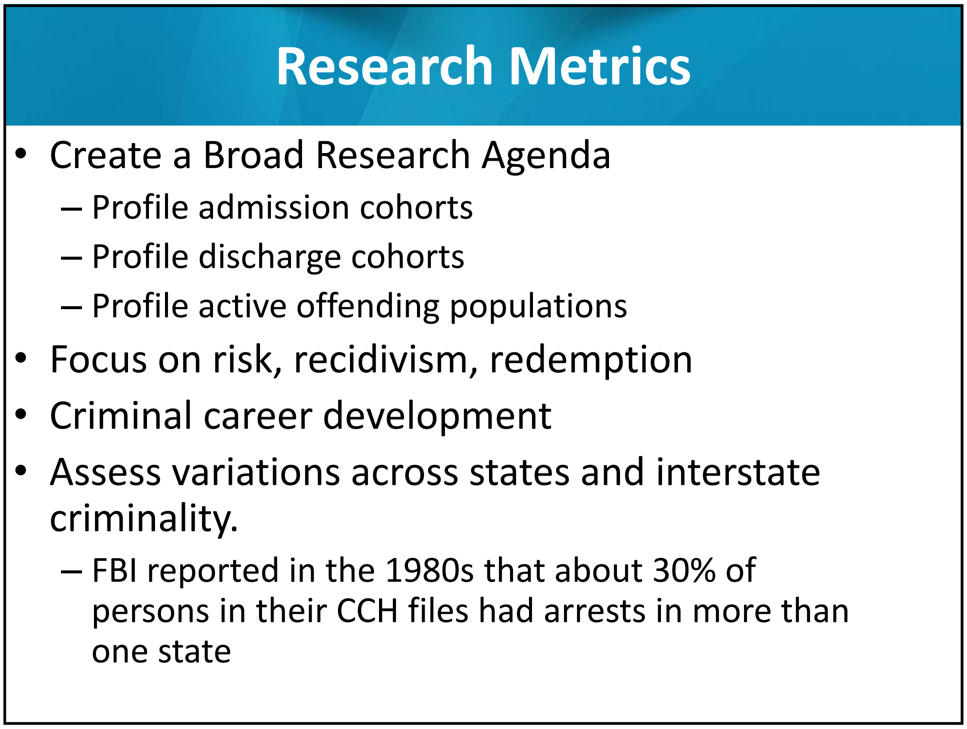


State 1: First-time Arrestee Cohorts by Subsequent Arrest by Year

CCH Analytics – Chart 4

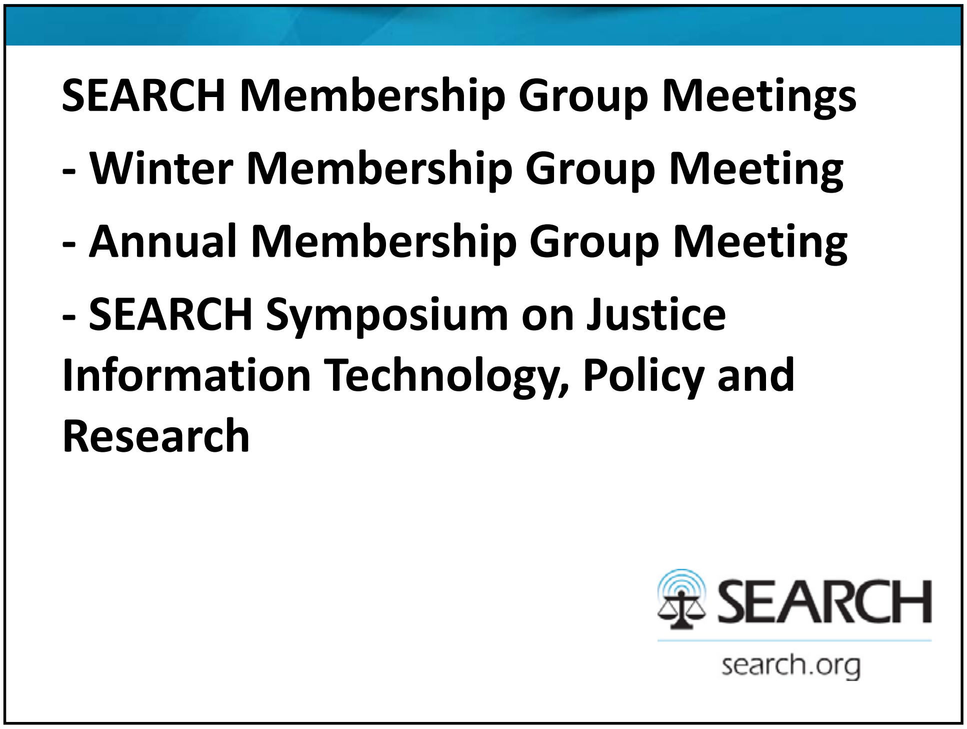


State 2: First-time Arrestee Cohorts by Subsequent Arrest by Year



Research Metrics

- Create a Broad Research Agenda
  - Profile admission cohorts
  - Profile discharge cohorts
  - Profile active offending populations
- Focus on risk, recidivism, redemption
- Criminal career development
- Assess variations across states and interstate criminality.
  - FBI reported in the 1980s that about 30% of persons in their CCH files had arrests in more than one state



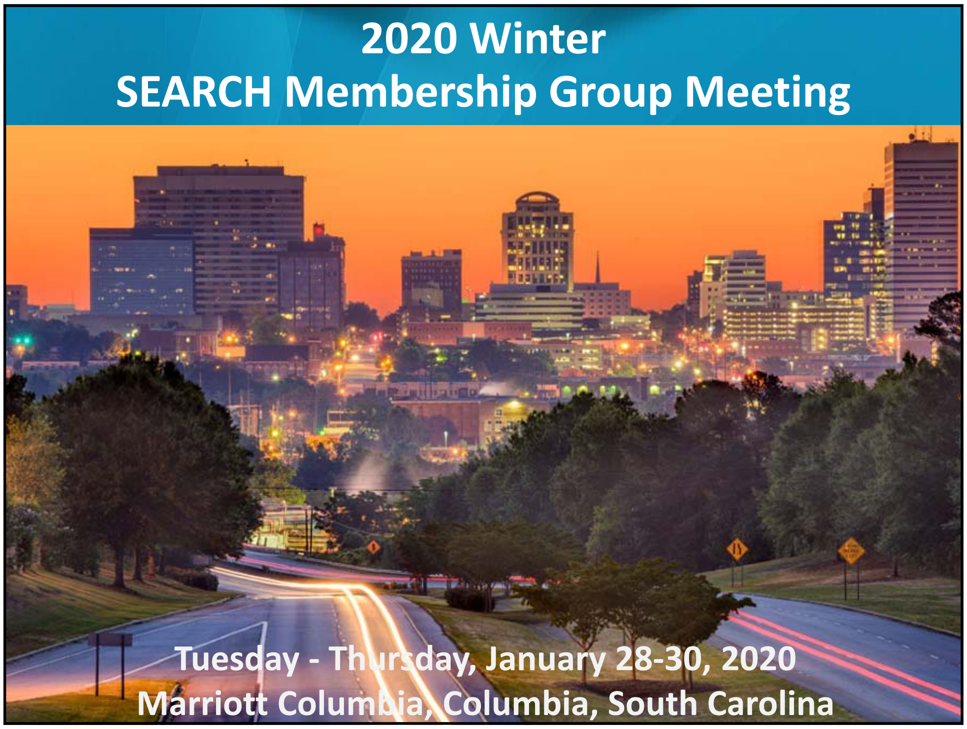
SEARCH Membership Group Meetings

- Winter Membership Group Meeting

- Annual Membership Group Meeting

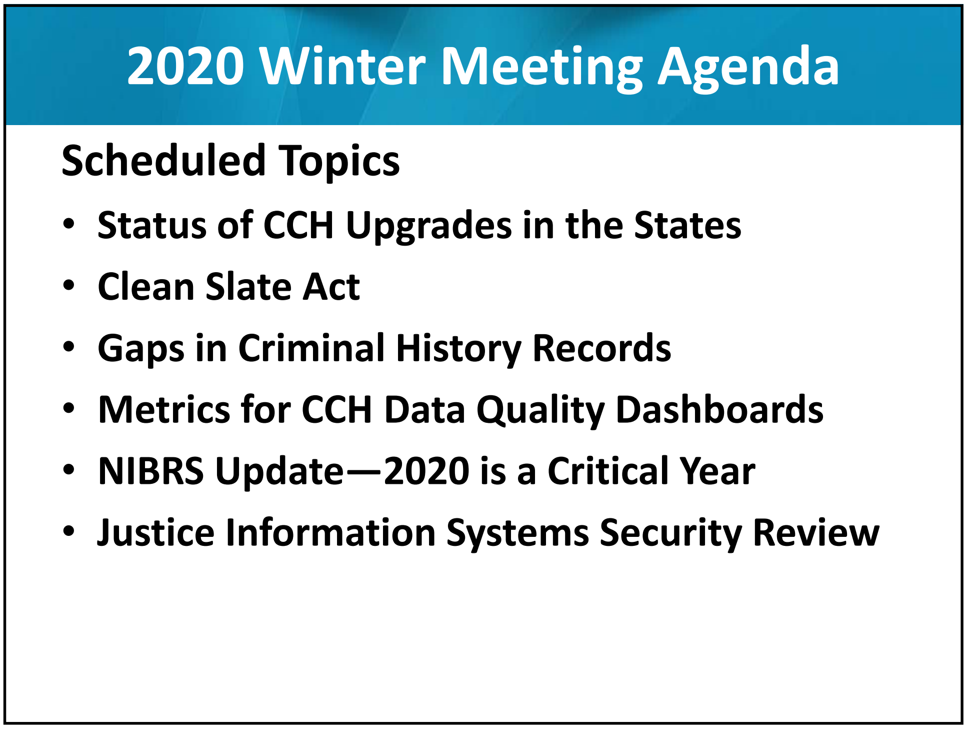
- SEARCH Symposium on Justice Information Technology, Policy and Research

SEARCH
search.org



2020 Winter
SEARCH Membership Group Meeting

Tuesday - Thursday, January 28-30, 2020
Marriott Columbia, Columbia, South Carolina



2020 Winter Meeting Agenda

Scheduled Topics

- Status of CCH Upgrades in the States
- Clean Slate Act
- Gaps in Criminal History Records
- Metrics for CCH Data Quality Dashboards
- NIBRS Update—2020 is a Critical Year
- Justice Information Systems Security Review

2020 Annual Membership Group Meeting

Monday July 20, 2020
St. Louis Union Station Hotel, St. Louis, Missouri

2020 SEARCH Symposium on Justice Information Technology, Policy & Research

Tuesday – Wednesday, July 21-22, 2020
St. Louis Union Station Hotel, St. Louis, Missouri

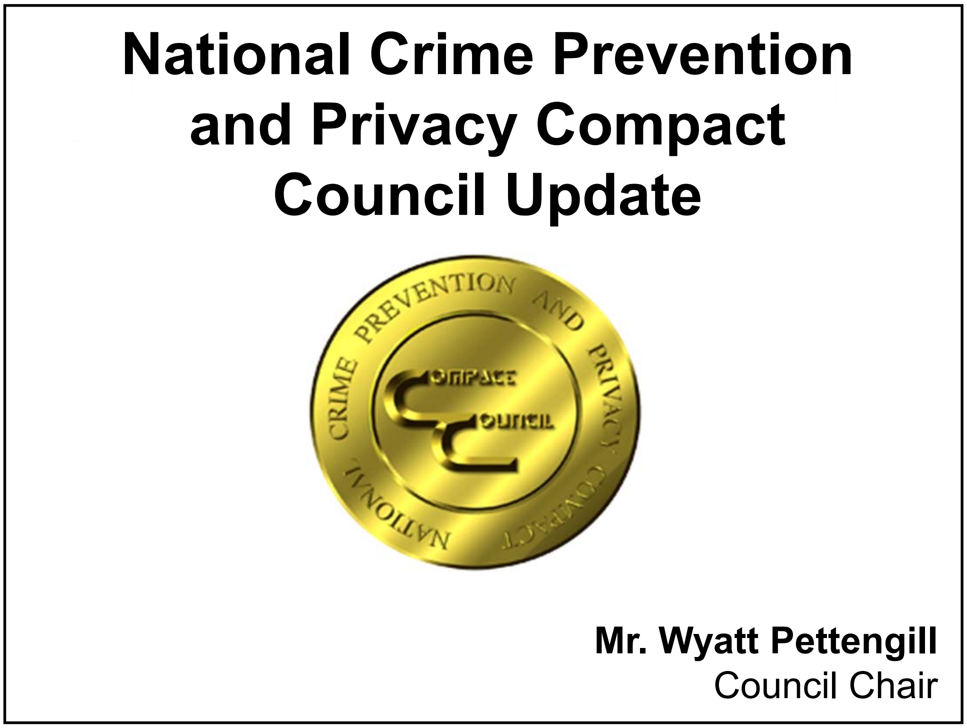
Thank You

David J. Roberts
Executive Director
djroberts@search.org
(202) 909-0298

Becki Goggins
Director, Law & Policy Program
Becki.Goggins@search.org
(916) 392-2550, x306

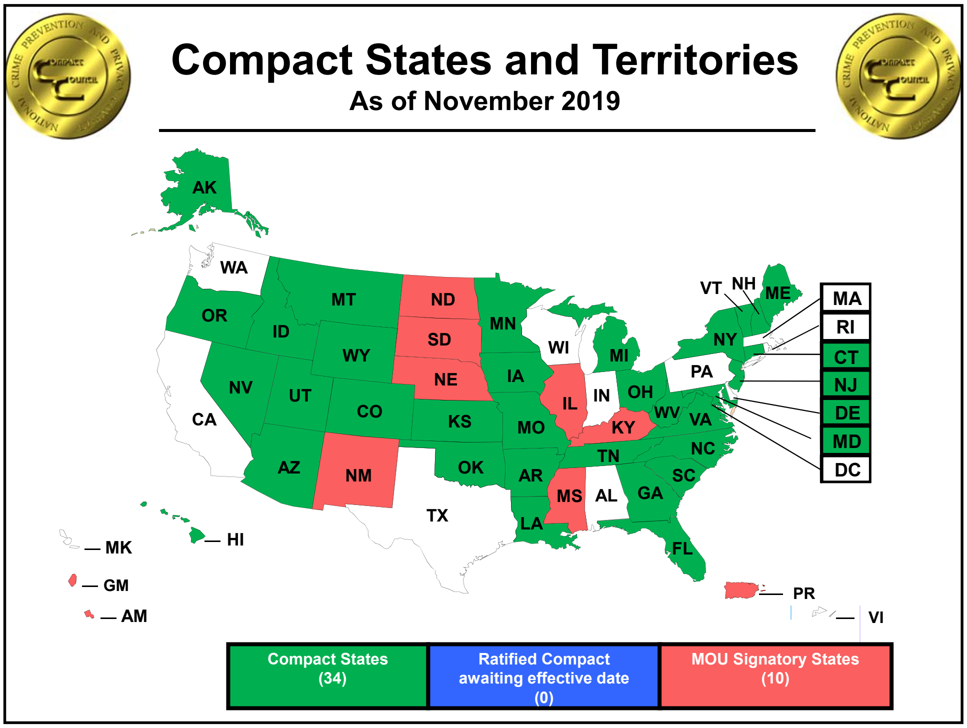
Dennis DeBacco
Justice Information Services Specialist
dennis@search.org
(916) 392-2550, x325

Intentionally Left Blank



National Crime Prevention and Privacy Compact Council Update

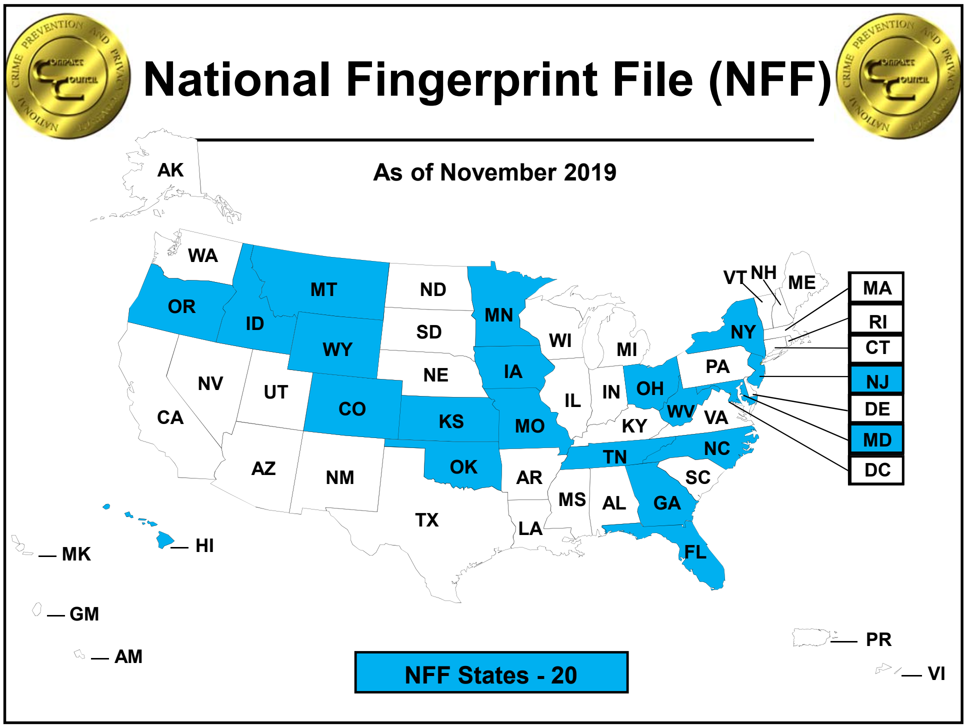
Mr. Wyatt Pettengill
Council Chair



Compact States and Territories

As of November 2019

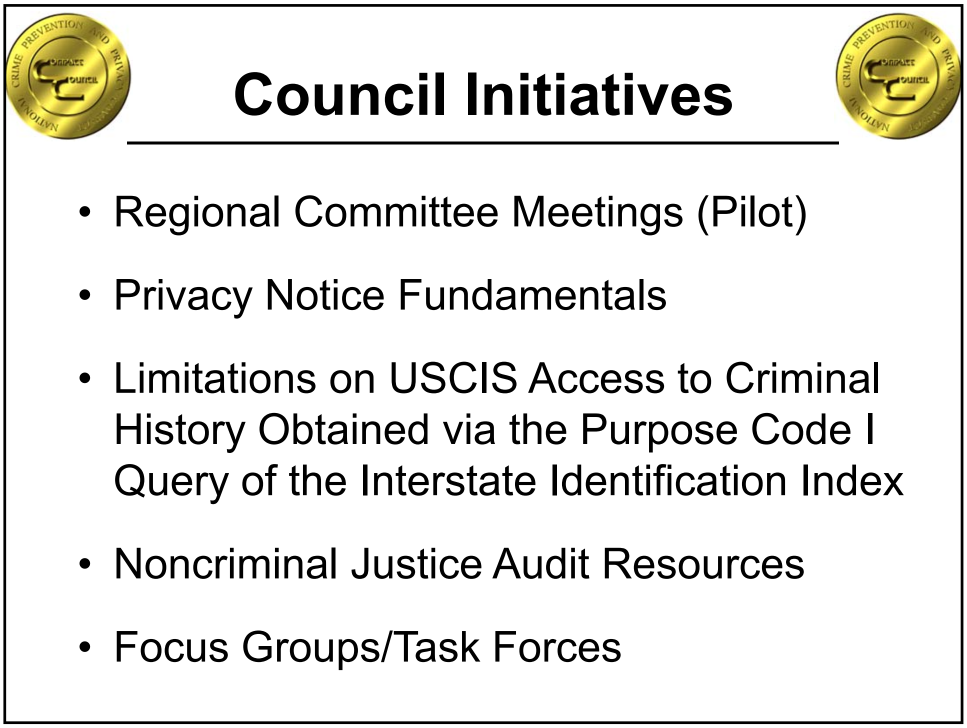
🟩 Compact States (34)	🟦 Ratified Compact awaiting effective date (0)	🟥 MOU Signatory States (10)



National Fingerprint File (NFF)

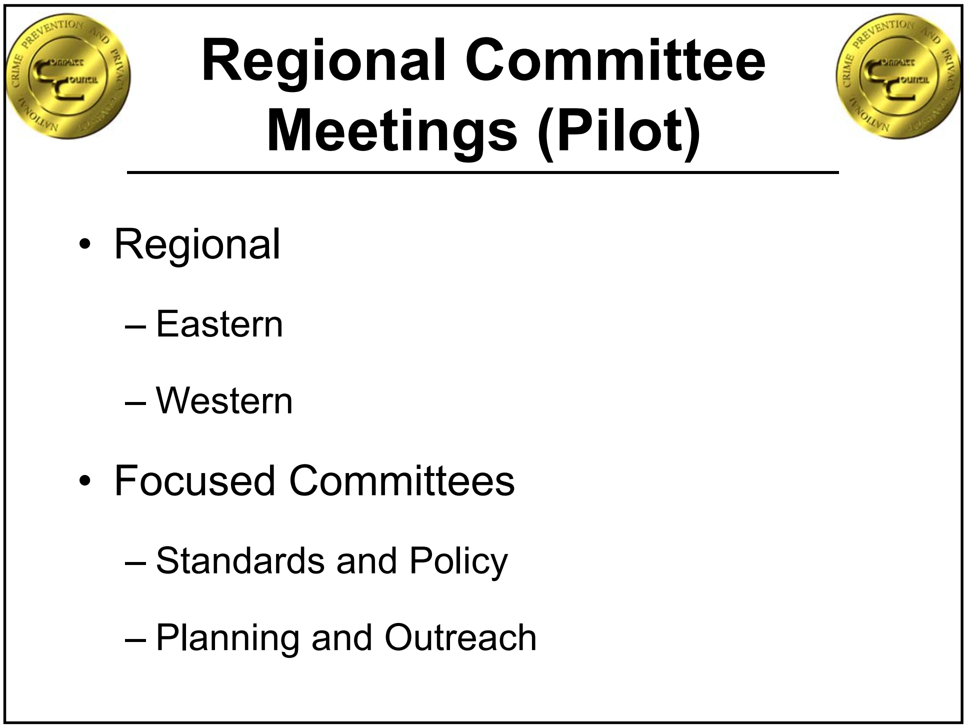
As of November 2019

NFF States - 20



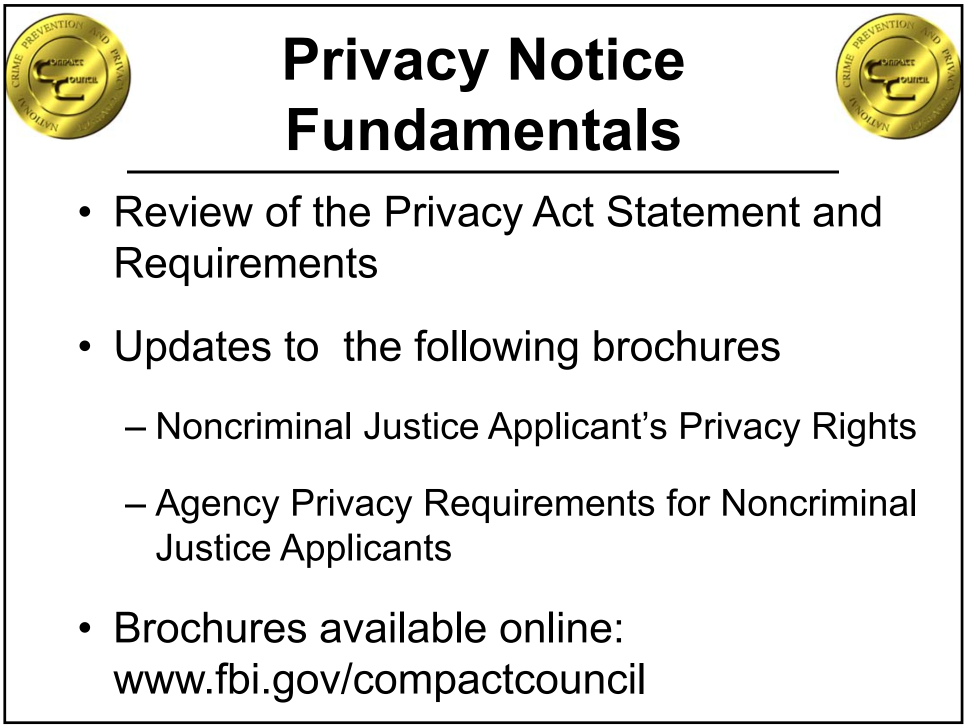
Council Initiatives

- Regional Committee Meetings (Pilot)
- Privacy Notice Fundamentals
- Limitations on USCIS Access to Criminal History Obtained via the Purpose Code I Query of the Interstate Identification Index
- Noncriminal Justice Audit Resources
- Focus Groups/Task Forces



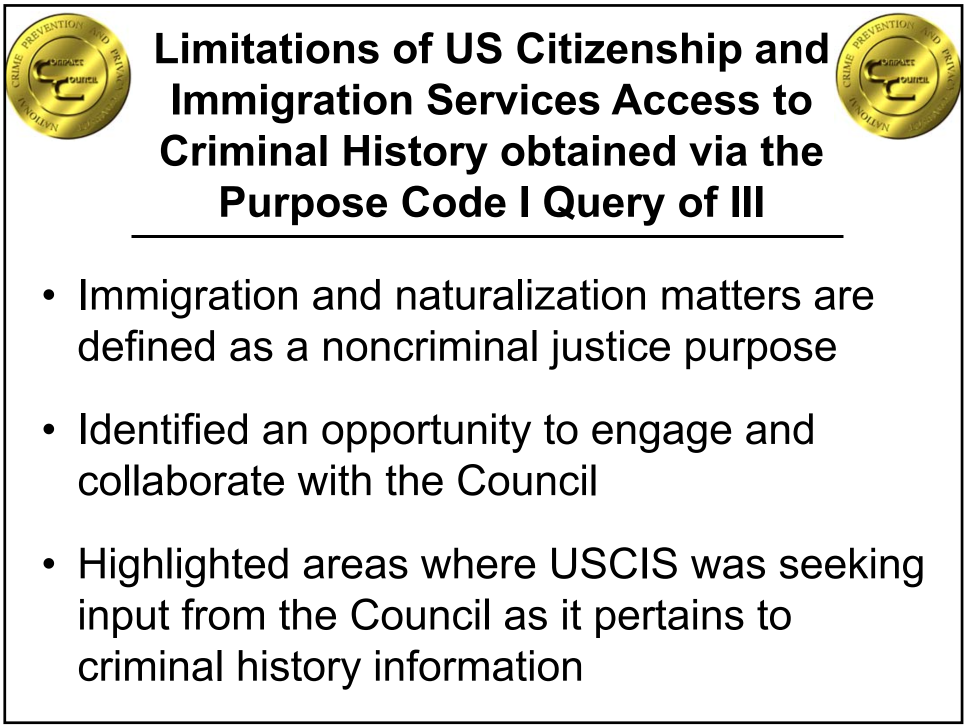
Regional Committee Meetings (Pilot)

- Regional
  - Eastern
  - Western
- Focused Committees
  - Standards and Policy
  - Planning and Outreach



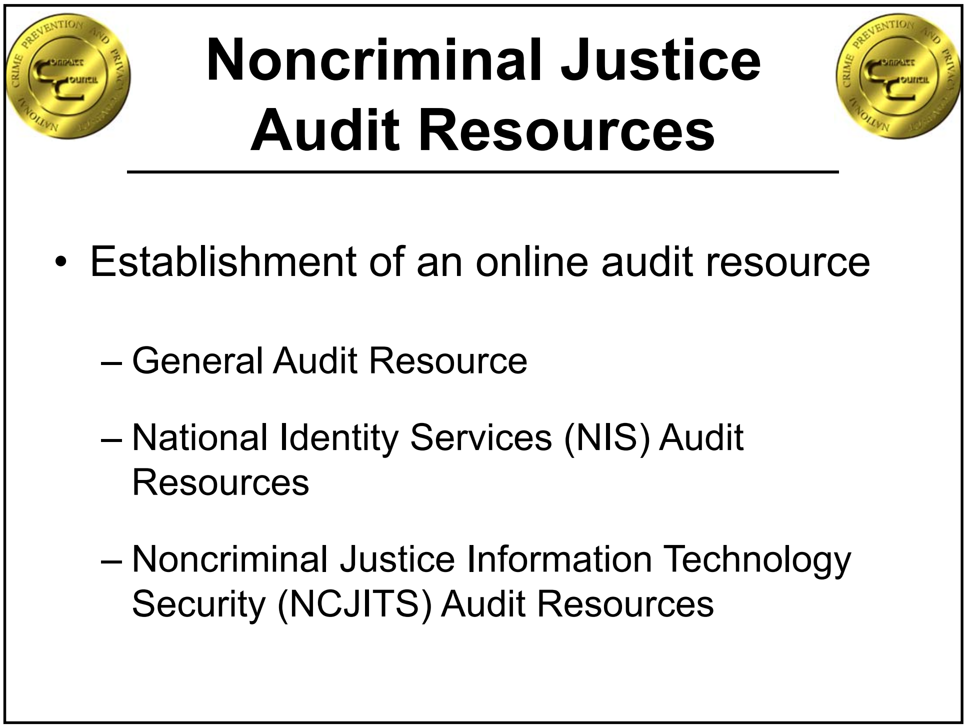
Privacy Notice Fundamentals

- Review of the Privacy Act Statement and Requirements
- Updates to the following brochures
  - Noncriminal Justice Applicant's Privacy Rights
  - Agency Privacy Requirements for Noncriminal Justice Applicants
- Brochures available online: www.fbi.gov/compactcouncil



Limitations of US Citizenship and Immigration Services Access to Criminal History obtained via the Purpose Code I Query of III

- Immigration and naturalization matters are defined as a noncriminal justice purpose
- Identified an opportunity to engage and collaborate with the Council
- Highlighted areas where USCIS was seeking input from the Council as it pertains to criminal history information



Noncriminal Justice Audit Resources

- Establishment of an online audit resource
  - General Audit Resource
  - National Identity Services (NIS) Audit Resources
  - Noncriminal Justice Information Technology Security (NCJITS) Audit Resources

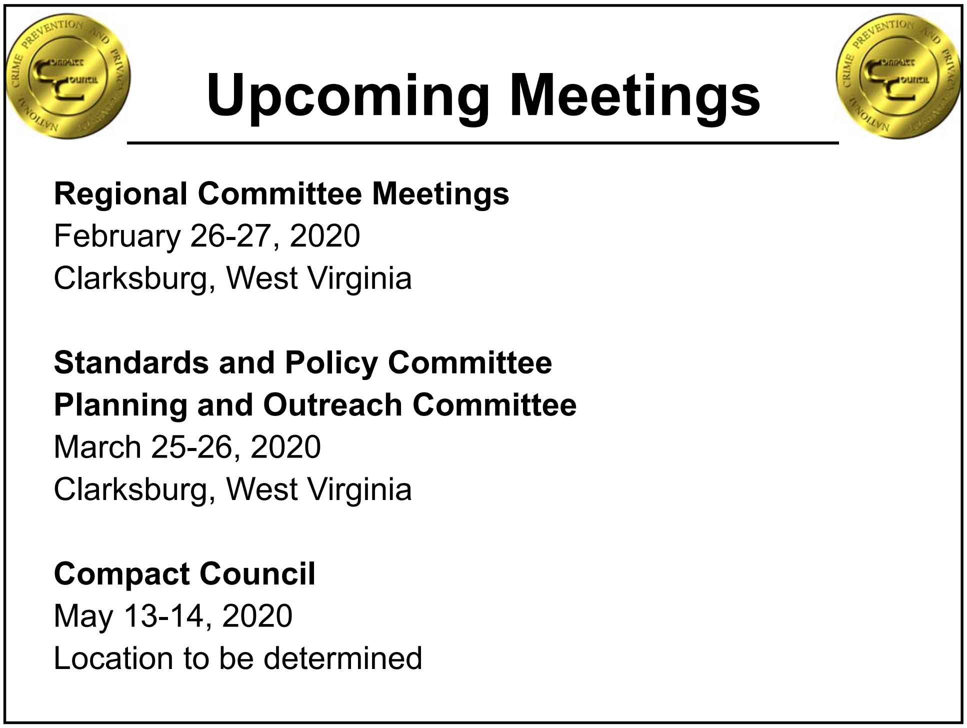
Focus Group and Task Force Updates

- NFF Quals Focus Group
- NFF Disposition Task Force
- Outsourcing Task Force

Council Updates

- Council Chair and Vice-Chair Election

  - Mr. Wyatt Pettengill – North Carolina
  - Ms. Leslie Moore - Kansas

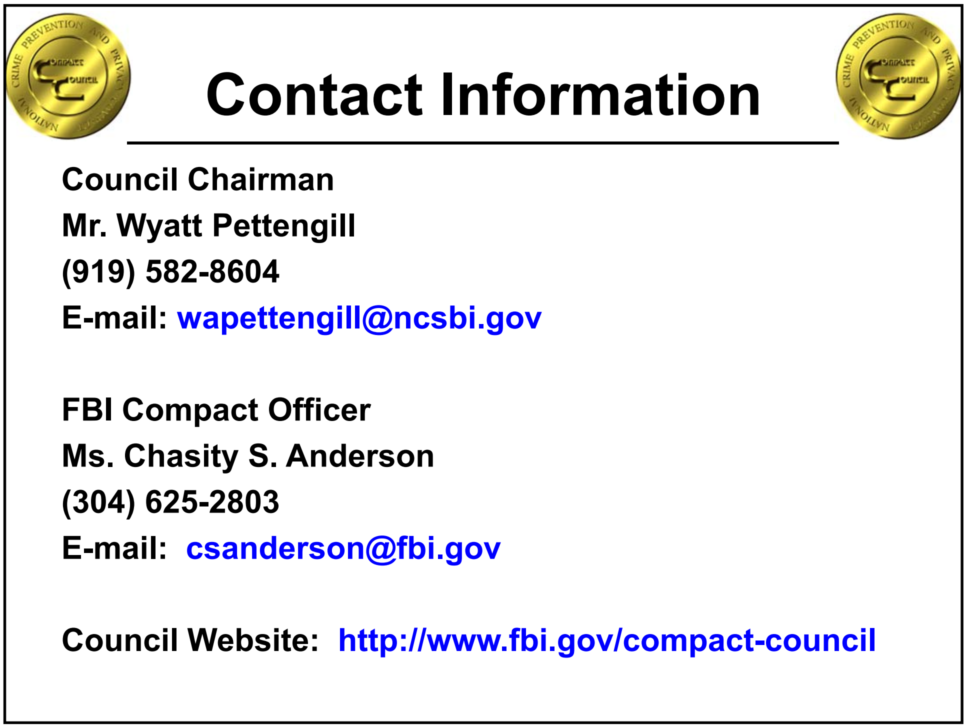


Upcoming Meetings

Regional Committee Meetings
February 26-27, 2020
Clarksburg, West Virginia

Standards and Policy Committee
Planning and Outreach Committee
March 25-26, 2020
Clarksburg, West Virginia

Compact Council
May 13-14, 2020
Location to be determined



Contact Information

Council Chairman
Mr. Wyatt Pettengill
(919) 582-8604
E-mail: wapettengill@ncsbi.gov

FBI Compact Officer
Ms. Chasity S. Anderson
(304) 625-2803
E-mail: csanderson@fbi.gov

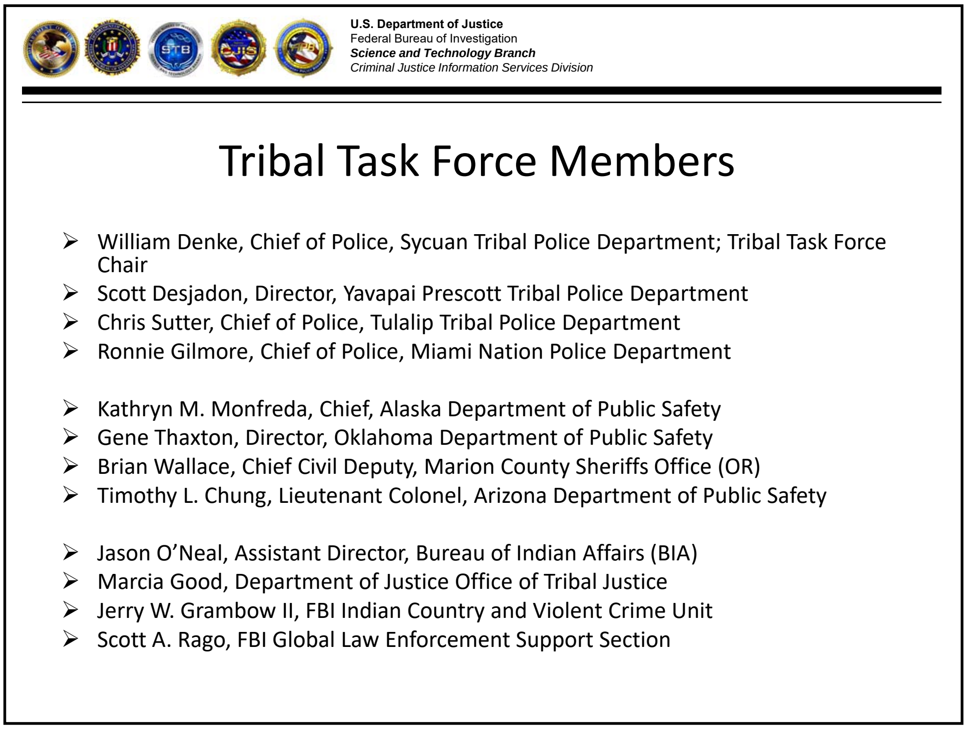
Council Website: http://www.fbi.gov/compact-council

Tribal Task Force Update

Mr. William J. Denke, Task Force Chair
Federal Bureau of Investigation (FBI)
Criminal Justice Information Services (CJIS)
Advisory Policy Board Meeting
Atlanta, GA
December 3-5, 2019

The Mission of the Tribal Task Force is to enhance officer and public safety by improving federal, state, local, tribal, and territorial participation in CJIS Division systems.

The Task Force will review relevant issues that may prevent or discourage tribal law enforcement agencies from entering records/data into the CJIS Division systems and make recommendations that will address those issues.



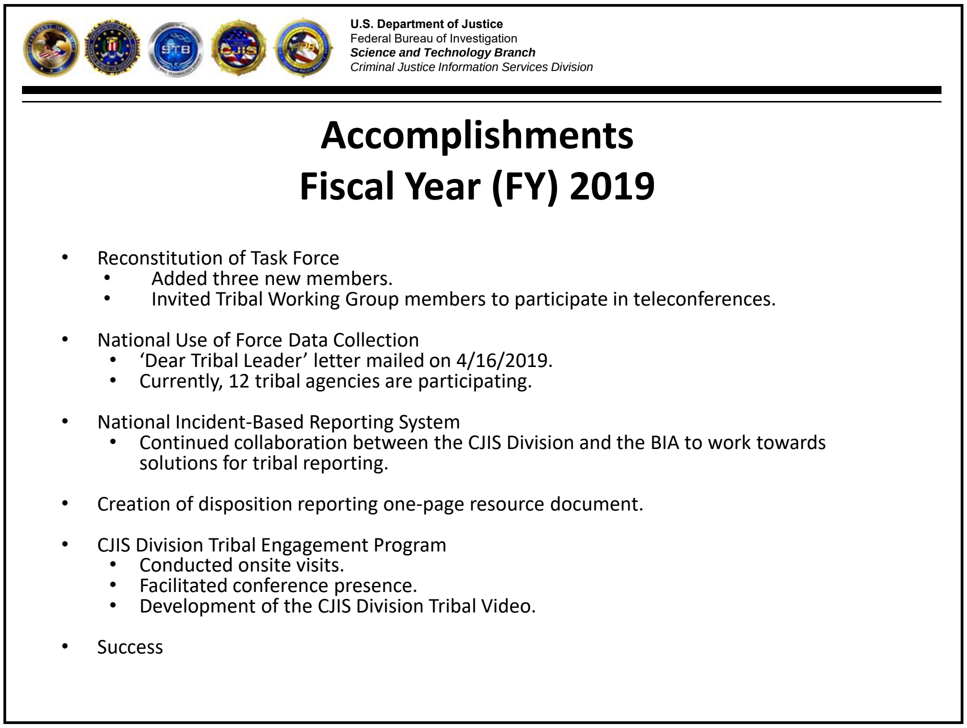
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Tribal Task Force Members

- William Denke, Chief of Police, Sycuan Tribal Police Department; Tribal Task Force Chair
- Scott Desjadon, Director, Yavapai Prescott Tribal Police Department
- Chris Sutter, Chief of Police, Tulalip Tribal Police Department
- Ronnie Gilmore, Chief of Police, Miami Nation Police Department

- Kathryn M. Monfreda, Chief, Alaska Department of Public Safety
- Gene Thaxton, Director, Oklahoma Department of Public Safety
- Brian Wallace, Chief Civil Deputy, Marion County Sheriffs Office (OR)
- Timothy L. Chung, Lieutenant Colonel, Arizona Department of Public Safety

- Jason O'Neal, Assistant Director, Bureau of Indian Affairs (BIA)
- Marcia Good, Department of Justice Office of Tribal Justice
- Jerry W. Grambow II, FBI Indian Country and Violent Crime Unit
- Scott A. Rago, FBI Global Law Enforcement Support Section



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Accomplishments Fiscal Year (FY) 2019

- Reconstitution of Task Force
  - Added three new members.
  - Invited Tribal Working Group members to participate in teleconferences.

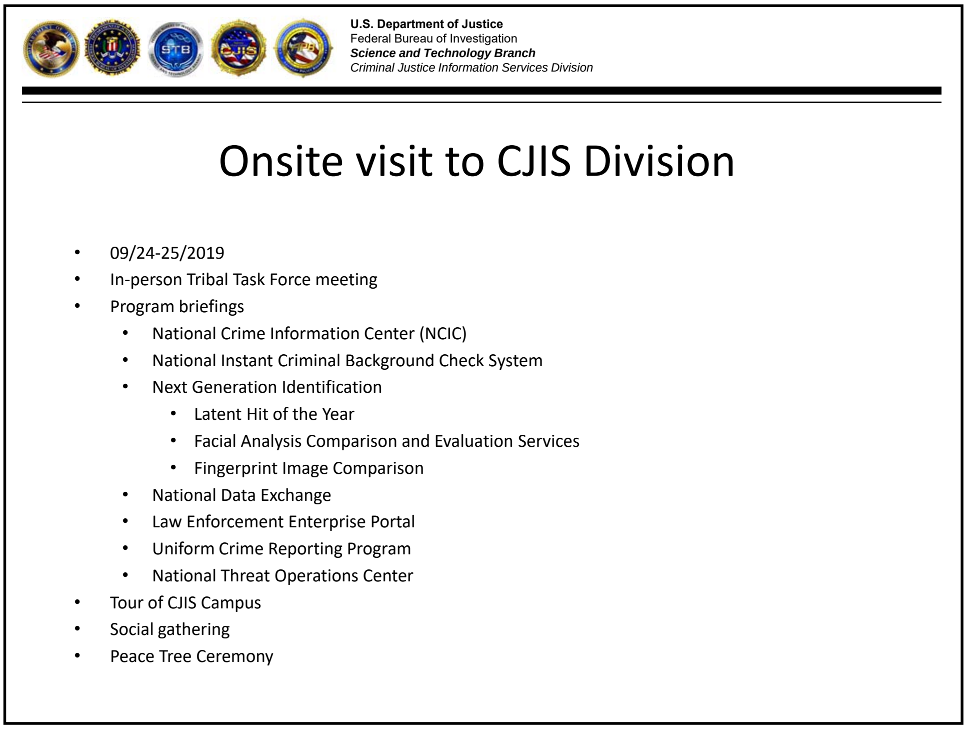
- National Use of Force Data Collection
  - 'Dear Tribal Leader' letter mailed on 4/16/2019.
  - Currently, 12 tribal agencies are participating.

- National Incident-Based Reporting System
  - Continued collaboration between the CJIS Division and the BIA to work towards solutions for tribal reporting.

- Creation of disposition reporting one-page resource document.

- CJIS Division Tribal Engagement Program
  - Conducted onsite visits.
  - Facilitated conference presence.
  - Development of the CJIS Division Tribal Video.

- Success



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Onsite visit to CJIS Division

- 09/24-25/2019
- In-person Tribal Task Force meeting
- Program briefings
  - National Crime Information Center (NCIC)
  - National Instant Criminal Background Check System
  - Next Generation Identification
    - Latent Hit of the Year
    - Facial Analysis Comparison and Evaluation Services
    - Fingerprint Image Comparison
  - National Data Exchange
  - Law Enforcement Enterprise Portal
  - Uniform Crime Reporting Program
  - National Threat Operations Center
- Tour of CJIS Campus
- Social gathering
- Peace Tree Ceremony

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

CJIS Division Peace Tree Ceremony

The Tribal Task Force participated in the CJIS Divisions Peace Tree ceremony.

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

FY20 Initiatives

- Access Project
- NCIC 3rd Generation support of NCIC Extradition Codes for tribal agencies
- Tribal fingerprint submission cascades of Unsolved Latent File
- Continued outreach and support to tribal partners

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

CJIS Division Advisory Process Tribal Representatives

Advisory Policy Board
William J. Denke
Sycuan Tribal Police Department,
El Cajon, CA
<bdenke@sycuan-nsn.gov>
619-445-8710

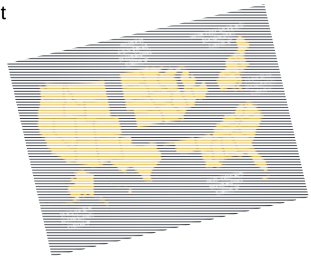
Northeastern Working Group
Robert Bryant
Penobscot Indian Nation Police
Indian Nation, ME
<Robert.Bryant@penobscotnation.org>
207-827-6336

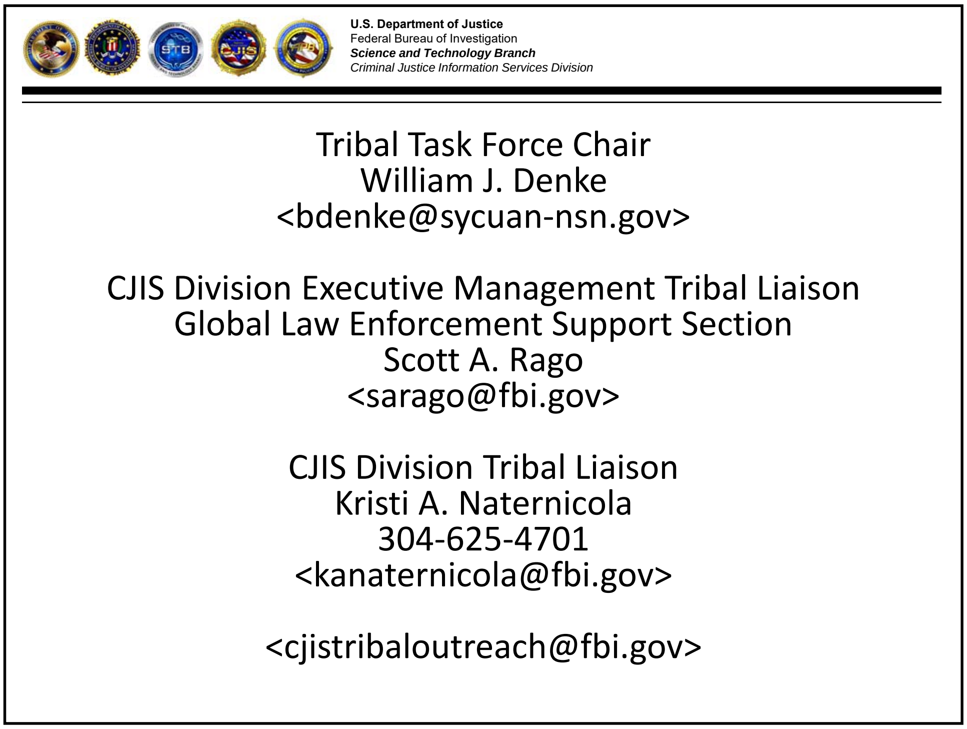
Western Working Group
Scott Desjadon
Yavapai Prescott Tribal Police Department, Prescott, AZ
<sdesjadon@ypit.com>
928-925-4581

Southern Working Group
Ronnie Gilmore
Miami Nation Police Department
Miami, OK
<rgilmore@miamination.com>
918-541-1453

North Central Working Group
Gary Gaikowski
Sisseton-Wahpeton Law Enforcement
Sisseton, SD
<gaikowski@Hotmail.com>
605-698-7661

Federal Working Group
Jason O'Neal
Bureau of Indian Affairs
Washington, DC
<jason.oneal@bia.gov>
918-221-1866





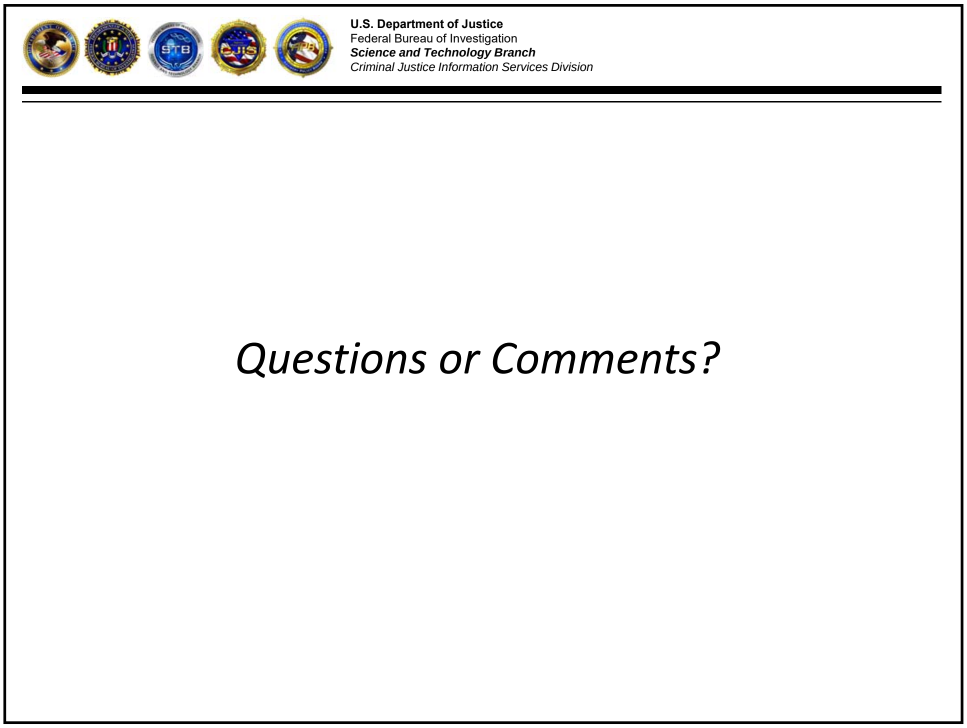
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Tribal Task Force Chair
William J. Denke
<bdenke@sycuan-nsn.gov>

CJIS Division Executive Management Tribal Liaison
Global Law Enforcement Support Section
Scott A. Rago
<sarago@fbi.gov>

CJIS Division Tribal Liaison
Kristi A. Naternicola
304-625-4701
<kanaternicola@fbi.gov>

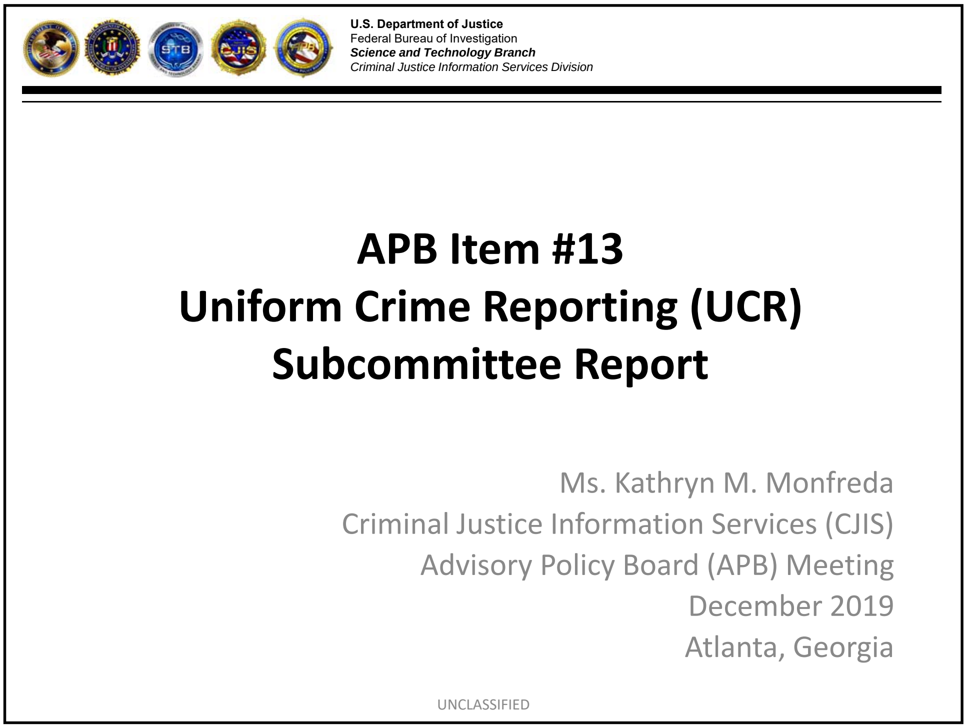
<cjistribaloutreach@fbi.gov>



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

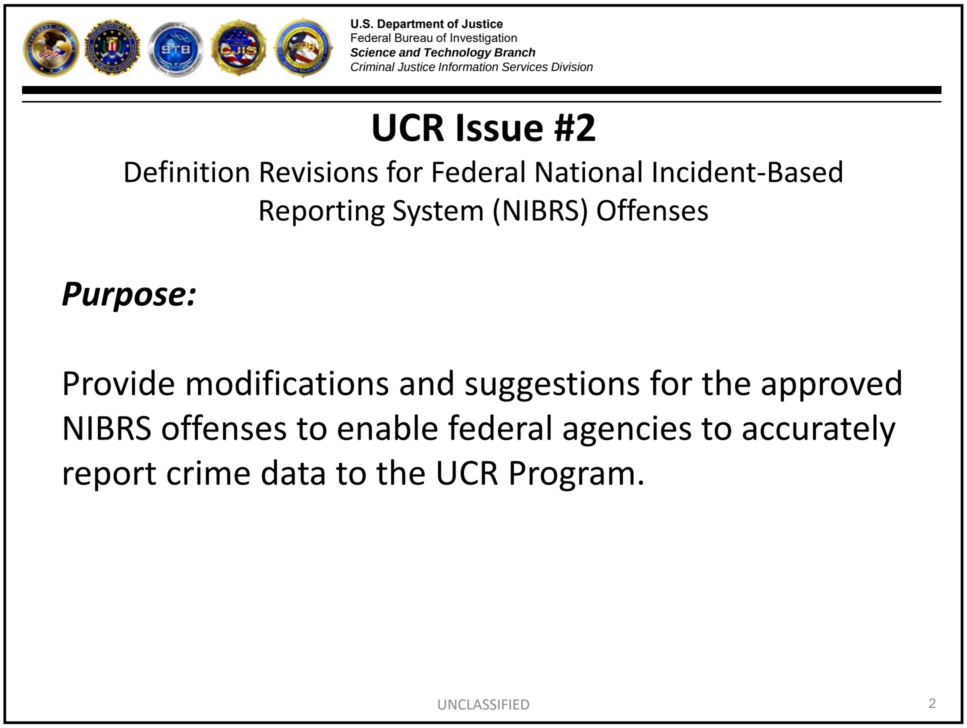
Questions or Comments?

Intentionally Left Blank



APB Item #13
Uniform Crime Reporting (UCR)
Subcommittee Report

Ms. Kathryn M. Monfreda
Criminal Justice Information Services (CJIS)
Advisory Policy Board (APB) Meeting
December 2019
Atlanta, Georgia

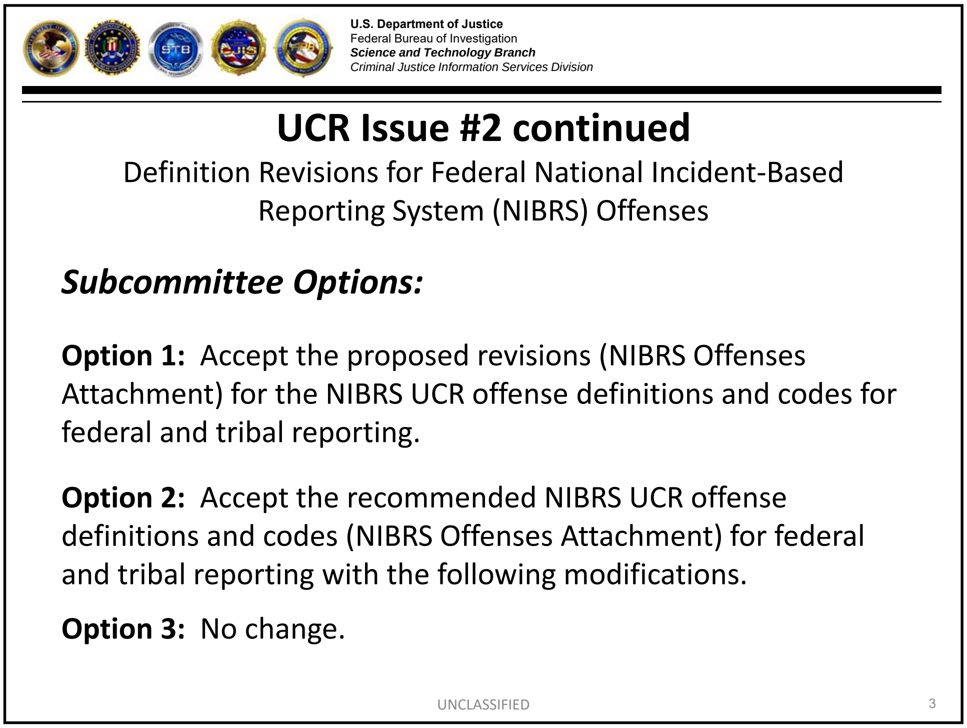


UCR Issue #2

Definition Revisions for Federal National Incident-Based Reporting System (NIBRS) Offenses

Purpose:

Provide modifications and suggestions for the approved NIBRS offenses to enable federal agencies to accurately report crime data to the UCR Program.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

UCR Issue #2 continued

Definition Revisions for Federal National Incident-Based Reporting System (NIBRS) Offenses

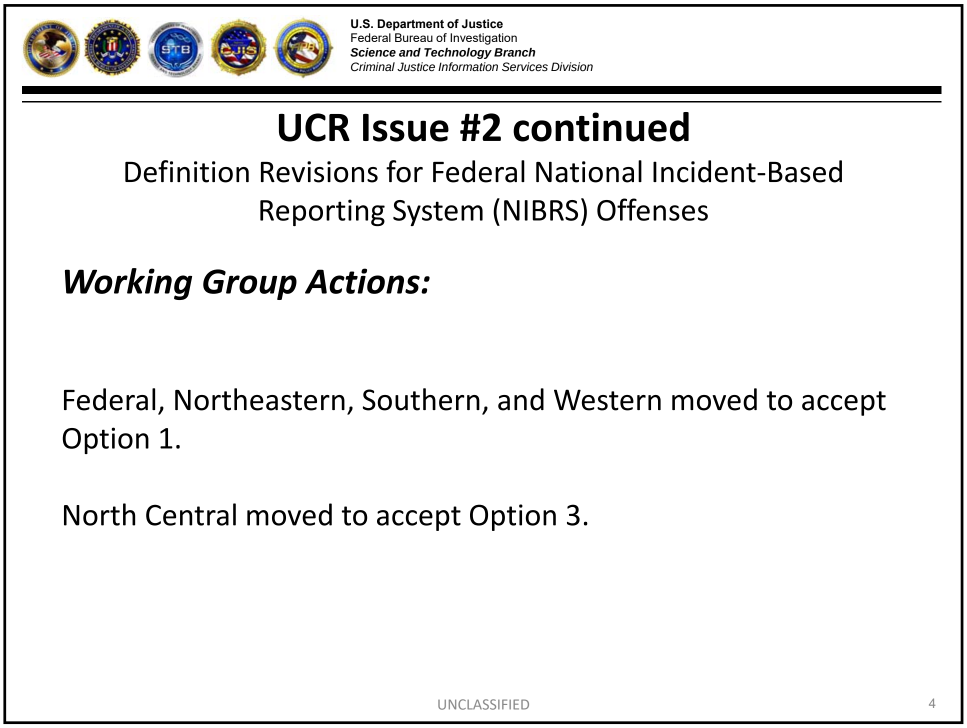
Subcommittee Options:

Option 1: Accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

Option 2: Accept the recommended NIBRS UCR offense definitions and codes (NIBRS Offenses Attachment) for federal and tribal reporting with the following modifications.

Option 3: No change.

UNCLASSIFIED 3



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

UCR Issue #2 continued

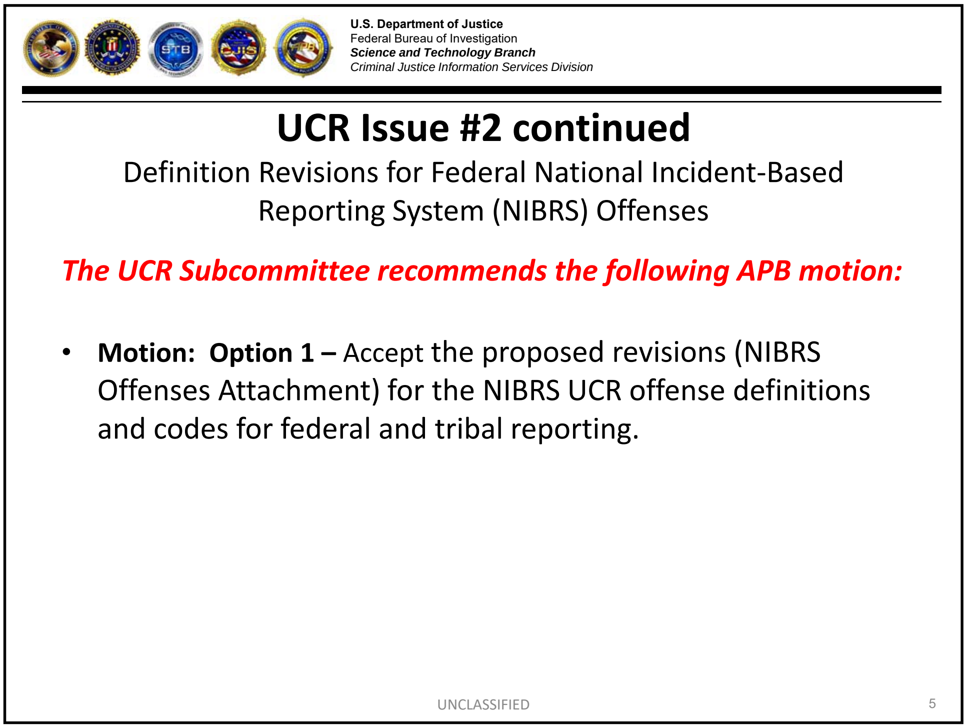
Definition Revisions for Federal National Incident-Based Reporting System (NIBRS) Offenses

Working Group Actions:

Federal, Northeastern, Southern, and Western moved to accept Option 1.

North Central moved to accept Option 3.

UNCLASSIFIED 4



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

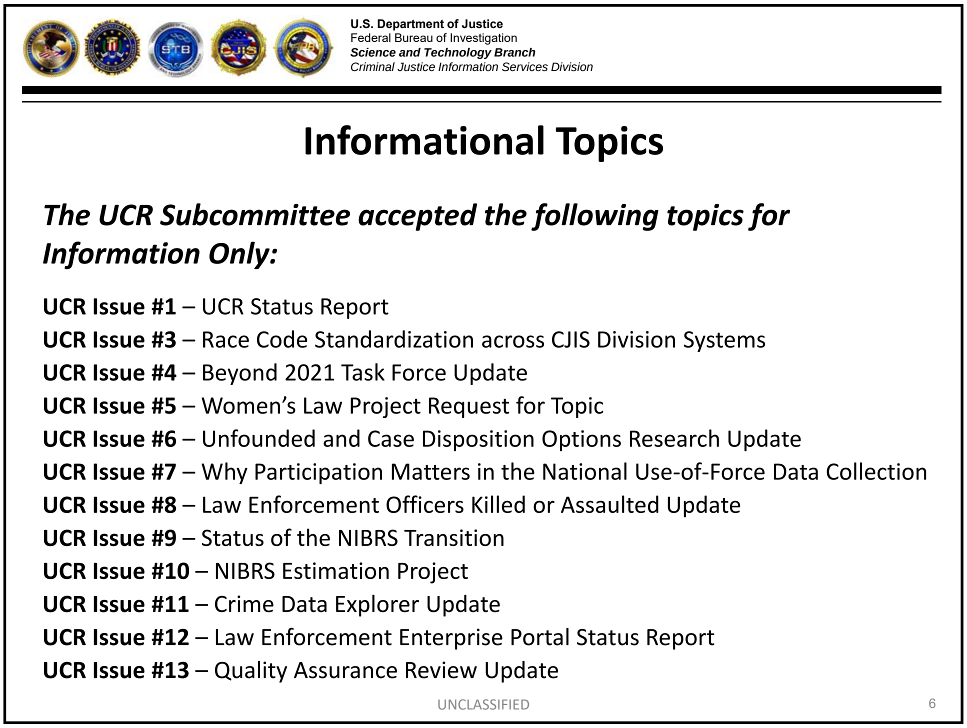
UCR Issue #2 continued

Definition Revisions for Federal National Incident-Based Reporting System (NIBRS) Offenses

The UCR Subcommittee recommends the following APB motion:

- **Motion: Option 1 –** Accept the proposed revisions (NIBRS Offenses Attachment) for the NIBRS UCR offense definitions and codes for federal and tribal reporting.

UNCLASSIFIED 5



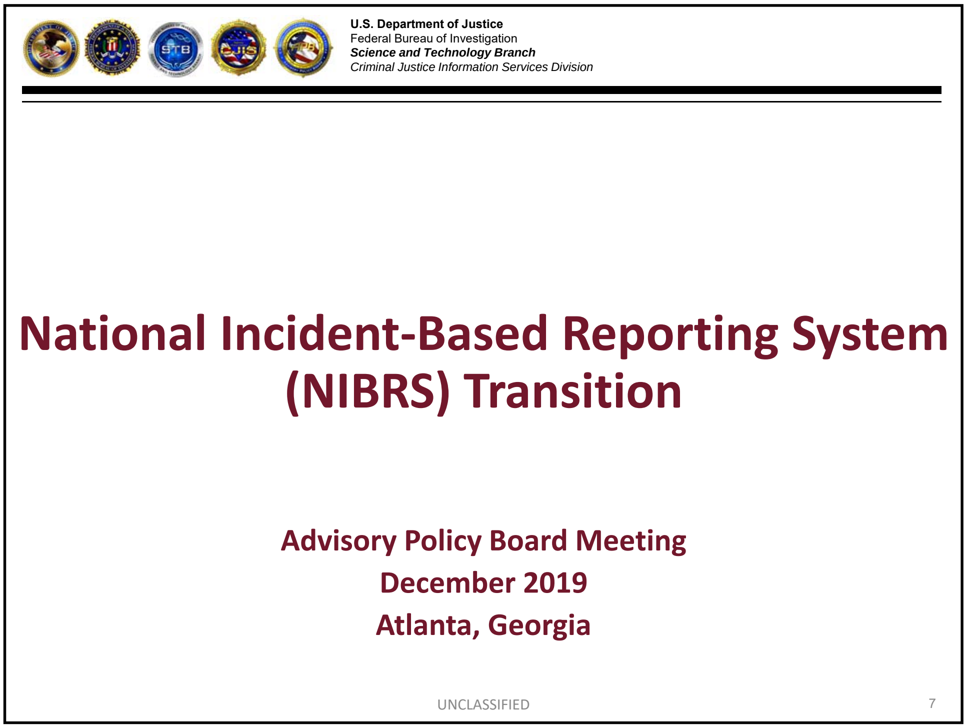
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Informational Topics

The UCR Subcommittee accepted the following topics for Information Only:

UCR Issue #1 – UCR Status Report
UCR Issue #3 – Race Code Standardization across CJIS Division Systems
UCR Issue #4 – Beyond 2021 Task Force Update
UCR Issue #5 – Women's Law Project Request for Topic
UCR Issue #6 – Unfounded and Case Disposition Options Research Update
UCR Issue #7 – Why Participation Matters in the National Use-of-Force Data Collection
UCR Issue #8 – Law Enforcement Officers Killed or Assaulted Update
UCR Issue #9 – Status of the NIBRS Transition
UCR Issue #10 – NIBRS Estimation Project
UCR Issue #11 – Crime Data Explorer Update
UCR Issue #12 – Law Enforcement Enterprise Portal Status Report
UCR Issue #13 – Quality Assurance Review Update

UNCLASSIFIED 6



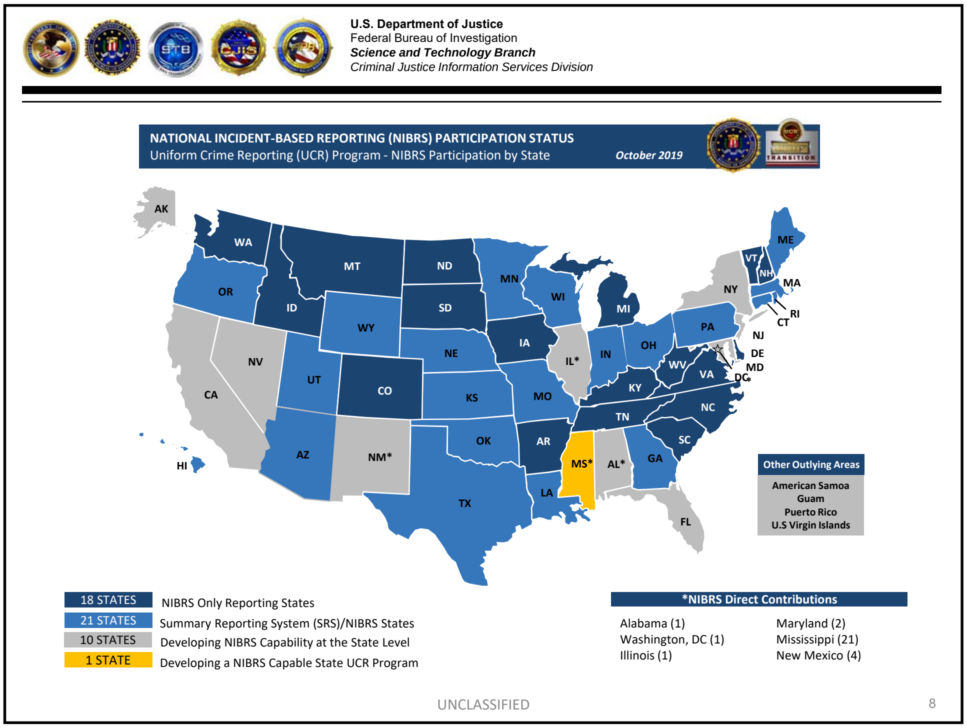
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

National Incident-Based Reporting System (NIBRS) Transition

Advisory Policy Board Meeting
December 2019
Atlanta, Georgia

UNCLASSIFIED

7



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NATIONAL INCIDENT-BASED REPORTING (NIBRS) PARTICIPATION STATUS
Uniform Crime Reporting (UCR) Program - NIBRS Participation by State *October 2019*

Other Outlying Areas
American Samoa
Guam
Puerto Rico
U.S Virgin Islands

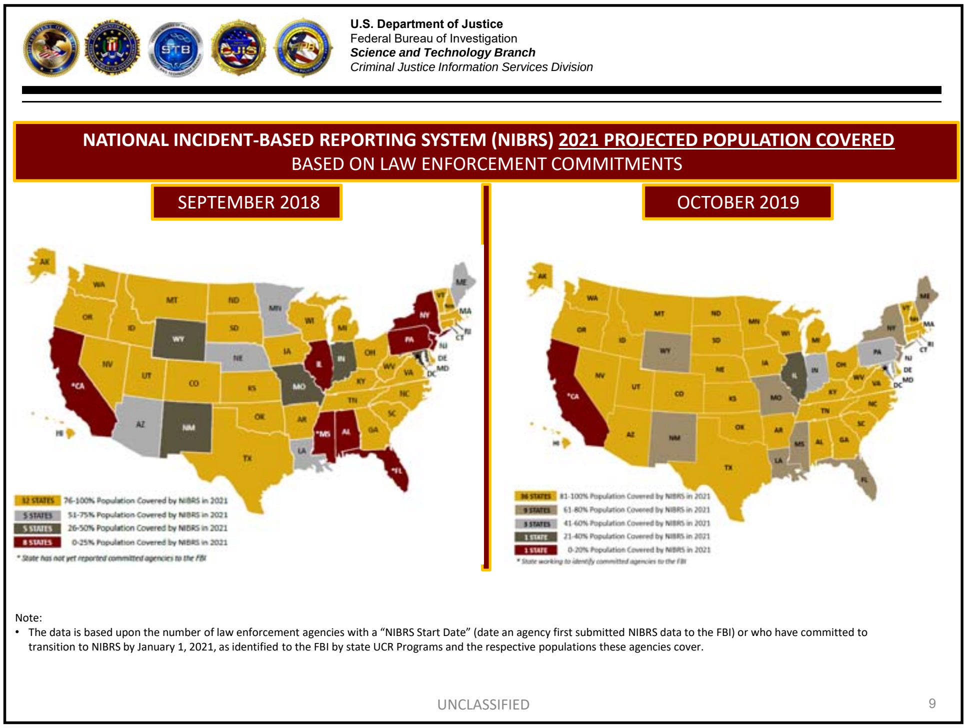
18 STATES	NIBRS Only Reporting States
21 STATES	Summary Reporting System (SRS)/NIBRS States
10 STATES	Developing NIBRS Capability at the State Level
1 STATE	Developing a NIBRS Capable State UCR Program

***NIBRS Direct Contributions**

Alabama (1)	Maryland (2)
Washington, DC (1)	Mississippi (21)
Illinois (1)	New Mexico (4)

UNCLASSIFIED

8



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS) 2021 PROJECTED POPULATION COVERED
BASED ON LAW ENFORCEMENT COMMITMENTS

SEPTEMBER 2018

32 STATES	76-100% Population Covered by NIBRS in 2021
5 STATES	51-75% Population Covered by NIBRS in 2021
5 STATES	26-50% Population Covered by NIBRS in 2021
8 STATES	0-25% Population Covered by NIBRS in 2021

** State has not yet reported committed agencies to the FBI*

OCTOBER 2019

36 STATES	81-100% Population Covered by NIBRS in 2021
9 STATES	61-80% Population Covered by NIBRS in 2021
3 STATES	41-60% Population Covered by NIBRS in 2021
1 STATE	21-40% Population Covered by NIBRS in 2021
1 STATE	0-20% Population Covered by NIBRS in 2021

** State working to identify committed agencies to the FBI*

Note:
- The data is based upon the number of law enforcement agencies with a "NIBRS Start Date" (date an agency first submitted NIBRS data to the FBI) or who have committed to transition to NIBRS by January 1, 2021, as identified to the FBI by state UCR Programs and the respective populations these agencies cover.

UNCLASSIFIED 9

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

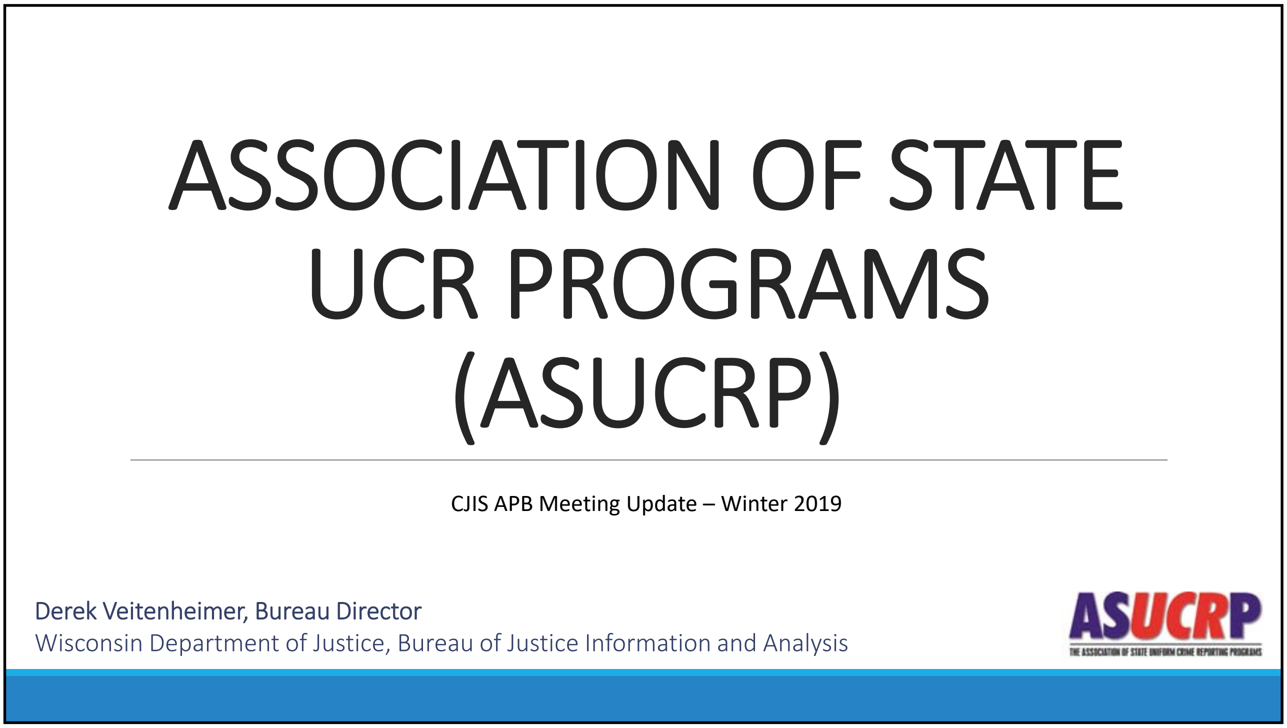
NIBRS
2021
Are You
Ready?
UCR
NIBRS
TRANSITION
Richer Data. Reliable Results.
Richer data. Reliable results.

Time Left to Transition to NIBRS:

12 Months

UNCLASSIFIED 10

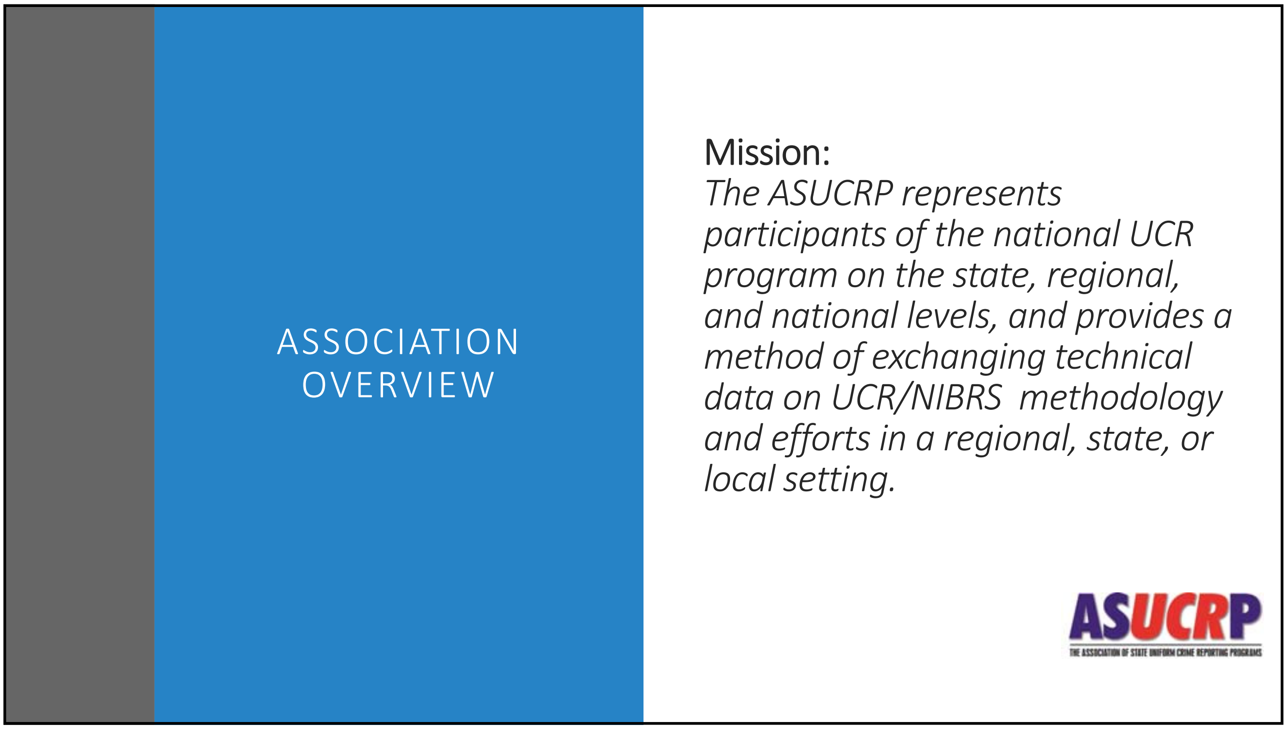
Intentionally Left Blank



ASSOCIATION OF STATE UCR PROGRAMS (ASUCRP)

CJIS APB Meeting Update – Winter 2019

Derek Veitenheimer, Bureau Director
Wisconsin Department of Justice, Bureau of Justice Information and Analysis



ASSOCIATION OVERVIEW

Mission:
The ASUCRP represents participants of the national UCR program on the state, regional, and national levels, and provides a method of exchanging technical data on UCR/NIBRS methodology and efforts in a regional, state, or local setting.

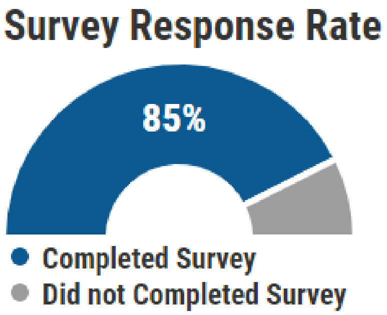
ASSOCIATION OVERVIEW

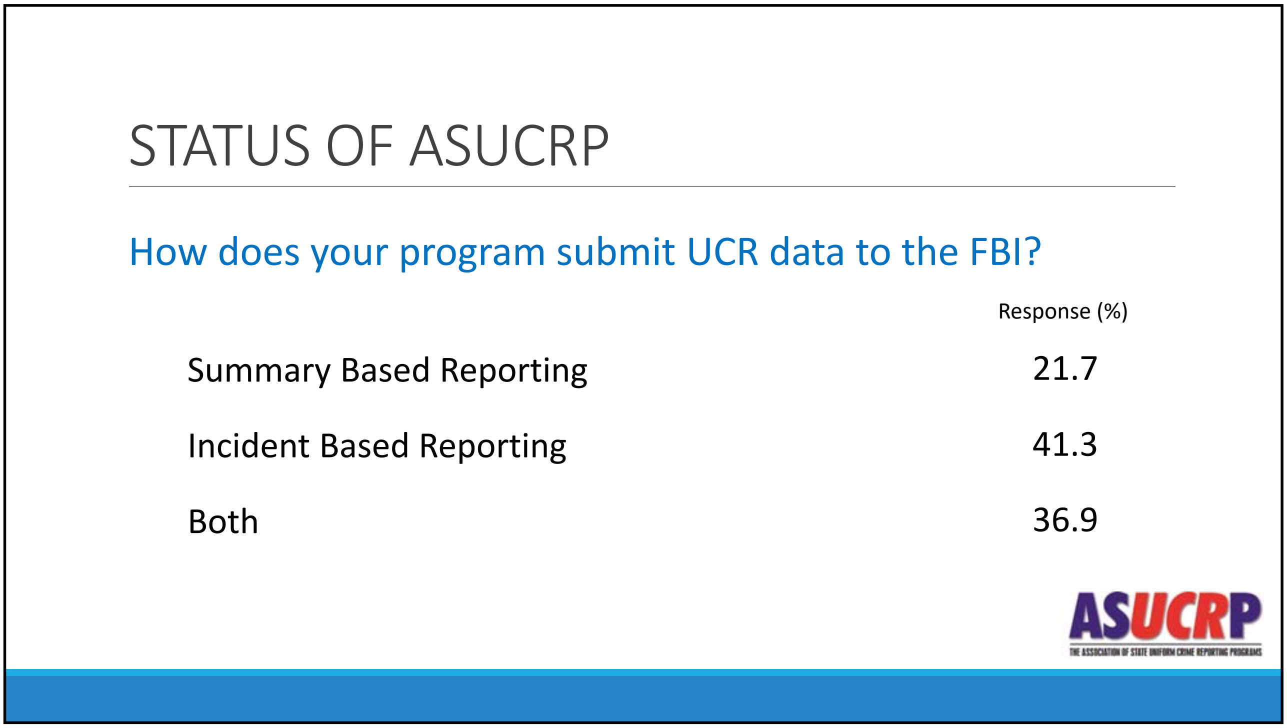
Goals:
The Association is dedicated to improving the collection, use, and the utility of crime data as reported through UCR/NIBRS, and all state and local crime reporting programs.

STATUS OF ASUCRP

Annual Survey

- Sent to State/Territory UCR Program Managers in late Summer
- 46 of the possible 45 managers completed the survey

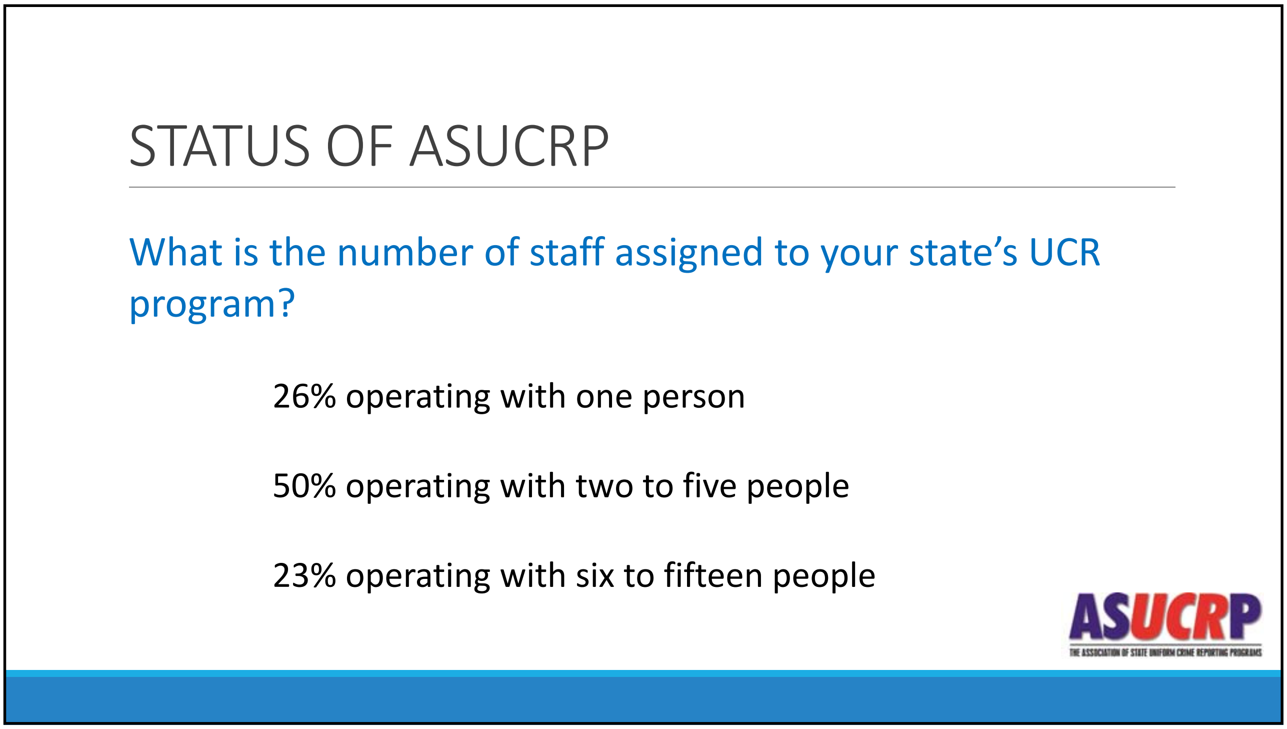




STATUS OF ASUCRP

How does your program submit UCR data to the FBI?

	Response (%)
Summary Based Reporting	21.7
Incident Based Reporting	41.3
Both	36.9



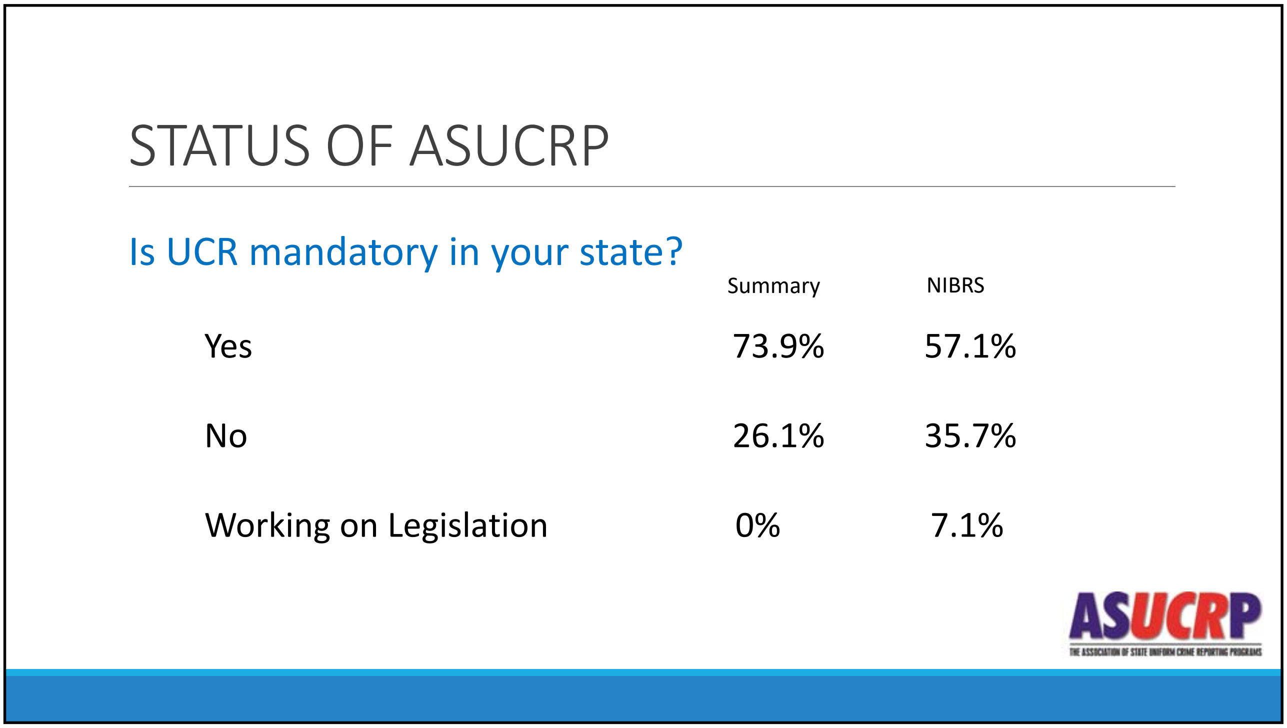
STATUS OF ASUCRP

What is the number of staff assigned to your state’s UCR program?

26% operating with one person

50% operating with two to five people

23% operating with six to fifteen people

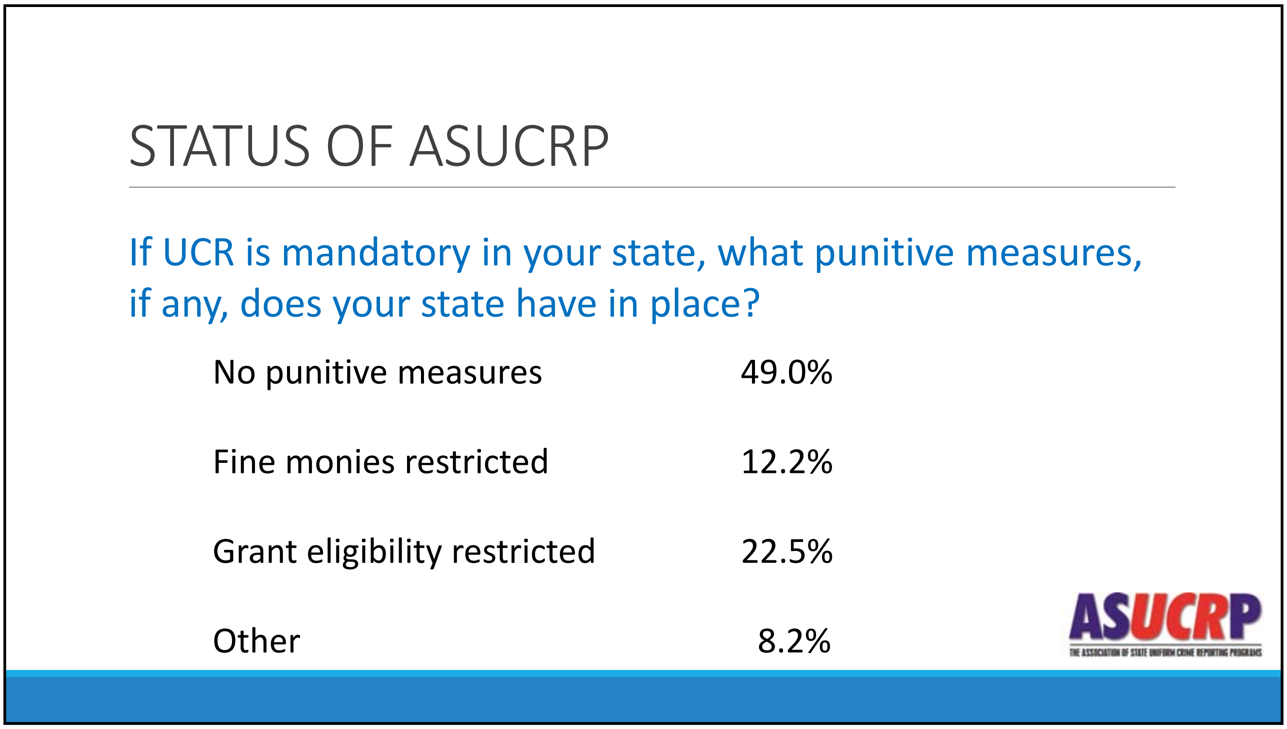


STATUS OF ASUCRP

Is UCR mandatory in your state?

	Summary	NIBRS
Yes	73.9%	57.1%
No	26.1%	35.7%
Working on Legislation	0%	7.1%

ASUCRP
THE ASSOCIATION OF STATE UNIFORM CRIME REPORTING PROGRAMS

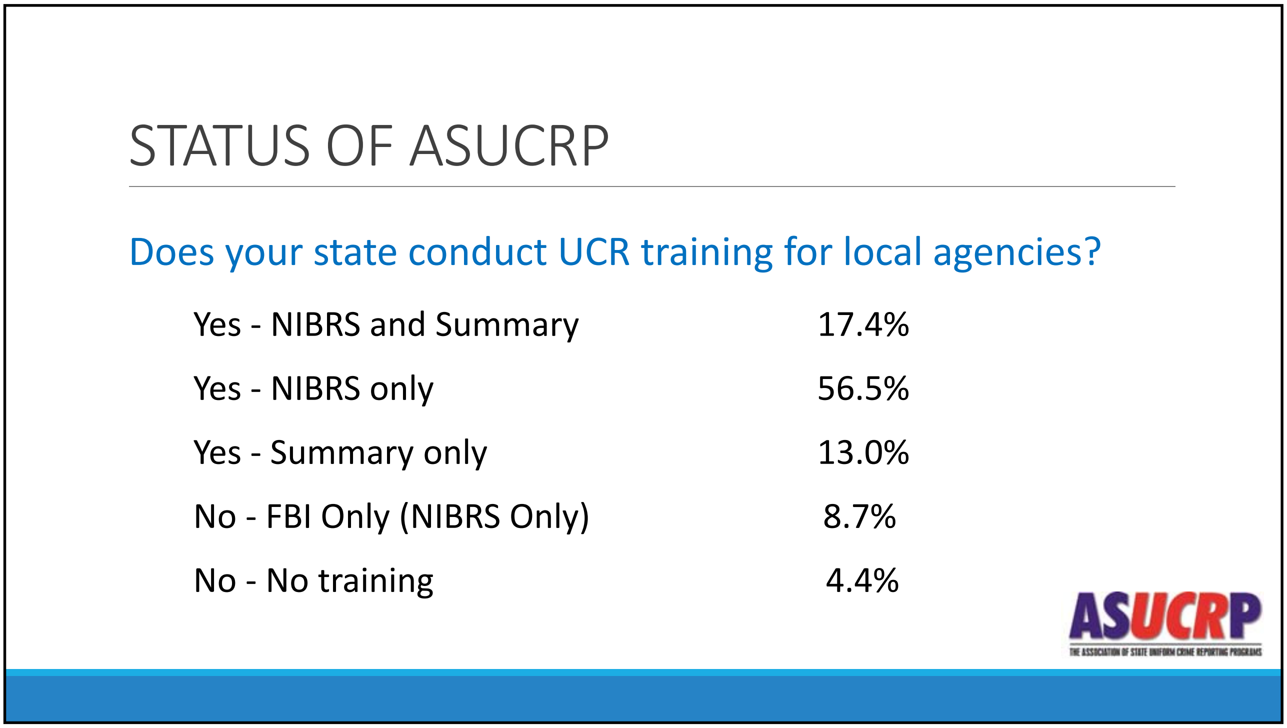


STATUS OF ASUCRP

If UCR is mandatory in your state, what punitive measures, if any, does your state have in place?

No punitive measures	49.0%
Fine monies restricted	12.2%
Grant eligibility restricted	22.5%
Other	8.2%

ASUCRP
THE ASSOCIATION OF STATE UNIFORM CRIME REPORTING PROGRAMS

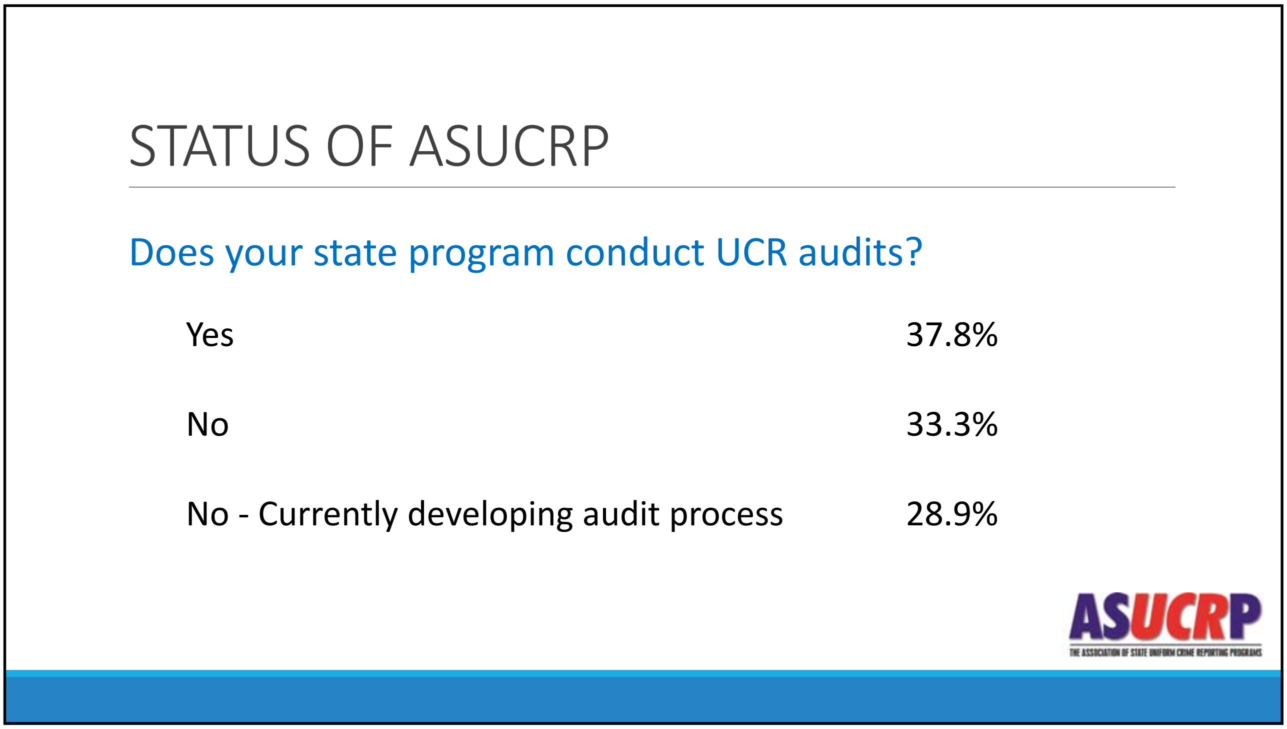


STATUS OF ASUCRP

Does your state conduct UCR training for local agencies?

Yes - NIBRS and Summary	17.4%
Yes - NIBRS only	56.5%
Yes - Summary only	13.0%
No - FBI Only (NIBRS Only)	8.7%
No - No training	4.4%

ASUCRP
THE ASSOCIATION OF STATE UNIFORM CRIME REPORTING PROGRAMS

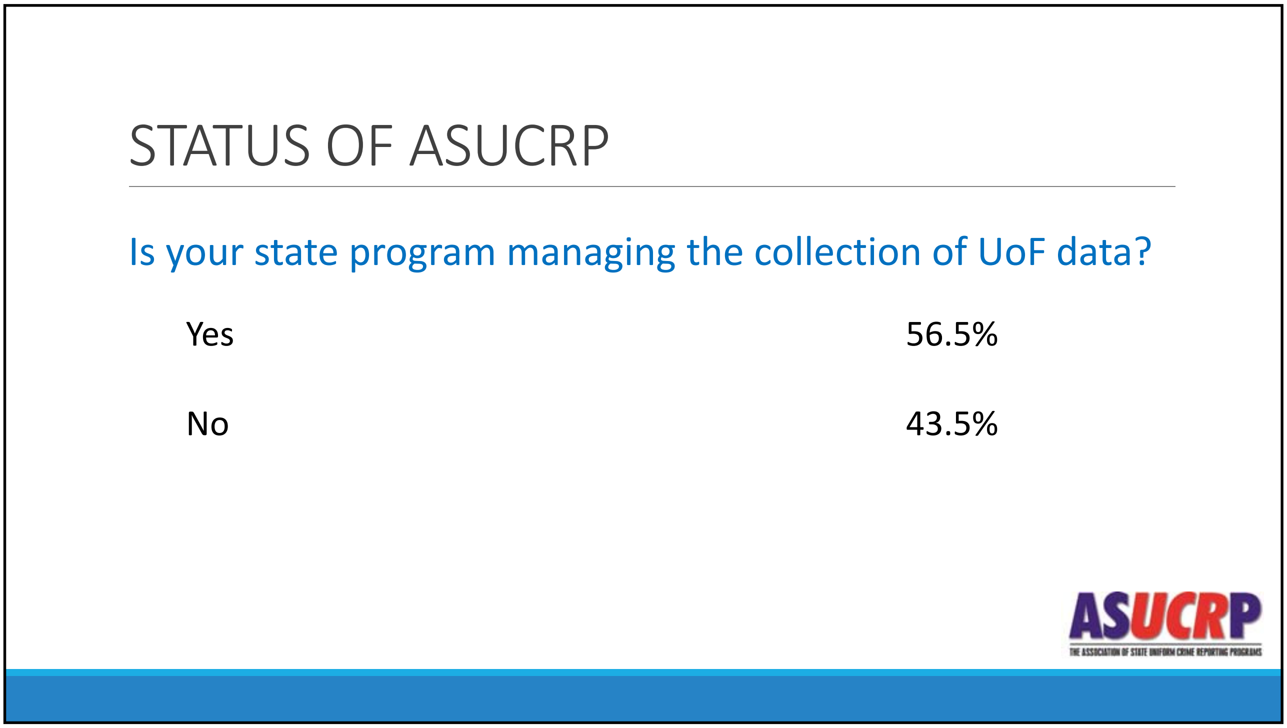


STATUS OF ASUCRP

Does your state program conduct UCR audits?

Yes	37.8%
No	33.3%
No - Currently developing audit process	28.9%

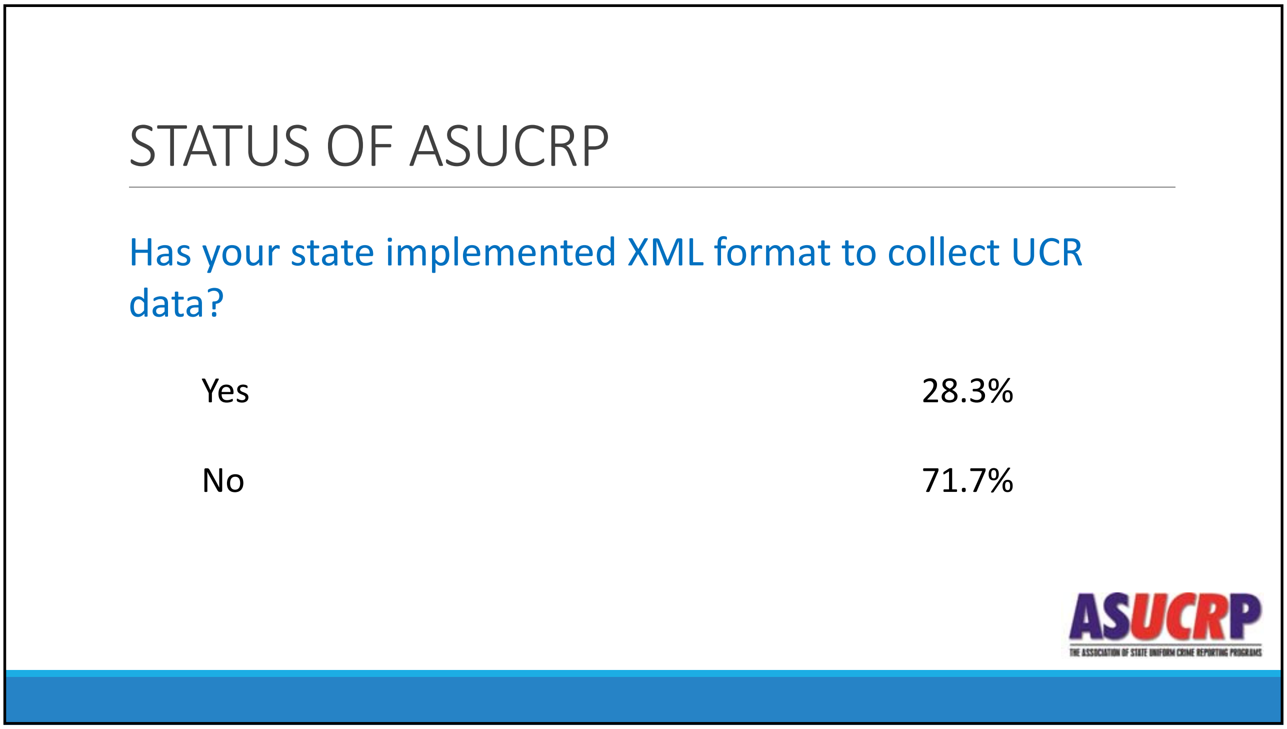
ASUCRP
THE ASSOCIATION OF STATE UNIFORM CRIME REPORTING PROGRAMS



STATUS OF ASUCRP

Is your state program managing the collection of UoF data?

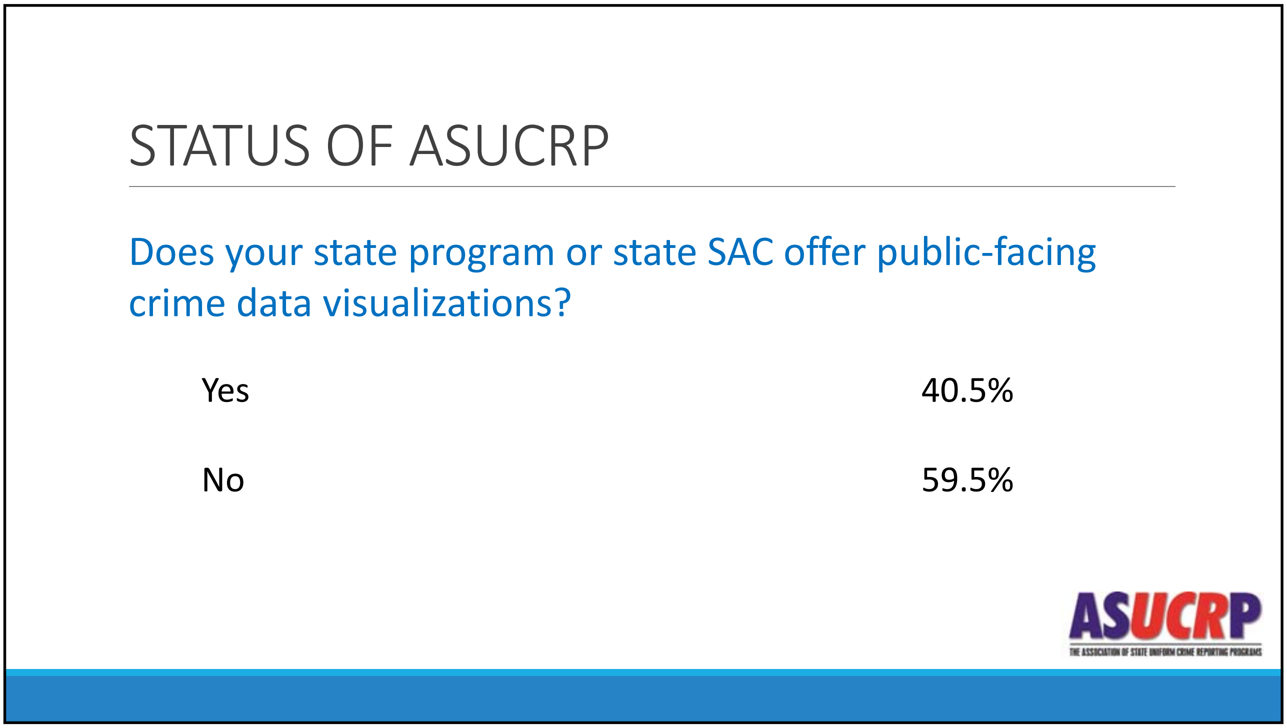
Yes	56.5%
No	43.5%



STATUS OF ASUCRP

Has your state implemented XML format to collect UCR data?

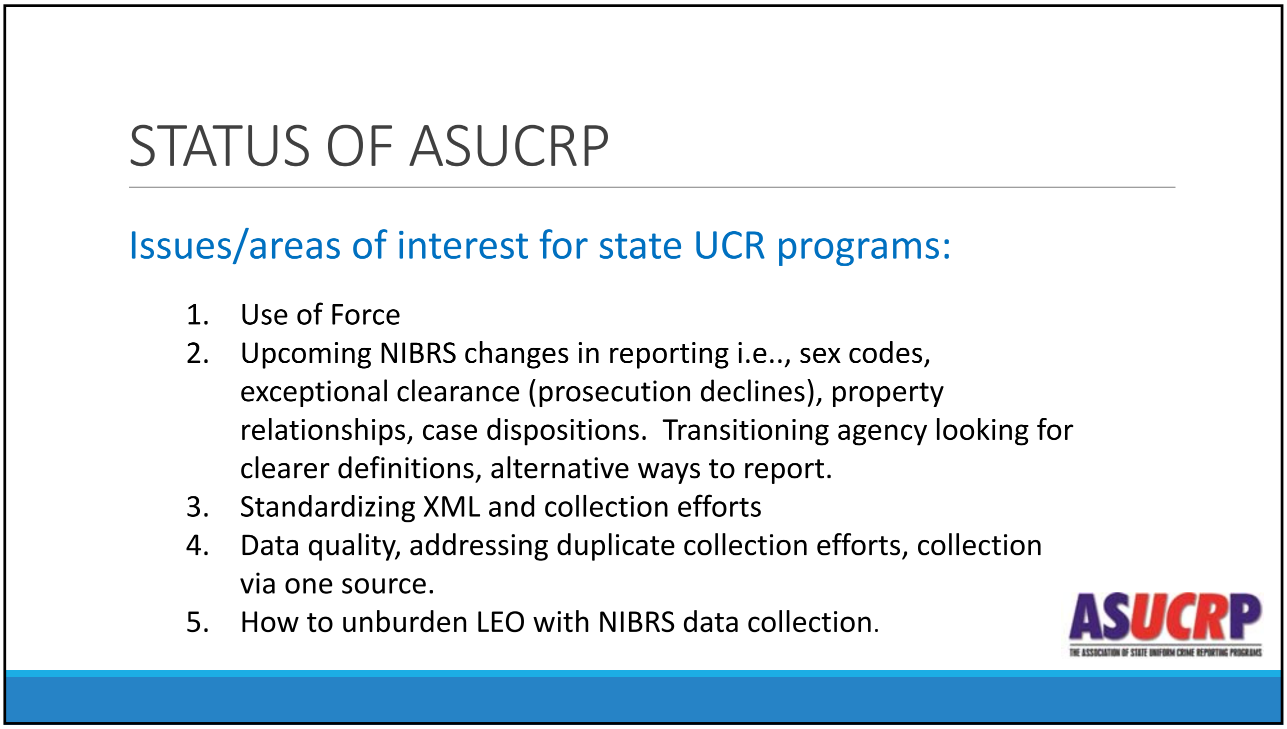
Yes	28.3%
No	71.7%



STATUS OF ASUCRP

Does your state program or state SAC offer public-facing crime data visualizations?

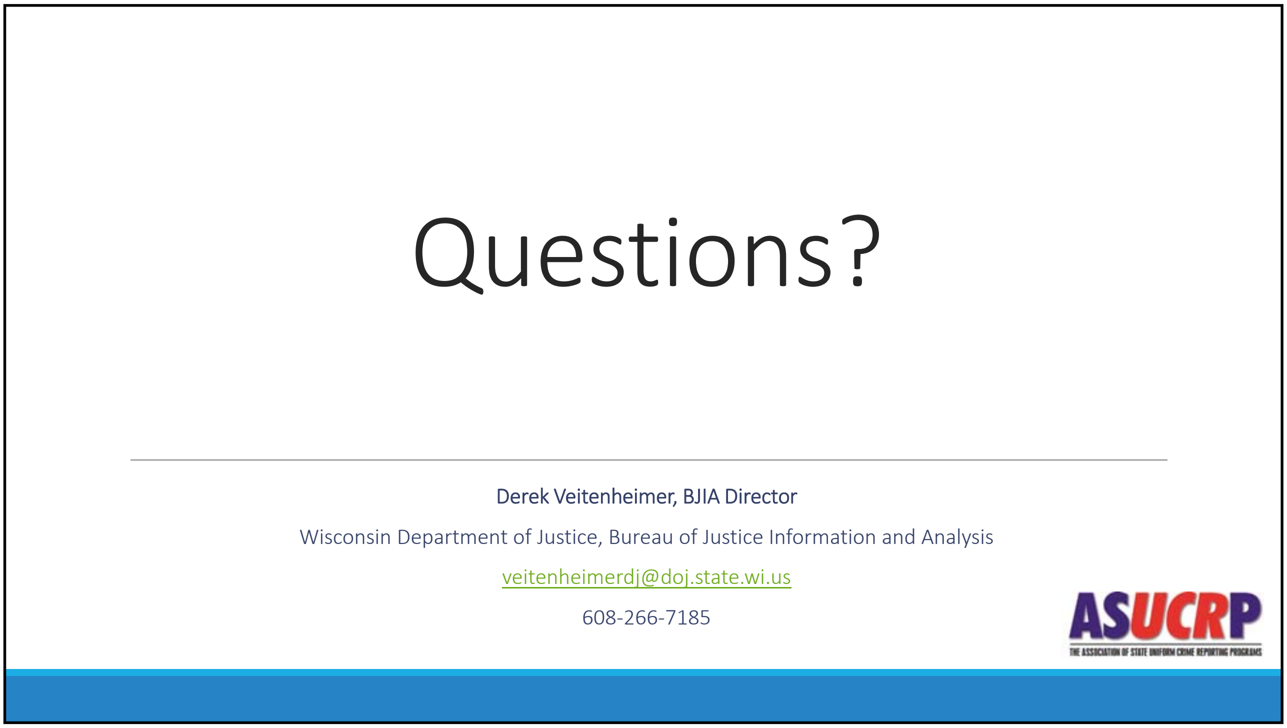
Yes	40.5%
No	59.5%



STATUS OF ASUCRP

Issues/areas of interest for state UCR programs:

1. Use of Force
2. Upcoming NIBRS changes in reporting i.e.., sex codes, exceptional clearance (prosecution declines), property relationships, case dispositions. Transitioning agency looking for clearer definitions, alternative ways to report.
3. Standardizing XML and collection efforts
4. Data quality, addressing duplicate collection efforts, collection via one source.
5. How to unburden LEO with NIBRS data collection.



Questions?

Derek Veitenheimer, BJIA Director

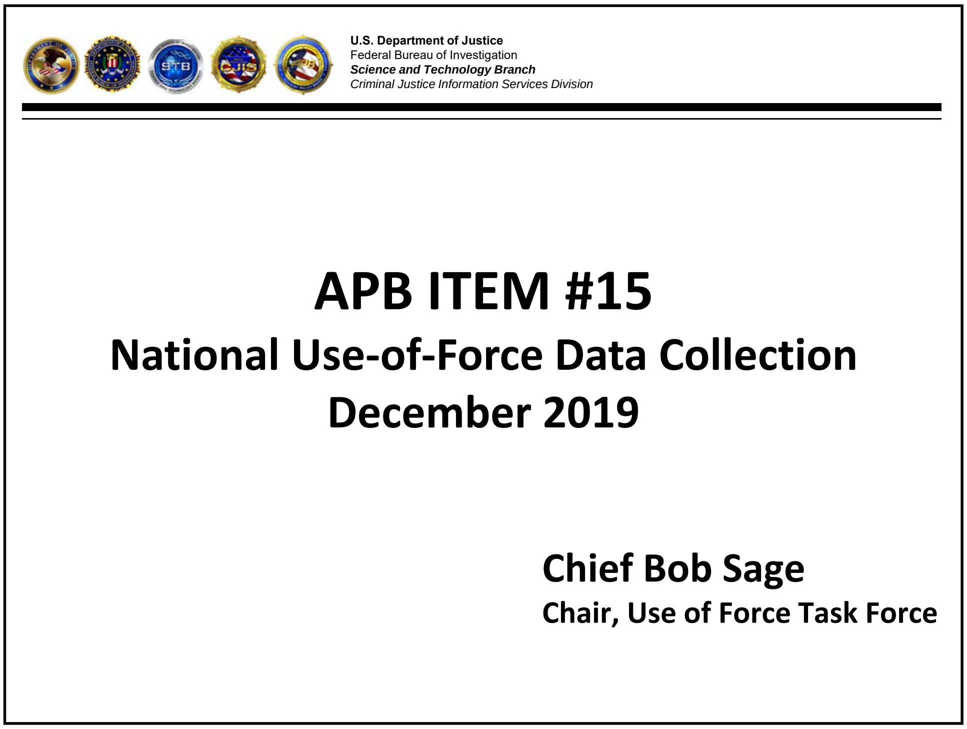
Wisconsin Department of Justice, Bureau of Justice Information and Analysis

veitenheimerdj@doj.state.wi.us

608-266-7185

ASUCRP

THE ASSOCIATION OF STATE UNIFORM CRIME REPORTING PROGRAMS

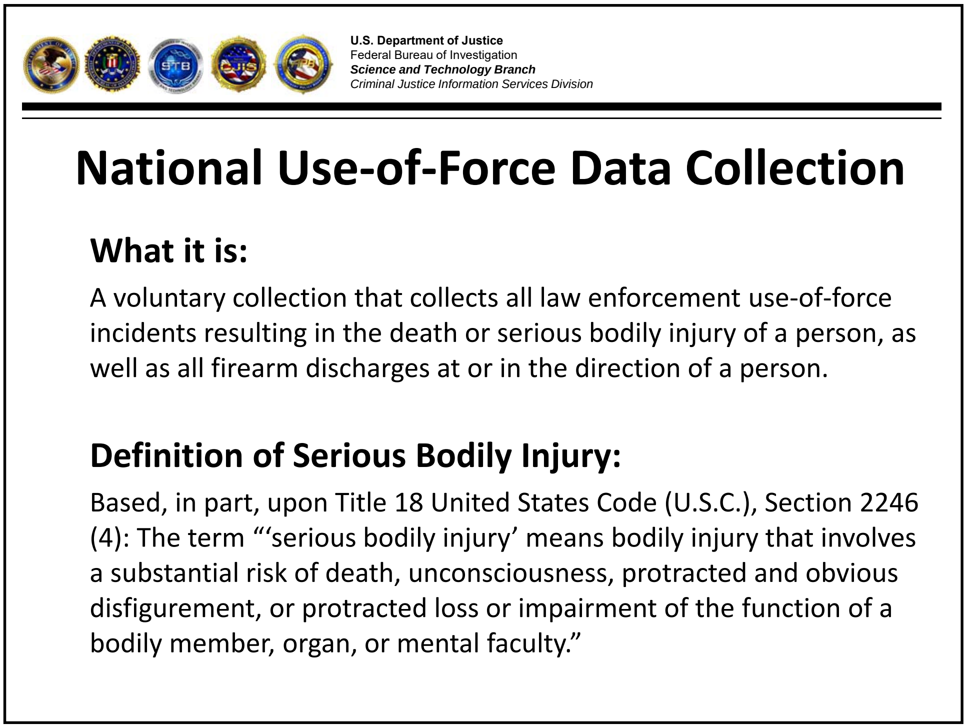


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB ITEM #15

National Use-of-Force Data Collection
December 2019

Chief Bob Sage
Chair, Use of Force Task Force



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

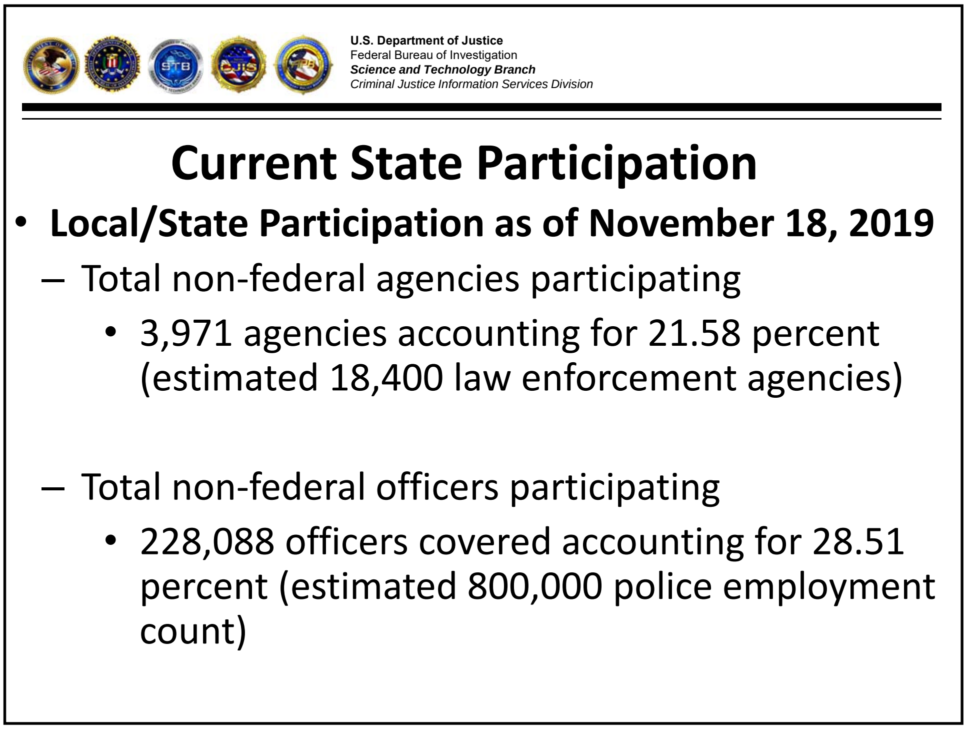
National Use-of-Force Data Collection

What it is:

A voluntary collection that collects all law enforcement use-of-force incidents resulting in the death or serious bodily injury of a person, as well as all firearm discharges at or in the direction of a person.

Definition of Serious Bodily Injury:

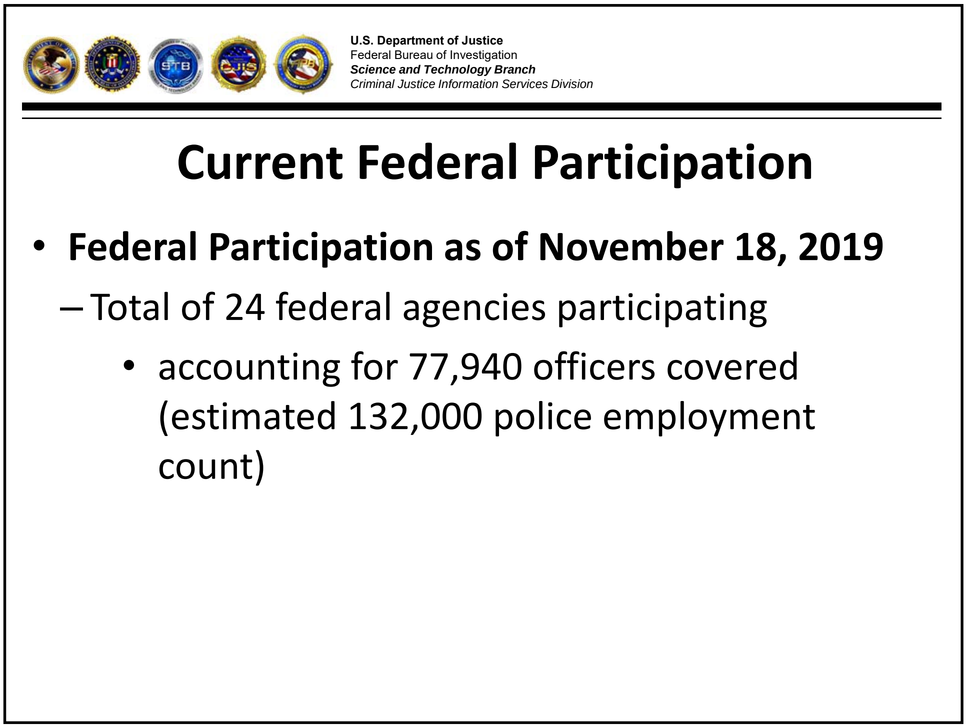
Based, in part, upon Title 18 United States Code (U.S.C.), Section 2246 (4): The term "'serious bodily injury' means bodily injury that involves a substantial risk of death, unconsciousness, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental faculty."



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Current State Participation

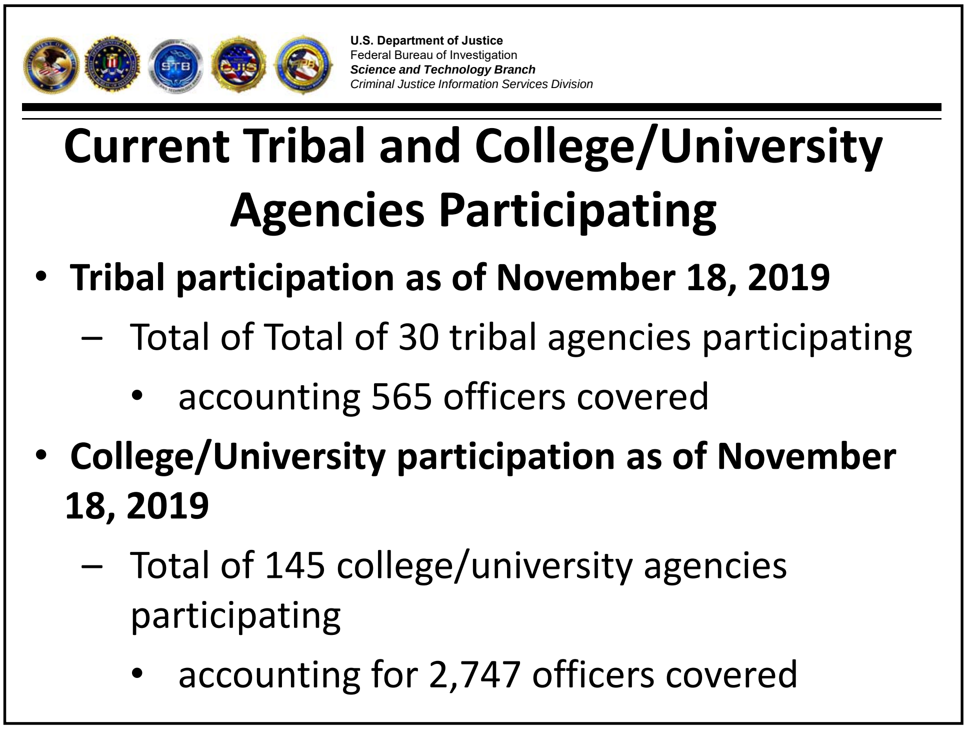
- **Local/State Participation as of November 18, 2019**
  - Total non-federal agencies participating
    - 3,971 agencies accounting for 21.58 percent (estimated 18,400 law enforcement agencies)
  - Total non-federal officers participating
    - 228,088 officers covered accounting for 28.51 percent (estimated 800,000 police employment count)



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Current Federal Participation

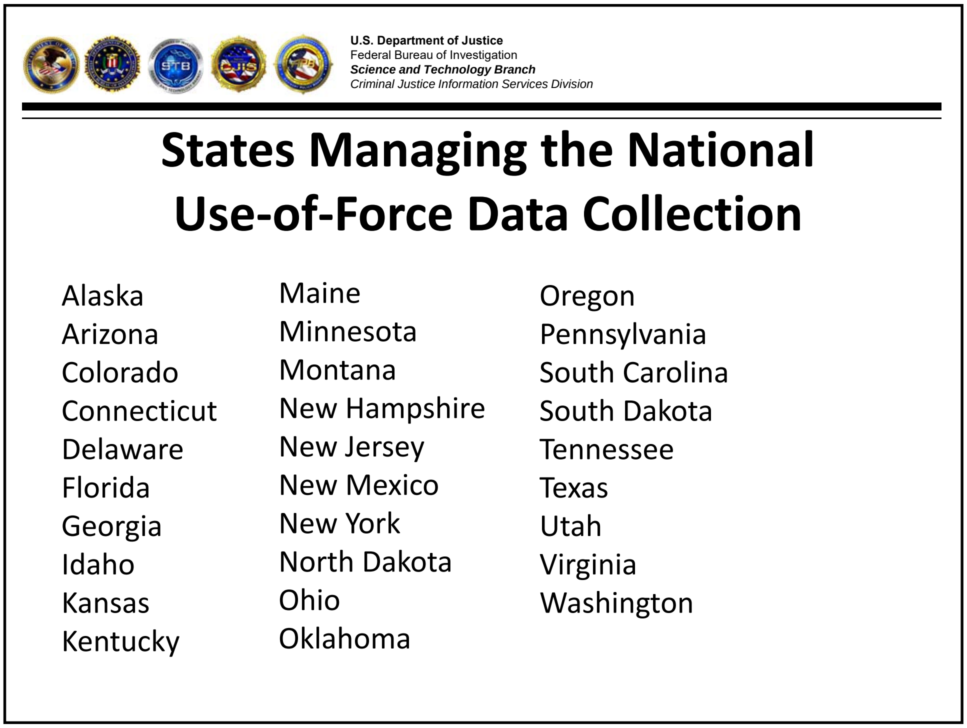
- **Federal Participation as of November 18, 2019**
  - Total of 24 federal agencies participating
    - accounting for 77,940 officers covered (estimated 132,000 police employment count)



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Current Tribal and College/University Agencies Participating

- **Tribal participation as of November 18, 2019**
  - Total of Total of 30 tribal agencies participating
    - accounting 565 officers covered
- **College/University participation as of November 18, 2019**
  - Total of 145 college/university agencies participating
    - accounting for 2,747 officers covered



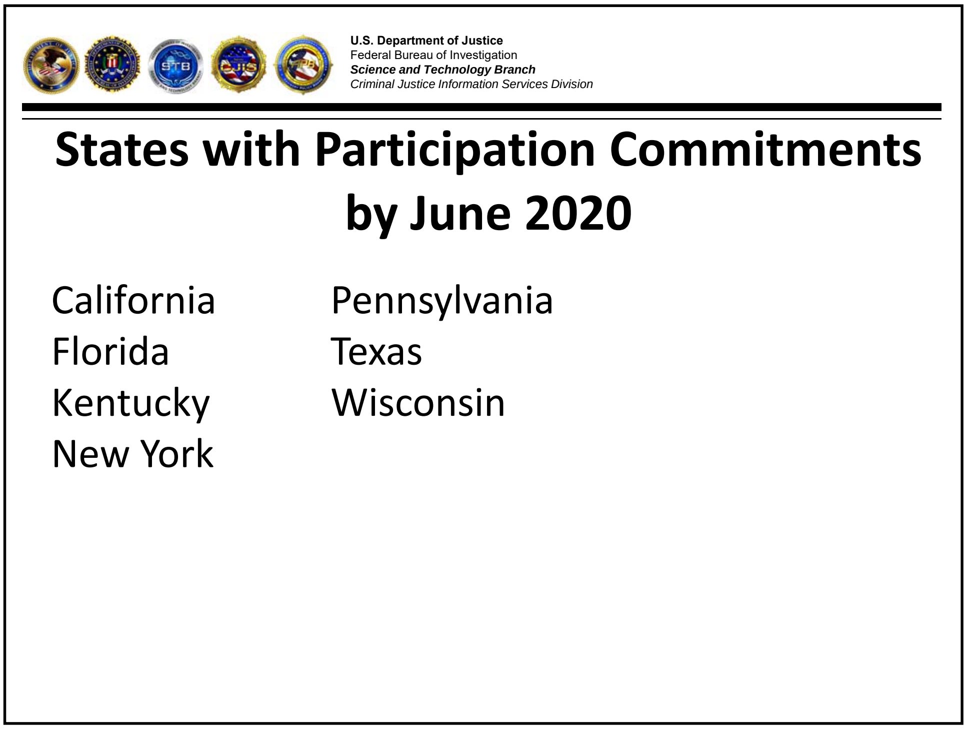
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

States Managing the National Use-of-Force Data Collection

Alaska
Arizona
Colorado
Connecticut
Delaware
Florida
Georgia
Idaho
Kansas
Kentucky

Maine
Minnesota
Montana
New Hampshire
New Jersey
New Mexico
New York
North Dakota
Ohio
Oklahoma

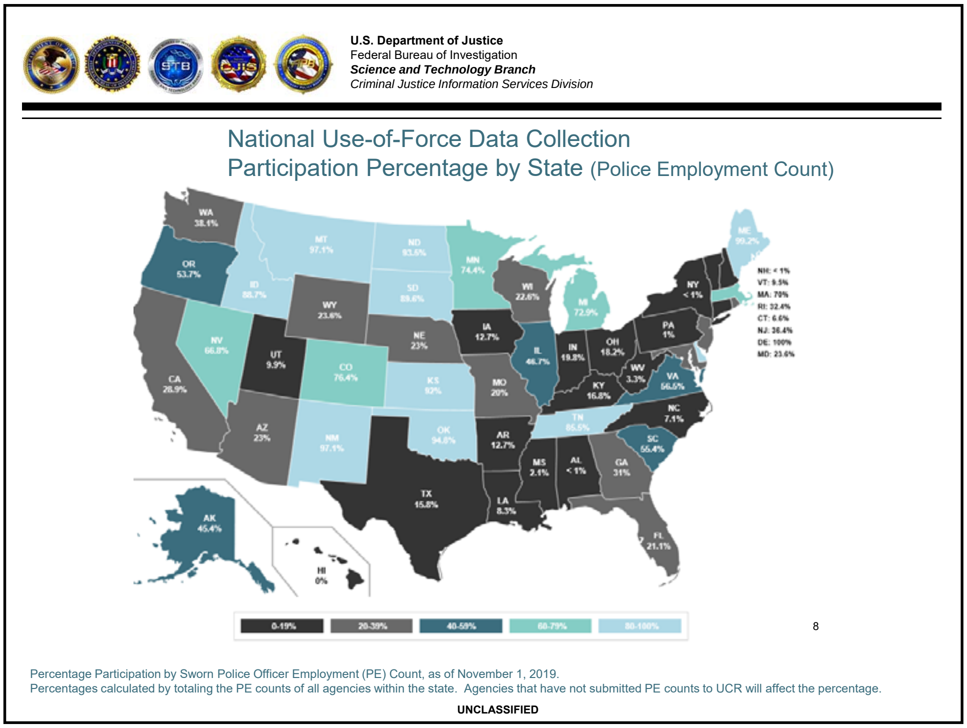
Oregon
Pennsylvania
South Carolina
South Dakota
Tennessee
Texas
Utah
Virginia
Washington



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

States with Participation Commitments by June 2020

California
Florida
Kentucky
New York
Pennsylvania
Texas
Wisconsin



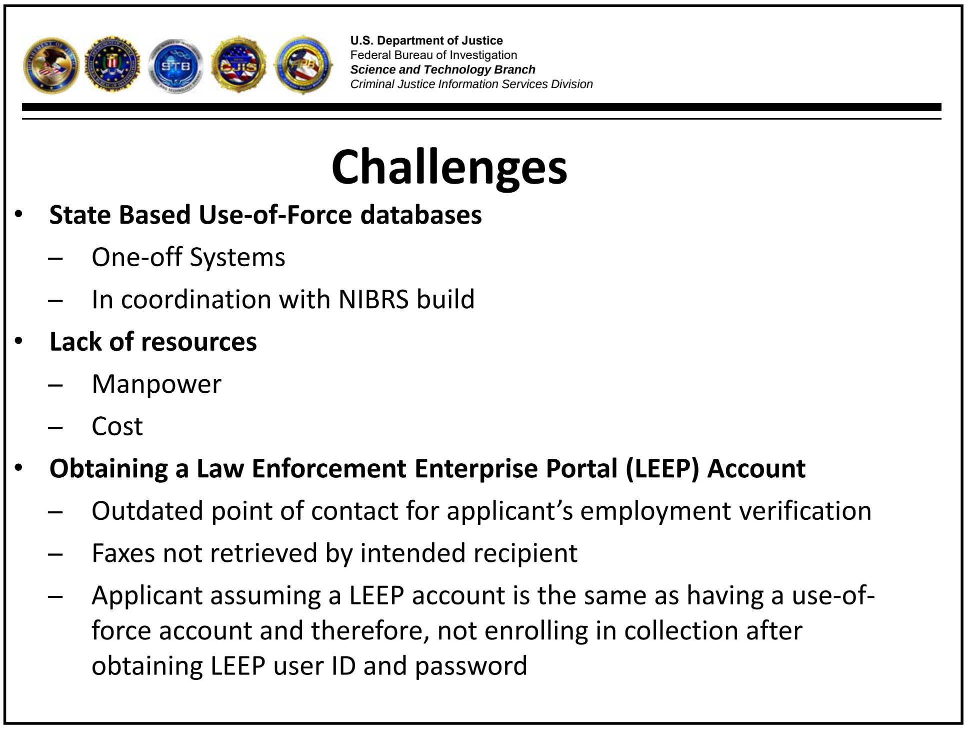
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

National Use-of-Force Data Collection
Participation Percentage by State (Police Employment Count)

8

Percentage Participation by Sworn Police Officer Employment (PE) Count, as of November 1, 2019.
Percentages calculated by totaling the PE counts of all agencies within the state. Agencies that have not submitted PE counts to UCR will affect the percentage.

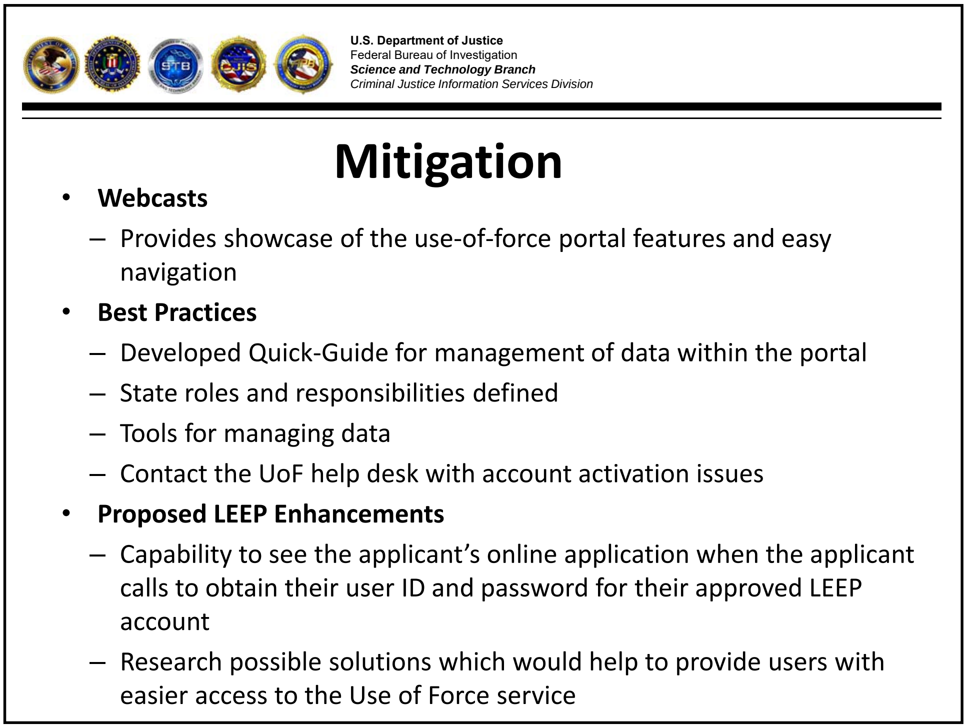
UNCLASSIFIED



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Challenges

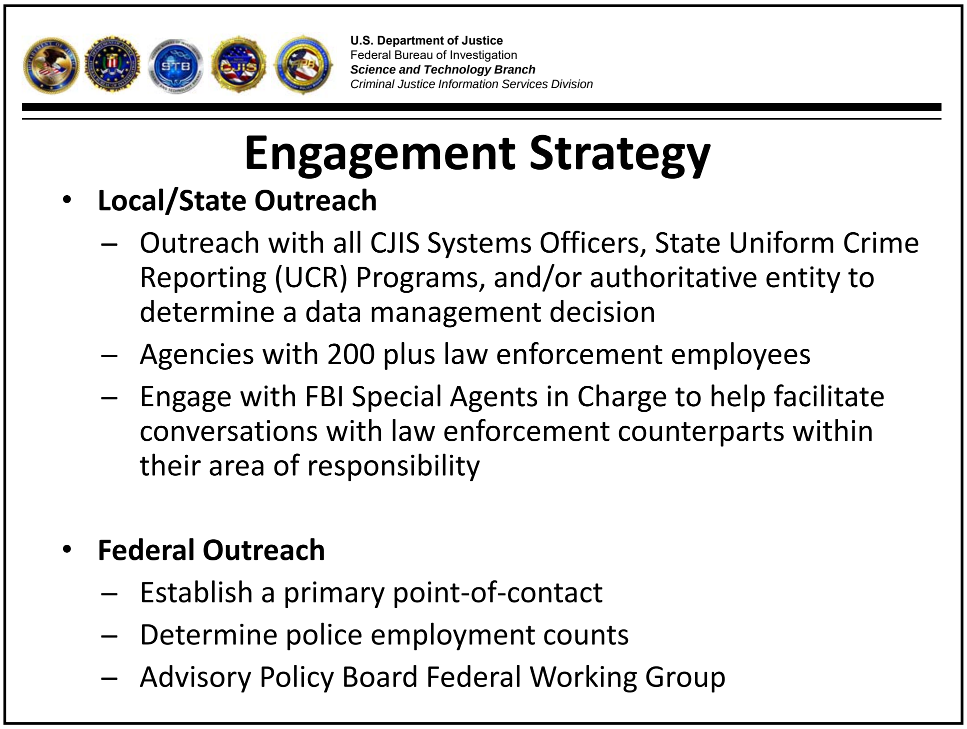
- **State Based Use-of-Force databases**
  - One-off Systems
  - In coordination with NIBRS build
- **Lack of resources**
  - Manpower
  - Cost
- **Obtaining a Law Enforcement Enterprise Portal (LEEP) Account**
  - Outdated point of contact for applicant's employment verification
  - Faxes not retrieved by intended recipient
  - Applicant assuming a LEEP account is the same as having a use-of-force account and therefore, not enrolling in collection after obtaining LEEP user ID and password



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Mitigation

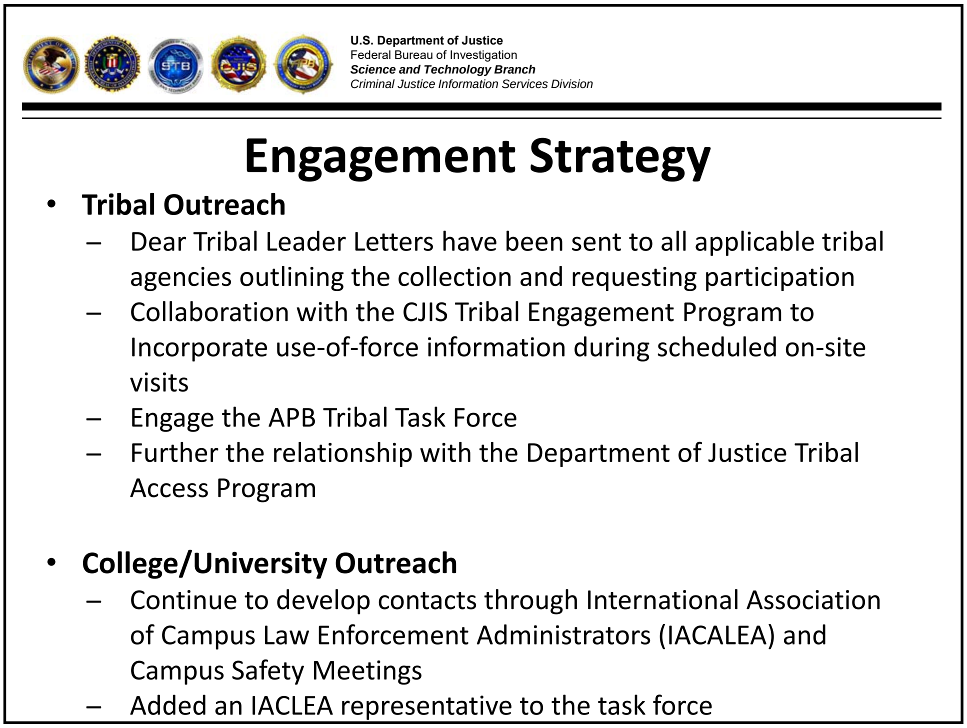
- **Webcasts**
  - Provides showcase of the use-of-force portal features and easy navigation
- **Best Practices**
  - Developed Quick-Guide for management of data within the portal
  - State roles and responsibilities defined
  - Tools for managing data
  - Contact the UoF help desk with account activation issues
- **Proposed LEEP Enhancements**
  - Capability to see the applicant's online application when the applicant calls to obtain their user ID and password for their approved LEEP account
  - Research possible solutions which would help to provide users with easier access to the Use of Force service



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Engagement Strategy

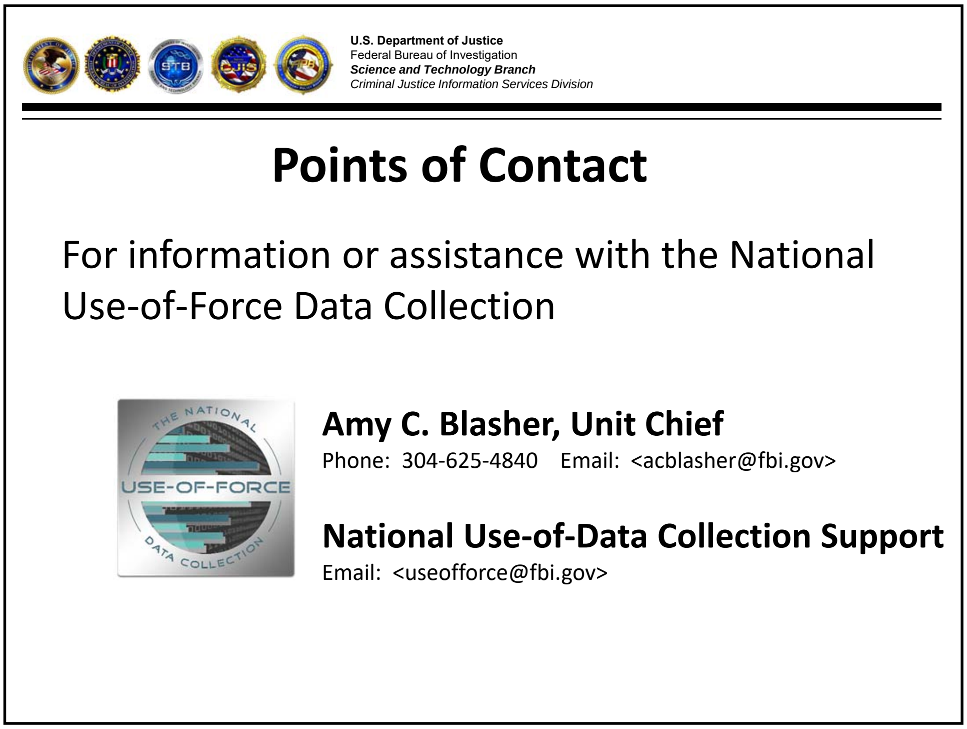
- **Local/State Outreach**
  - Outreach with all CJIS Systems Officers, State Uniform Crime Reporting (UCR) Programs, and/or authoritative entity to determine a data management decision
  - Agencies with 200 plus law enforcement employees
  - Engage with FBI Special Agents in Charge to help facilitate conversations with law enforcement counterparts within their area of responsibility
- **Federal Outreach**
  - Establish a primary point-of-contact
  - Determine police employment counts
  - Advisory Policy Board Federal Working Group



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Engagement Strategy

- **Tribal Outreach**
  - Dear Tribal Leader Letters have been sent to all applicable tribal agencies outlining the collection and requesting participation
  - Collaboration with the CJIS Tribal Engagement Program to Incorporate use-of-force information during scheduled on-site visits
  - Engage the APB Tribal Task Force
  - Further the relationship with the Department of Justice Tribal Access Program
- **College/University Outreach**
  - Continue to develop contacts through International Association of Campus Law Enforcement Administrators (IACALEA) and Campus Safety Meetings
  - Added an IACLEA representative to the task force


THE NATIONAL
USE-OF-FORCE
DATA COLLECTION

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Points of Contact

For information or assistance with the National Use-of-Force Data Collection

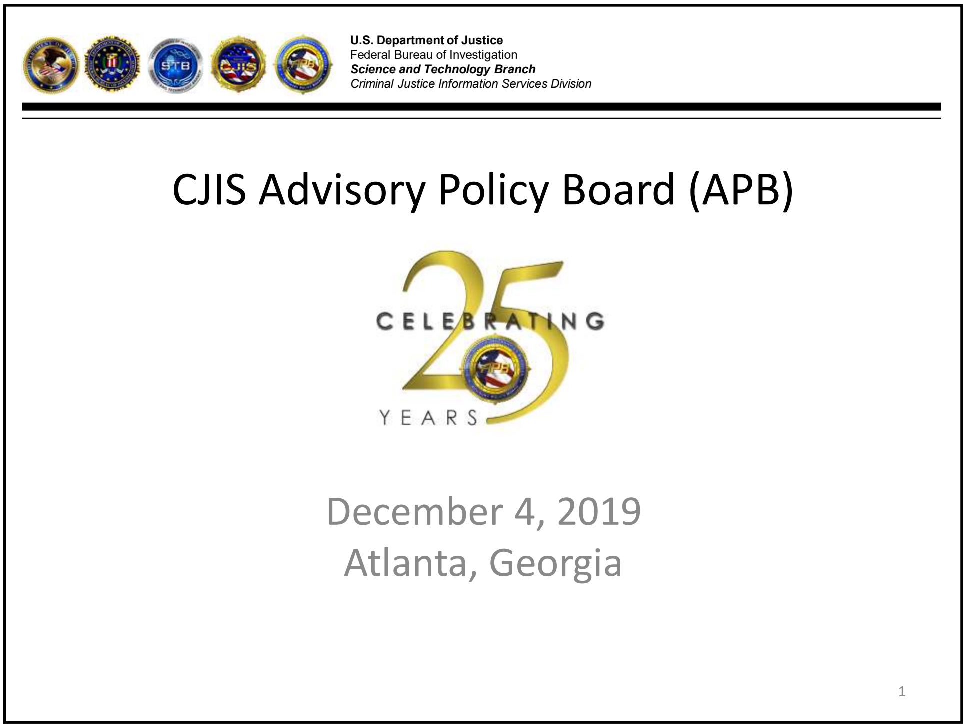
Amy C. Blasher, Unit Chief

Phone: 304-625-4840 Email: <acblasher@fbi.gov>

National Use-of-Data Collection Support

Email: <useofforce@fbi.gov>

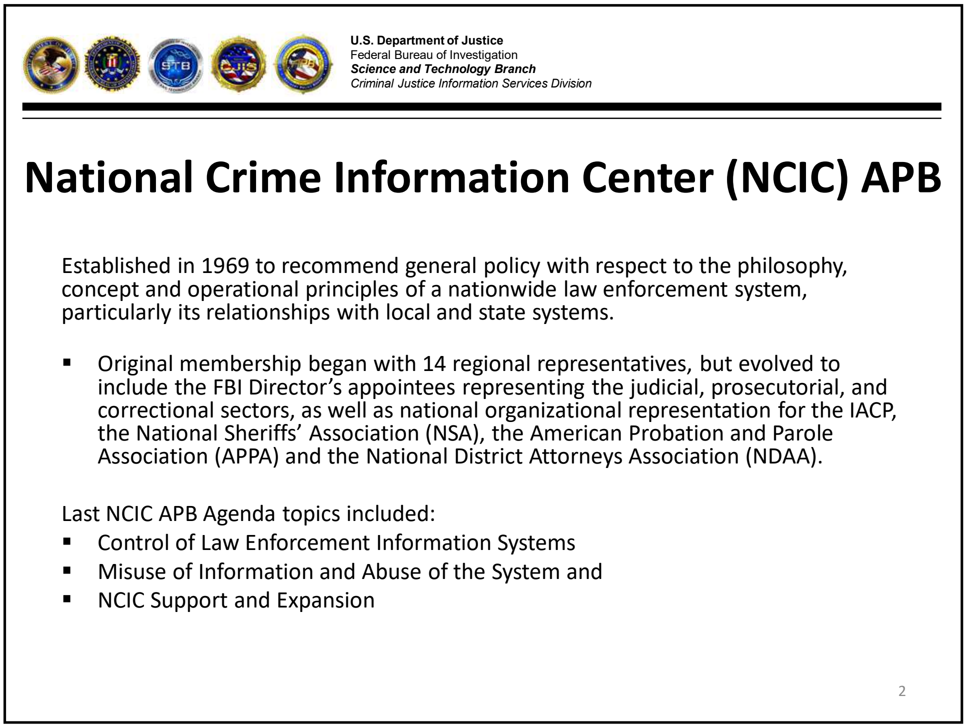
Intentionally Left Blank



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

CJIS Advisory Policy Board (APB)

December 4, 2019
Atlanta, Georgia



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

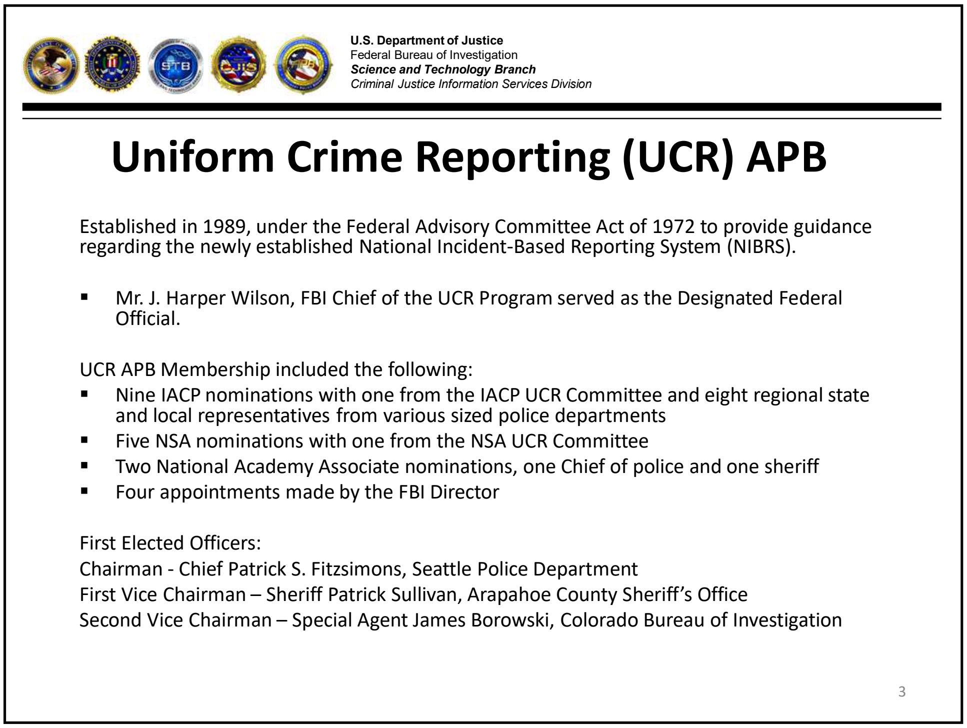
National Crime Information Center (NCIC) APB

Established in 1969 to recommend general policy with respect to the philosophy, concept and operational principles of a nationwide law enforcement system, particularly its relationships with local and state systems.

- Original membership began with 14 regional representatives, but evolved to include the FBI Director's appointees representing the judicial, prosecutorial, and correctional sectors, as well as national organizational representation for the IACP, the National Sheriffs' Association (NSA), the American Probation and Parole Association (APPA) and the National District Attorneys Association (NDAA).

Last NCIC APB Agenda topics included:

- Control of Law Enforcement Information Systems
- Misuse of Information and Abuse of the System and
- NCIC Support and Expansion



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Uniform Crime Reporting (UCR) APB

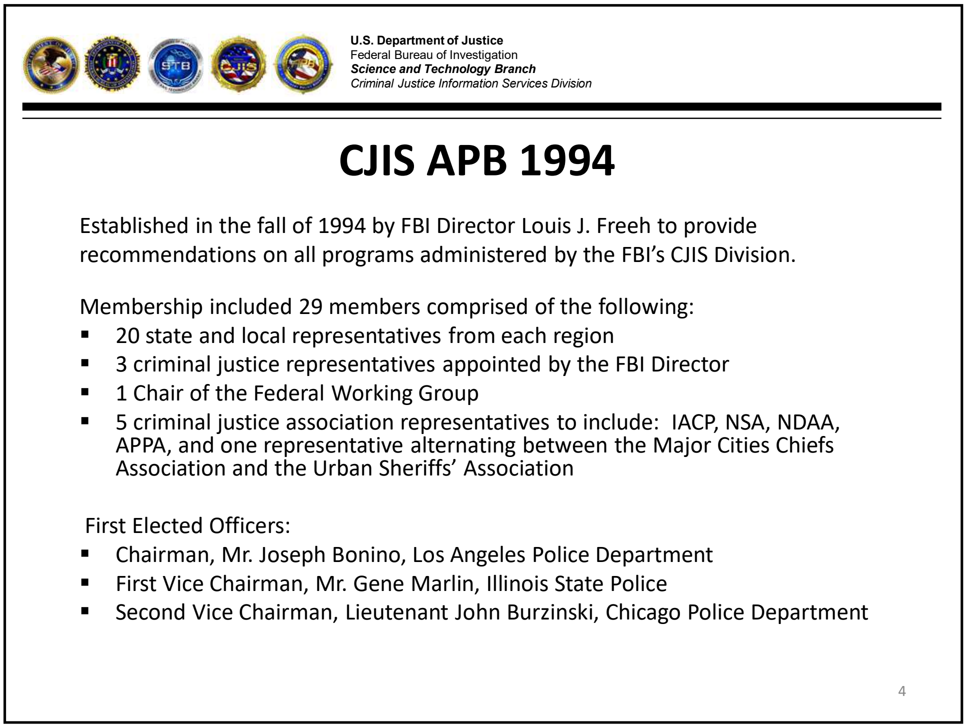
Established in 1989, under the Federal Advisory Committee Act of 1972 to provide guidance regarding the newly established National Incident-Based Reporting System (NIBRS).

- Mr. J. Harper Wilson, FBI Chief of the UCR Program served as the Designated Federal Official.

UCR APB Membership included the following:

- Nine IACP nominations with one from the IACP UCR Committee and eight regional state and local representatives from various sized police departments
- Five NSA nominations with one from the NSA UCR Committee
- Two National Academy Associate nominations, one Chief of police and one sheriff
- Four appointments made by the FBI Director

First Elected Officers:
Chairman - Chief Patrick S. Fitzsimons, Seattle Police Department
First Vice Chairman – Sheriff Patrick Sullivan, Arapahoe County Sheriff's Office
Second Vice Chairman – Special Agent James Borowski, Colorado Bureau of Investigation



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

CJIS APB 1994

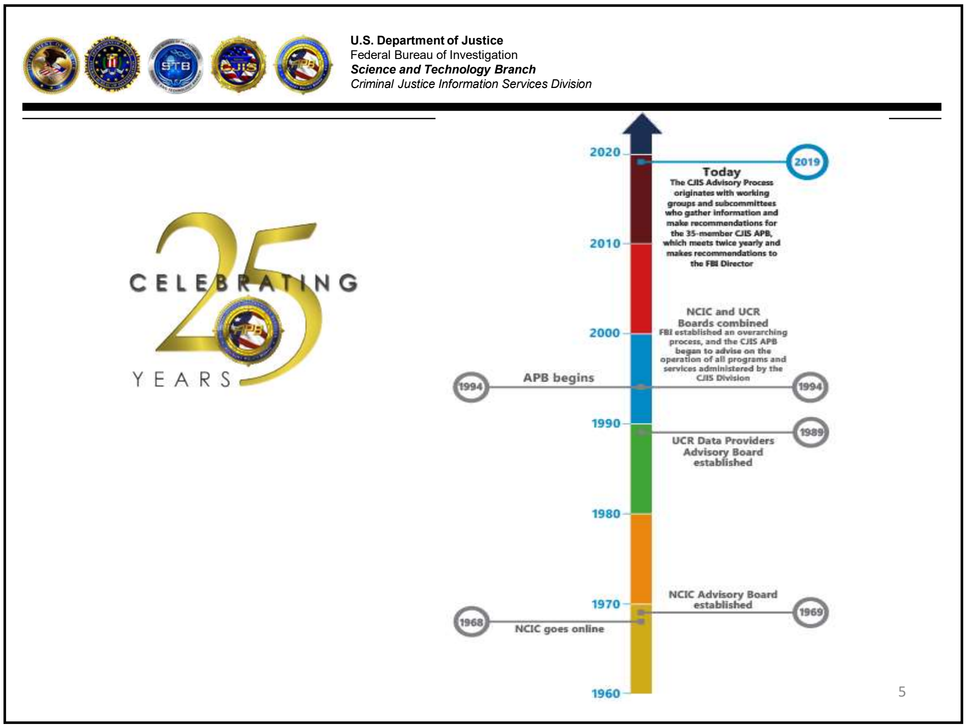
Established in the fall of 1994 by FBI Director Louis J. Freeh to provide recommendations on all programs administered by the FBI's CJIS Division.

Membership included 29 members comprised of the following:

- 20 state and local representatives from each region
- 3 criminal justice representatives appointed by the FBI Director
- 1 Chair of the Federal Working Group
- 5 criminal justice association representatives to include: IACP, NSA, NDAA, APPA, and one representative alternating between the Major Cities Chiefs Association and the Urban Sheriffs' Association

First Elected Officers:

- Chairman, Mr. Joseph Bonino, Los Angeles Police Department
- First Vice Chairman, Mr. Gene Marlin, Illinois State Police
- Second Vice Chairman, Lieutenant John Burzinski, Chicago Police Department



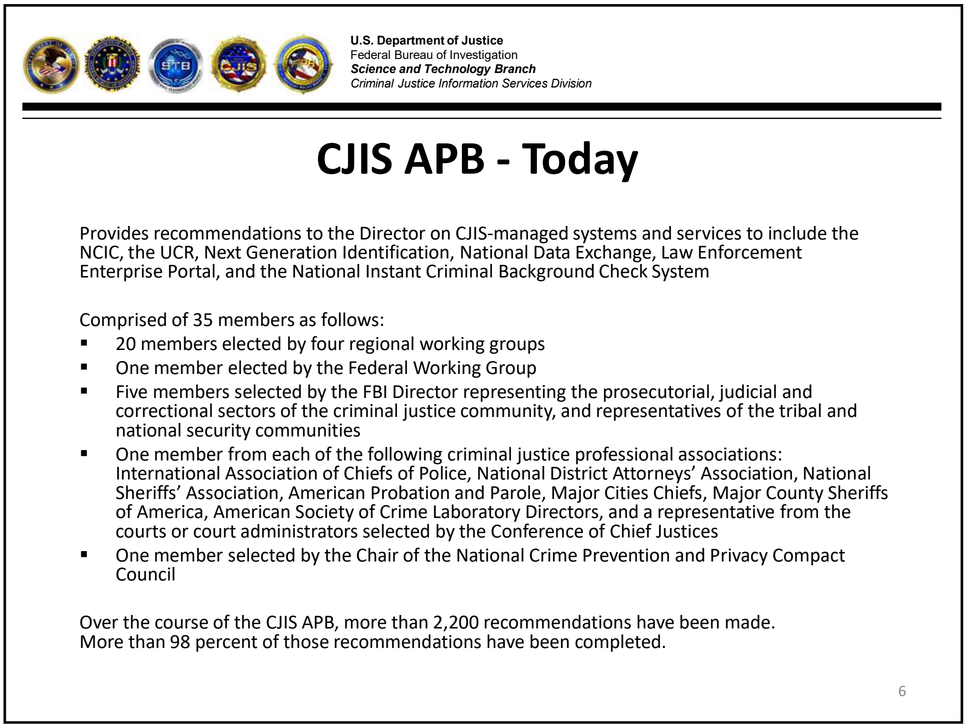
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Today
The CJIS Advisory Process originates with working groups and subcommittees who gather information and make recommendations for the 35-member CJIS APB, which meets twice yearly and makes recommendations to the FBI Director

NCIC and UCR Boards combined
FBI established an overarching process, and the CJIS APB began to advise on the operation of all programs and services administered by the CJIS Division

UCR Data Providers Advisory Board established

NCIC Advisory Board established



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

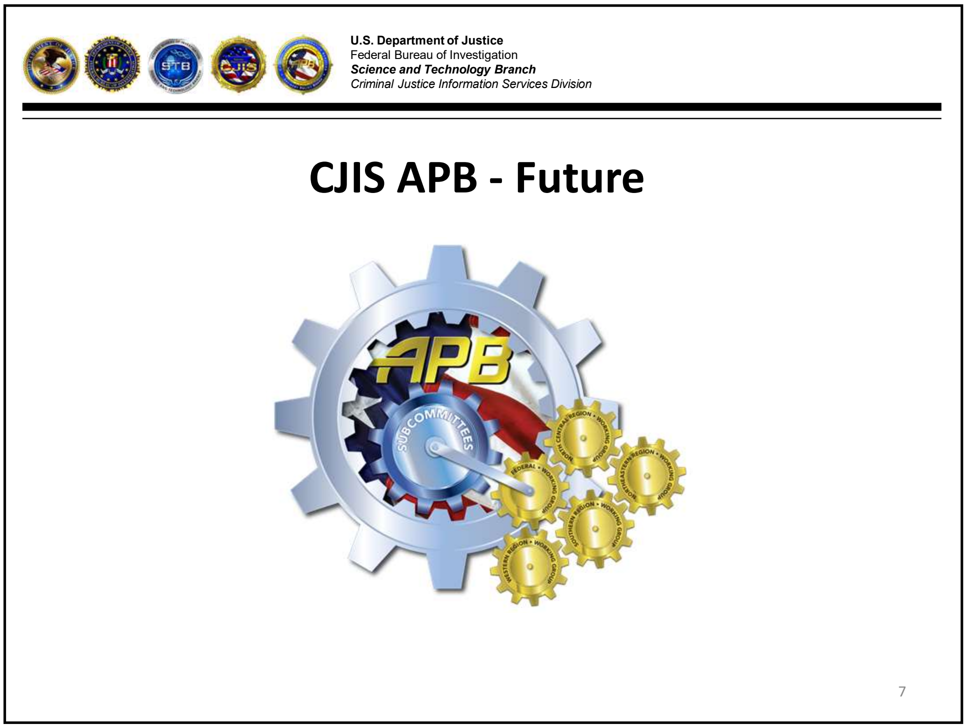
CJIS APB - Today

Provides recommendations to the Director on CJIS-managed systems and services to include the NCIC, the UCR, Next Generation Identification, National Data Exchange, Law Enforcement Enterprise Portal, and the National Instant Criminal Background Check System

Comprised of 35 members as follows:

- 20 members elected by four regional working groups
- One member elected by the Federal Working Group
- Five members selected by the FBI Director representing the prosecutorial, judicial and correctional sectors of the criminal justice community, and representatives of the tribal and national security communities
- One member from each of the following criminal justice professional associations: International Association of Chiefs of Police, National District Attorneys' Association, National Sheriffs' Association, American Probation and Parole, Major Cities Chiefs, Major County Sheriffs of America, American Society of Crime Laboratory Directors, and a representative from the courts or court administrators selected by the Conference of Chief Justices
- One member selected by the Chair of the National Crime Prevention and Privacy Compact Council

Over the course of the CJIS APB, more than 2,200 recommendations have been made.
More than 98 percent of those recommendations have been completed.

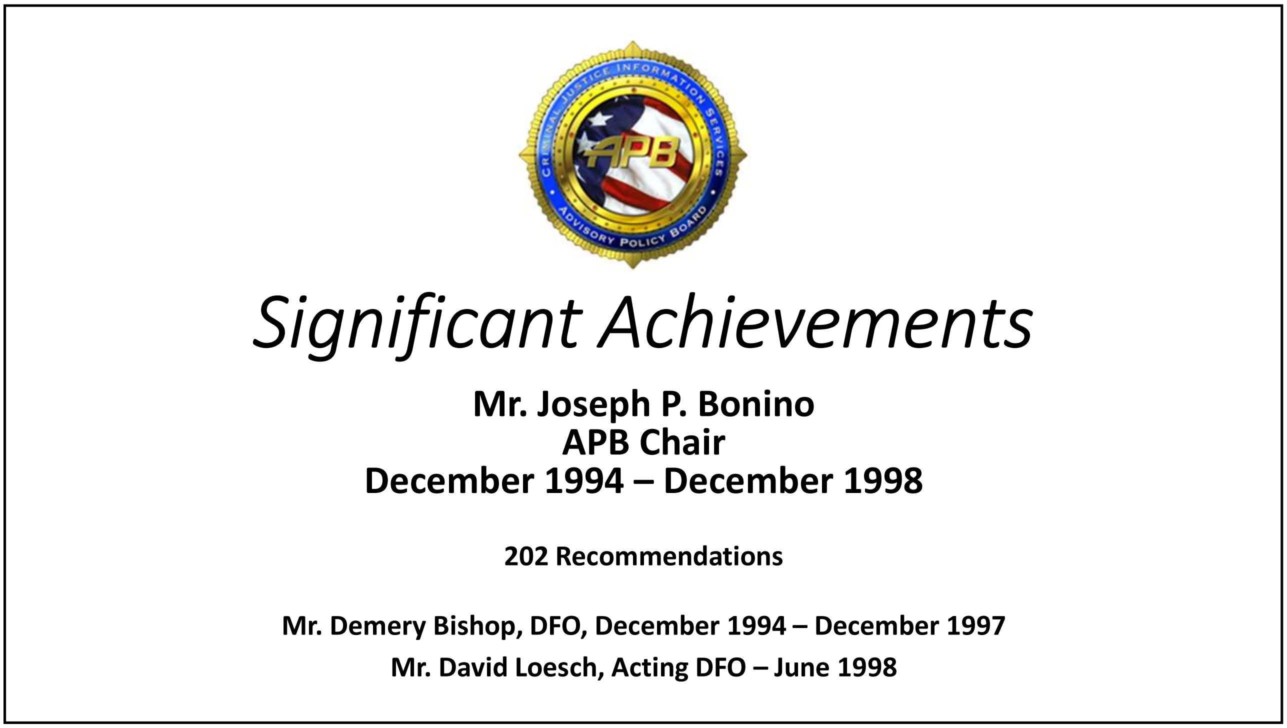


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

CJIS APB - Future

APB
SUBCOMMITTEES
FEDERAL • WORKING GROUP
NORTH CENTRAL REGION • WORKING GROUP
NORTHEASTERN REGION • WORKING GROUP
SOUTHERN REGION • WORKING GROUP
WESTERN REGION • WORKING GROUP

7



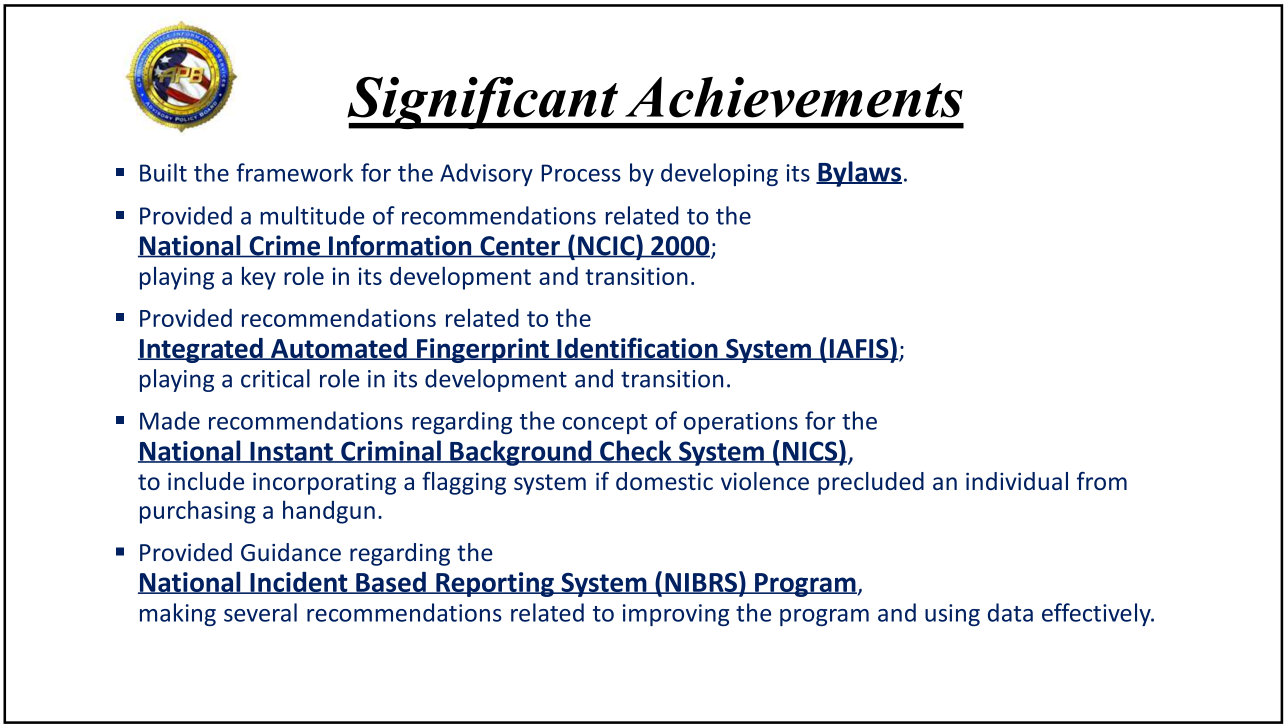
Significant Achievements

Mr. Joseph P. Bonino
APB Chair
December 1994 – December 1998

202 Recommendations

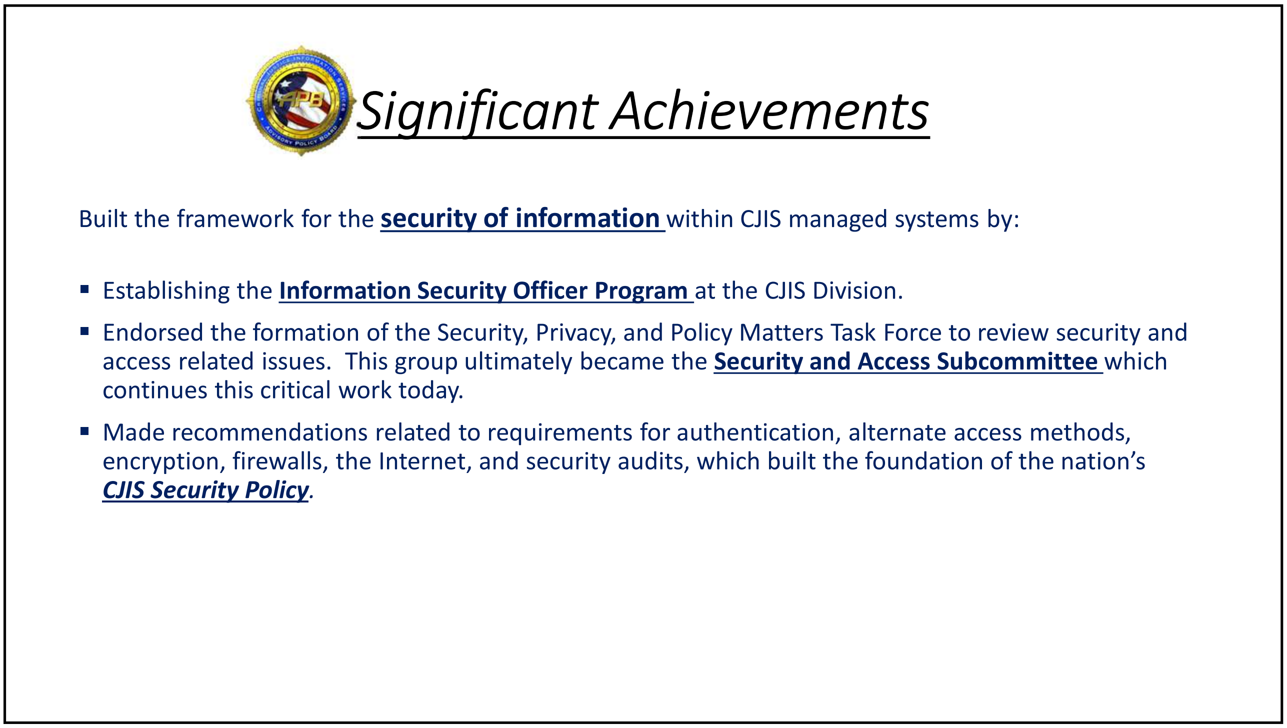
Mr. Demery Bishop, DFO, December 1994 – December 1997

Mr. David Loesch, Acting DFO – June 1998



Significant Achievements

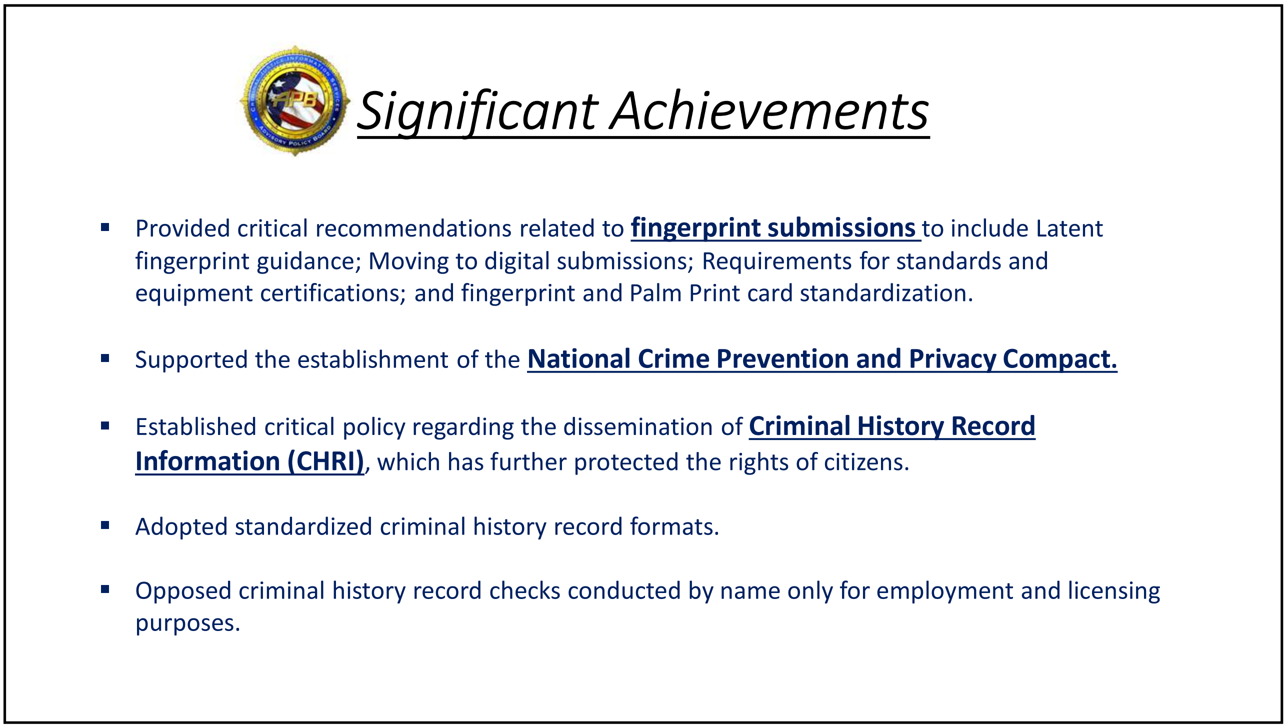
- Built the framework for the Advisory Process by developing its **Bylaws**.
- Provided a multitude of recommendations related to the **National Crime Information Center (NCIC) 2000**; playing a key role in its development and transition.
- Provided recommendations related to the **Integrated Automated Fingerprint Identification System (IAFIS)**; playing a critical role in its development and transition.
- Made recommendations regarding the concept of operations for the **National Instant Criminal Background Check System (NICS)**, to include incorporating a flagging system if domestic violence precluded an individual from purchasing a handgun.
- Provided Guidance regarding the **National Incident Based Reporting System (NIBRS) Program**, making several recommendations related to improving the program and using data effectively.



Significant Achievements

Built the framework for the **security of information** within CJIS managed systems by:

- Establishing the **Information Security Officer Program** at the CJIS Division.
- Endorsed the formation of the Security, Privacy, and Policy Matters Task Force to review security and access related issues. This group ultimately became the **Security and Access Subcommittee** which continues this critical work today.
- Made recommendations related to requirements for authentication, alternate access methods, encryption, firewalls, the Internet, and security audits, which built the foundation of the nation's ***CJIS Security Policy***.



Significant Achievements

- Provided critical recommendations related to **fingerprint submissions** to include Latent fingerprint guidance; Moving to digital submissions; Requirements for standards and equipment certifications; and fingerprint and Palm Print card standardization.
- Supported the establishment of the **National Crime Prevention and Privacy Compact.**
- Established critical policy regarding the dissemination of **Criminal History Record Information (CHRI)**, which has further protected the rights of citizens.
- Adopted standardized criminal history record formats.
- Opposed criminal history record checks conducted by name only for employment and licensing purposes.

Significant Achievements

Made important recommendations related to **Missing and Unidentified Files** to include:

- Establishing the **Dental Task Force**, which made multiple recommendations for improve information included in the NCIC Missing and Unidentified Person Files.
- Providing the **National Center for Missing and Exploited Children "real time" notification of all NCIC Unidentified Person records**.
- Adding fields to indicate if a **DNA** profile was available, and where the profile was located.
- Creation of the "flagging" mechanism for missing person entries, to call attention to **estranged or abducted children** to authorities more easily.

Intentionally Left Blank

David Gavin's Comments to CJIS APB December 2019

My name is David Gavin. As Assistant Chief of Administration at the Texas Department of Public Safety, I participated in the Advisory Process for approximately 18 years. During that time, I was honored to serve a term as Chair of the APB.

Over the course of those years, and especially during the planning and development of NCIC 2000 and IAFIS when I sat as first vice chair to Joe Bonino, I realized there were a number of core challenges we had to overcome and principles we had to embrace to ensure the ongoing success of the Advisory Process. I want to mention just two that I believe are of special importance. I know you are all aware of these issues, and I raise them here respectfully, only for affirmation and emphasis—as a reminder.

1. The first principle is the most obvious: both FBI staff and all Advisory Process members must embrace the importance of the process itself. If there were no Advisory Process external entities such as Congress and the media would be demanding, "What controls exist over these national police information systems?" In the fifty years since FBI so wisely chose the shared management approach of the Advisory Process to oversee these systems, our answer to that question of governance has proven itself adequate and reliable.

   Clearly it is a primary responsibility of the APB and FBI to ensure the APB and the Advisory Process as a whole remain a relevant and responsible governance structure. We must safeguard against getting into a position where an investigation by Congress, the media, or other entity could point to demonstrable weaknesses in the Advisory Process that suggest it is not a fully functioning, well controlled and well-controlling governance of the CJIS Systems.

   Key to that safeguarding is diligence and dedication to the work from all members at all levels of the Advisory Process, from the Working Groups to the ABP. We can all attest that participation puts non-trivial demands upon our time, ourselves, and our agencies. A significant challenge in and of itself is just the responsibility to read the Topic Papers, understand them, share them with the appropriate staff for review and feedback, and develop recommendations within the context of our own jurisdictions and those of neighboring and related agencies. It becomes clear from our first meetings we cannot just read these Topics on the plane trip in. It is our responsibility to do the work necessary to make the meetings successful.

   We also all share the responsibility to be thinking critically about our own agencies' experiences and to bring forward new ideas for Topics Papers relevant to the implementation and operation of these systems. We generally do pretty well in these areas, but we must remain vigilant and willing to make improvements.

   Equally important for the health of the Advisory Process is that we remember we come to the meetings to answer only one question: *What is the best solution for the entire nation?* This was especially important during the planning for NCIC 2000 and IAFIS. We cannot allow our own priorities to become our singularly promoted agendas—we must know the Topics, listen in the meetings, and contribute to discussions that find and recommend the best solutions for the country as a whole—not for our state, not for our jurisdiction, not for the FBI—but the best solution for the country that is built from all the insights of all the represented jurisdictions. For all members of the Advisory Process, but especially for us as members of the APB, we have a deep responsibility to put our own private agendas aside.

2. Consistent with the first principle, a second consideration that surfaces at certain times specifically for us as members of the APB is the need for us to always be mindful of the executive role of the APB itself. The excellent work done by the Working Groups, Subcommittees, Task Forces—and of course the irreplaceable work done by the FBI staff—does not create a license for the APB meetings to become just rubber stamps of those resulting recommendations. We as APB members must watch carefully that our decisions are not—or cannot be construed as—inappropriately lessening privacy, security, or other critical controls in the name of expediency, convenience, or mere fiscal reserve. We must read the topics and recommendations from the Subcommittees critically—because that is how they will be read by third parties if they come under scrutiny. An appropriate example is when the subcommittees recommended extending the training requirement for CJIS systems users to every three years rather than every two years. The APB rejected that proposal first because of the increasing complexities within the systems, and second because the existence of a robust training regimen is a hallmark of a serious governance structure responsibly managing a complex information system—all the more so with the life altering outcomes that result from the use of the CJIS systems. We as APB members must always be watchful from the strategic and executive perspectives.

Related to both the above principles I would make one recommendation. Mike Lesko and I have recently been discussing the re-constitution of the Public Safety Strategy Subcommittee, which was previously created by the CJIS APB as comprised of the APB Officers and the Chairs of the Subcommittees, as I recall. Its mission was to keep the APB thinking strategically. I will leave it to Mike to discuss it in detail, but I recommend it to you APB members as relevant to both of the above points and much more regarding the mission of the APB and Advisory Process.

In closing, it was an honor to play a small role in this important enterprise. I offer my sincere appreciation to the CJIS executives for their critical support of the Advisory Process and to the hard working CJIS staff for their consistently amazing work on the Topics. Most importantly, I say "Thank You" to you current members of the APB for stepping up to do this important work for our country—and for embracing the significant responsibilities of doing so. I am sure you will all continue to find it as rewarding as I did, and—I'm sure—as all the other prior Chairs have, as well.

David Gavin's Comments to CJIS APB December 2019

Mike:

In your discussions of the Public Safety Strategy Subcommittee you could suggest to the current APB that the PSSS develop an anniversary message to all Advisory Process members comprised of the current theirs and the APB's thoughts and insights from this meeting after listening to the video, and the previous chairs, and their own ideas from this meeting. I'm thinking of a message from the current leadership regarding their core guiding principles for the continued success of the Advisory Process going forward. Just a thought.

Intentionally Left Blank

Significant Achievements

Mr. David Gavin
APB Chair
December 1998 – December 2000

165 Recommendations

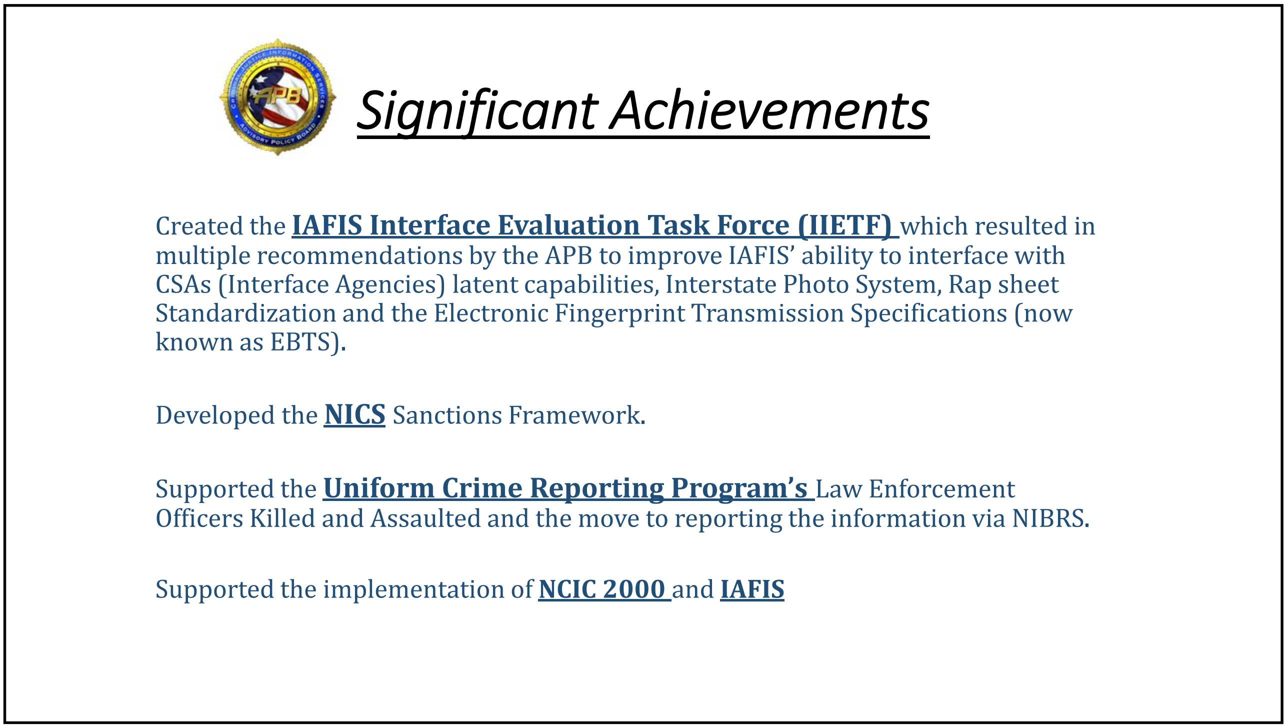
DFOs Mr. Don Johnson and Mr. Roy Weise

Significant Achievements

Made significant recommendations to improve the effective use of **NCIC** to include:

- Changes to online validation, notifications, reject messages, locate transactions, and modifications to the following files: Protection Order File, License Plate Records, Article File, Convicted Sex Offender File, Vehicle File, and the Originating Agency Identifier File.

Reviewed and made recommendations on numerous **NCIC 2000** requirements, which included beginning the exploration of using Extensible Markup Language (XML).



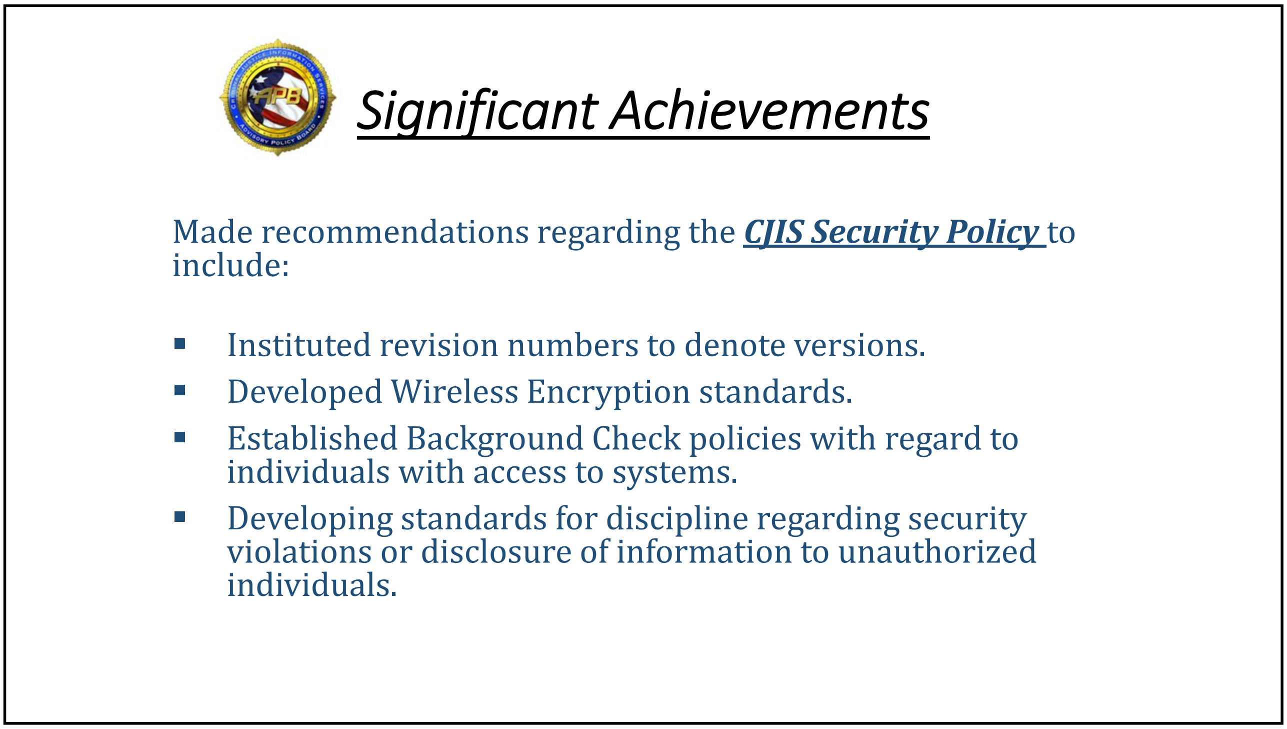
Significant Achievements

Created the **IAFIS Interface Evaluation Task Force (IIETF)** which resulted in multiple recommendations by the APB to improve IAFIS' ability to interface with CSAs (Interface Agencies) latent capabilities, Interstate Photo System, Rap sheet Standardization and the Electronic Fingerprint Transmission Specifications (now known as EBTS).

Developed the **NICS** Sanctions Framework.

Supported the **Uniform Crime Reporting Program's** Law Enforcement Officers Killed and Assaulted and the move to reporting the information via NIBRS.

Supported the implementation of **NCIC 2000** and **IAFIS**



Significant Achievements

Made recommendations regarding the ***CJIS Security Policy*** to include:

- Instituted revision numbers to denote versions.
- Developed Wireless Encryption standards.
- Established Background Check policies with regard to individuals with access to systems.
- Developing standards for discipline regarding security violations or disclosure of information to unauthorized individuals.

Significant Achievements

Mr. William Casey
APB Chair
December 2000 – December 2004

440 Recommendations

Mr. Roy Weise, DFO

Significant Achievements

Multiple recommendations to improve **NCIC functionality** related to validation, notifications, administrative messages, timely entry, search and matching criteria, as well as changes to the following files:

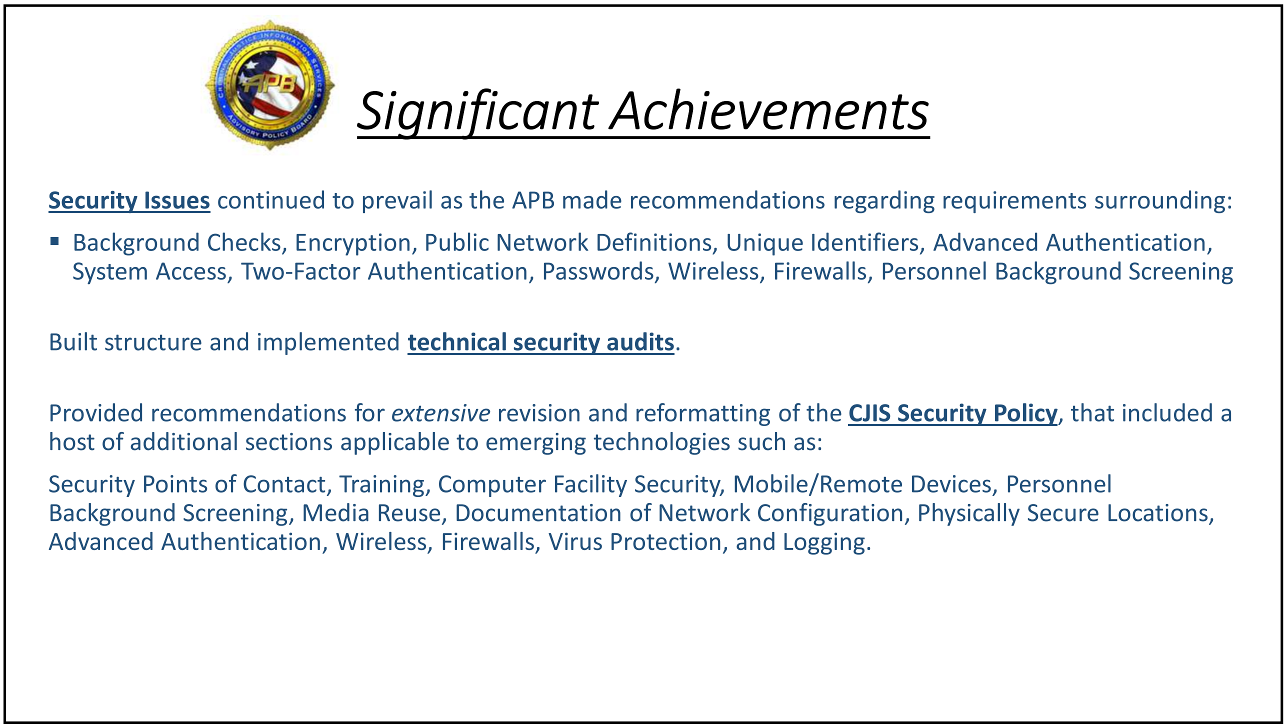
> Protection Order; Persons; Image; Vehicle; Deported Felon and Absconder; Securities; Gun; Article; Violent Gang and Terrorist Organization; Immigration Violators; and Convicted Person on Supervised Release files.

Continued to support the transition to Extensible Markup Language (XML).

Established policy requiring states to transition to NCIC 2000.

Tracked and supported state transitions to NCIC 2000.

Supported the creation of the Identity Theft File.



Significant Achievements

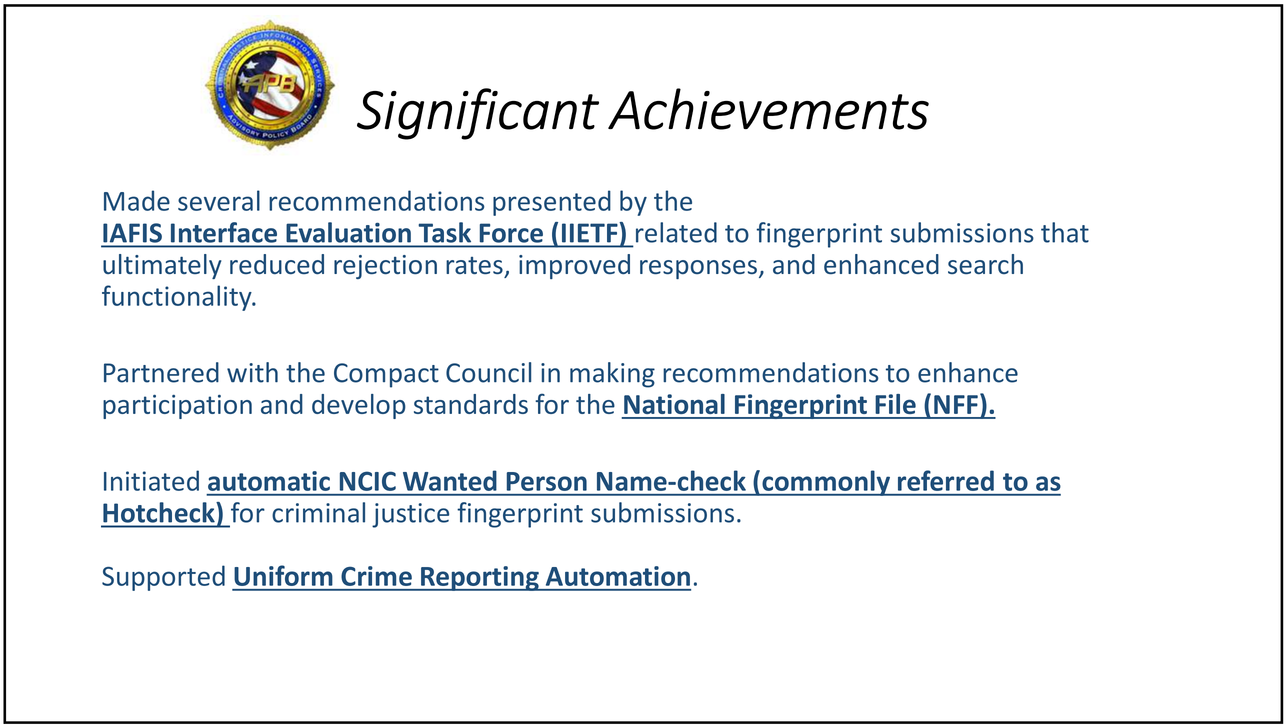
Security Issues continued to prevail as the APB made recommendations regarding requirements surrounding:

- Background Checks, Encryption, Public Network Definitions, Unique Identifiers, Advanced Authentication, System Access, Two-Factor Authentication, Passwords, Wireless, Firewalls, Personnel Background Screening

Built structure and implemented **technical security audits**.

Provided recommendations for *extensive* revision and reformatting of the **CJIS Security Policy**, that included a host of additional sections applicable to emerging technologies such as:

Security Points of Contact, Training, Computer Facility Security, Mobile/Remote Devices, Personnel Background Screening, Media Reuse, Documentation of Network Configuration, Physically Secure Locations, Advanced Authentication, Wireless, Firewalls, Virus Protection, and Logging.



Significant Achievements

Made several recommendations presented by the **IAFIS Interface Evaluation Task Force (IIETF)** related to fingerprint submissions that ultimately reduced rejection rates, improved responses, and enhanced search functionality.

Partnered with the Compact Council in making recommendations to enhance participation and develop standards for the **National Fingerprint File (NFF).**

Initiated **automatic NCIC Wanted Person Name-check (commonly referred to as Hotcheck)** for criminal justice fingerprint submissions.

Supported **Uniform Crime Reporting Automation**.

Significant Changes

Endorsed the American Association of Motor Vehicle Administrators (AAMVA) proposal for a **standardized Driver's License**.

Began policy discussions on the use of **License Plate Readers**.

Recommended changes for improving the
Electronic Fingerprint Transmission Specification

Issued **letters of support** for the continued development and funding of CJIS managed systems to include NCIC 2000 and IAFIS. These letters ultimately resulted in national support and full participation.

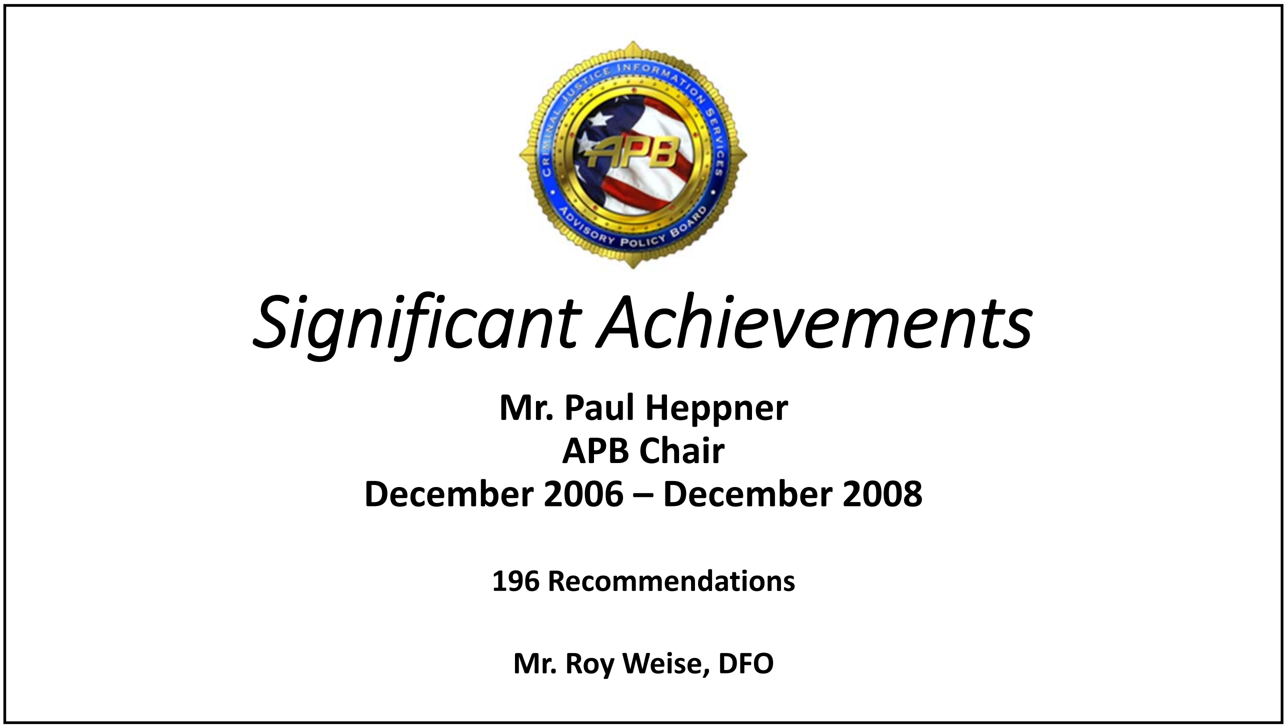
Made several recommendations regarding submission and retention of **disposition data** in IAFIS.

Significant Achievements

Began review of the design for the **Next Generation IAFIS (NGI) System**.

Made recommendations supporting the creation of the **National Data Exchange (N-DEx) System.**

Intentionally Left Blank



Significant Achievements

Mr. Paul Heppner
APB Chair
December 2006 – December 2008

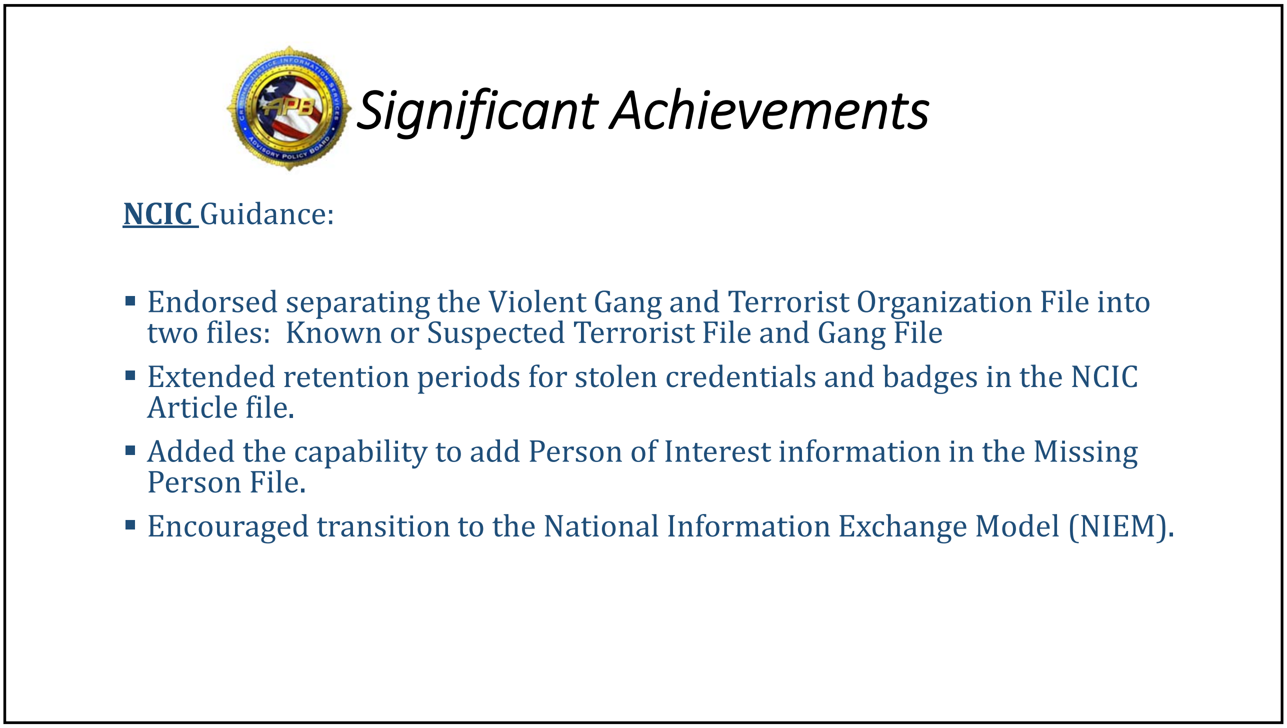
196 Recommendations

Mr. Roy Weise, DFO

Significant Achievements

Made recommendations to improve the **National Crime Information Center (NCIC)** to include:

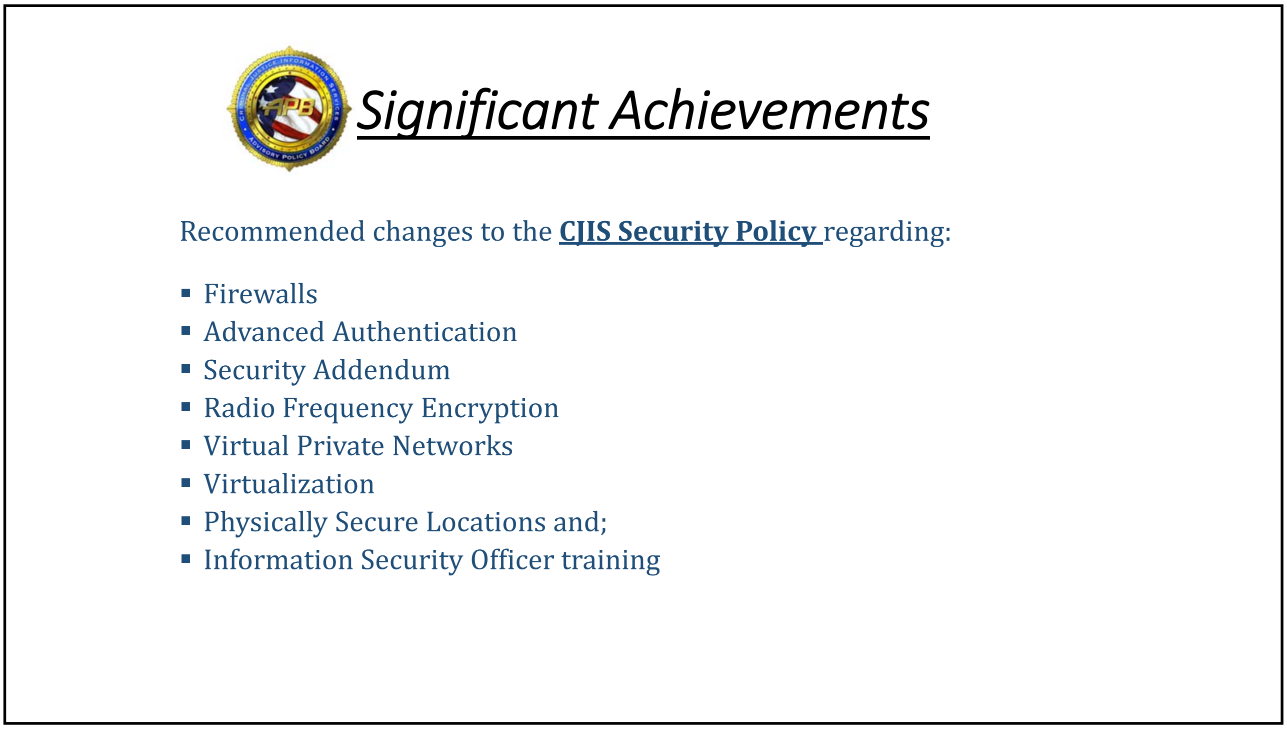
- Changes to the following files: Wanted Person, Missing Person, Protection Order, United States Secret Service Protection, Vehicle, Boat, Immigration Violator, Supervised Release, and Foreign Fugitive Files
- License Plate Reader Project
- Allowed unsolicited notification to be sent when administrative responsibility changes to another Originating Agency Identifier.
- Improvements to the Convicted Sexual Offender Registry, which included changing the file name to the Sex Offender File
- Automatically populated NCIC Wanted Person File records with an image from the Integrated Automated Fingerprint Identification System (IAFIS) Interstate Photo System, if available.



Significant Achievements

NCIC Guidance:

- Endorsed separating the Violent Gang and Terrorist Organization File into two files: Known or Suspected Terrorist File and Gang File
- Extended retention periods for stolen credentials and badges in the NCIC Article file.
- Added the capability to add Person of Interest information in the Missing Person File.
- Encouraged transition to the National Information Exchange Model (NIEM).



Significant Achievements

Recommended changes to the **CJIS Security Policy** regarding:

- Firewalls
- Advanced Authentication
- Security Addendum
- Radio Frequency Encryption
- Virtual Private Networks
- Virtualization
- Physically Secure Locations and;
- Information Security Officer training

Significant Achievements

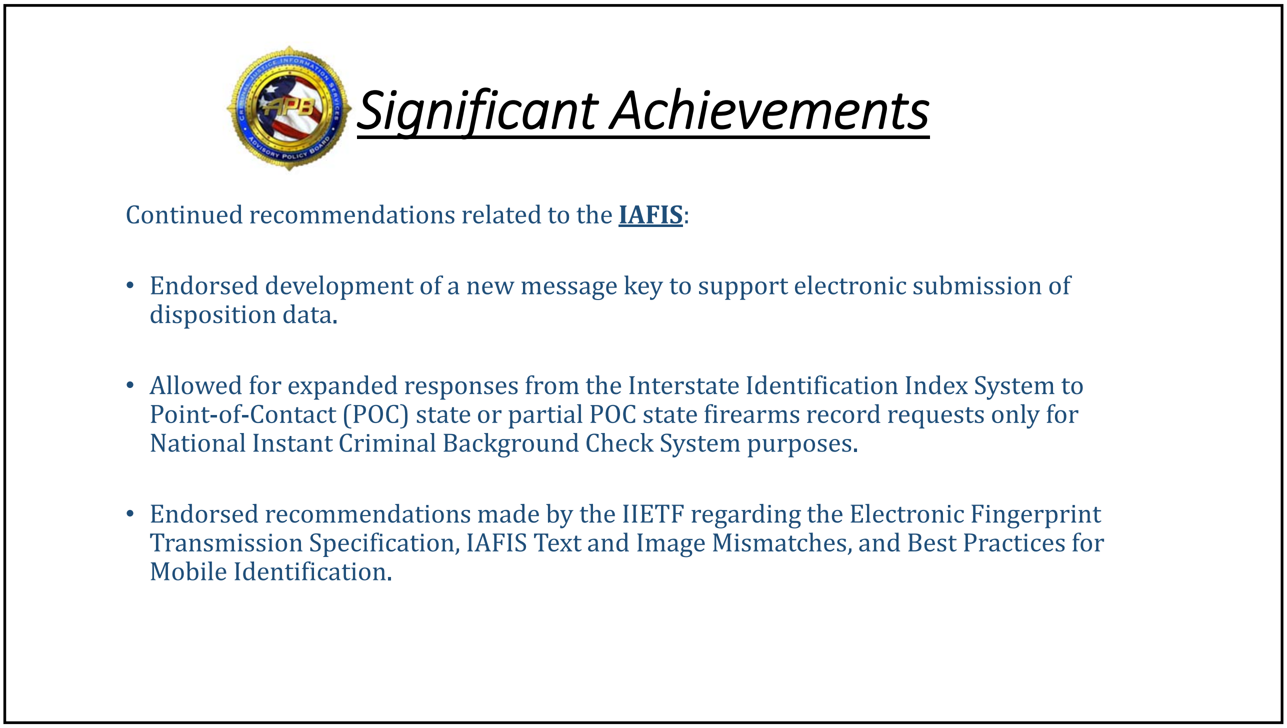
Recommended changes to the **Uniform Crime Reporting (UCR)** Program to include:

- Cargo Theft Collection
- Additional of Multiple Bias Motivations per Offense Type
- Revision of Law Enforcement Officers Killed and Assaulted forms
- Elimination of the Arrest Category of "Runaways"

Significant Achievements

Endorsed the following recommendations related to the **IAFIS** as follows:

- Nine data protection strategies in regard to IDENT/IAFIS Interoperability--Strategies for Data Security.
- Proposal to create a test environment for IAFIS, under the review of the IAFIS Interface Evaluation Task Force (IIETF).
- Changes implemented to IAFIS responses to indicate fraudulent identity for cases when exact match for name, date of birth, and social security number, but fingerprints do not match.
- Structure of the Rap Back service.
- Return of Information as it related to the Repository for Individuals of Special Concern.



Significant Achievements

Continued recommendations related to the **IAFIS**:

- Endorsed development of a new message key to support electronic submission of disposition data.
- Allowed for expanded responses from the Interstate Identification Index System to Point-of-Contact (POC) state or partial POC state firearms record requests only for National Instant Criminal Background Check System purposes.
- Endorsed recommendations made by the IIETF regarding the Electronic Fingerprint Transmission Specification, IAFIS Text and Image Mismatches, and Best Practices for Mobile Identification.

Significant Achievements

Mr. Steven Cumoletti
APB Chair
December 2008 – December 2012

359 Recommendations

Mr. Roy Weise, DFO, December 2008 - December 2010
Mr. Scott Trent, DFO, June 2011 – December 2012

Significant Achievements

Made recommendations related to the **National Crime Information Center (NCIC)** to include the following:

- Changes to the Article, Persons, and Gun files.
- Improvements to enhance the National Sex Offender Registry, which included a revision of audit and validation requirements.
- Endorsed the creation of the NICS Denied Persons and Violent Person File.
- Incorporated the Social Security Administration's Death Master File with NCIC Persons Files to help determine fraudulent use.
- Endorsed the sharing of missing and unidentified person record data sets with the National Missing and Unidentified Persons System.
- Changes to increase record completeness.
- Endorsed the Warrant Task Force recommendations regarding which fields should be assessed and scored as incomplete errors during NCIC audits.

Significant Achievements

Made recommendations to the ***CJIS Security Policy*** regarding:

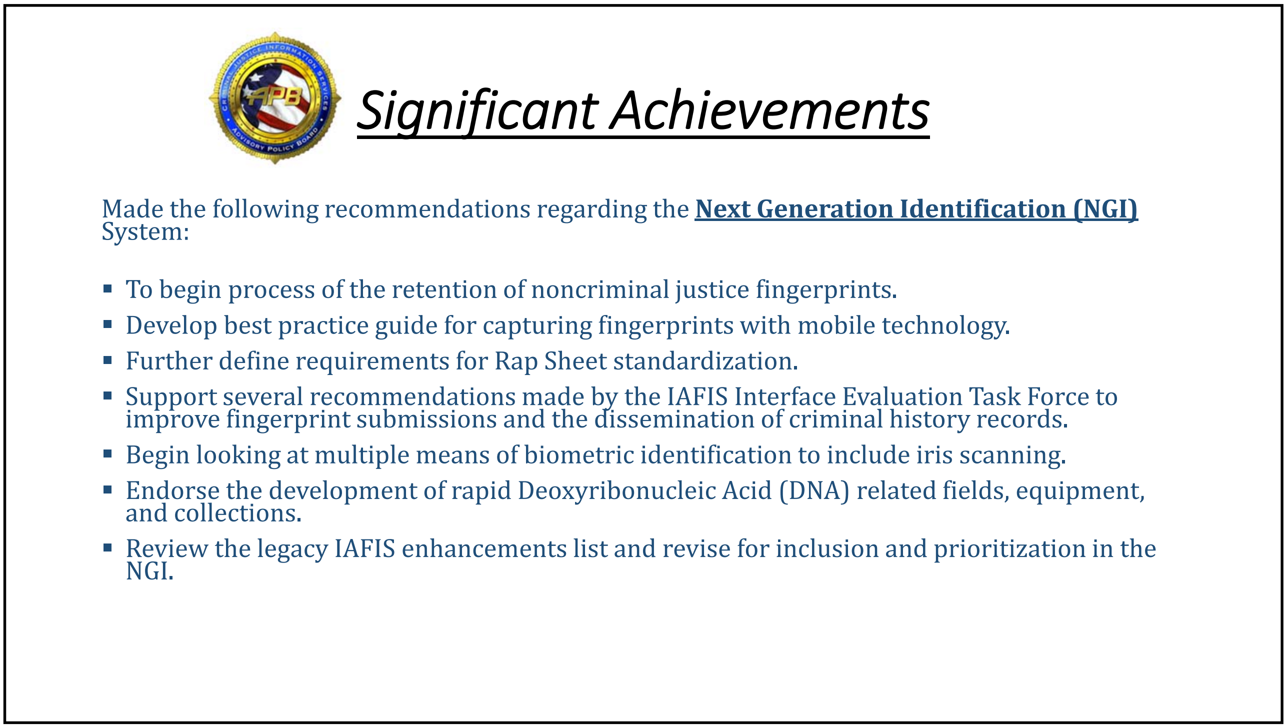
- CJIS Systems Officers
- Training Requirements
- Definition and Requirements for Local Agency Security Officers
- Information Flow Security Controls
- Login Attempts and Session Locks
- Voice over Internet Protocol
- Mobile Device Management
- Incorporation of the noncriminal justice agency community.

Reviewed and endorsed the extensive 2-year revision of the *CJIS Security Policy.*

Significant Achievements

Made the following recommendations regarding the **Uniform Crime Reporting (UCR)** Program:

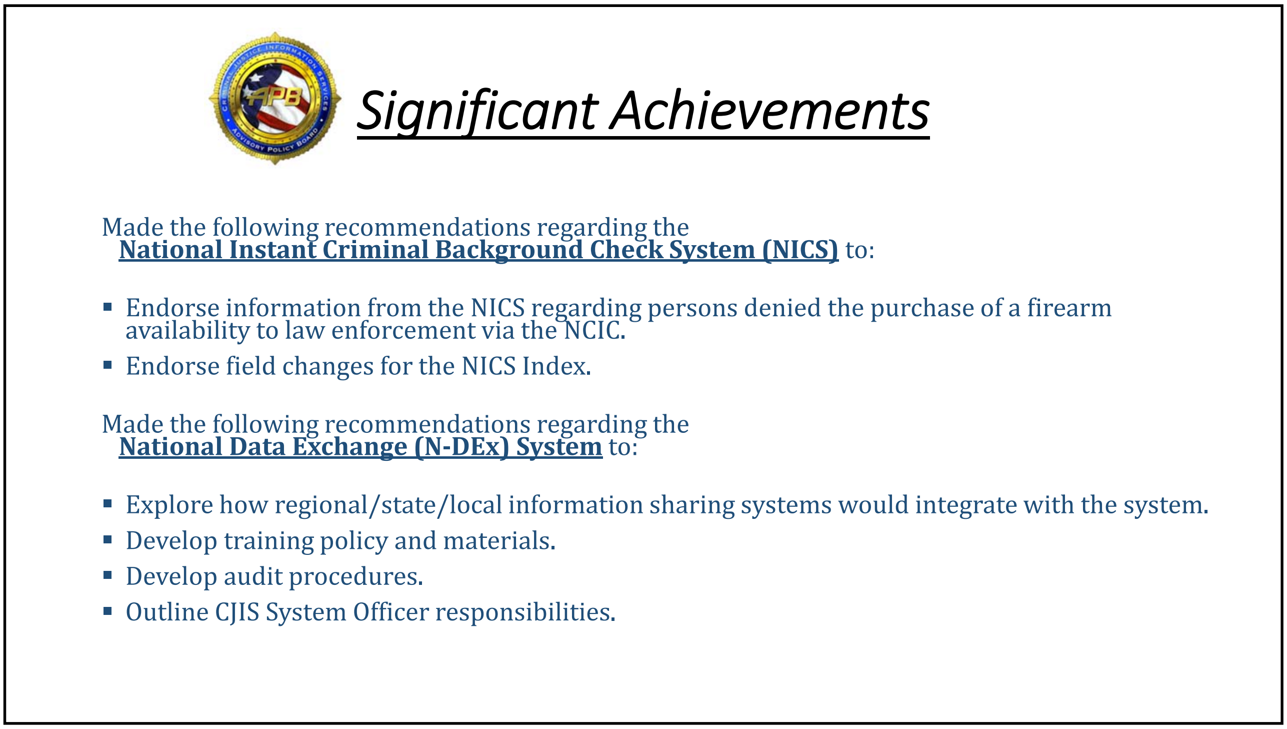
- To add twenty additional location data values and twenty-seven new property descriptions to the National Incident-Based Reporting System.
- To endorse submission guidelines for cargo theft data collection.
- To support Suicide by Cop data collection.
- Provide for clarification and better descriptions for circumstances surrounding arrests.
- To endorse the policies and forms related to and begin collecting human trafficking data.
- To revise race and ethnicity categories to align with the Office of Management and Budget standards.
- To support for the UCR Redevelopment Project.
- To make changes to prostitution data collection.
- To make changes to hate crime data collection to include new/revised definitions and new/revised location and categories.
- To support changes to the rape definition within UCR Summary reporting.
- To endorse move to the electronic submission of data only.



Significant Achievements

Made the following recommendations regarding the **Next Generation Identification (NGI)** System:

- To begin process of the retention of noncriminal justice fingerprints.
- Develop best practice guide for capturing fingerprints with mobile technology.
- Further define requirements for Rap Sheet standardization.
- Support several recommendations made by the IAFIS Interface Evaluation Task Force to improve fingerprint submissions and the dissemination of criminal history records.
- Begin looking at multiple means of biometric identification to include iris scanning.
- Endorse the development of rapid Deoxyribonucleic Acid (DNA) related fields, equipment, and collections.
- Review the legacy IAFIS enhancements list and revise for inclusion and prioritization in the NGI.



Significant Achievements

Made the following recommendations regarding the **National Instant Criminal Background Check System (NICS)** to:

- Endorse information from the NICS regarding persons denied the purchase of a firearm availability to law enforcement via the NCIC.
- Endorse field changes for the NICS Index.

Made the following recommendations regarding the **National Data Exchange (N-DEx) System** to:

- Explore how regional/state/local information sharing systems would integrate with the system.
- Develop training policy and materials.
- Develop audit procedures.
- Outline CJIS System Officer responsibilities.

Intentionally Left Blank

Significant Achievements

Captain Tom Turner
APB Chair
December 2012 – December 2016

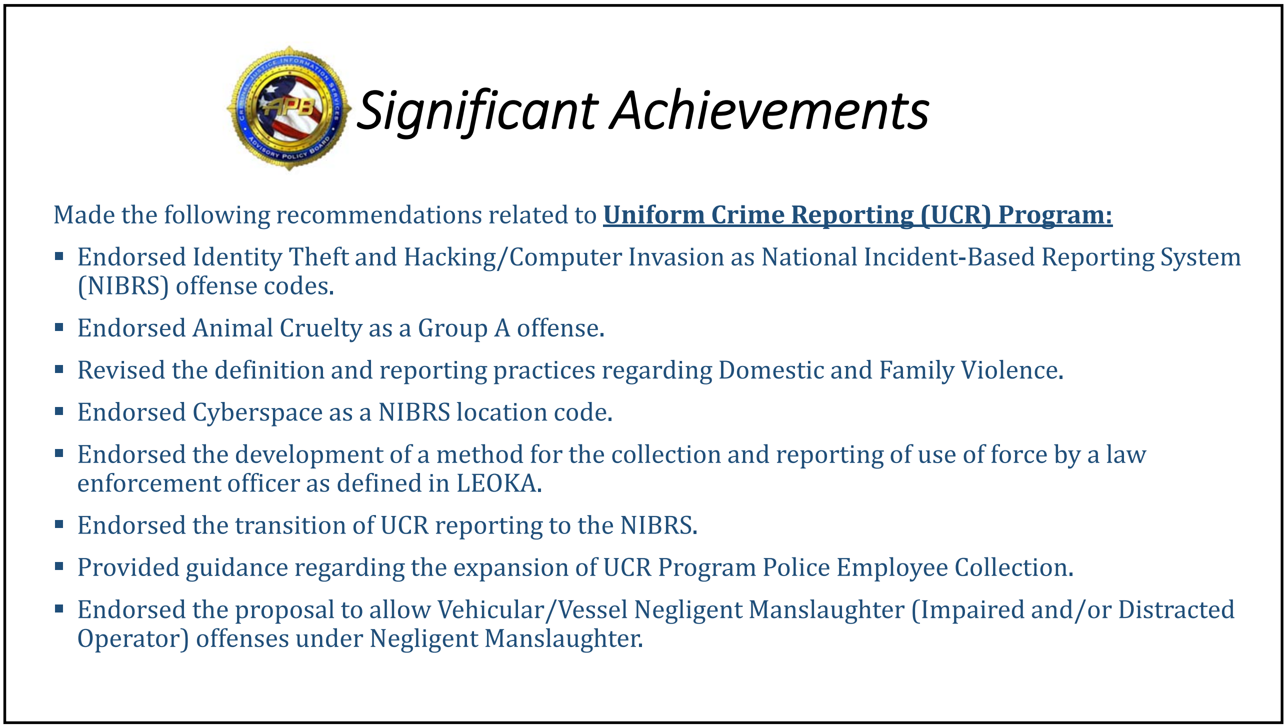
224 Recommendations

Mr. Scott Trent, DFO

Significant Achievements

Made the following recommendations related to **Next Generation Identification (NGI)**:

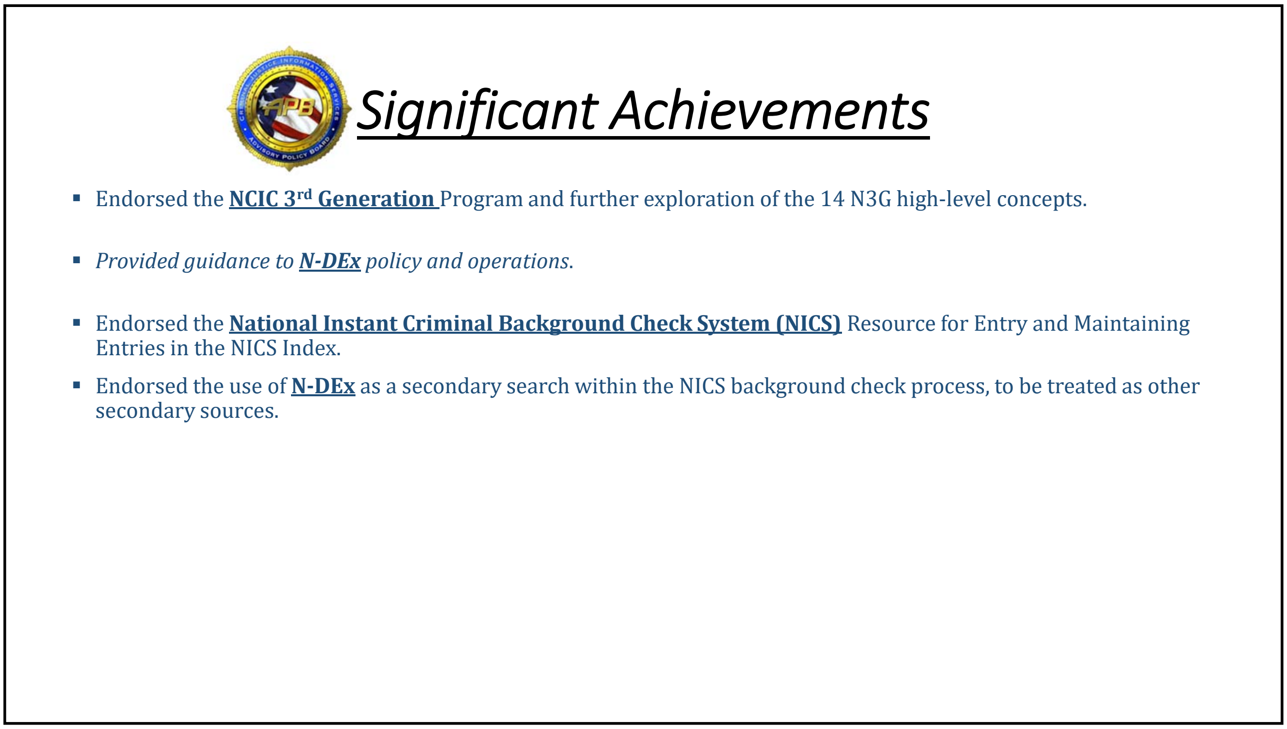
- Endorsed the NGI changes to the Electronic Biometric Transmission Specification.
- Endorsed the *NGI Rap Back Service Criminal Justice Policy and Implementation Guideline*.
- Endorsed the *Interstate Photo System Policy and Implementation Guide*.
- Endorsed standards for the Interstate Identification Index Identification for Firearms Sales.
- Endorsed the Automated Disposition and Processing Technology concept.
- Endorsed the *Disposition Task Force: Best Practices Guide*.



Significant Achievements

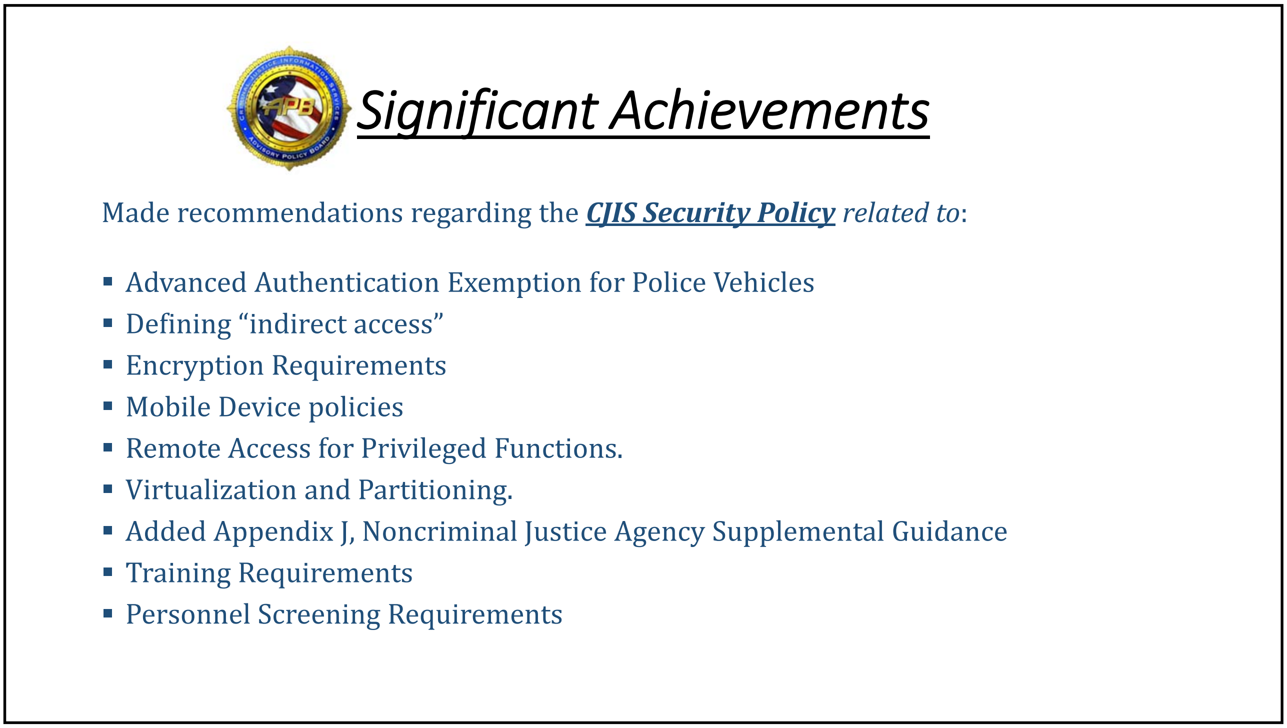
Made the following recommendations related to **Uniform Crime Reporting (UCR) Program:**

- Endorsed Identity Theft and Hacking/Computer Invasion as National Incident-Based Reporting System (NIBRS) offense codes.
- Endorsed Animal Cruelty as a Group A offense.
- Revised the definition and reporting practices regarding Domestic and Family Violence.
- Endorsed Cyberspace as a NIBRS location code.
- Endorsed the development of a method for the collection and reporting of use of force by a law enforcement officer as defined in LEOKA.
- Endorsed the transition of UCR reporting to the NIBRS.
- Provided guidance regarding the expansion of UCR Program Police Employee Collection.
- Endorsed the proposal to allow Vehicular/Vessel Negligent Manslaughter (Impaired and/or Distracted Operator) offenses under Negligent Manslaughter.



Significant Achievements

- Endorsed the **NCIC 3rd Generation** Program and further exploration of the 14 N3G high-level concepts.
- *Provided guidance to **N-DEx** policy and operations.*
- Endorsed the **National Instant Criminal Background Check System (NICS)** Resource for Entry and Maintaining Entries in the NICS Index.
- Endorsed the use of **N-DEx** as a secondary search within the NICS background check process, to be treated as other secondary sources.



Significant Achievements

Made recommendations regarding the ***CJIS Security Policy*** *related to*:

- Advanced Authentication Exemption for Police Vehicles
- Defining “indirect access”
- Encryption Requirements
- Mobile Device policies
- Remote Access for Privileged Functions.
- Virtualization and Partitioning.
- Added Appendix J, Noncriminal Justice Agency Supplemental Guidance
- Training Requirements
- Personnel Screening Requirements

Intentionally Left Blank

Significant Achievements

Mr. John "Jack" Donohue
APB Chair
December 2016 – December 2018

94 Recommendations

Mr. Mike McIntyre, DFO, June 2017
Mr. Scott Trent, DFO, December 2016, December 2017
Mr. Nick Megna, DFO, June 2018 - present

Significant Achievements

Made recommendations regarding the **National Data Exchange (N-DEx)** System to:

- Establish *N-DEx Policy* to allow for the system to be used as a National Instant Criminal Background Check System secondary resource.
- Endorse standardized audit requirements as recommended by the N-DEx Audit Task Force.

Made recommendations regarding the **Uniform Crime Reporting (UCR)** Program to:

- Add UCR Offenses for Federal Crime Reporting
- Endorse proposals to enhance crime-reporting timeliness in the area of frequency of submission and frequency of release.

Significant Achievements

Made recommendations regarding the **National Crime Information Center (NCIC)** to:

- Endorse multiple concepts and requirements for the NCIC 3rd Generation (N3G) related to Enhanced Multimedia, Access Data Repositories, Enhanced Data Searches, Name Search Algorithm, Enhanced Training Environment, Tailored Functionality, System Search, Improved Outbound Communications, Record Content, Enhanced Training Resources, Improved Data Management, Alternative Outbound Communications, and Flexible Data Format.
- Establish an Agile friendly APB process in support of N3G Development.

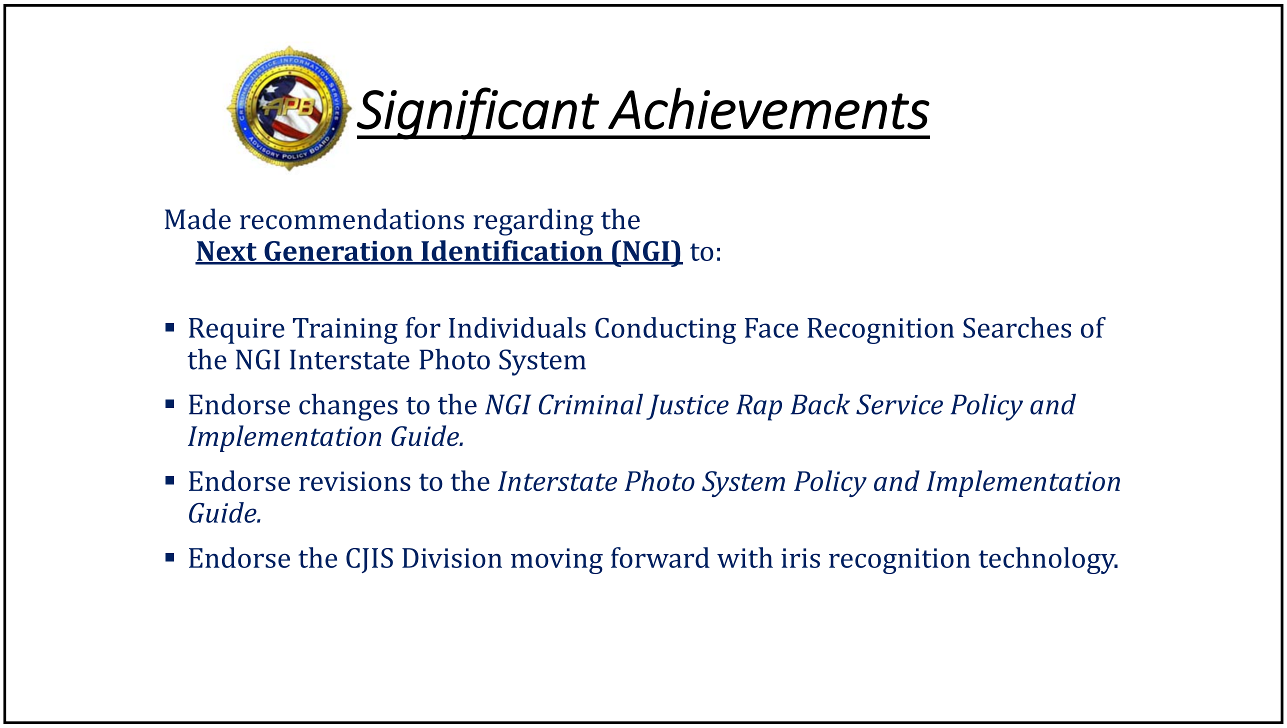
Significant Achievements

Made recommendations regarding the ***CJIS Security Policy*** related to:

- Collection and Use of Metadata by Cloud Service Providers.
- Criminal Justice Information stored in Offshore Cloud Computing Facilities.
- Intrusion Detection and Prevention Systems.
- New Standards for Passwords.
- Mobile Device Management.
- Local Agency Security Officer training requirements.

Made recommendations regarding the **National Instant Criminal Background System (NICS)** to:

- Evaluate Information Required with the Submission of a Record to the NICS Indices.



Significant Achievements

Made recommendations regarding the
Next Generation Identification (NGI) to:

- Require Training for Individuals Conducting Face Recognition Searches of the NGI Interstate Photo System
- Endorse changes to the *NGI Criminal Justice Rap Back Service Policy and Implementation Guide.*
- Endorse revisions to the *Interstate Photo System Policy and Implementation Guide.*
- Endorse the CJIS Division moving forward with iris recognition technology.

Intentionally Left Blank

Dave Loesch's Comments to CJIS APB December 2019

I was really looking forward to being here with all of you to celebrate this significant mile stone of the CJIS Advisory Process unfortunately a recent medical issue has changed all that.

I did not want to miss the opportunity to Thank all of you for what you have done and continue to do on a daily basis, individually and collectively, to keep our Citizens and Country Safe. You are the Unsung Heroes that most of our Citizens never hear about in the News. There is a tremendous amount of work that goes on at CJIS, The APB Working Groups, The Ad-Hoc Subcommittees, and various Task Forces leading up to these APB Meetings. The success of this process is the result of a lot of hard work behind the scenes and incredible coordination and cooperation of many individuals and organizations.

I want to recognize some of these.

> The CJIS Training and Advisory Process Unit (CATP). Many of us remember this as The Advisory Groups Management Unit (AGMU). This Unit is the focal point for this process in CJIS. They are responsible for the detailed planning, staffing, administration, and coordination of the CJIS Advisory Process. These responsibilities include developing meeting agendas through coordination with other CJIS Division Offices, other FBI entities, other Government, and CJIS customers. They do an exceptional Job. Thank You All.
>
> The Multi Media Production Group and Logistical Support Unit. These entities are responsible for transporting and setting up all the necessary equipment for the meetings. They also do an exceptional job. I know Tommy LeHosit has been doing this for about 20 years. Thank You Tommy and Crew.
>
> To ALL the CJIS Employees that may be watching this Meeting, I want you to know how much I admire and respect what each of you do every day. It does not matter what job you are in. You all play an important role in the CJIS Mission of Serving the entire Criminal Justice, National Security, and Intelligence Communities in protecting our citizens and our country. NEVER FORGET THAT.
>
> The Current Chairman and Vice Chairs, Former APB Chairs, Vice Chairs, and Members involved on the Board, The Working Groups, Subcommittees, and Task Forces.
>
> The Royal Canadian Mounted Police- RCMP. Longtime partner and friend of the FBI and Board.
>
> Compact Council Members
>
> SEARCH
>
> NLETS

> All our contractors and vendors that assist us in developing solutions for numerous tasks, designing, building and maintaining our systems, and assisting us in accomplishing our mission.

I realize that all of you have full time jobs and many other responsibilities yet continue to offer your time and talents because you want to contribute to improving our Criminal Justice Community and keeping our Law Enforcement Officers, vulnerable populations, and citizens safe.

In my time at CJIS, I attended numerous Working Group, Subcommittee, and APB meetings. I found each representative brought their agency perspective to the table so together we could find a solution that was best for the country. This process made sure that EVERY VOICE WAS HEARD. There was much debate but it was always civil, respectful, and in the end we always did what was right and best for our country. All were interested in improving our information systems and getting ACCURATE, COMPLETE, AND TIMELY INFORMATION in the hands of those who needed it to do their jobs.

I found it helpful that many of the individuals involved in the APB Process were also involved with the Compact Council and SEARCH. This provided a healthy perspective on many issues and policy discussions and promoted collaboration, cooperation, support, and trust. I counted a great deal on so many of you to educate me on the state and local issues and help me prepare for testimony before congress.

I want to recognize Retired Assistant Director Chuck Archer who was the first CJIS Assistant Director to actually move to West Virginia. Chuck played a key role in the movement of the Division to West Virginia and made the Advisory Process and Shared Management a Priority of the Division. I am sure Joe Bonino, the First Chair of the New APB, can provide more history about Chuck's early role.

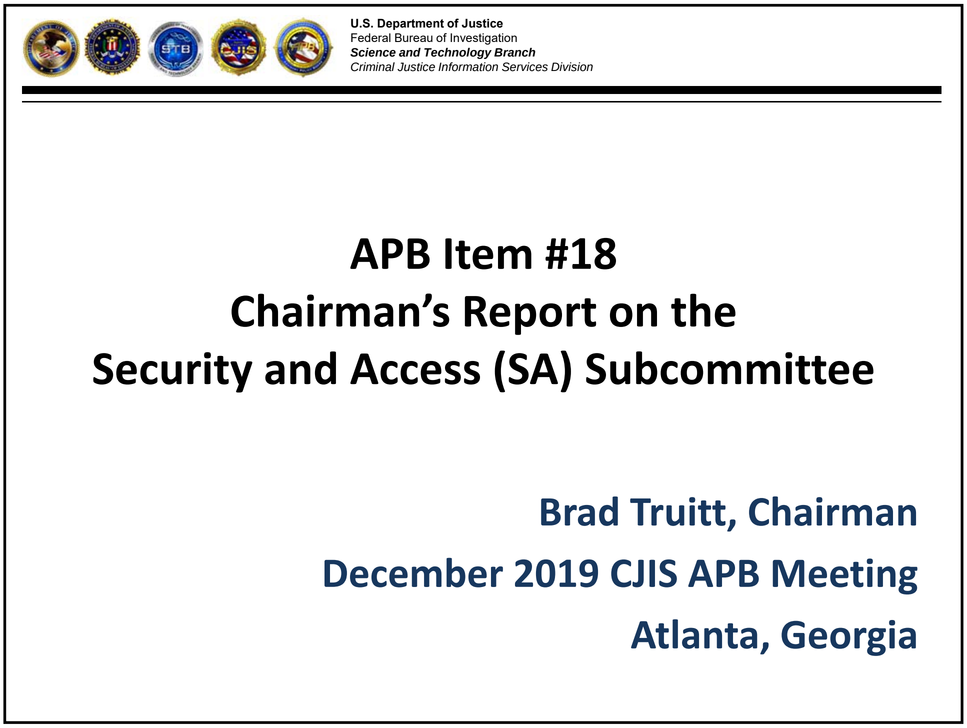
We also had incredible support from Attorney General Janet Reno, Director Louis Freeh, and Deputy Directors Weldon Kennedy and William Esposito. I recall several meetings with the Attorney General where she asked me "What does Joe Bonino think about that?"

I am Honored and Most Thankful to have worked with such a dedicated and talented group of Professionals. You have all made my time in CJIS and participating in this Advisory Process the Highlight of my career in the FBI. THANK YOU.

Wishing You All Continued Success and a Safe and Happy Holiday Season.

DAVE LOESCH

FRIEND OF CJIS AND THE APB



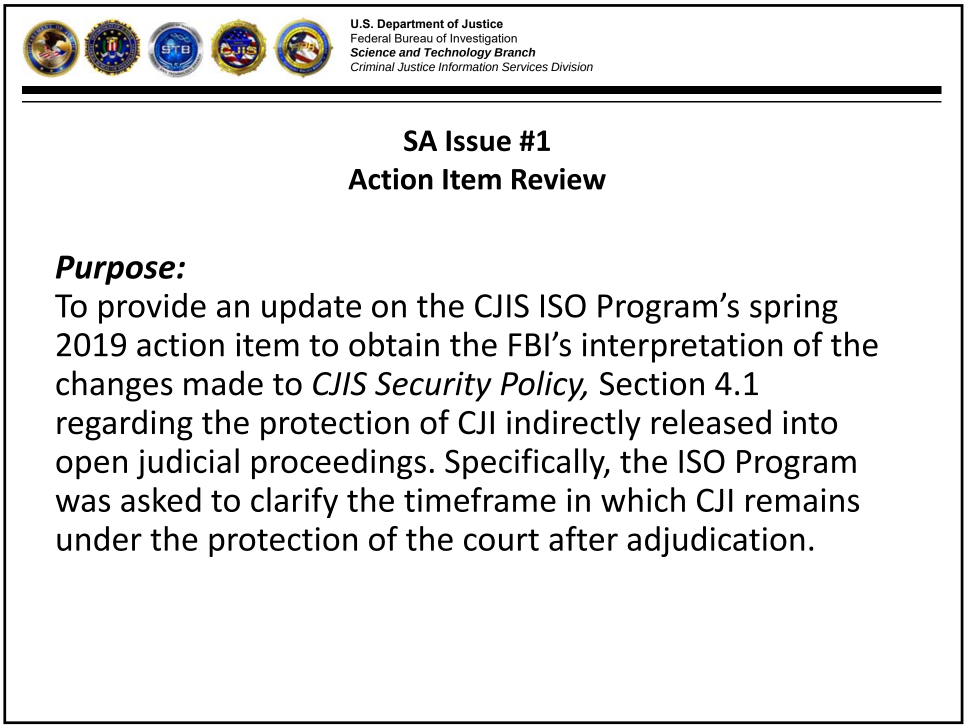
U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB Item #18
Chairman's Report on the
Security and Access (SA) Subcommittee

Brad Truitt, Chairman

December 2019 CJIS APB Meeting

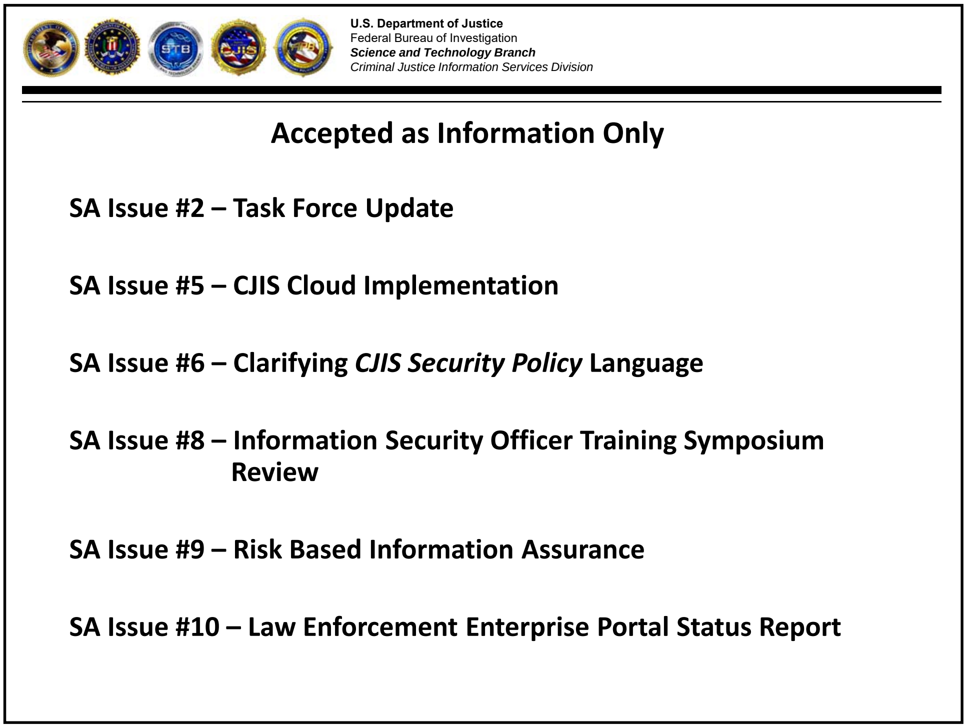
Atlanta, Georgia



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #1
Action Item Review

Purpose:
To provide an update on the CJIS ISO Program's spring 2019 action item to obtain the FBI's interpretation of the changes made to *CJIS Security Policy,* Section 4.1 regarding the protection of CJI indirectly released into open judicial proceedings. Specifically, the ISO Program was asked to clarify the timeframe in which CJI remains under the protection of the court after adjudication.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

Accepted as Information Only

SA Issue #2 – Task Force Update

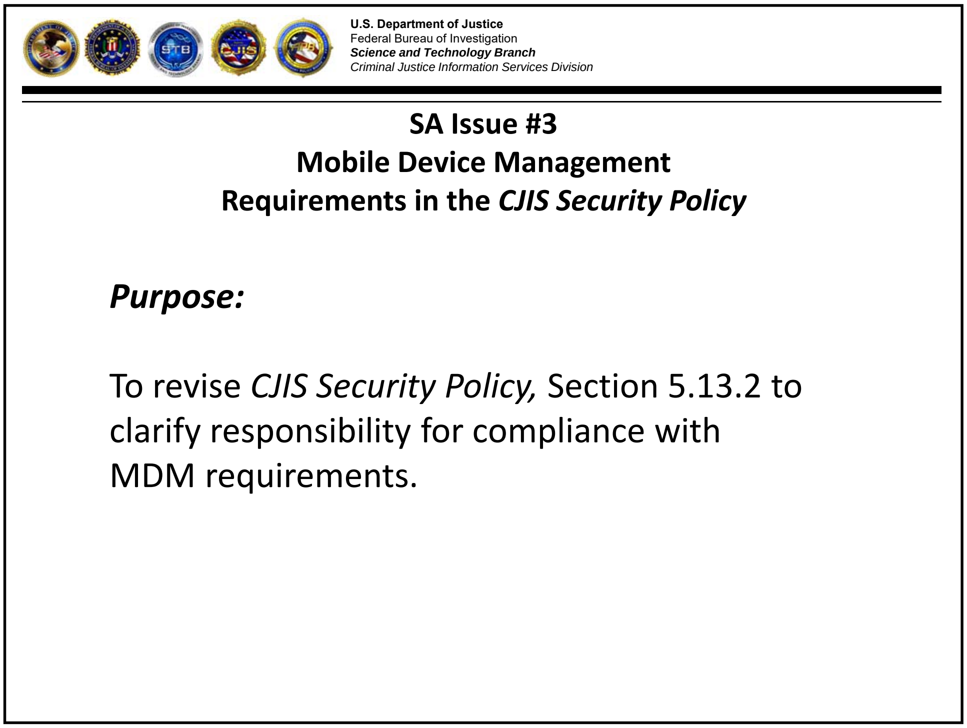
SA Issue #5 – CJIS Cloud Implementation

SA Issue #6 – Clarifying *CJIS Security Policy* Language

SA Issue #8 – Information Security Officer Training Symposium Review

SA Issue #9 – Risk Based Information Assurance

SA Issue #10 – Law Enforcement Enterprise Portal Status Report

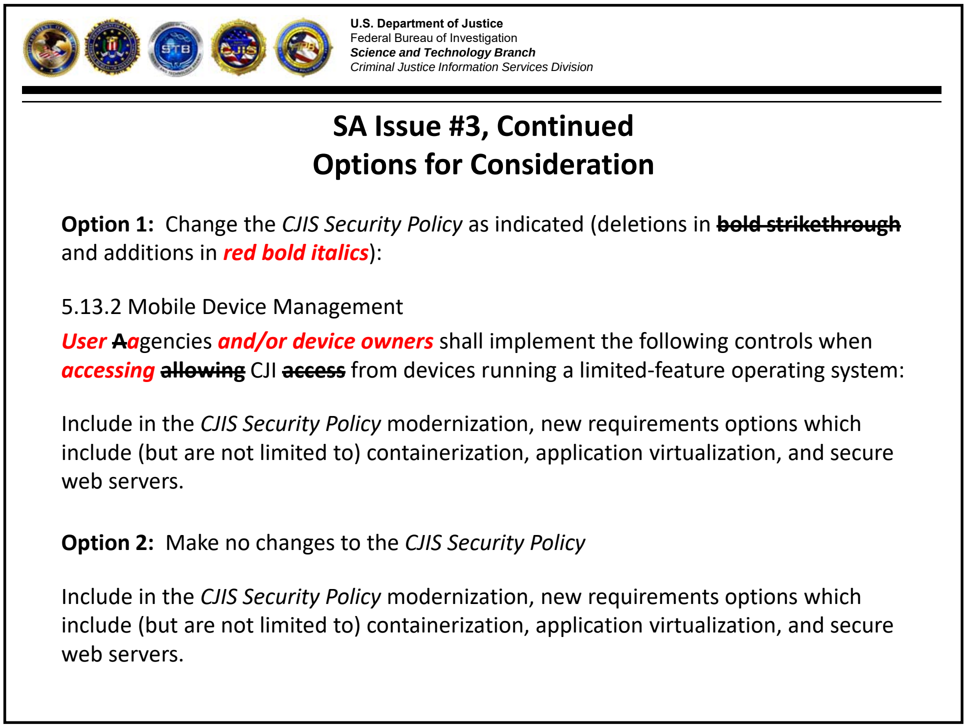


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #3
Mobile Device Management
Requirements in the *CJIS Security Policy*

Purpose:

To revise *CJIS Security Policy,* Section 5.13.2 to clarify responsibility for compliance with MDM requirements.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #3, Continued
Options for Consideration

Option 1: Change the *CJIS Security Policy* as indicated (deletions in **~~bold strikethrough~~** and additions in ***red bold italics***):

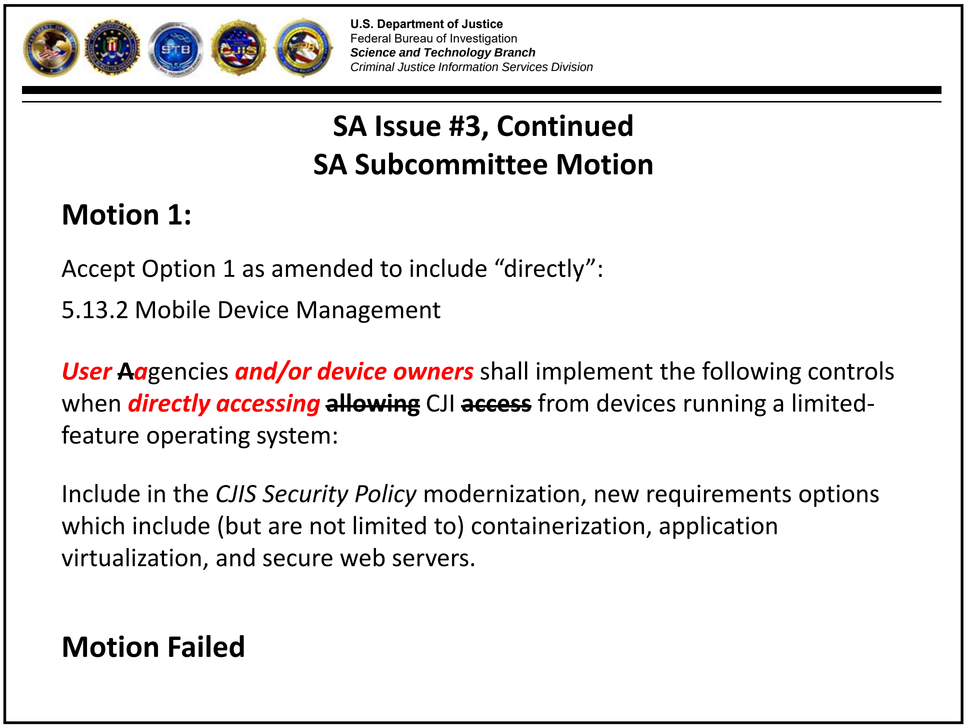
5.13.2 Mobile Device Management

User **~~A~~*a***gencies ***and/or device owners*** shall implement the following controls when ***accessing*** **~~allowing~~** CJI **~~access~~** from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Option 2: Make no changes to the *CJIS Security Policy*

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #3, Continued
SA Subcommittee Motion

Motion 1:

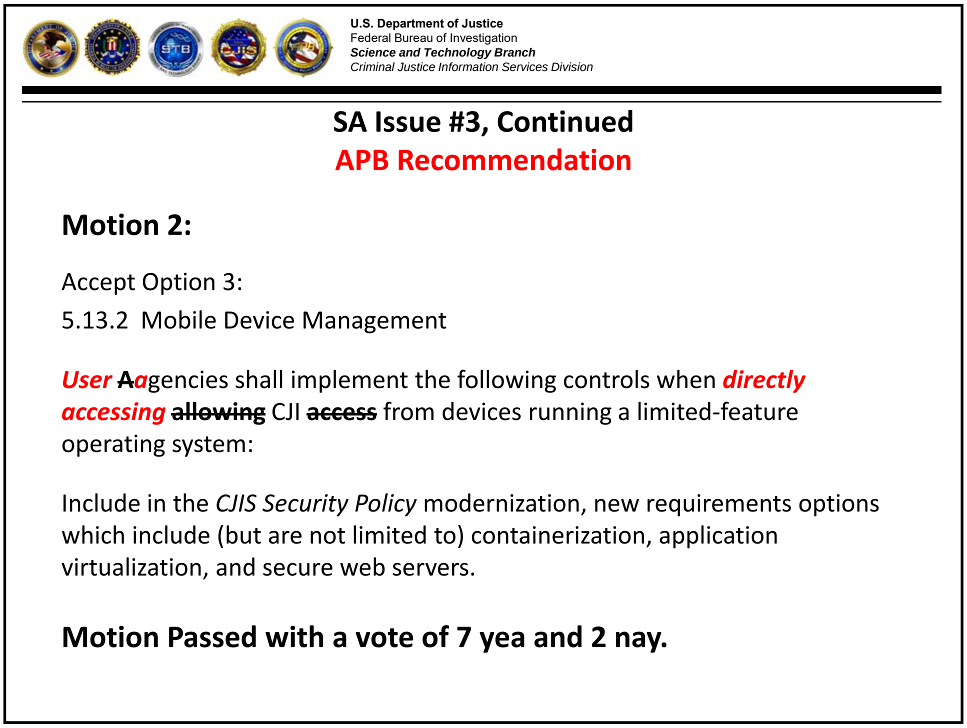
Accept Option 1 as amended to include "directly":

5.13.2 Mobile Device Management

User **~~A~~*a***gencies ***and/or device owners*** shall implement the following controls when ***directly accessing*** **~~allowing~~** CJI **~~access~~** from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Motion Failed



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #3, Continued
APB Recommendation

Motion 2:

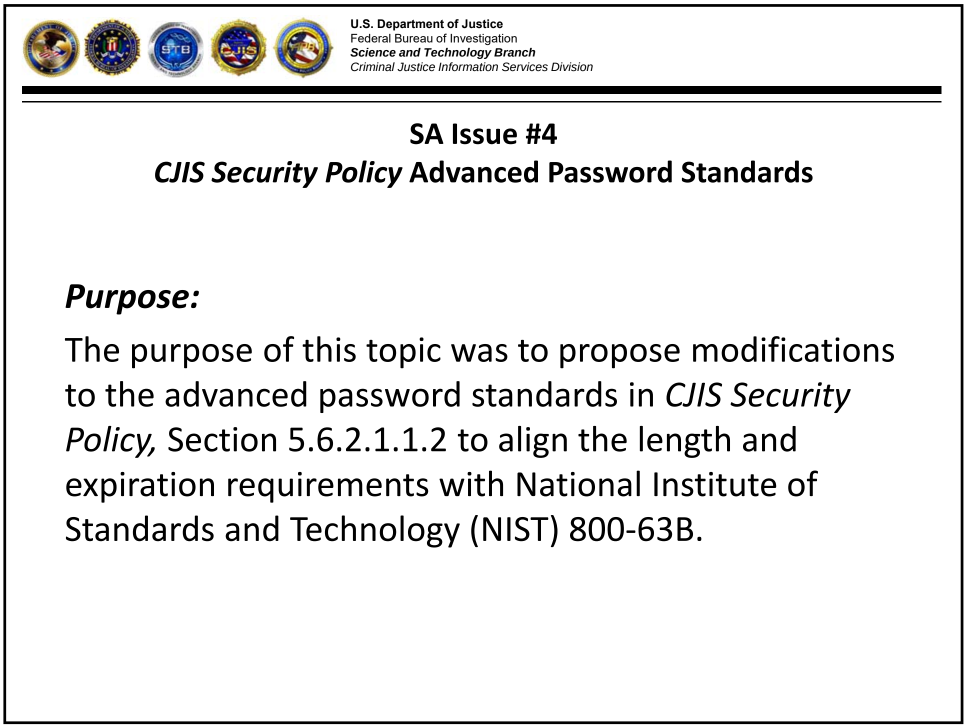
Accept Option 3:

5.13.2 Mobile Device Management

User ~~A~~*a*gencies shall implement the following controls when ***directly accessing*** ~~allowing~~ CJI ~~access~~ from devices running a limited-feature operating system:

Include in the *CJIS Security Policy* modernization, new requirements options which include (but are not limited to) containerization, application virtualization, and secure web servers.

Motion Passed with a vote of 7 yea and 2 nay.

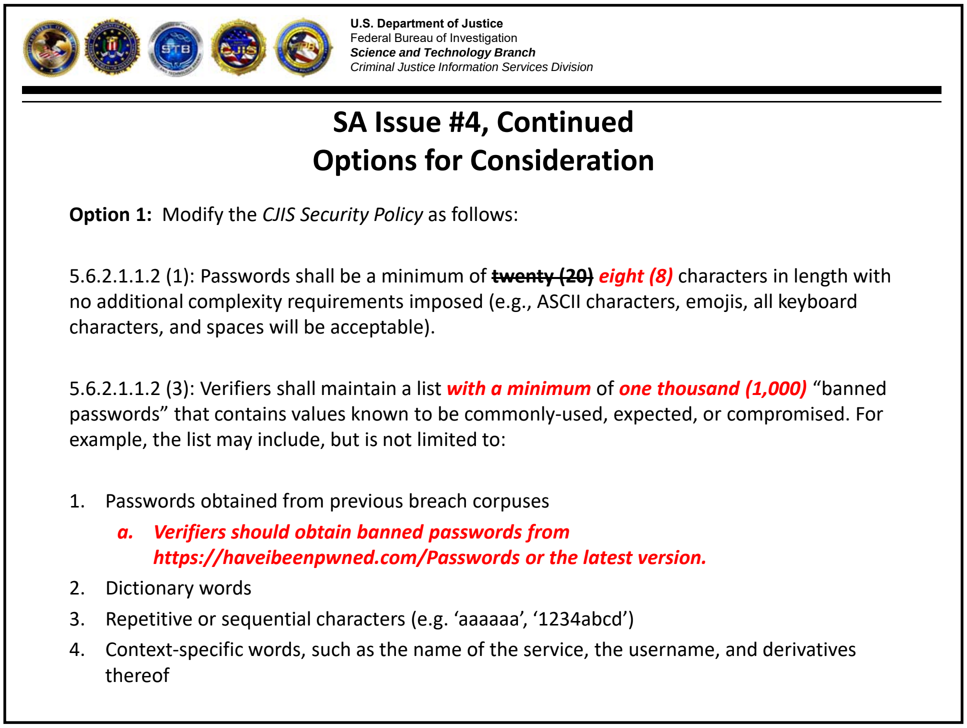


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #4
CJIS Security Policy Advanced Password Standards

Purpose:

The purpose of this topic was to propose modifications to the advanced password standards in *CJIS Security Policy,* Section 5.6.2.1.1.2 to align the length and expiration requirements with National Institute of Standards and Technology (NIST) 800-63B.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

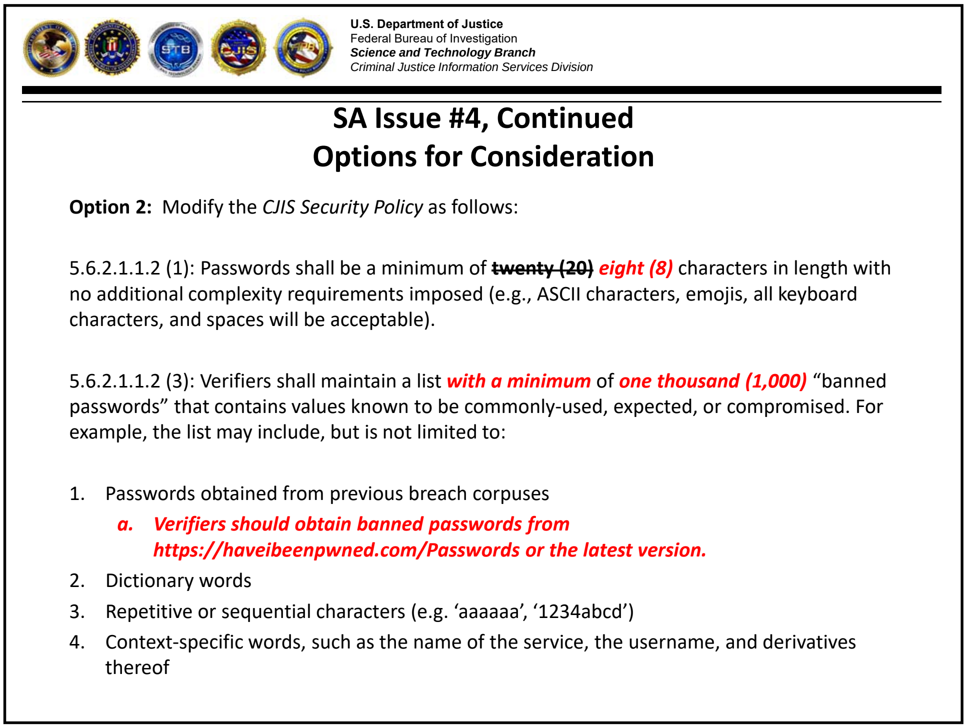
SA Issue #4, Continued
Options for Consideration

Option 1: Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~twenty (20)~~ *eight (8)* characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** “banned passwords” that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses
   a. ***Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.***
2. Dictionary words
3. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
4. Context-specific words, such as the name of the service, the username, and derivatives thereof



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #4, Continued
Options for Consideration

Option 2: Modify the *CJIS Security Policy* as follows:

5.6.2.1.1.2 (1): Passwords shall be a minimum of ~~twenty (20)~~ *eight (8)* characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

5.6.2.1.1.2 (3): Verifiers shall maintain a list ***with a minimum*** of ***one thousand (1,000)*** “banned passwords” that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

1. Passwords obtained from previous breach corpuses
   a. ***Verifiers should obtain banned passwords from https://haveibeenpwned.com/Passwords or the latest version.***
2. Dictionary words
3. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
4. Context-specific words, such as the name of the service, the username, and derivatives thereof

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #4, Continued
Options for Consideration

Option 2: Continued

5.6.2.1.1.2 (4): When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list. ***Agencies shall reconcile their directory service against the "banned password" list at least every 90 days. If a "banned password" is discovered, the Agency shall notify affected user to execute a password change***.

5.6.2.1.1.2 (7): Verifiers shall force a password change if there is evidence of authenticator compromise. ~~**or every 365 days from the last password change**~~

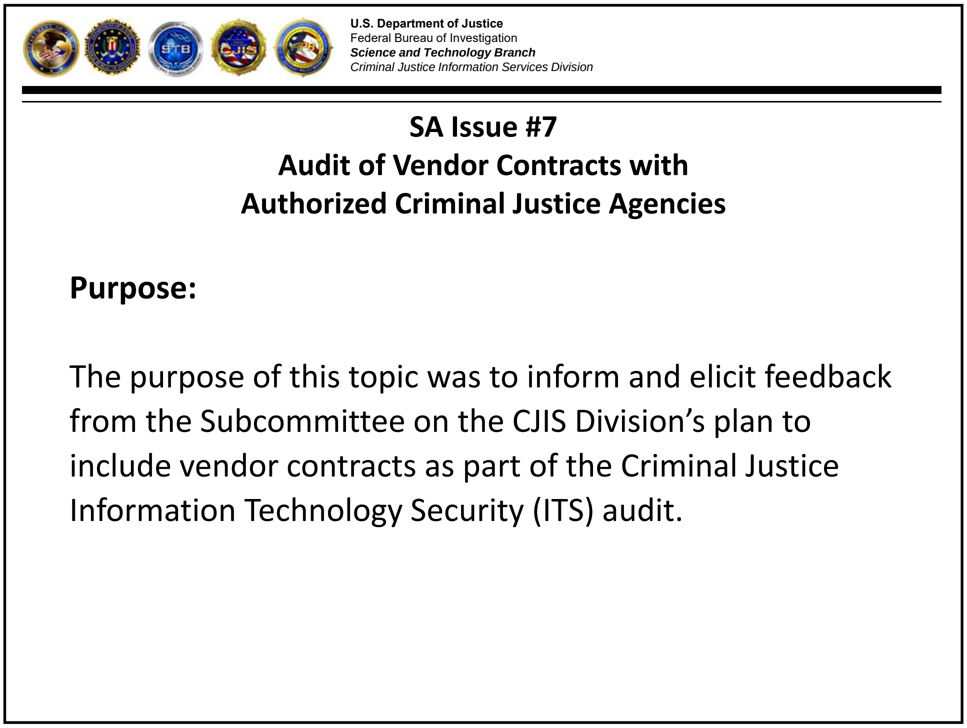
Option 3: Make no changes to the *CJIS Security Policy*

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #4, Continued
APB Recommendation

Accept Option 3:

Make no changes to the *CJIS Security Policy*

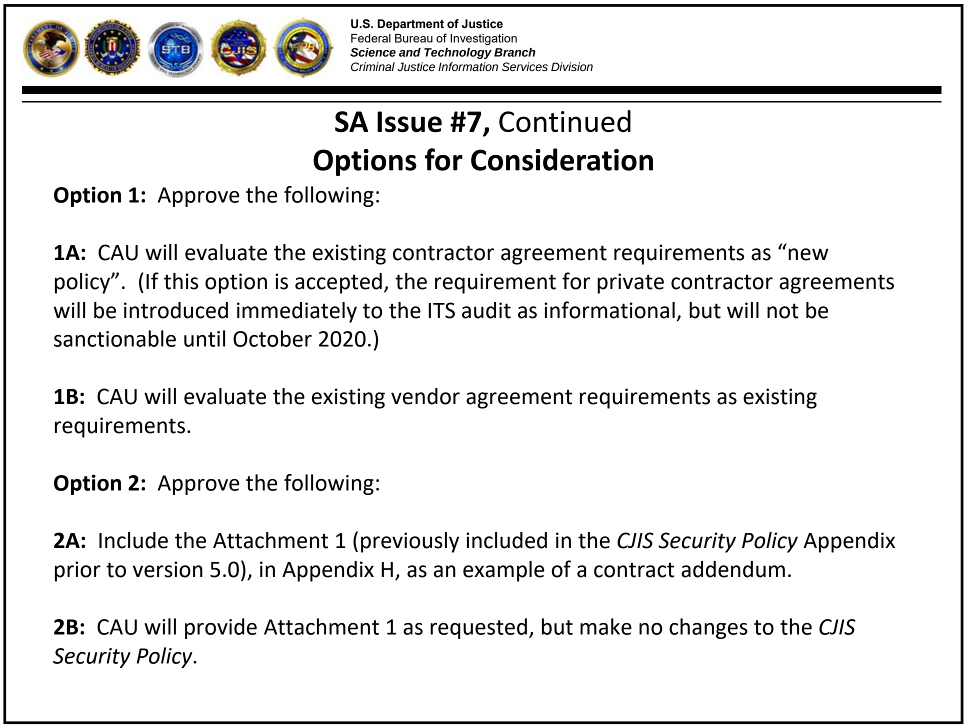


U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #7
Audit of Vendor Contracts with Authorized Criminal Justice Agencies

Purpose:

The purpose of this topic was to inform and elicit feedback from the Subcommittee on the CJIS Division's plan to include vendor contracts as part of the Criminal Justice Information Technology Security (ITS) audit.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #7, Continued
Options for Consideration

Option 1: Approve the following:

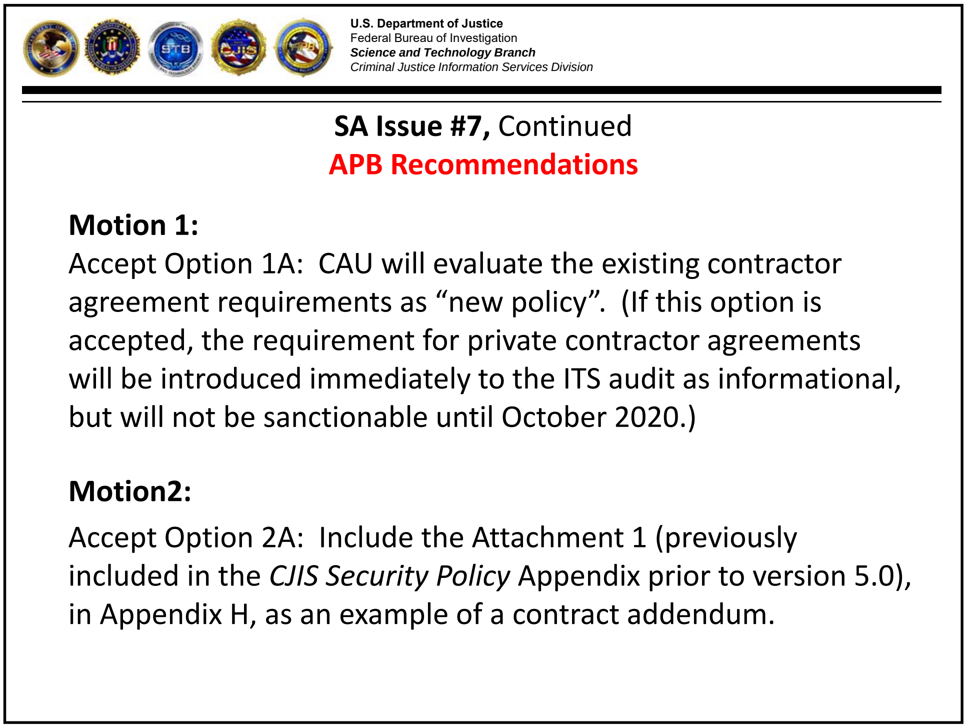
1A: CAU will evaluate the existing contractor agreement requirements as "new policy". (If this option is accepted, the requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)

1B: CAU will evaluate the existing vendor agreement requirements as existing requirements.

Option 2: Approve the following:

2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.

2B: CAU will provide Attachment 1 as requested, but make no changes to the *CJIS Security Policy*.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

SA Issue #7, Continued

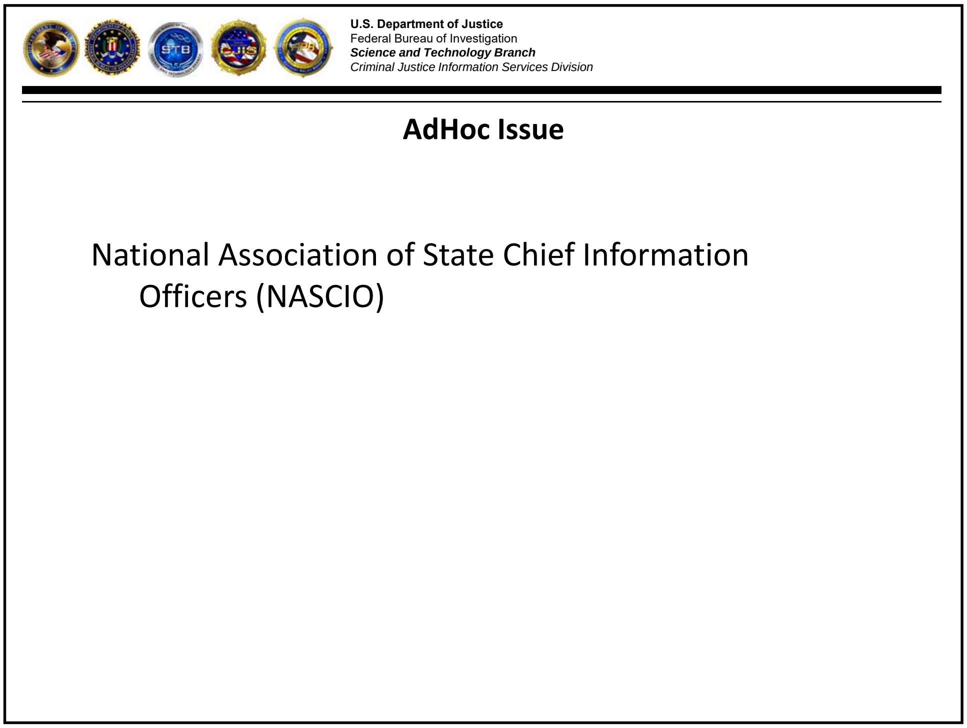
APB Recommendations

Motion 1:

Accept Option 1A: CAU will evaluate the existing contractor agreement requirements as “new policy”. (If this option is accepted, the requirement for private contractor agreements will be introduced immediately to the ITS audit as informational, but will not be sanctionable until October 2020.)

Motion2:

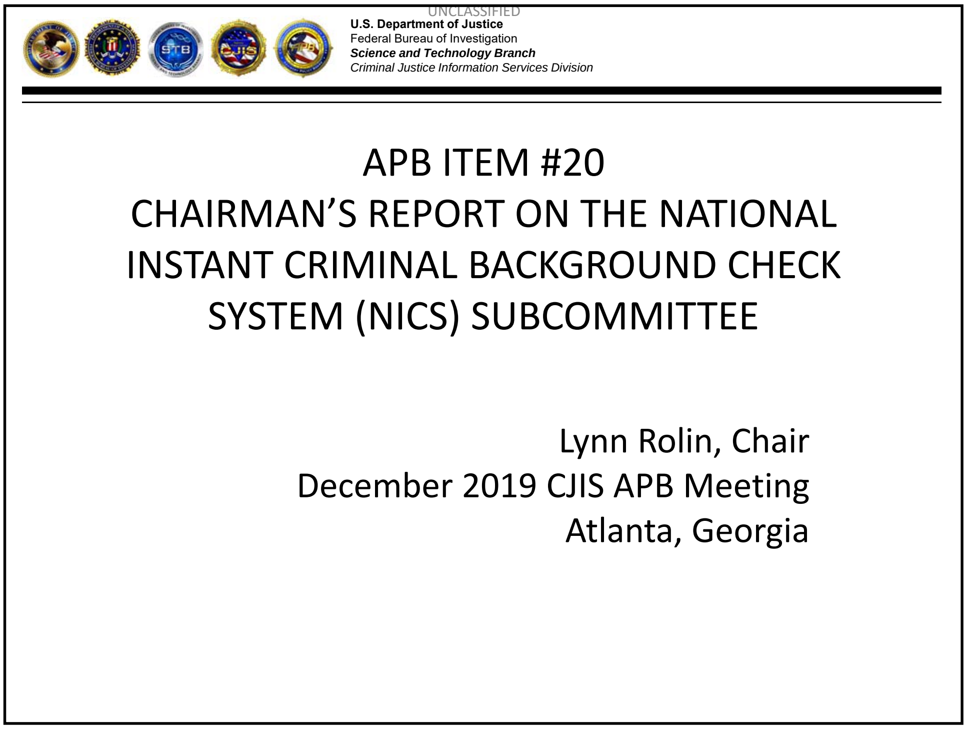
Accept Option 2A: Include the Attachment 1 (previously included in the *CJIS Security Policy* Appendix prior to version 5.0), in Appendix H, as an example of a contract addendum.



U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

AdHoc Issue

National Association of State Chief Information Officers (NASCIO)

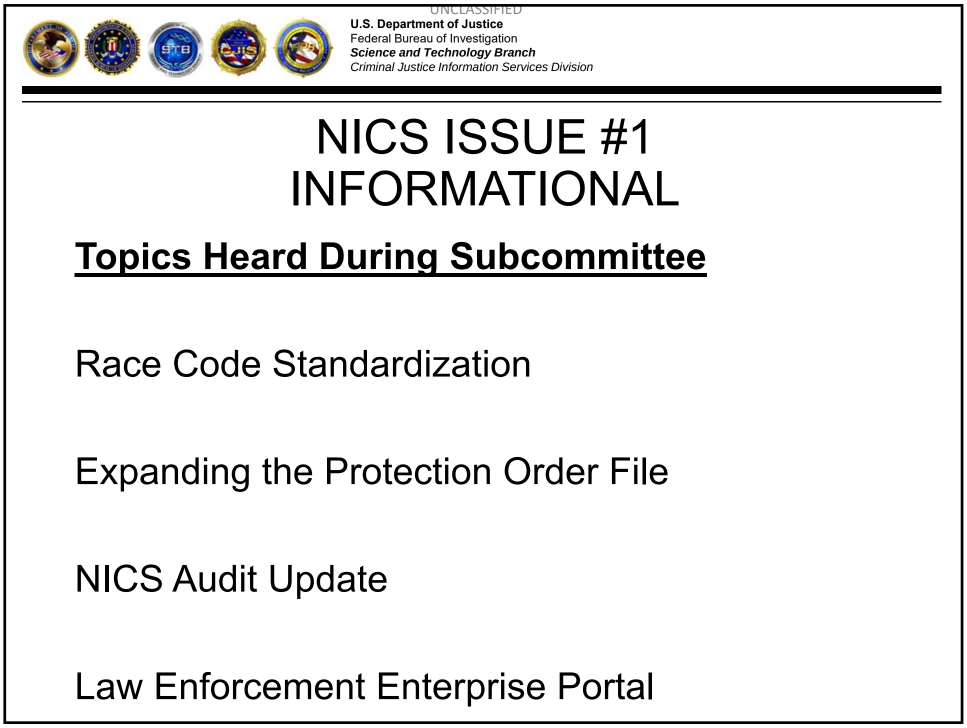


UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

APB ITEM #20 CHAIRMAN'S REPORT ON THE NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) SUBCOMMITTEE

Lynn Rolin, Chair
December 2019 CJIS APB Meeting
Atlanta, Georgia



UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

NICS ISSUE #1 INFORMATIONAL

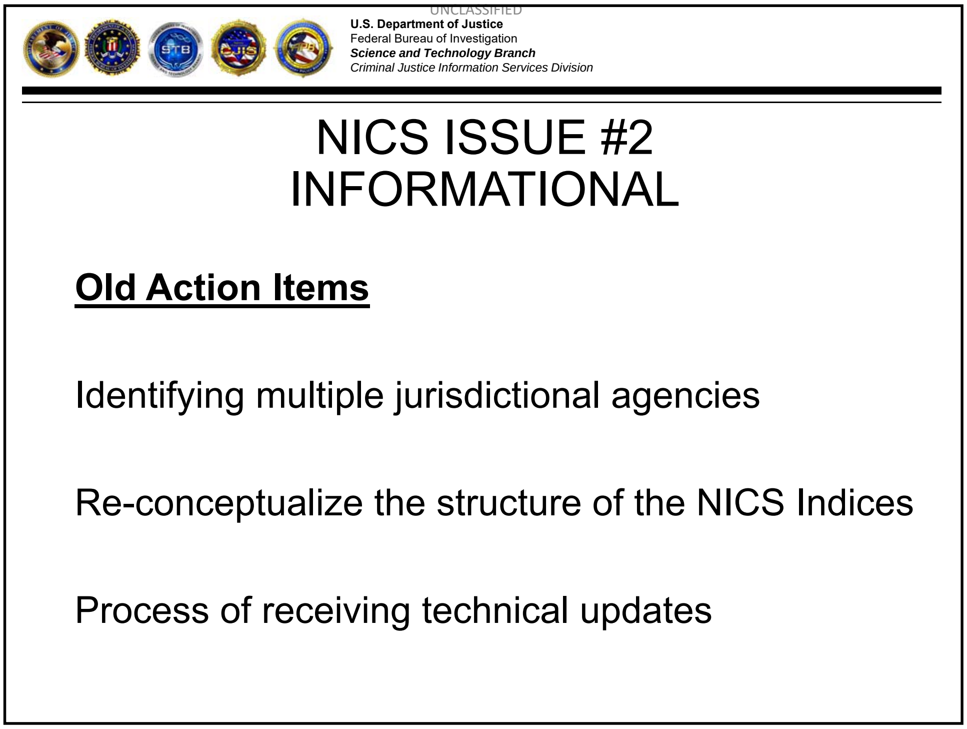
Topics Heard During Subcommittee

Race Code Standardization

Expanding the Protection Order File

NICS Audit Update

Law Enforcement Enterprise Portal



UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

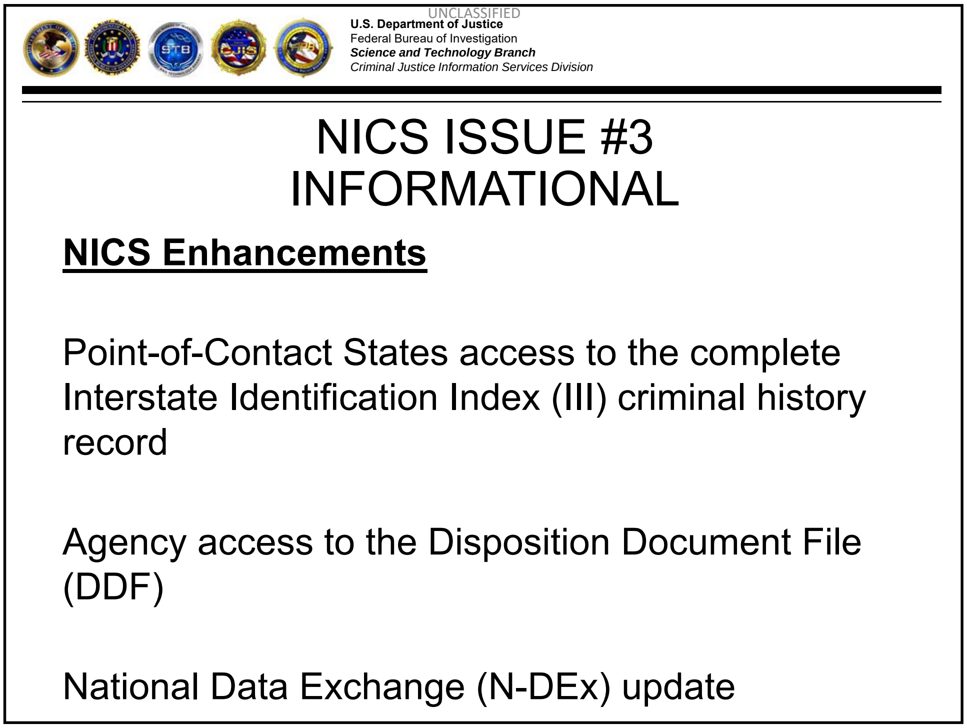
NICS ISSUE #2
INFORMATIONAL

Old Action Items

Identifying multiple jurisdictional agencies

Re-conceptualize the structure of the NICS Indices

Process of receiving technical updates



UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

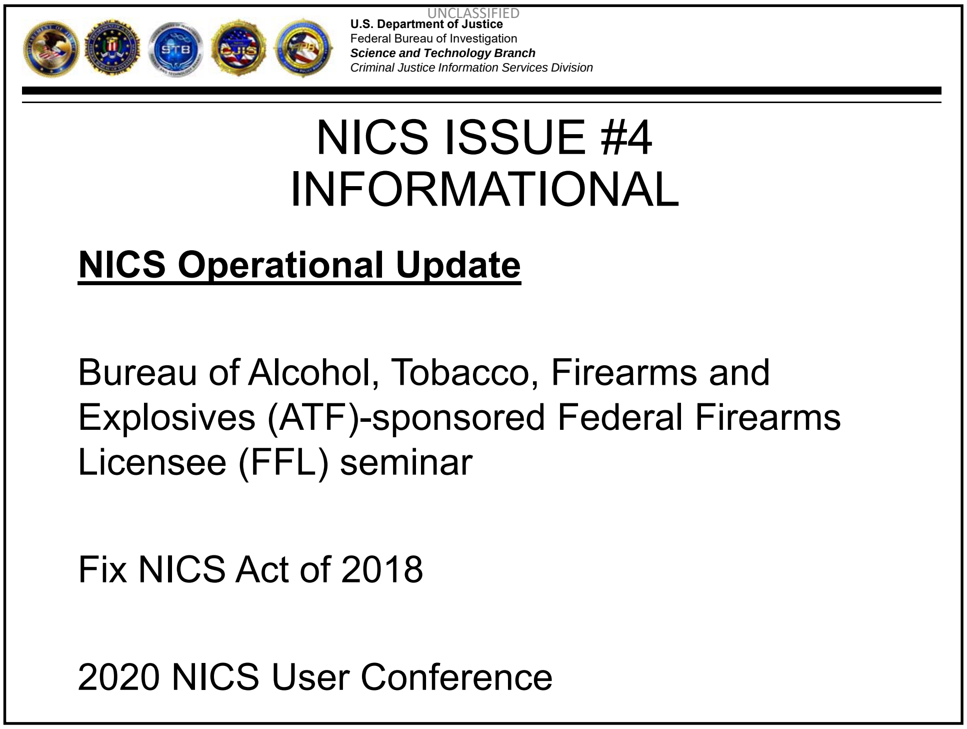
NICS ISSUE #3
INFORMATIONAL

NICS Enhancements

Point-of-Contact States access to the complete Interstate Identification Index (III) criminal history record

Agency access to the Disposition Document File (DDF)

National Data Exchange (N-DEx) update



UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

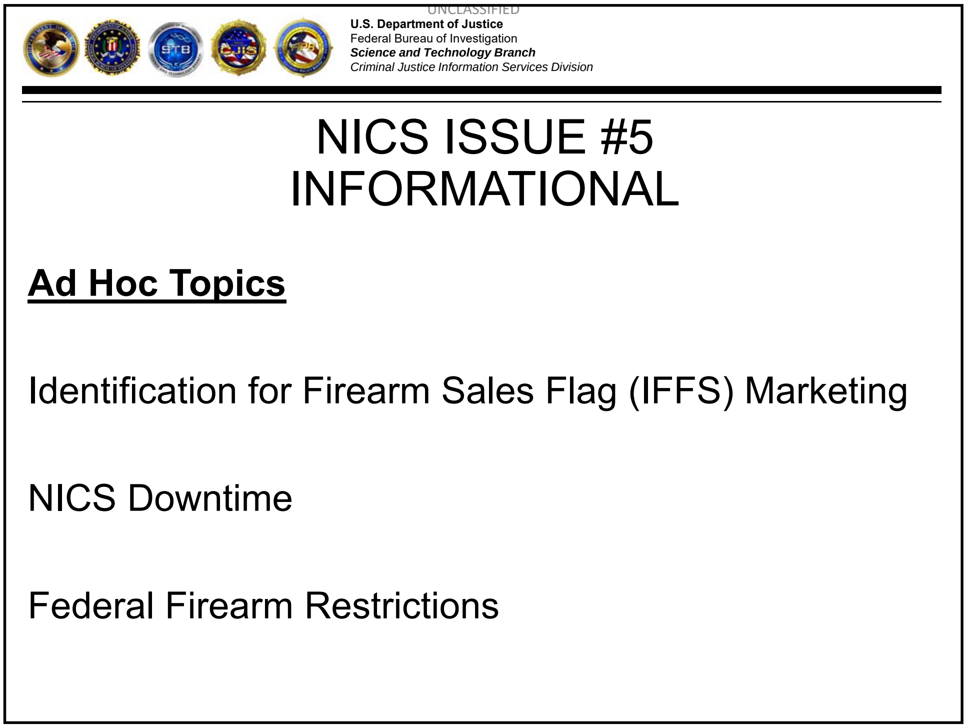
NICS ISSUE #4
INFORMATIONAL

<u>NICS Operational Update</u>

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)-sponsored Federal Firearms Licensee (FFL) seminar

Fix NICS Act of 2018

2020 NICS User Conference



UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

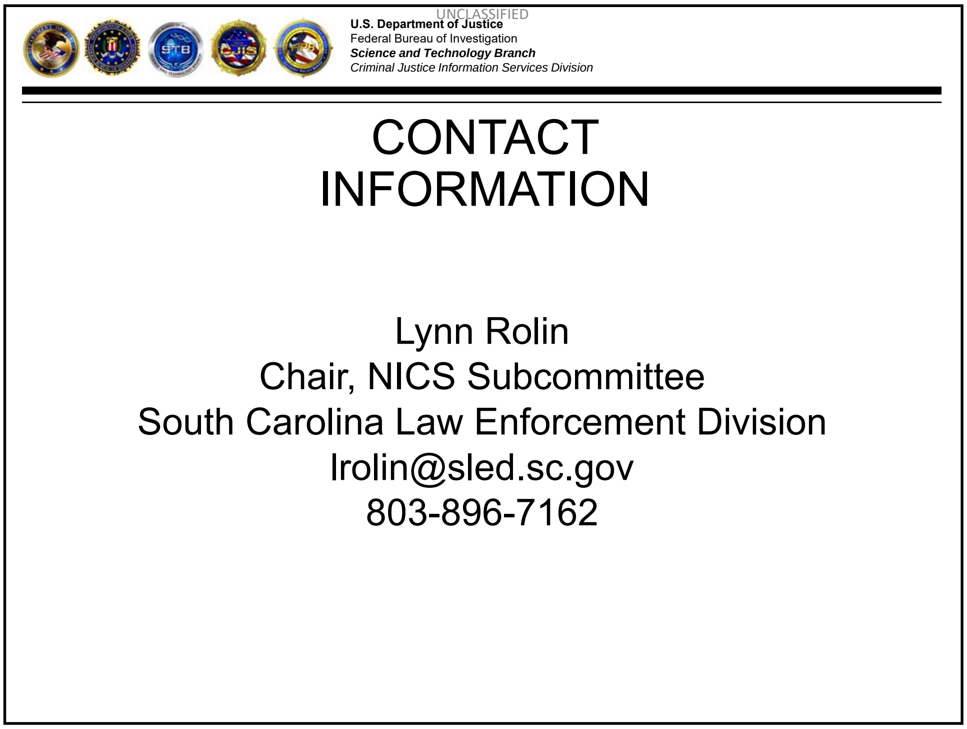
NICS ISSUE #5
INFORMATIONAL

<u>Ad Hoc Topics</u>

Identification for Firearm Sales Flag (IFFS) Marketing

NICS Downtime

Federal Firearm Restrictions



UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation
Science and Technology Branch
Criminal Justice Information Services Division

CONTACT INFORMATION

Lynn Rolin
Chair, NICS Subcommittee
South Carolina Law Enforcement Division
lrolin@sled.sc.gov
803-896-7162

UNCLASSIFIED // FOR OFFICIAL USE ONLY

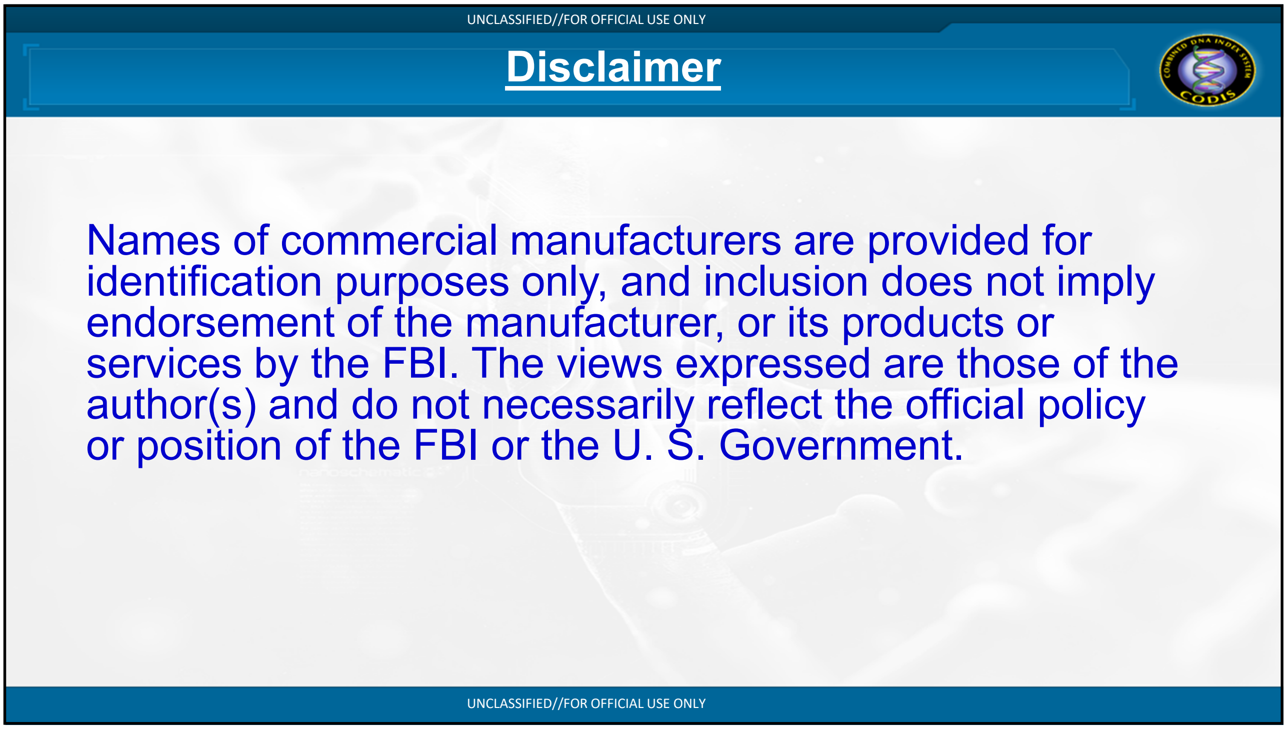
Booking Station Rapid DNA & non-CODIS Crime Scene Analysis

CJIS APB Meeting
Atlanta, GA
December 5, 2019

Thomas Callaghan, PhD.
Chief Biometric Scientist
FBI Laboratory

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY: The information in this document is the property of the Federal Bureau of Investigation and may be distributed to government (federal, state, tribal, or local) employees and contractors with a need to know. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). Dissemination to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized FBI official is prohibited. Precautions must be taken to ensure this information is controlled, stored, handled, transmitted, distributed, and disposed of in a manner that precludes unauthorized access.

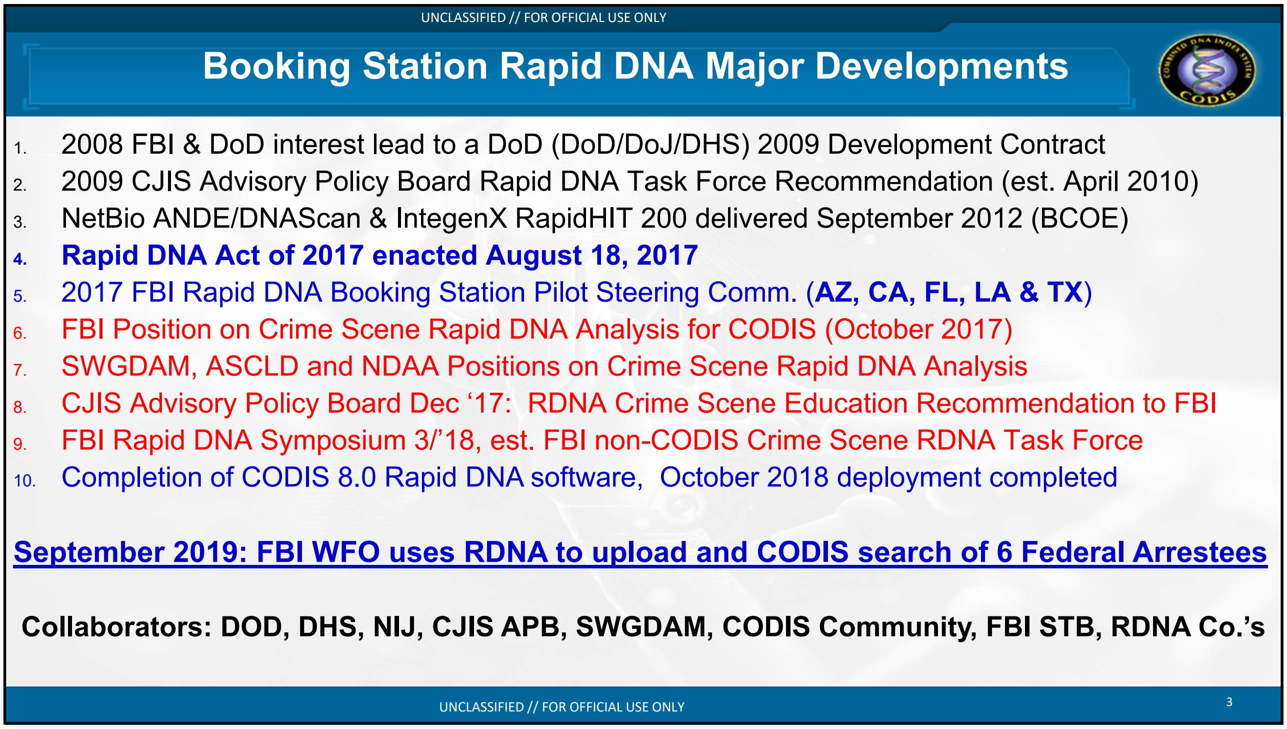


UNCLASSIFIED//FOR OFFICIAL USE ONLY

Disclaimer

Names of commercial manufacturers are provided for identification purposes only, and inclusion does not imply endorsement of the manufacturer, or its products or services by the FBI. The views expressed are those of the author(s) and do not necessarily reflect the official policy or position of the FBI or the U. S. Government.

UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

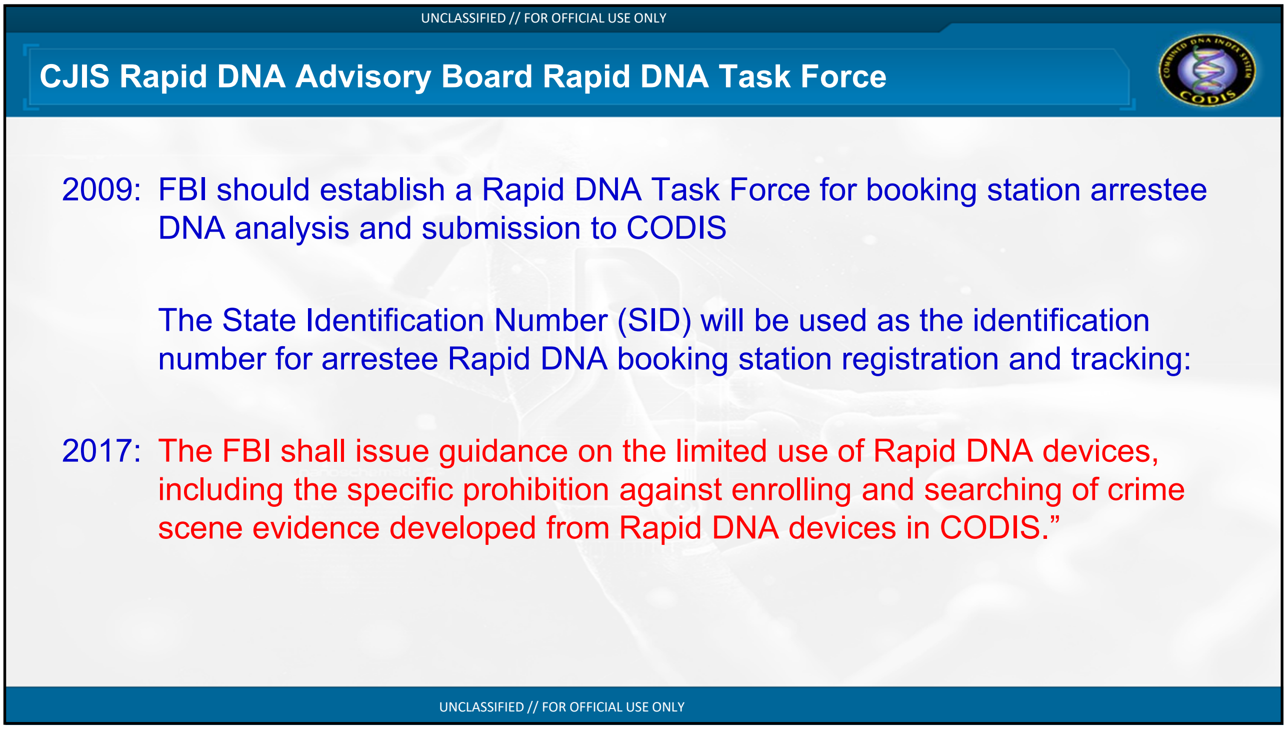
Booking Station Rapid DNA Major Developments

1. 2008 FBI & DoD interest lead to a DoD (DoD/DoJ/DHS) 2009 Development Contract
2. 2009 CJIS Advisory Policy Board Rapid DNA Task Force Recommendation (est. April 2010)
3. NetBio ANDE/DNAScan & IntegenX RapidHIT 200 delivered September 2012 (BCOE)
4. **Rapid DNA Act of 2017 enacted August 18, 2017**
5. 2017 FBI Rapid DNA Booking Station Pilot Steering Comm. (**AZ, CA, FL, LA & TX**)
6. FBI Position on Crime Scene Rapid DNA Analysis for CODIS (October 2017)
7. SWGDAM, ASCLD and NDAA Positions on Crime Scene Rapid DNA Analysis
8. CJIS Advisory Policy Board Dec '17: RDNA Crime Scene Education Recommendation to FBI
9. FBI Rapid DNA Symposium 3/'18, est. FBI non-CODIS Crime Scene RDNA Task Force
10. Completion of CODIS 8.0 Rapid DNA software, October 2018 deployment completed

September 2019: FBI WFO uses RDNA to upload and CODIS search of 6 Federal Arrestees

Collaborators: DOD, DHS, NIJ, CJIS APB, SWGDAM, CODIS Community, FBI STB, RDNA Co.'s

UNCLASSIFIED // FOR OFFICIAL USE ONLY 3



UNCLASSIFIED // FOR OFFICIAL USE ONLY

CJIS Rapid DNA Advisory Board Rapid DNA Task Force

2009: FBI should establish a Rapid DNA Task Force for booking station arrestee DNA analysis and submission to CODIS

The State Identification Number (SID) will be used as the identification number for arrestee Rapid DNA booking station registration and tracking:

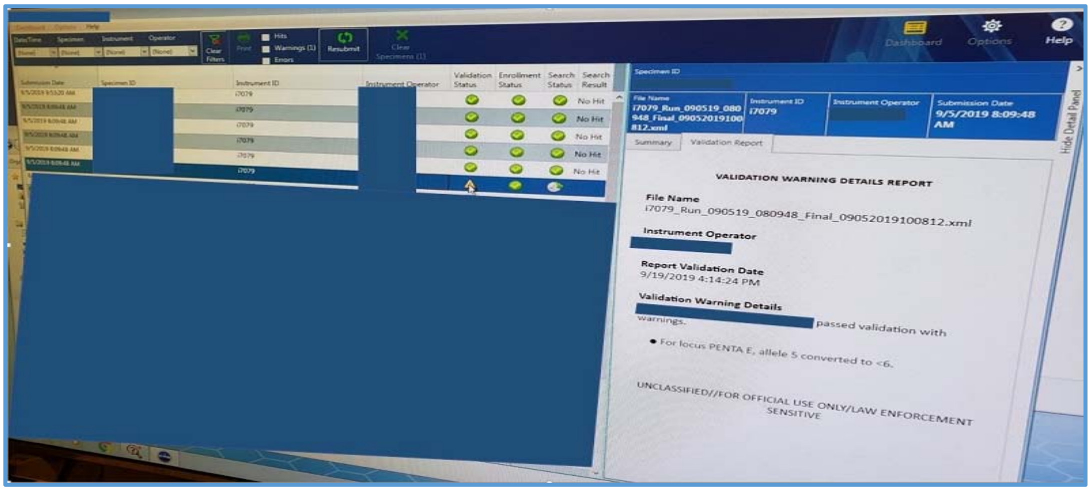
2017: The FBI shall issue guidance on the limited use of Rapid DNA devices, including the specific prohibition against enrolling and searching of crime scene evidence developed from Rapid DNA devices in CODIS."

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA Pilot FDDU-WFO

Rapid Pilot at WFO booking facility

Rapid DNA Pilot FDDU-WFO



Submission Date	Specimen ID	Instrument ID	Instrument Operator	Validation Status	Enrollment Status	Search Status	Search Result
9/5/2019 8:53:20 AM	[redacted]	i7079	[redacted]	✓	✓	✓	No Hit
9/5/2019 8:09:48 AM	[redacted]	i7079	[redacted]	✓	✓	✓	No Hit
9/5/2019 8:09:48 AM	[redacted]	i7079	[redacted]	✓	✓	✓	No Hit
9/5/2019 8:09:48 AM	[redacted]	i7079	[redacted]	✓	✓	✓	No Hit
9/5/2019 8:09:48 AM	[redacted]	i7079	[redacted]	✓	✓	✓	No Hit
9/5/2019 8:09:48 AM	[redacted]	i7079	[redacted]	⚠	✓		

[redacted]

Specimen ID
[redacted]

File Name	Instrument ID	Instrument Operator	Submission Date
i7079_Run_090519_080948_Final_09052019100812.xml	i7079	[redacted]	9/5/2019 8:09:48 AM

VALIDATION WARNING DETAILS REPORT

File Name
i7079_Run_090519_080948_Final_09052019100812.xml

Instrument Operator
[redacted]

Report Validation Date
9/19/2019 4:14:24 PM

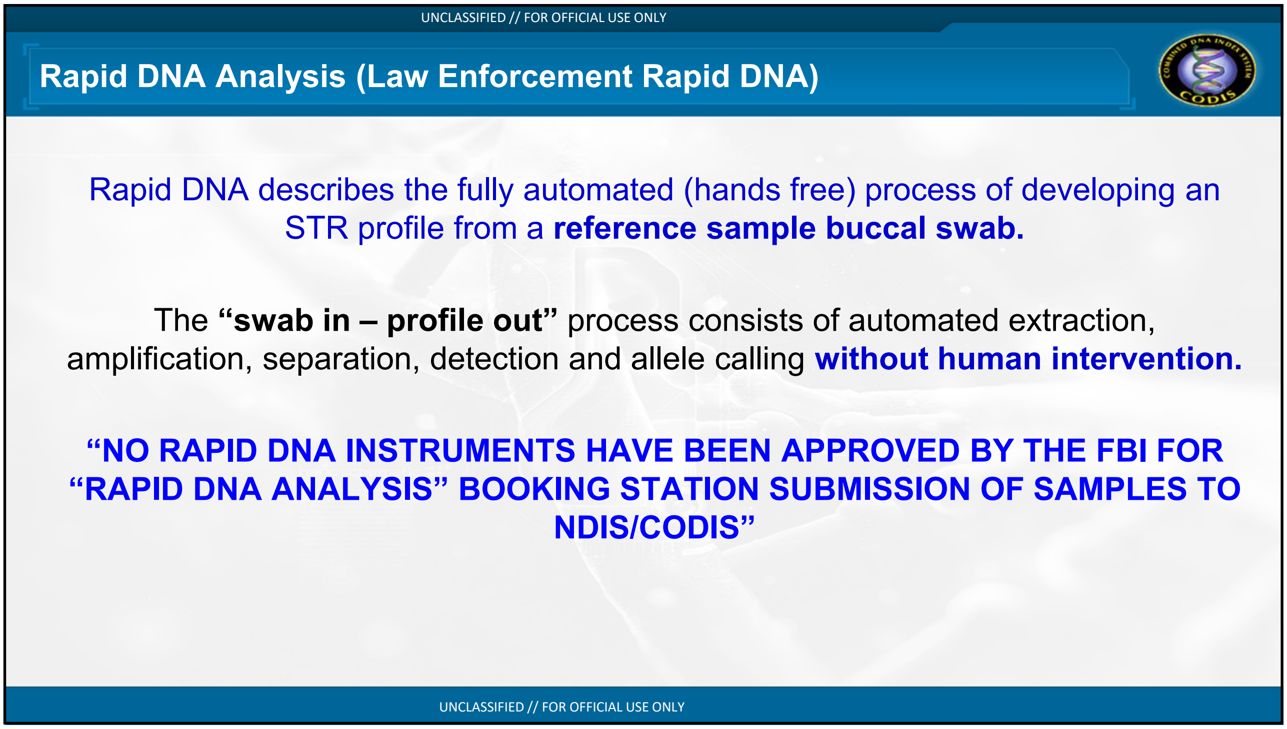
Validation Warning Details
[redacted] passed validation with warnings.

- For locus PENTA E, allele 5 converted to <6.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/LAW ENFORCEMENT SENSITIVE

Successful CRE enrollment and search

APPENDIX EE



UNCLASSIFIED // FOR OFFICIAL USE ONLY

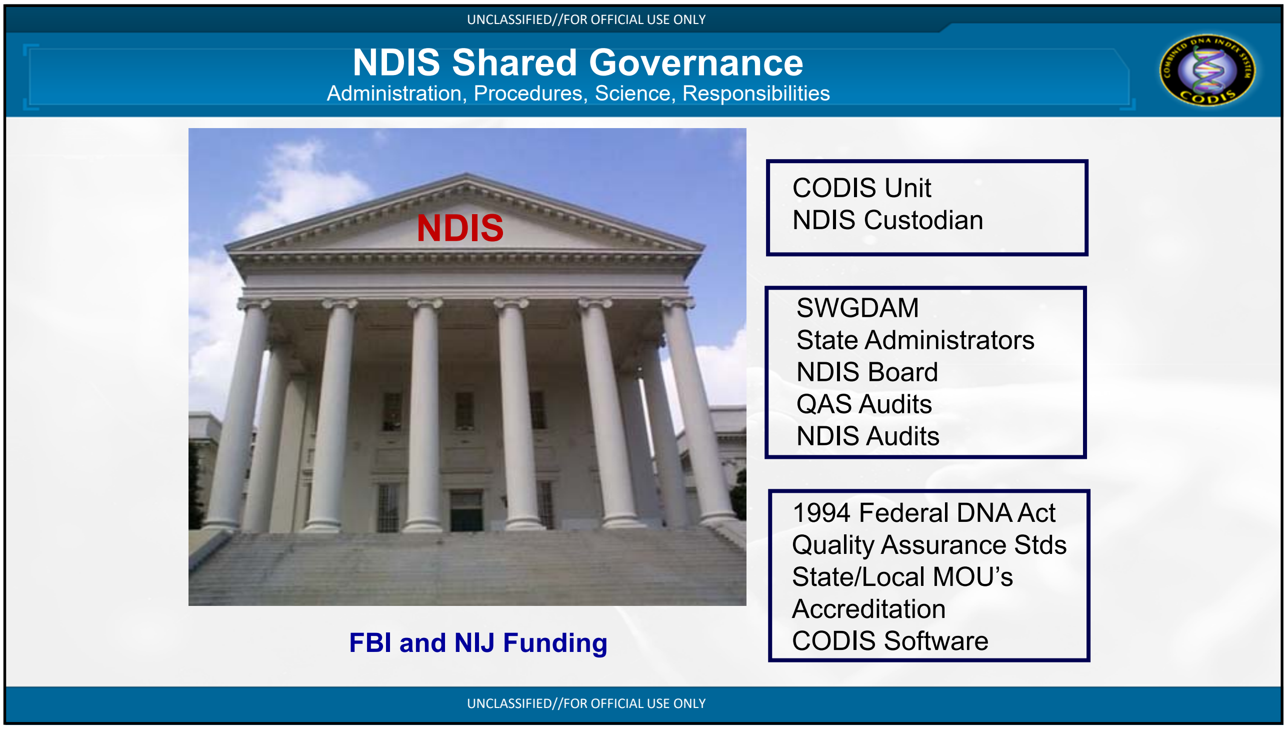
Rapid DNA Analysis (Law Enforcement Rapid DNA)

Rapid DNA describes the fully automated (hands free) process of developing an STR profile from a **reference sample buccal swab.**

The **“swab in – profile out”** process consists of automated extraction, amplification, separation, detection and allele calling **without human intervention.**

“NO RAPID DNA INSTRUMENTS HAVE BEEN APPROVED BY THE FBI FOR “RAPID DNA ANALYSIS” BOOKING STATION SUBMISSION OF SAMPLES TO NDIS/CODIS”

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED//FOR OFFICIAL USE ONLY

NDIS Shared Governance

Administration, Procedures, Science, Responsibilities

FBI and NIJ Funding

CODIS Unit
NDIS Custodian

SWGDAM
State Administrators
NDIS Board
QAS Audits
NDIS Audits

1994 Federal DNA Act
Quality Assurance Stds
State/Local MOU’s
Accreditation
CODIS Software

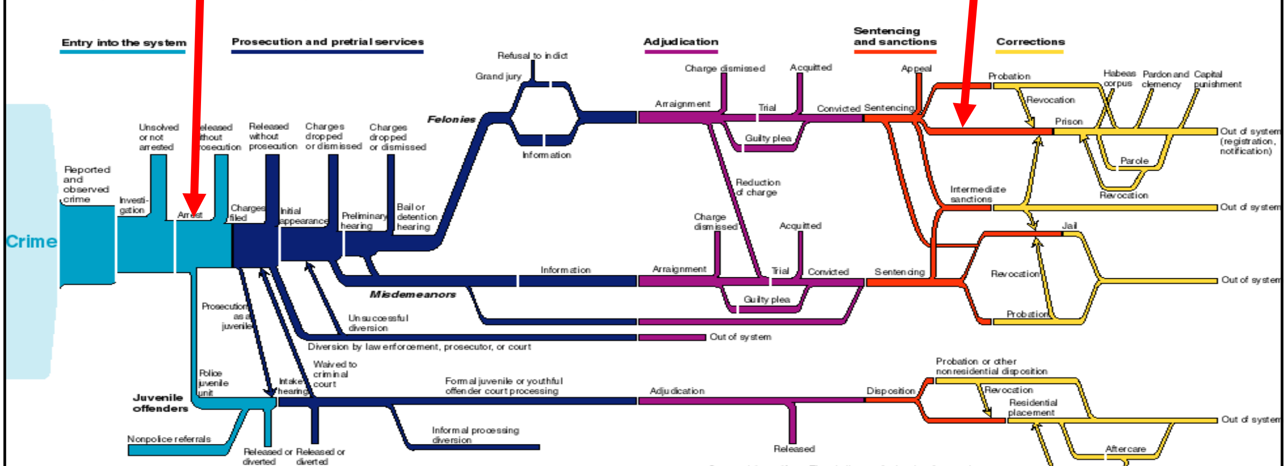
UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Consequences of Arrestee DNA Collection

DNA can now be collected upon arrest

What is the sequence of events in the criminal justice system?

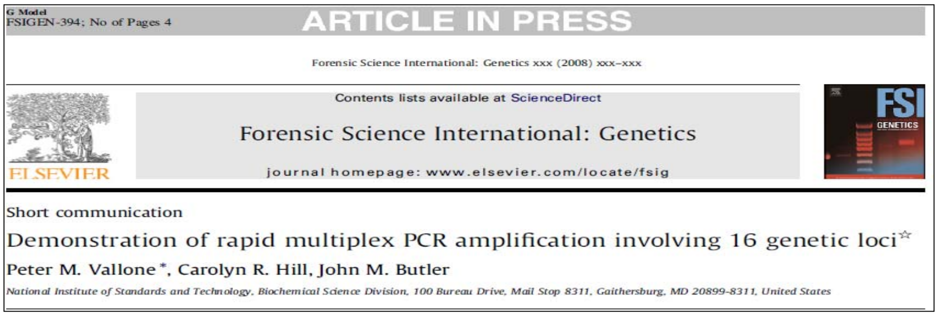


Note: This chart gives a simplified view of caseflow through the criminal justice system. Procedures vary among jurisdictions. The weights of the lines are not intended to show actual size of caseloads.

Source: Adapted from *The challenge of crime in a free society*. President's Commission on Law Enforcement and Administration of Justice, 1967. This revision, a result of the Symposium on the 30th Anniversary of the President's Commission, was prepared by the Bureau of Justice Statistics in 1997.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid PCR Article



G Model
FSIGEN-394; No of Pages 4

ARTICLE IN PRESS

Forensic Science International: Genetics xxx (2008) xxx–xxx

Contents lists available at ScienceDirect

Forensic Science International: Genetics

journal homepage: www.elsevier.com/locate/fsig

ELSEVIER

FSI GENETICS

Short communication

Demonstration of rapid multiplex PCR amplification involving 16 genetic loci☆

Peter M. Vallone*, Carolyn R. Hill, John M. Butler

National Institute of Standards and Technology, Biochemical Science Division, 100 Bureau Drive, Mail Stop 8311, Gaithersburg, MD 20899-8311, United States

Vallone, P.M., Hill, C.R., Butler, J.M. (2008) Demonstration of rapid multiplex PCR amplification involving 16 genetic loci. *FSI Genetics* 3(1): 42-45.

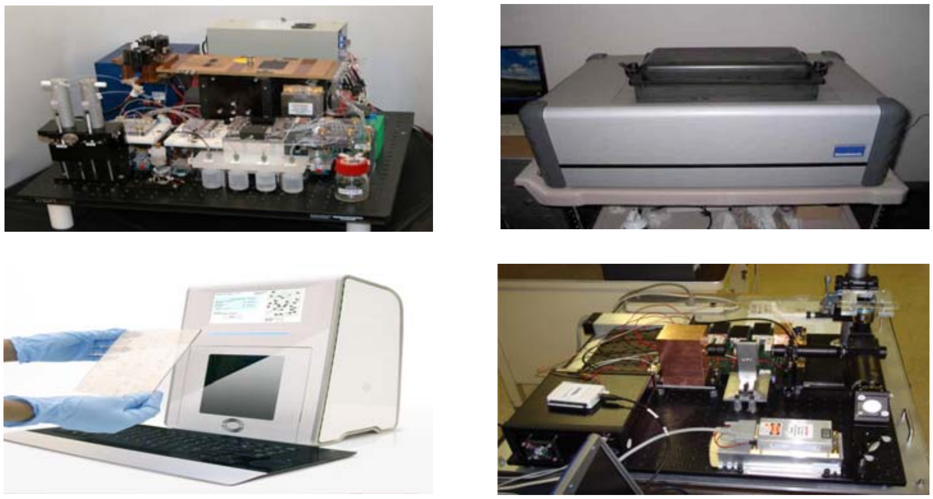
Rapid PCR Amplification of STR Typing Kits 20th Annual International Symposium on Human Identification (Promega Meeting) October 14, 2009, Las Vegas, NV

Rapid Amplification of Commercial STR Typing Kits, International Society of Forensic Genetics (ISFG), September 16, 2009, Buenos Aires, Argentina

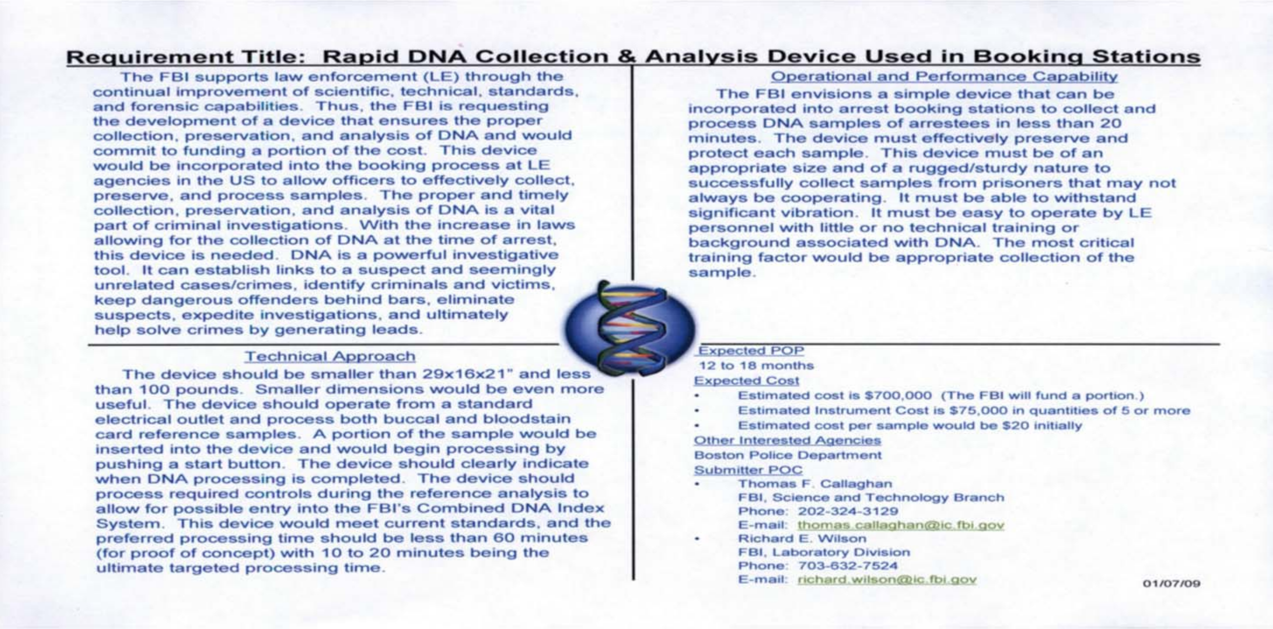
http://www.cstl.nist.gov/biotech/strbase/NISTpub.htm

Not Ready for Lab Use, But Not Science Fiction

(Under Development R-DNA Systems)



Unclassified



Requirement Title: Rapid DNA Collection & Analysis Device Used in Booking Stations

The FBI supports law enforcement (LE) through the continual improvement of scientific, technical, standards, and forensic capabilities. Thus, the FBI is requesting the development of a device that ensures the proper collection, preservation, and analysis of DNA and would commit to funding a portion of the cost. This device would be incorporated into the booking process at LE agencies in the US to allow officers to effectively collect, preserve, and process samples. The proper and timely collection, preservation, and analysis of DNA is a vital part of criminal investigations. With the increase in laws allowing for the collection of DNA at the time of arrest, this device is needed. DNA is a powerful investigative tool. It can establish links to a suspect and seemingly unrelated cases/crimes, identify criminals and victims, keep dangerous offenders behind bars, eliminate suspects, expedite investigations, and ultimately help solve crimes by generating leads.

Technical Approach

The device should be smaller than 29x16x21" and less than 100 pounds. Smaller dimensions would be even more useful. The device should operate from a standard electrical outlet and process both buccal and bloodstain card reference samples. A portion of the sample would be inserted into the device and would begin processing by pushing a start button. The device should clearly indicate when DNA processing is completed. The device should process required controls during the reference analysis to allow for possible entry into the FBI's Combined DNA Index System. This device would meet current standards, and the preferred processing time should be less than 60 minutes (for proof of concept) with 10 to 20 minutes being the ultimate targeted processing time.

Operational and Performance Capability

The FBI envisions a simple device that can be incorporated into arrest booking stations to collect and process DNA samples of arrestees in less than 20 minutes. The device must effectively preserve and protect each sample. This device must be of an appropriate size and of a rugged/sturdy nature to successfully collect samples from prisoners that may not always be cooperating. It must be able to withstand significant vibration. It must be easy to operate by LE personnel with little or no technical training or background associated with DNA. The most critical training factor would be appropriate collection of the sample.

Expected POP

12 to 18 months

Expected Cost

- Estimated cost is $700,000 (The FBI will fund a portion.)
- Estimated Instrument Cost is $75,000 in quantities of 5 or more
- Estimated cost per sample would be $20 initially

Other Interested Agencies

Boston Police Department

Submitter POC

- Thomas F. Callaghan
  FBI, Science and Technology Branch
  Phone: 202-324-3129
  E-mail: thomas.callaghan@ic.fbi.gov
- Richard E. Wilson
  FBI, Laboratory Division
  Phone: 703-632-7524
  E-mail: richard.wilson@ic.fbi.gov

01/07/09

12

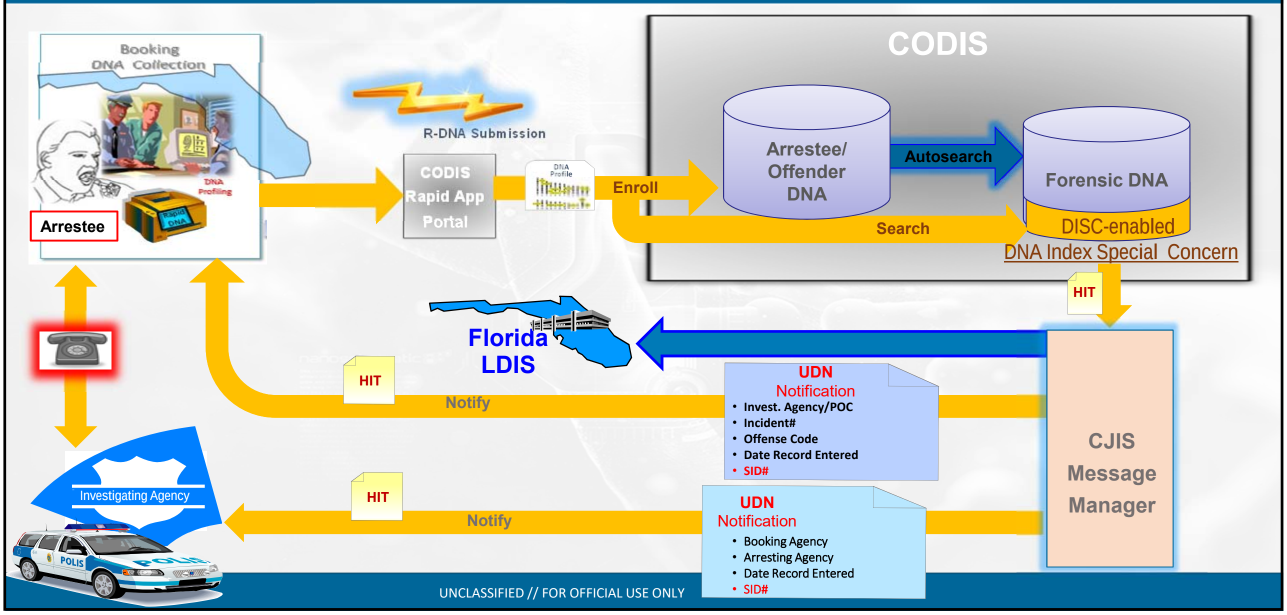
Cooperative Model

ANDE:

- Stakeholder consensus: Combine efforts to create common core automated DNA analysis instrument
- MIT LL-facilitated process to develop and issue RFP for hardware development
  - Synthesized stakeholder requirements into SOW for RFP
  - Developed evaluation plan reflective of stakeholder priorities
  - Proposals received, evaluated, and ranked

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid-DNA Arrestee Enrollment, Search & Notification



Booking DNA Collection

DNA Profiling

Rapid DNA

Arrestee

R-DNA Submission

CODIS Rapid App Portal

DNA Profile

Enroll

CODIS

Arrestee/ Offender DNA

Autosearch

Forensic DNA

Search

DISC-enabled DNA Index Special Concern

HIT

Florida LDIS

UDN Notification

- Invest. Agency/POC
- Incident#
- Offense Code
- Date Record Entered
- SID#

HIT

Notify

CJIS Message Manager

Investigating Agency

POLIS

HIT

Notify

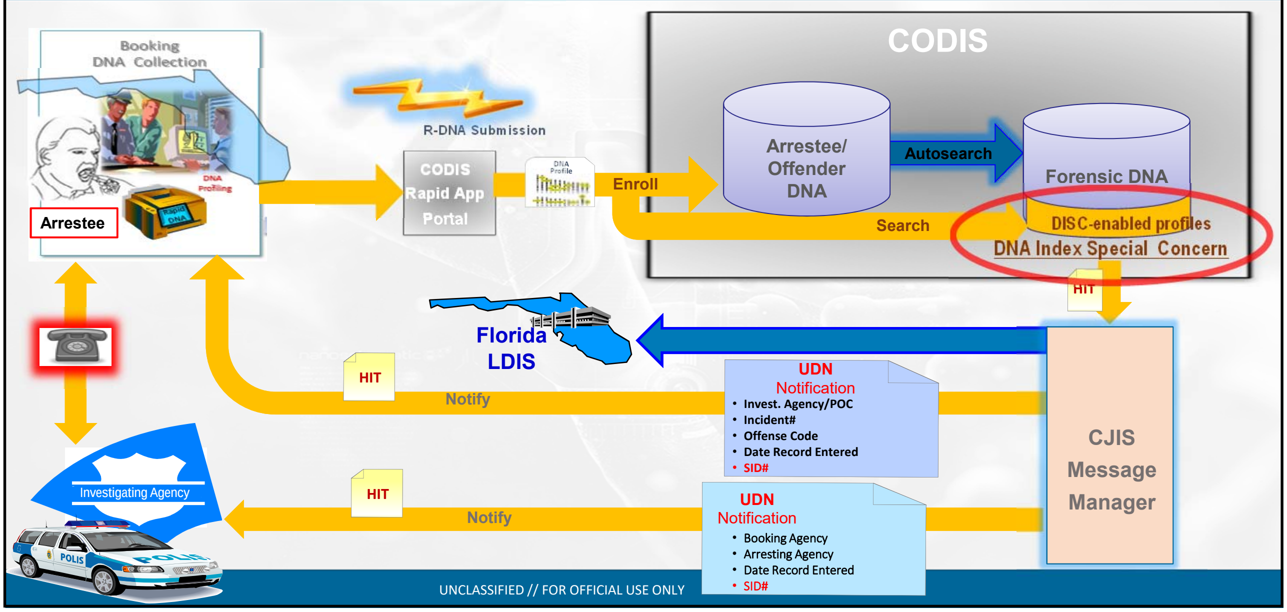
UDN Notification

- Booking Agency
- Arresting Agency
- Date Record Entered
- SID#

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid-DNA Arrestee Enrollment, Search & Notification



Booking DNA Collection

DNA Profiling

Rapid DNA

Arrestee

R-DNA Submission

CODIS Rapid App Portal

DNA Profile

Enroll

CODIS

Arrestee/ Offender DNA

Autosearch

Forensic DNA

Search

DISC-enabled profiles

DNA Index Special Concern

HIT

Florida LDIS

HIT

Notify

UDN Notification

- Invest. Agency/POC
- Incident#
- Offense Code
- Date Record Entered
- SID#

CJIS Message Manager

Investigating Agency

HIT

Notify

UDN Notification

- Booking Agency
- Arresting Agency
- Date Record Entered
- SID#

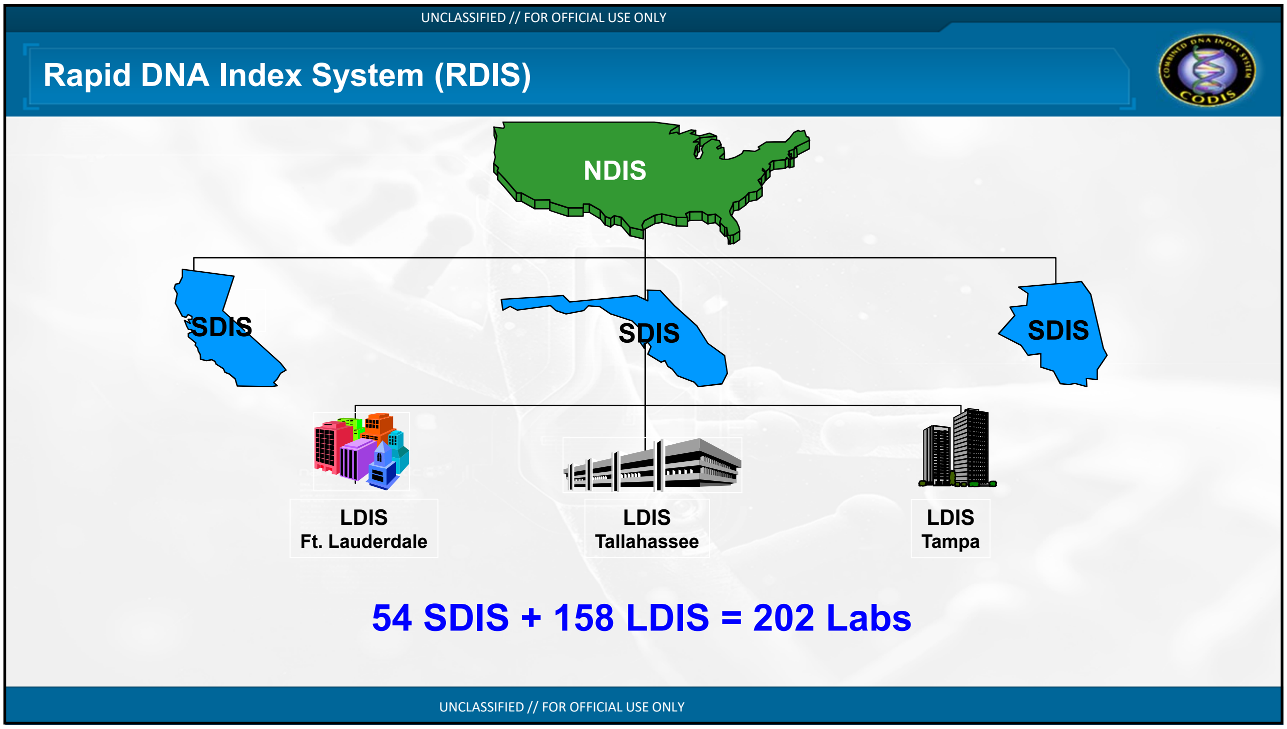
UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

DNA Index of Special Concern (DISC) Search

- High stringency search automatically when arrestee profile analyzed by Rapid DNA system at the booking station is enrolled into CODIS
- Unsolved forensic unknown 13 original core profiles in the DNA Index of Special Concern (DISC)
- DISC profiles must be from unsolved crimes = Homicide, Sexual Assault/Rape, Kidnapping & Terrorism investigations
- The enrolled arrestee profile will be searched against the non DISC-enabled forensic profiles during next routine CODIS autosearch process

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA Index System (RDIS)

NDIS

SDIS

SDIS

SDIS

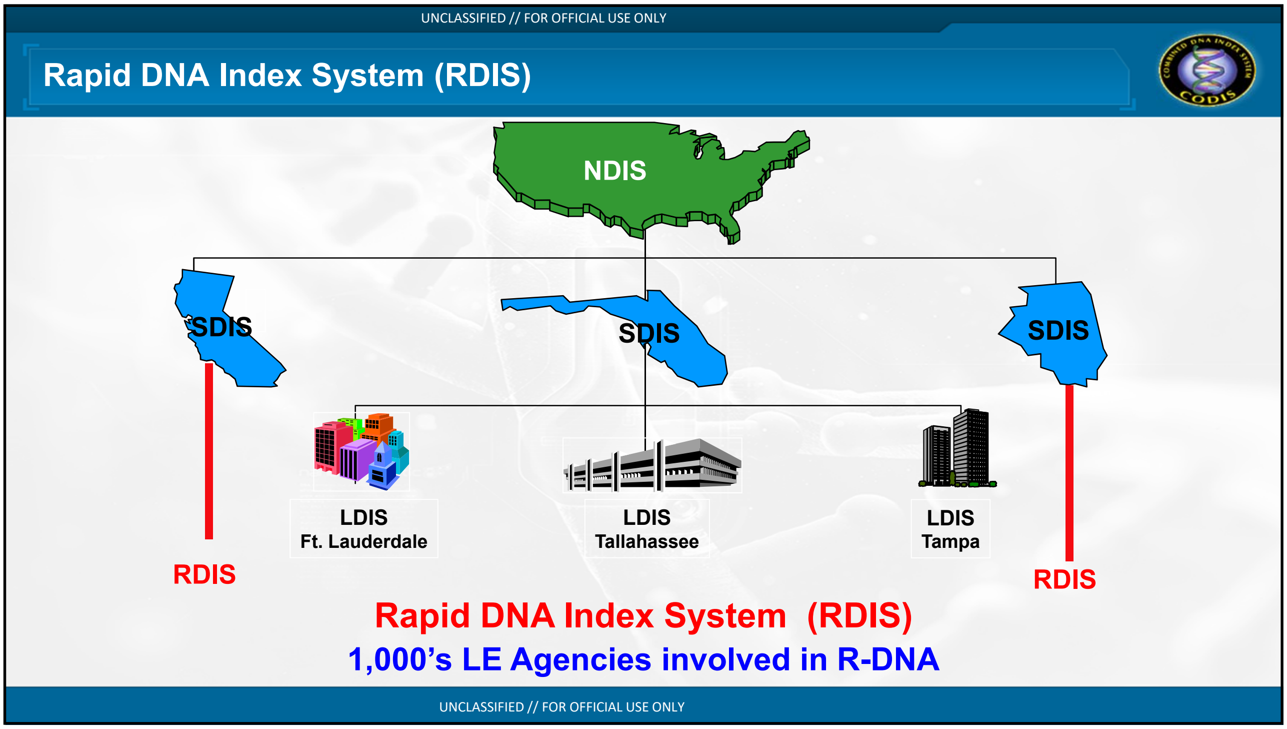
LDIS
Ft. Lauderdale

LDIS
Tallahassee

LDIS
Tampa

54 SDIS + 158 LDIS = 202 Labs

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA Index System (RDIS)

NDIS

SDIS

SDIS

SDIS

LDIS
Ft. Lauderdale

LDIS
Tallahassee

LDIS
Tampa

RDIS

RDIS

Rapid DNA Index System (RDIS)

1,000’s LE Agencies involved in R-DNA

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Unsolicited DNA Notification (UDN) Message

****** UNSOLICITED DNA NOTIFICATION ******

This message is being sent to law enforcement agencies in response to a subject that was recently processed at a booking location. The SUBJECT is potentially linked to an unsolved crime of special concern by a DNA Hit/Match.

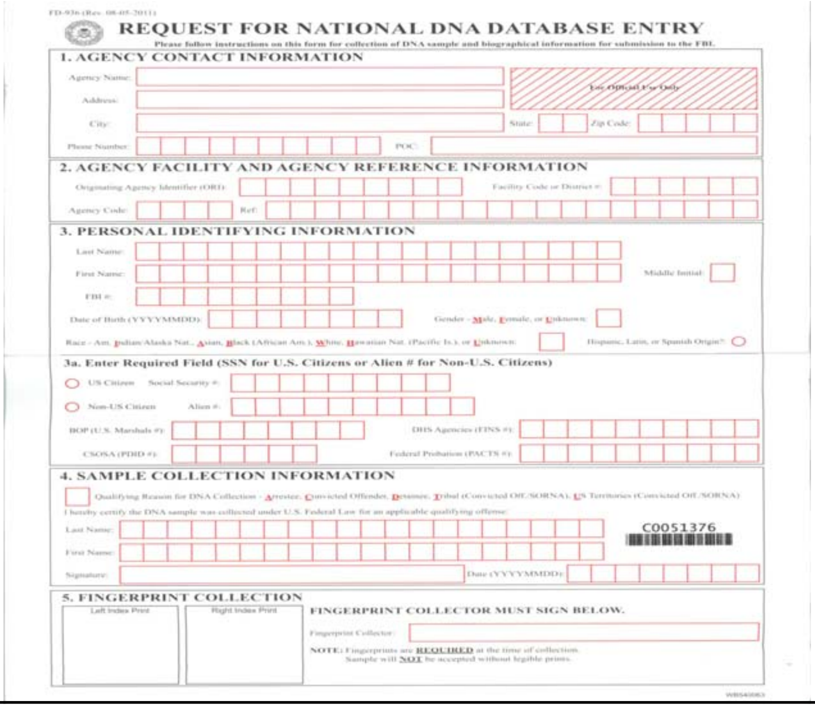
The investigating agency should immediately contact the booking agency to determine the status of the subject.

Booking Agency Information
Booking Agency ORI: FL037010A
Arresting Agency ORI: FL037010B

Arrestee SID: FL012345678

Livescan Unique Event ID: 20140624001
Fingerprint Date/Time: 2014-12-31T20:44:12
Arrest Date/Time: 2014-12-31T20:30:44
Booking Agency #: FLXYZ099
Arresting Agency #: FLABC099

Investigative Agency Information
Investigative Agency ORI: VA122015Z1
Investigative Case ID: GL19960712
Investigative Offense: Aggravated Assault
Statute of Limitations: 2030-07-12T00:00:00
Investigator Phone Number: 703-576-5555
Investigative Agency Contact Information: Detective XXX at the Criminal Investigative Division – Cold Case Unit of the Richmond Police Department. Department: Address: 9000 Jefferson Way, Richmond, VA 23240
Extradition Information:



FD-936 (Rev. 08-05-2011)

REQUEST FOR NATIONAL DNA DATABASE ENTRY

Please follow instructions on this form for collection of DNA sample and biographical information for submission to the FBI.

1. AGENCY CONTACT INFORMATION

Agency Name:
Address:
City:
State:
Zip Code:
Phone Number:
POC:
For Official Use Only

2. AGENCY FACILITY AND AGENCY REFERENCE INFORMATION

Originating Agency Identifier (ORI):
Facility Code or District #:
Agency Code:
Ref:

3. PERSONAL IDENTIFYING INFORMATION

Last Name:
First Name:
Middle Initial:
FBI #:
Date of Birth (YYYYMMDD):
Gender - Male, Female, or Unknown:
Race - Am. Indian/Alaska Nat., Asian, Black (African Am.), White, Hawaiian Nat. (Pacific Is.), or Unknown:
Hispanic, Latin, or Spanish Origin? ○

3a. Enter Required Field (SSN for U.S. Citizens or Alien # for Non-U.S. Citizens)

○ US Citizen Social Security #:
○ Non-US Citizen Alien #:
BOP (U.S. Marshals #):
DHS Agencies (FINS #):
CSOSA (PDID #):
Federal Probation (PACTS #):

4. SAMPLE COLLECTION INFORMATION

□ Qualifying Reason for DNA Collection - Arrestee, Convicted Offender, Detainee, Tribal (Convicted Off./SORNA), US Territories (Convicted Off./SORNA)
I hereby certify the DNA sample was collected under U.S. Federal Law for an applicable qualifying offense:
Last Name:
First Name:
Signature:
Date (YYYYMMDD):

C0051376

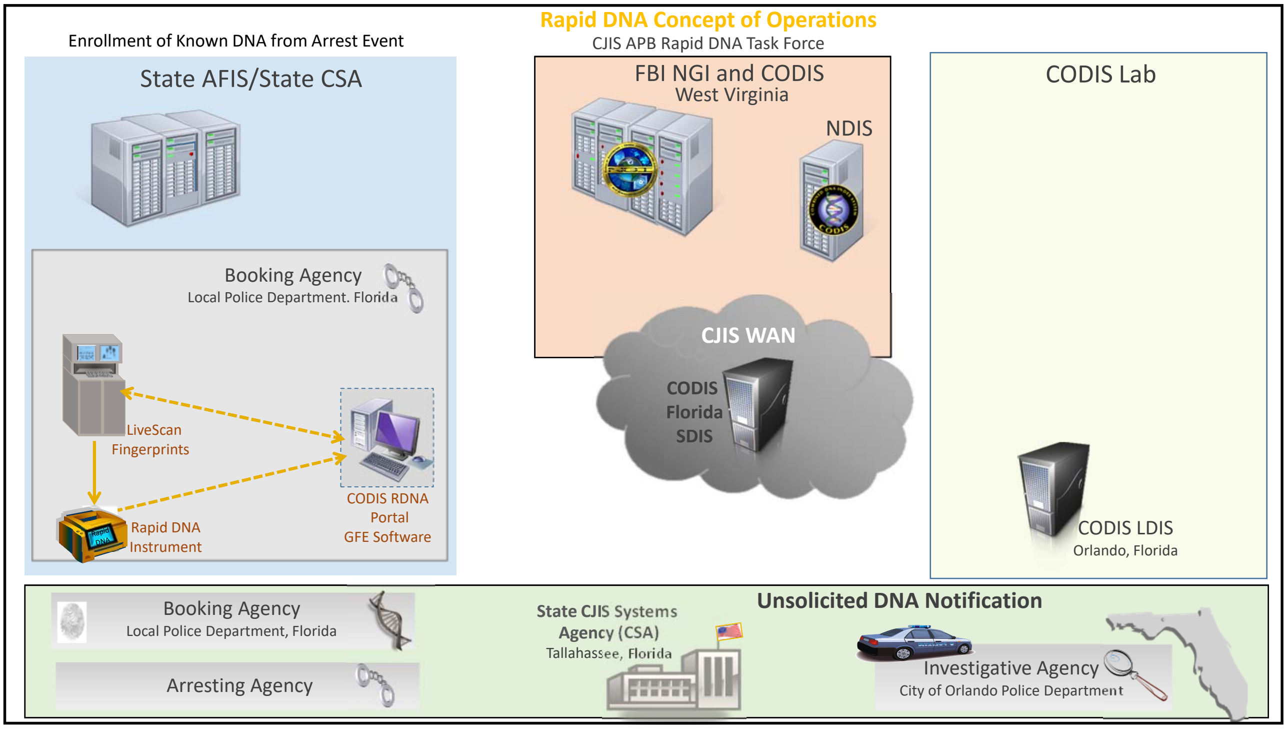
5. FINGERPRINT COLLECTION

Left Index Print
Right Index Print

FINGERPRINT COLLECTOR MUST SIGN BELOW.

Fingerprint Collector:

NOTE: Fingerprints are **REQUIRED** at the time of collection.
Sample will **NOT** be accepted without legible prints.



Rapid DNA Concept of Operations

CJIS APB Rapid DNA Task Force

Enrollment of Known DNA from Arrest Event

State AFIS/State CSA

Booking Agency
Local Police Department. Florida

LiveScan
Fingerprints

Rapid DNA
Instrument

CODIS RDNA
Portal
GFE Software

FBI NGI and CODIS
West Virginia

NDIS

CJIS WAN

CODIS
Florida
SDIS

CODIS Lab

CODIS LDIS
Orlando, Florida

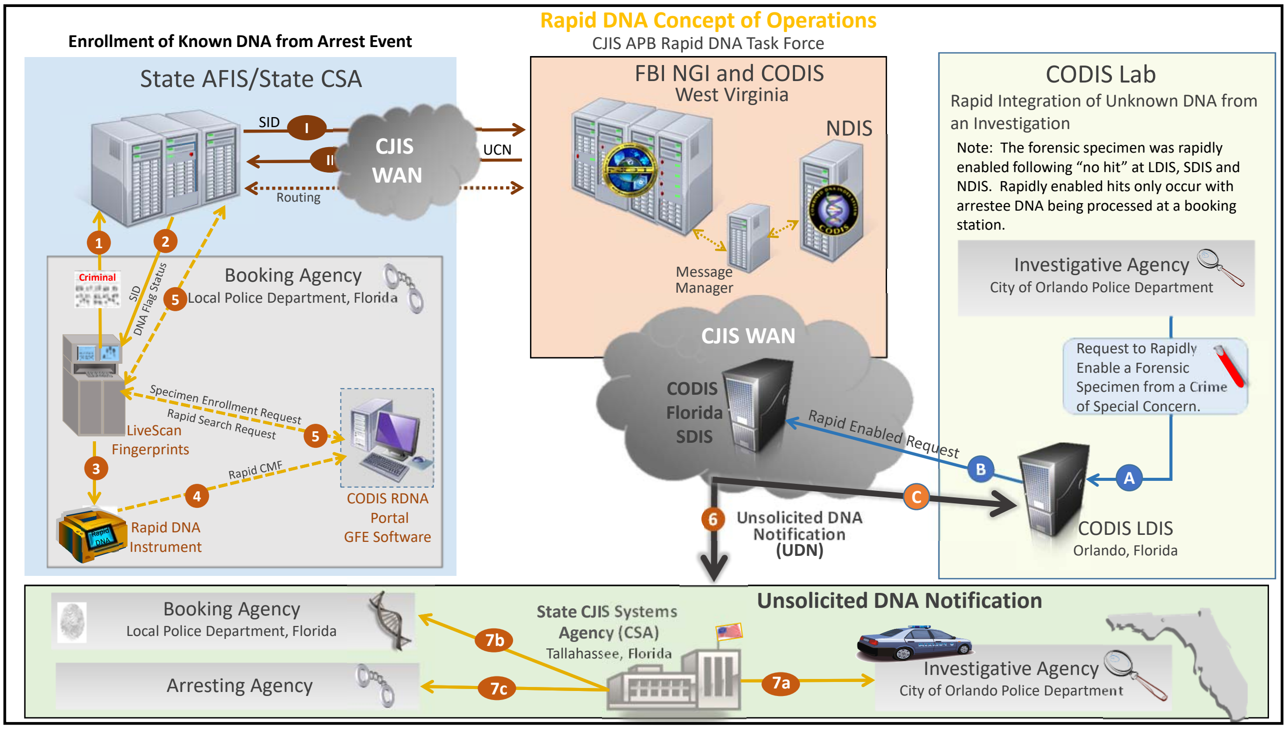
Unsolicited DNA Notification

Booking Agency
Local Police Department, Florida

Arresting Agency

State CJIS Systems
Agency (CSA)
Tallahassee, Florida

Investigative Agency
City of Orlando Police Department



Rapid DNA Concept of Operations

CJIS APB Rapid DNA Task Force

Enrollment of Known DNA from Arrest Event

State AFIS/State CSA

SID
I
II
CJIS
WAN
UCN
Routing

1
2
SID
DNA Flag Status
5
Criminal

Booking Agency
Local Police Department, Florida

Specimen Enrollment Request
Rapid Search Request
5

LiveScan
Fingerprints

3
4
Rapid CMF

Rapid DNA
Instrument

CODIS RDNA
Portal
GFE Software

FBI NGI and CODIS
West Virginia

NDIS

Message
Manager

CJIS WAN

CODIS
Florida
SDIS

Rapid Enabled Request

6
Unsolicited DNA
Notification
(UDN)

CODIS Lab
Rapid Integration of Unknown DNA from an Investigation

Note: The forensic specimen was rapidly enabled following "no hit" at LDIS, SDIS and NDIS. Rapidly enabled hits only occur with arrestee DNA being processed at a booking station.

Investigative Agency
City of Orlando Police Department

Request to Rapidly Enable a Forensic Specimen from a Crime of Special Concern.

A
B
C

CODIS LDIS
Orlando, Florida

Unsolicited DNA Notification

Booking Agency
Local Police Department, Florida

7b

Arresting Agency

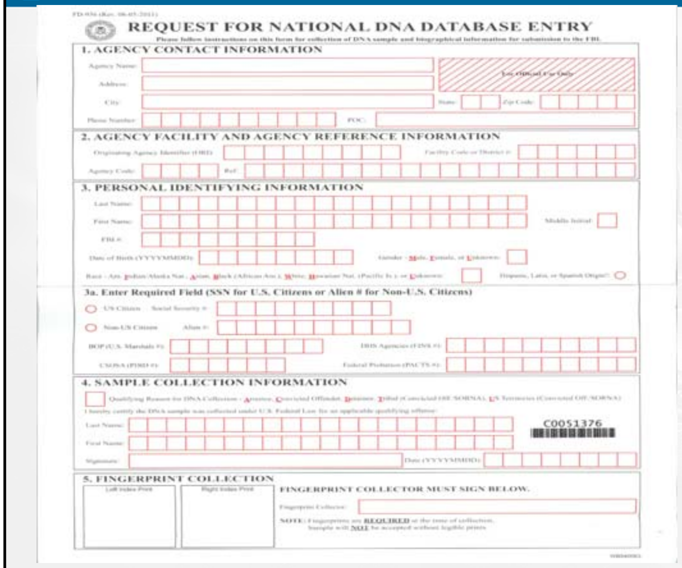
7c

State CJIS Systems
Agency (CSA)
Tallahassee, Florida

7a

Investigative Agency
City of Orlando Police Department

Data Submission: Arrestee Enrollment Format (AEF)



FD-936 (Rev. 06-05-2011)

REQUEST FOR NATIONAL DNA DATABASE ENTRY

Please follow instructions on this form for collection of DNA sample and biographical information for submission to the FBI.

1. AGENCY CONTACT INFORMATION

Agency Name:

Address:

For Official Use Only

City: State: Zip Code:

Phone Number: POC:

2. AGENCY FACILITY AND AGENCY REFERENCE INFORMATION

Originating Agency Identifier (ORI): Facility Code or District #:

Agency Code: Ref:

3. PERSONAL IDENTIFYING INFORMATION

Last Name:

First Name: Middle Initial:

FBI #:

Date of Birth (YYYYMMDD): Gender - Male, Female, or Unknown:

Race - Am. Indian/Alaska Nat., Asian, Black (African Am.), White, Hawaiian Nat. (Pacific Is.) or Unknown: Hispanic, Latin, or Spanish Origin? ○

3a. Enter Required Field (SSN for U.S. Citizens or Alien # for Non-U.S. Citizens)

○ US Citizen Social Security #:

○ Non-US Citizen Alien #:

BOP (U.S. Marshals #): DHS Agencies (FINS #):

CSOSA (PSID #): Federal Probation (PACTS #):

4. SAMPLE COLLECTION INFORMATION

□ Qualifying Reason for DNA Collection - Arrestee, Convicted Offender, Detainee, Tribal (Convicted OF/SORNA), US Territories (Convicted OF/SORNA)

I hereby certify the DNA sample was collected under U.S. Federal Law for an applicable qualifying offense:

Last Name:

First Name:

C0051376

Signature: Date (YYYYMMDD):

5. FINGERPRINT COLLECTION

Left Index Print

Right Index Print

FINGERPRINT COLLECTOR MUST SIGN BELOW.

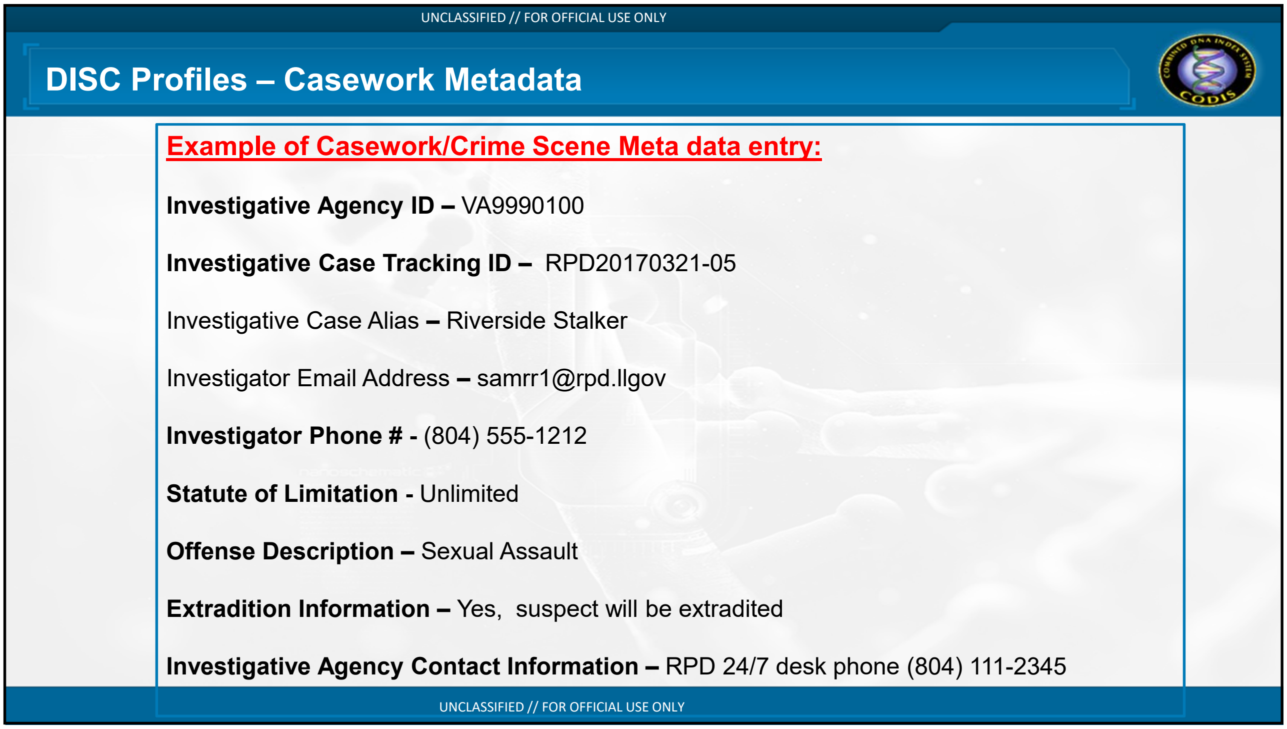
Fingerprint Collector:

NOTE: Fingerprints are REQUIRED at the time of collection. Sample will NOT be accepted without legible prints.

FBI Rapid DNA staff traveled to California in January and February to meet with District Attorneys, Police Chiefs, Sheriffs and the California Department of Justices' CJIS and Laboratory Division to brief them on Rapid DNA Booking Station pilot requirements, pilot plans and non-CODIS crime scene applications.

Arrestee Enrollment Format (AEF)

- CMF/AEF Header Version
- CMF/AEF Message Type
- Booking Agency ID
- Arresting Agency ID
- Instrument ID
- Instrument Manufacturer
- Instrument Model & Serial #
- Instrument Software Version
- Instrument Operator User ID
- Batch ID
- Specimen ID
- Specimen Category
- Loci
- Kit
- Export Date/Time
- State Identification Number
- FBI Number/UCN
- Enrollment Event Identifier (ETN)
- Agency Configurable Identifier
- Arrest Date
- Fingerprint Capture Date
- Offense Category
- Specimen Comment



UNCLASSIFIED // FOR OFFICIAL USE ONLY

DISC Profiles – Casework Metadata

Example of Casework/Crime Scene Meta data entry:

Investigative Agency ID – VA9990100

Investigative Case Tracking ID – RPD20170321-05

Investigative Case Alias **–** Riverside Stalker

Investigator Email Address **–** samrr1@rpd.llgov

Investigator Phone # - (804) 555-1212

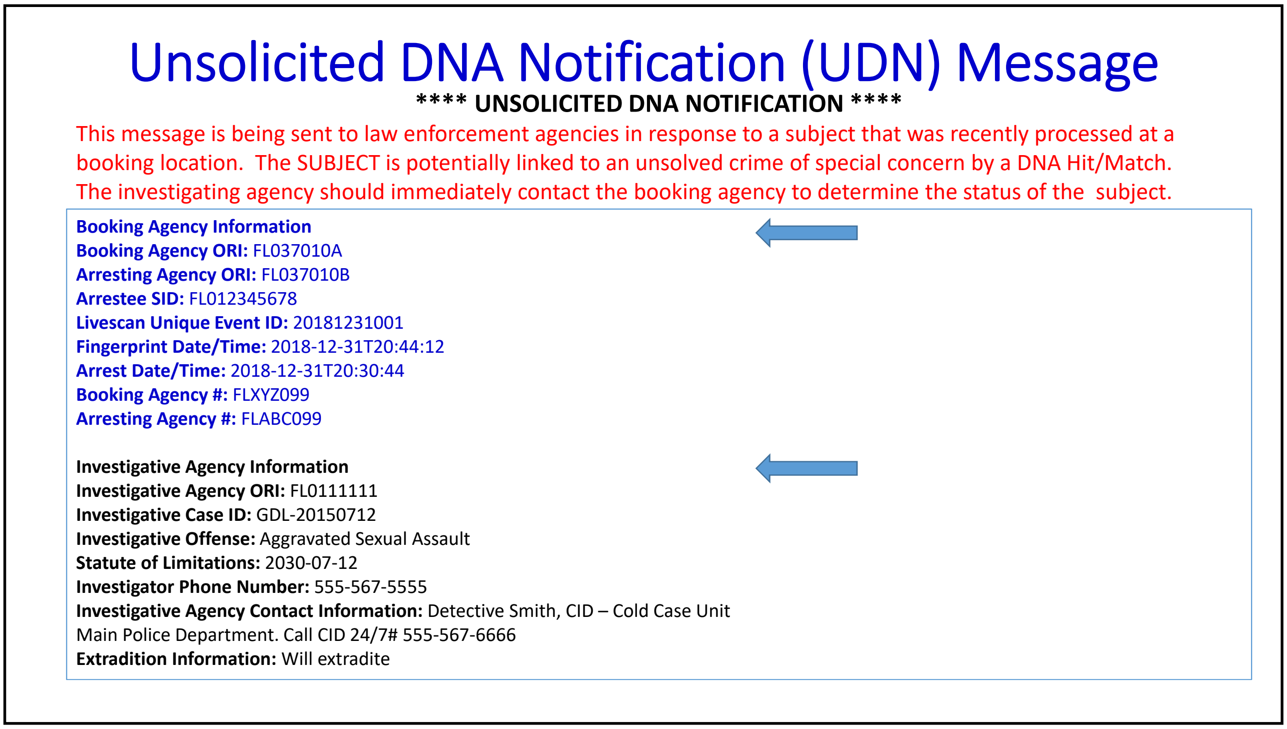
Statute of Limitation - Unlimited

Offense Description – Sexual Assault

Extradition Information – Yes, suspect will be extradited

Investigative Agency Contact Information – RPD 24/7 desk phone (804) 111-2345

UNCLASSIFIED // FOR OFFICIAL USE ONLY



Unsolicited DNA Notification (UDN) Message

****** UNSOLICITED DNA NOTIFICATION ******

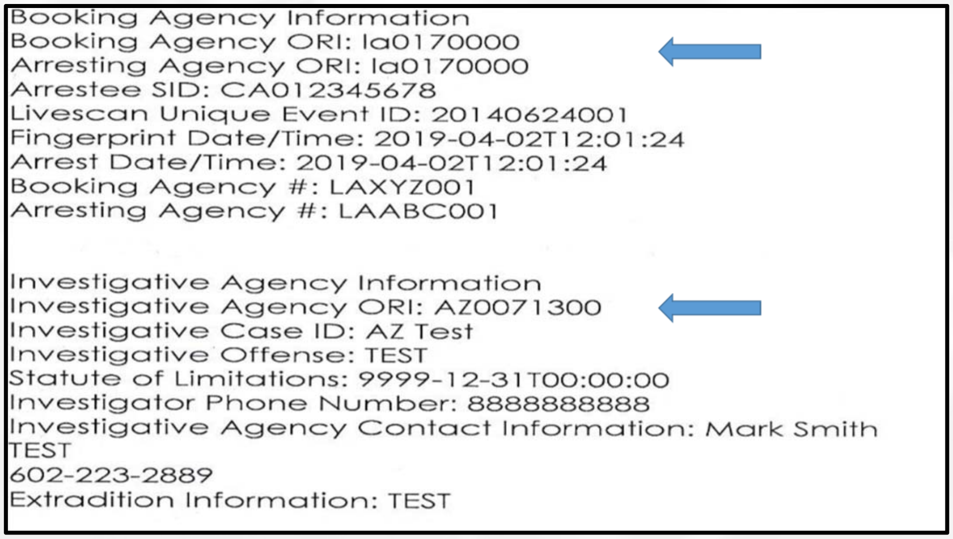
This message is being sent to law enforcement agencies in response to a subject that was recently processed at a booking location. The SUBJECT is potentially linked to an unsolved crime of special concern by a DNA Hit/Match. The investigating agency should immediately contact the booking agency to determine the status of the subject.

Booking Agency Information
Booking Agency ORI: FL037010A
Arresting Agency ORI: FL037010B
Arrestee SID: FL012345678
Livescan Unique Event ID: 20181231001
Fingerprint Date/Time: 2018-12-31T20:44:12
Arrest Date/Time: 2018-12-31T20:30:44
Booking Agency #: FLXYZ099
Arresting Agency #: FLABC099

Investigative Agency Information
Investigative Agency ORI: FL0111111
Investigative Case ID: GDL-20150712
Investigative Offense: Aggravated Sexual Assault
Statute of Limitations: 2030-07-12
Investigator Phone Number: 555-567-5555
Investigative Agency Contact Information: Detective Smith, CID – Cold Case Unit Main Police Department. Call CID 24/7# 555-567-6666
Extradition Information: Will extradite

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UDN Message Transmission Test



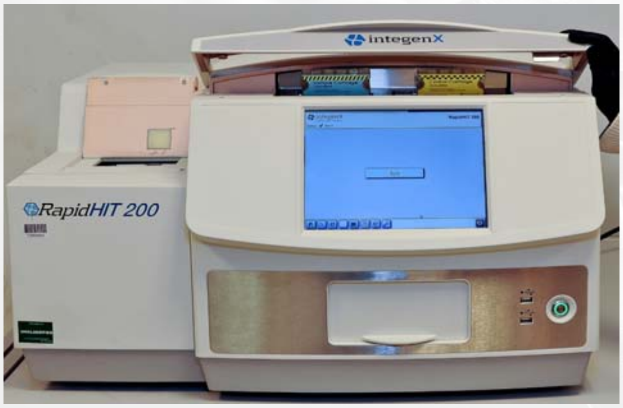
Booking Agency Information
Booking Agency ORI: la0170000
Arresting Agency ORI: la0170000
Arrestee SID: CA012345678
Livescan Unique Event ID: 20140624001
Fingerprint Date/Time: 2019-04-02T12:01:24
Arrest Date/Time: 2019-04-02T12:01:24
Booking Agency #: LAXYZ001
Arresting Agency #: LAABC001

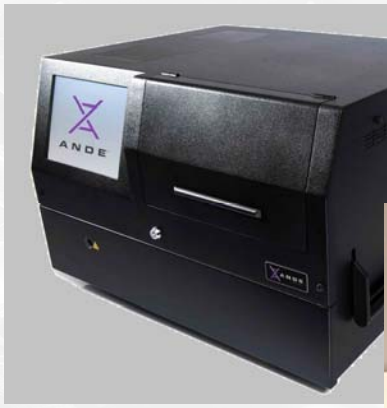
Investigative Agency Information
Investigative Agency ORI: AZ0071300
Investigative Case ID: AZ Test
Investigative Offense: TEST
Statute of Limitations: 9999-12-31T00:00:00
Investigator Phone Number: 8888888888
Investigative Agency Contact Information: Mark Smith
TEST
602-223-2889
Extradition Information: TEST

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

CURRENT RAPID DNA MACHINES





UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY: The information in this document is the property of the Federal Bureau of Investigation and may be distributed to government (federal, state, tribal, or local) employees and information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). Dissemination to the public, the media, or other personnel who do not have a valid need to know without prior ap prohibited. Precautions must be taken to ensure this information is controlled, stored, handled, transmitted, distributed, and disposed of in a manner that precludes unauthorized access.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

NDIS Statistics

Totals Through October 31, 2019

Category	***Total Number of Profiles***
Convicted Offender	**13,880,381**
Arrestees	**3,760,209**
Detainees	**28,378**
Legal	**104,924**
Forensic	**979,841**
Total Offender	**17,773,892**
Total Forensic	**966,782**
Total Profiles	**18,593,420**

Through October 31, 2019

- **477,812** Investigations Aided
- **357,782** Offender Hits
  - Crime scene to offender within a state
- **55,055** National Offender Hits
  - Crime scene in one state to an offender in another state
- **75,481** Forensic Hits
  - Crime scene to crime scene

*Numbers represent confirmed matches where CODIS helped provide new information to a case

Number of Profiles added in 2018:

497,940 Convicted Offender Profiles
440,314 Arrestee Profiles
84,059 Forensic Profiles
48,814 Investigations Aided

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

115TH CONGRESS
1ST SESSION

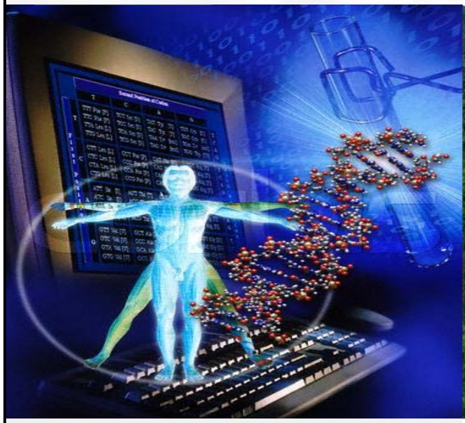
S. 139

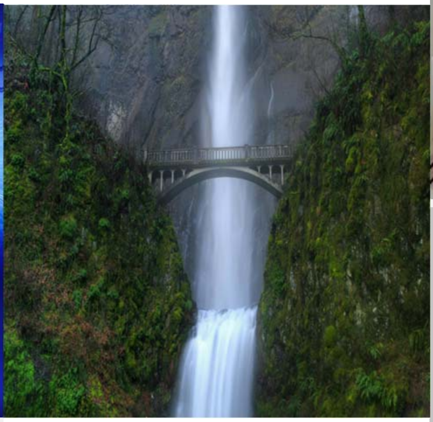
AN ACT

To implement the use of Rapid DNA instruments to inform decisions about pretrial release or detention and their conditions, to solve and prevent violent crimes and other crimes, to exonerate the innocent, to prevent DNA analysis backlogs, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

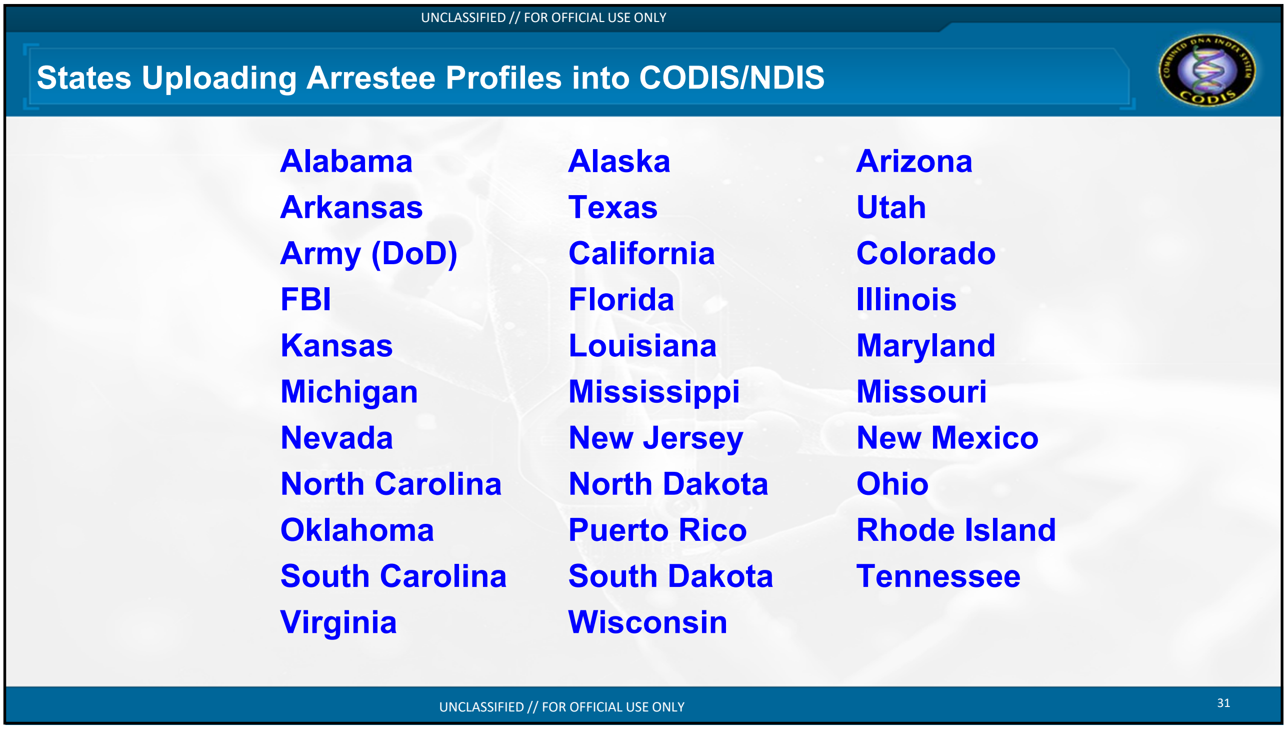




"(3) The term 'Rapid DNA instruments' means instrumentation that carries out a fully automated process to derive a DNA analysis from a DNA sample.".

Passed the Senate May 16, 2017.

UNCLASSIFIED // FOR OFFICIAL USE ONLY



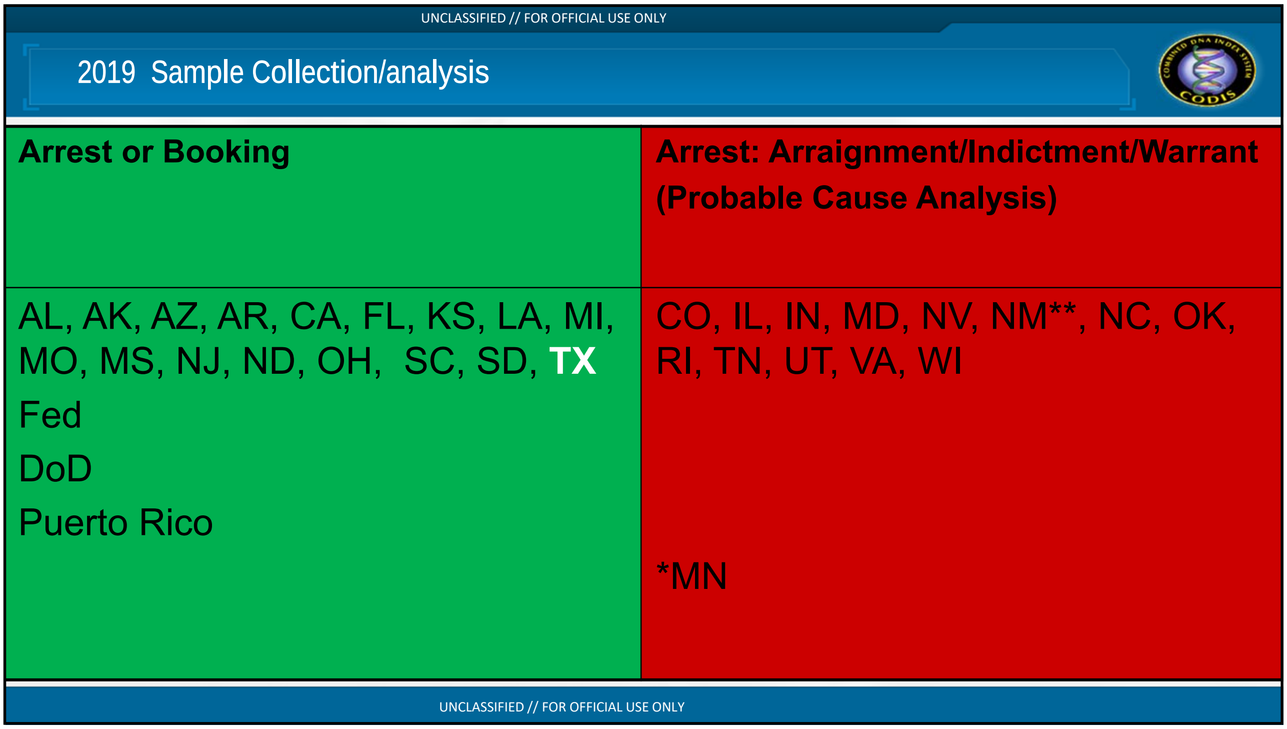
UNCLASSIFIED // FOR OFFICIAL USE ONLY

States Uploading Arrestee Profiles into CODIS/NDIS

Alabama	Alaska	Arizona
Arkansas	Texas	Utah
Army (DoD)	California	Colorado
FBI	Florida	Illinois
Kansas	Louisiana	Maryland
Michigan	Mississippi	Missouri
Nevada	New Jersey	New Mexico
North Carolina	North Dakota	Ohio
Oklahoma	Puerto Rico	Rhode Island
South Carolina	South Dakota	Tennessee
Virginia	Wisconsin	

UNCLASSIFIED // FOR OFFICIAL USE ONLY

31

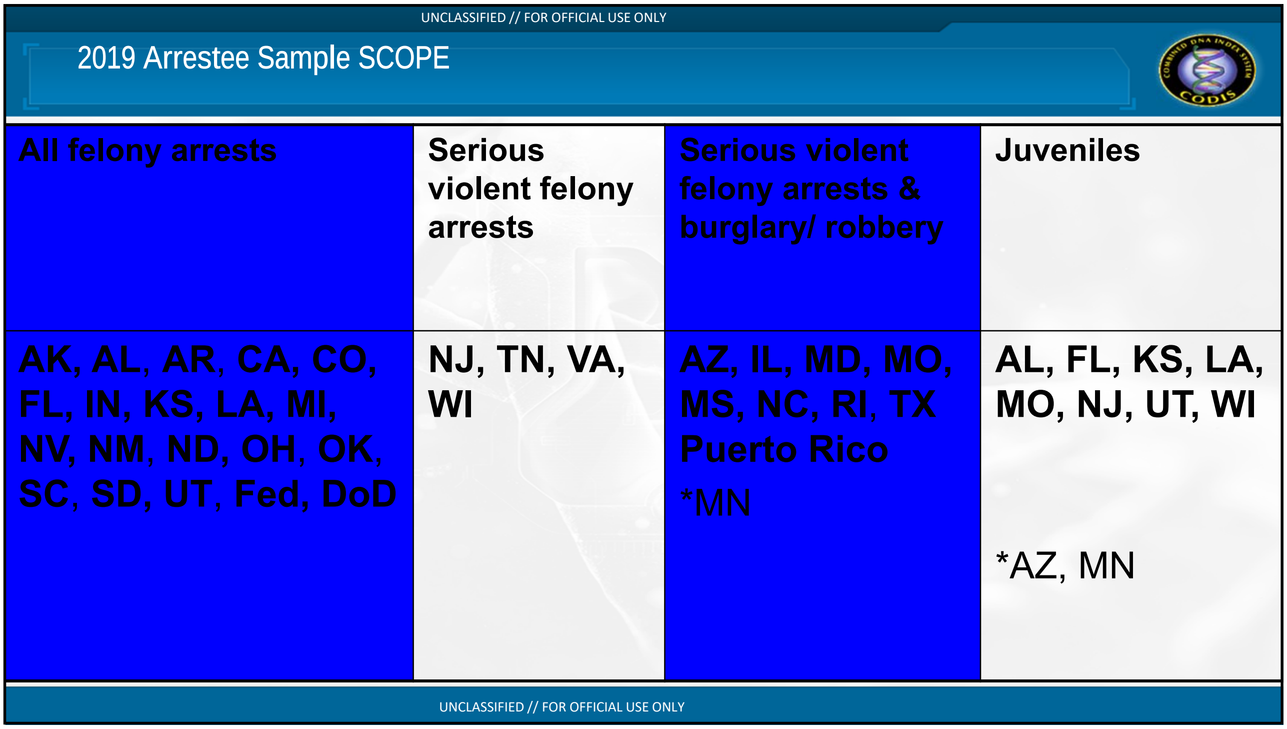


UNCLASSIFIED // FOR OFFICIAL USE ONLY

2019 Sample Collection/analysis

Arrest or Booking	**Arrest: Arraignment/Indictment/Warrant (Probable Cause Analysis)**
AL, AK, AZ, AR, CA, FL, KS, LA, MI, MO, MS, NJ, ND, OH, SC, SD, **TX** Fed DoD Puerto Rico	CO, IL, IN, MD, NV, NM**, NC, OK, RI, TN, UT, VA, WI *MN

UNCLASSIFIED // FOR OFFICIAL USE ONLY

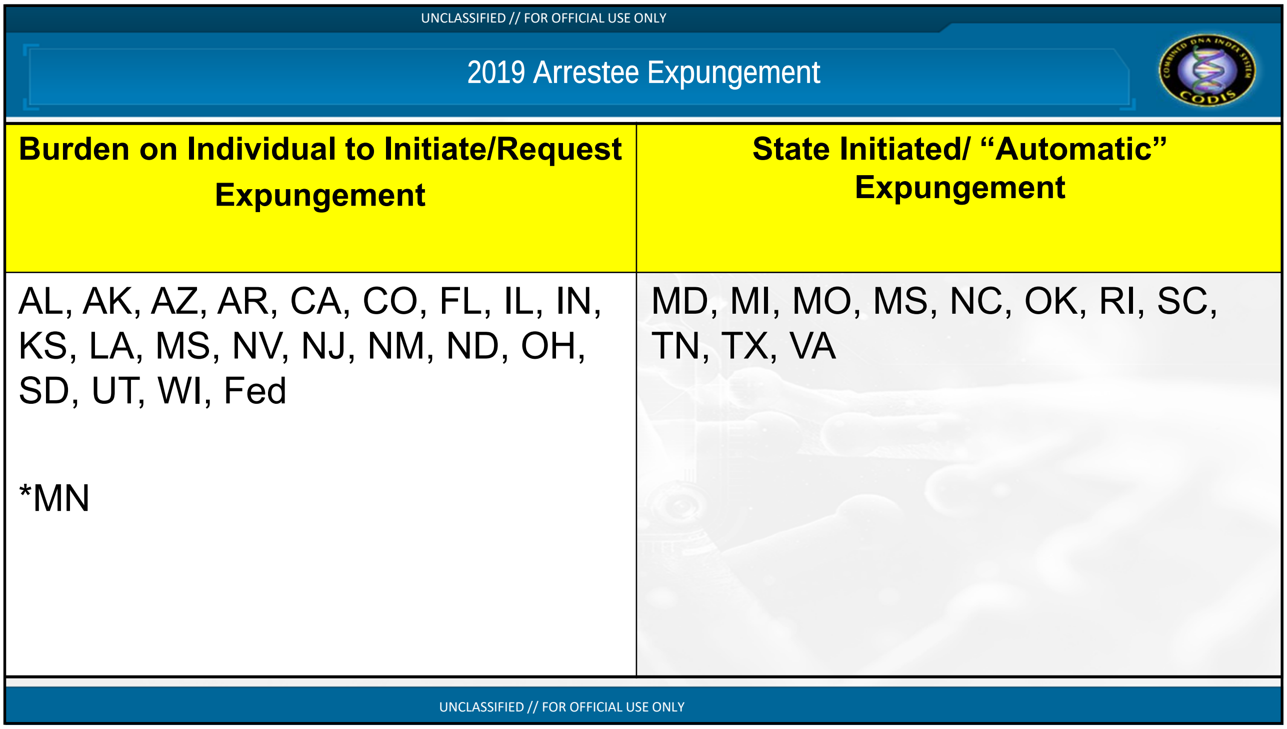


UNCLASSIFIED // FOR OFFICIAL USE ONLY

2019 Arrestee Sample SCOPE

All felony arrests	Serious violent felony arrests	Serious violent felony arrests & burglary/ robbery	Juveniles
AK, AL, AR, CA, CO, FL, IN, KS, LA, MI, NV, NM, ND, OH, OK, SC, SD, UT, Fed, DoD	NJ, TN, VA, WI	AZ, IL, MD, MO, MS, NC, RI, TX Puerto Rico *MN	AL, FL, KS, LA, MO, NJ, UT, WI *AZ, MN

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

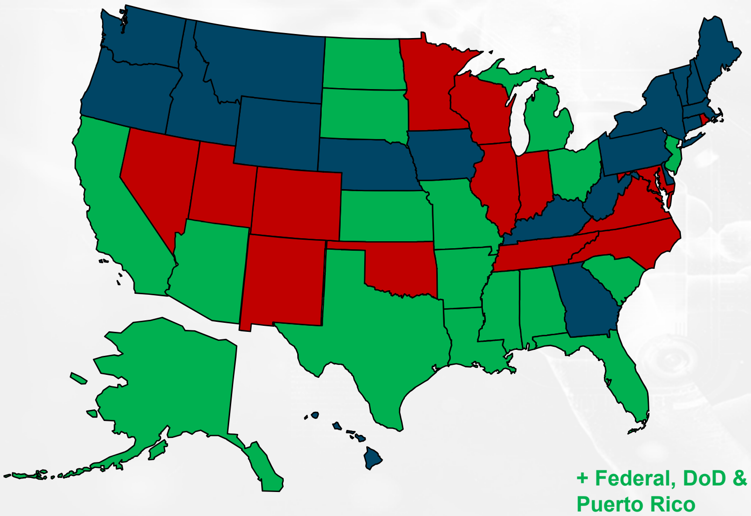
2019 Arrestee Expungement

Burden on Individual to Initiate/Request Expungement	State Initiated/ “Automatic” Expungement
AL, AK, AZ, AR, CA, CO, FL, IL, IN, KS, LA, MS, NV, NJ, NM, ND, OH, SD, UT, WI, Fed *MN	MD, MI, MO, MS, NC, OK, RI, SC, TN, TX, VA

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED

States with Arrestee Collection Laws



🟩 Collection at Arrest or Booking

🟥 Collection and/or Analysis Arraignment/Indictment/Warrant (Probable Cause Analysis)

■ No Arrestee Law

+ Federal, DoD & Puerto Rico

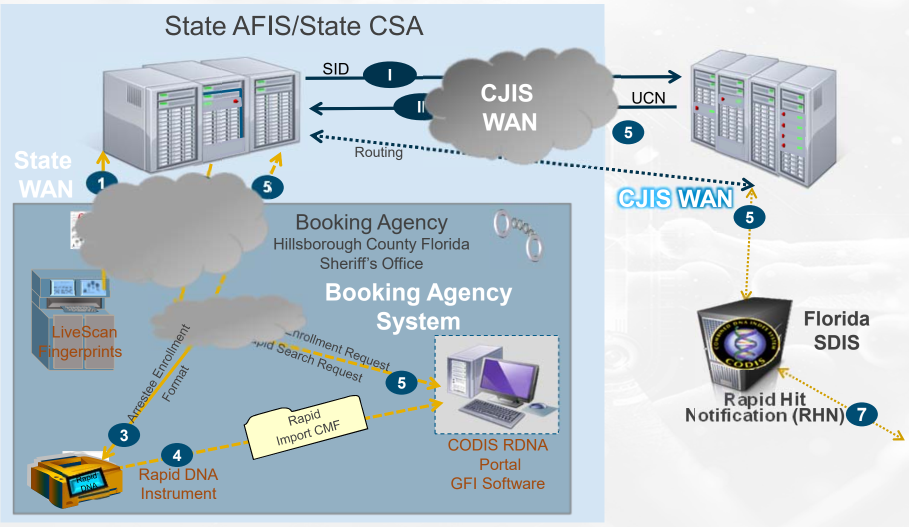
As of 11/06/2019

UNCLASSIFIED

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Booking Environment

Enrollment of Known DNA from Arrest Event



State AFIS/State CSA

SID I

II

CJIS WAN

UCN

5

Routing

State WAN

1

5

CJIS WAN

5

Booking Agency
Hillsborough County Florida
Sheriff's Office

Booking Agency System

LiveScan Fingerprints

Arrestee Enrollment Format

Enrollment Request

Rapid Search Request

5

3

4

Rapid Import CMF

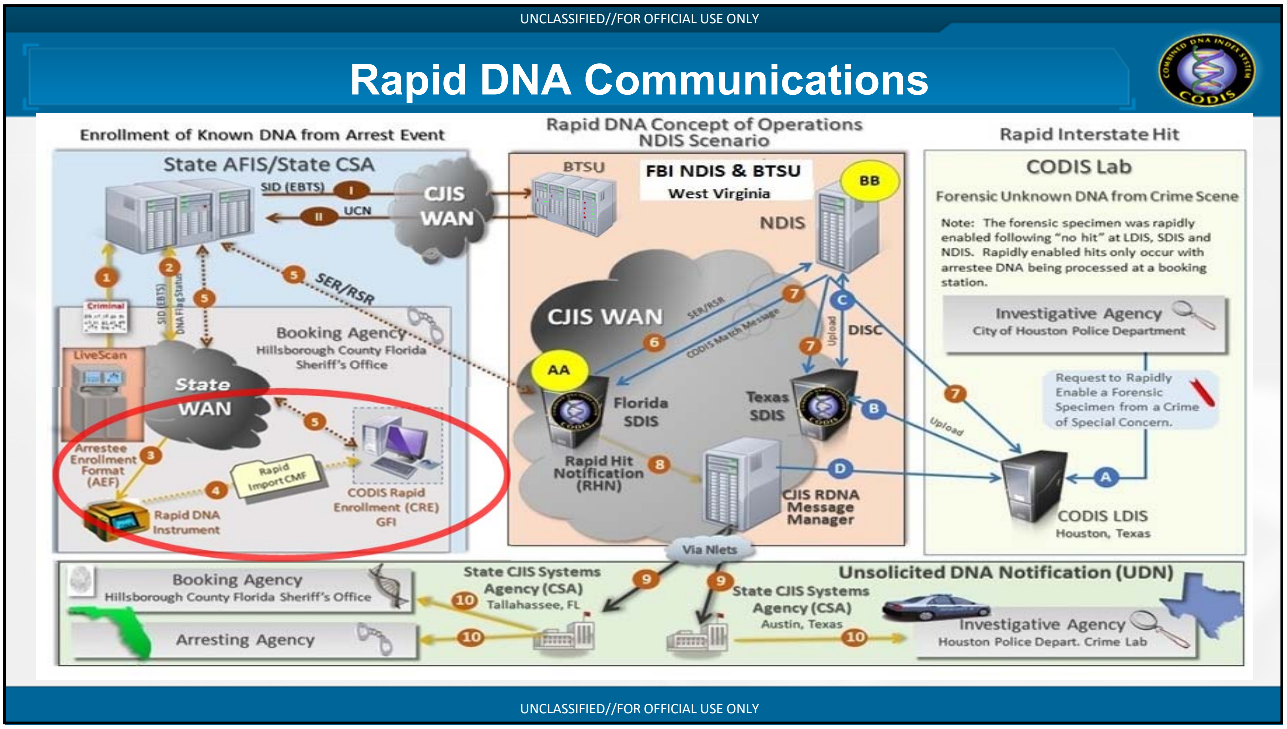
Rapid DNA Instrument

CODIS RDNA Portal
GFI Software

Florida SDIS

Rapid Hit Notification (RHN) 7

UNCLASSIFIED // FOR OFFICIAL USE ONLY



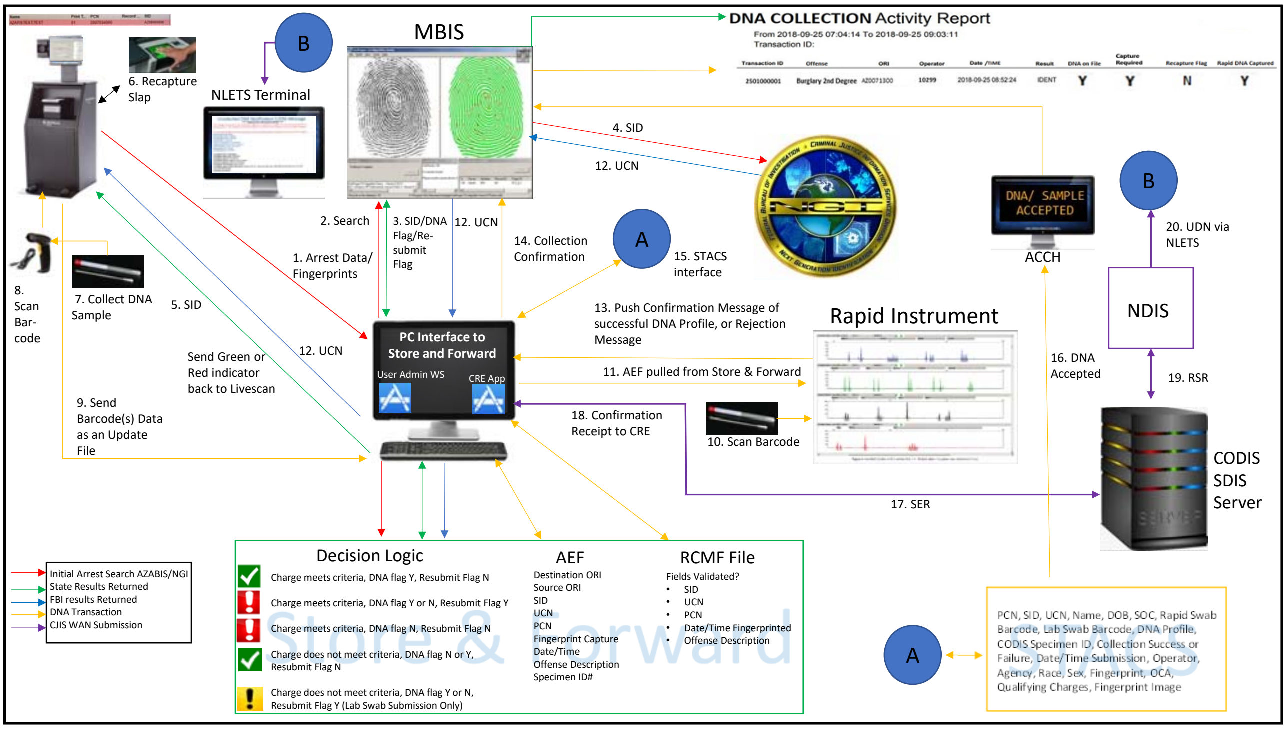
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Rapid DNA Communications

Enrollment of Known DNA from Arrest Event
Rapid DNA Concept of Operations
NDIS Scenario
Rapid Interstate Hit
State AFIS/State CSA
SID (EBTS)
I
UCN
II
CJIS WAN
BTSU
FBI NDIS & BTSU
West Virginia
BB
NDIS
CODIS Lab
Forensic Unknown DNA from Crime Scene
1
2
Criminal
SID (EBTS)
DNA Flag Status
5
SER/RSR
LiveScan
Booking Agency
Hillsborough County Florida Sheriff's Office
State WAN
Arrestee Enrollment Format (AEF)
3
4
Rapid Import CMF
CODIS Rapid Enrollment (CRE) GFI
Rapid DNA Instrument
CJIS WAN
SER/RSR
CODIS Match Message
6
7
C
Upload
DISC
AA
Florida SDIS
Texas SDIS
B
Rapid Hit Notification (RHN)
8
D
CJIS RDNA Message Manager
Investigative Agency
City of Houston Police Department
Request to Rapidly Enable a Forensic Specimen from a Crime of Special Concern.
7
Upload
A
CODIS LDIS
Houston, Texas
Via Nlets
Booking Agency
Hillsborough County Florida Sheriff's Office
State CJIS Systems Agency (CSA)
Tallahassee, FL
9
10
Arresting Agency
10
9
State CJIS Systems Agency (CSA)
Austin, Texas
Unsolicited DNA Notification (UDN)
Investigative Agency
Houston Police Depart. Crime Lab
10

Note: The forensic specimen was rapidly enabled following "no hit" at LDIS, SDIS and NDIS. Rapidly enabled hits only occur with arrestee DNA being processed at a booking station.

UNCLASSIFIED//FOR OFFICIAL USE ONLY



6. Recapture Slap
B
NLETS Terminal
MBIS
8. Scan Bar-code
7. Collect DNA Sample
5. SID
1. Arrest Data/ Fingerprints
2. Search
3. SID/DNA Flag/Re-submit Flag
12. UCN
4. SID
12. UCN
14. Collection Confirmation
A
15. STACS interface
12. UCN
Send Green or Red indicator back to Livescan
9. Send Barcode(s) Data as an Update File
PC Interface to Store and Forward
User Admin WS
CRE App
13. Push Confirmation Message of successful DNA Profile, or Rejection Message
11. AEF pulled from Store & Forward
18. Confirmation Receipt to CRE
10. Scan Barcode
Rapid Instrument
DNA/ SAMPLE ACCEPTED
ACCH
B
20. UDN via NLETS
NDIS
16. DNA Accepted
19. RSR
17. SER
CODIS SDIS Server
A
Store & Forward
STACS

DNA COLLECTION Activity Report

From 2018-09-25 07:04:14 To 2018-09-25 09:03:11
Transaction ID:

Transaction ID	Offense	ORI	Operator	Date /TIME	Result	DNA on File	Capture Required	Recapture Flag	Rapid DNA Captured
2501000001	Burglary 2nd Degree	AZ0071300	10299	2018-09-25 08:52:24	IDENT	Y	Y	N	Y

- 🟥 Initial Arrest Search AZABIS/NGI
- 🟩 State Results Returned
- 🟦 FBI results Returned
- 🟨 DNA Transaction
- 🟪 CJIS WAN Submission

Decision Logic

- ✓ Charge meets criteria, DNA flag Y, Resubmit Flag N
- ! Charge meets criteria, DNA flag Y or N, Resubmit Flag Y
- ! Charge meets criteria, DNA flag N, Resubmit Flag N
- ✓ Charge does not meet criteria, DNA flag N or Y, Resubmit Flag N
- ! Charge does not meet criteria, DNA flag Y or N, Resubmit Flag Y (Lab Swab Submission Only)

AEF

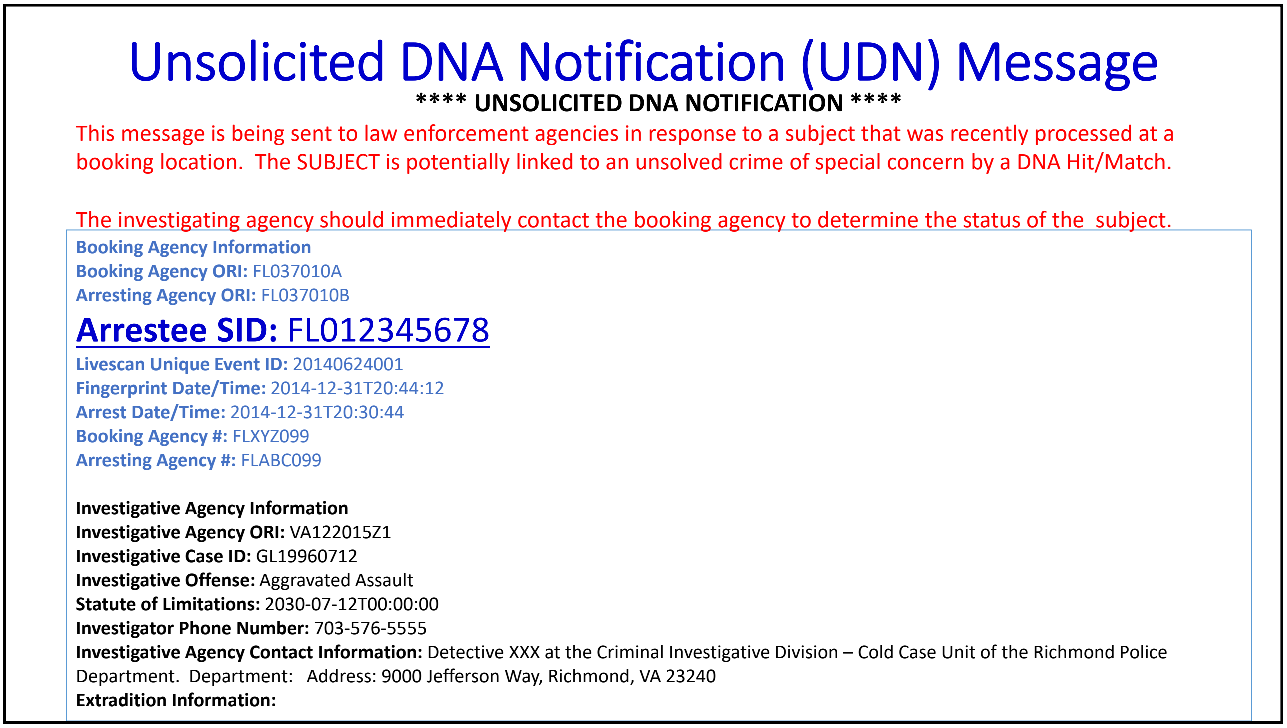
Destination ORI
Source ORI
SID
UCN
PCN
Fingerprint Capture Date/Time
Offense Description
Specimen ID#

RCMF File

Fields Validated?

- SID
- UCN
- PCN
- Date/Time Fingerprinted
- Offense Description

PCN, SID, UCN, Name, DOB, SOC, Rapid Swab Barcode, Lab Swab Barcode, DNA Profile, CODIS Specimen ID, Collection Success or Failure, Date/Time Submission, Operator, Agency, Race, Sex, Fingerprint, OCA, Qualifying Charges, Fingerprint Image



Unsolicited DNA Notification (UDN) Message

****** UNSOLICITED DNA NOTIFICATION ******

This message is being sent to law enforcement agencies in response to a subject that was recently processed at a booking location. The SUBJECT is potentially linked to an unsolved crime of special concern by a DNA Hit/Match.

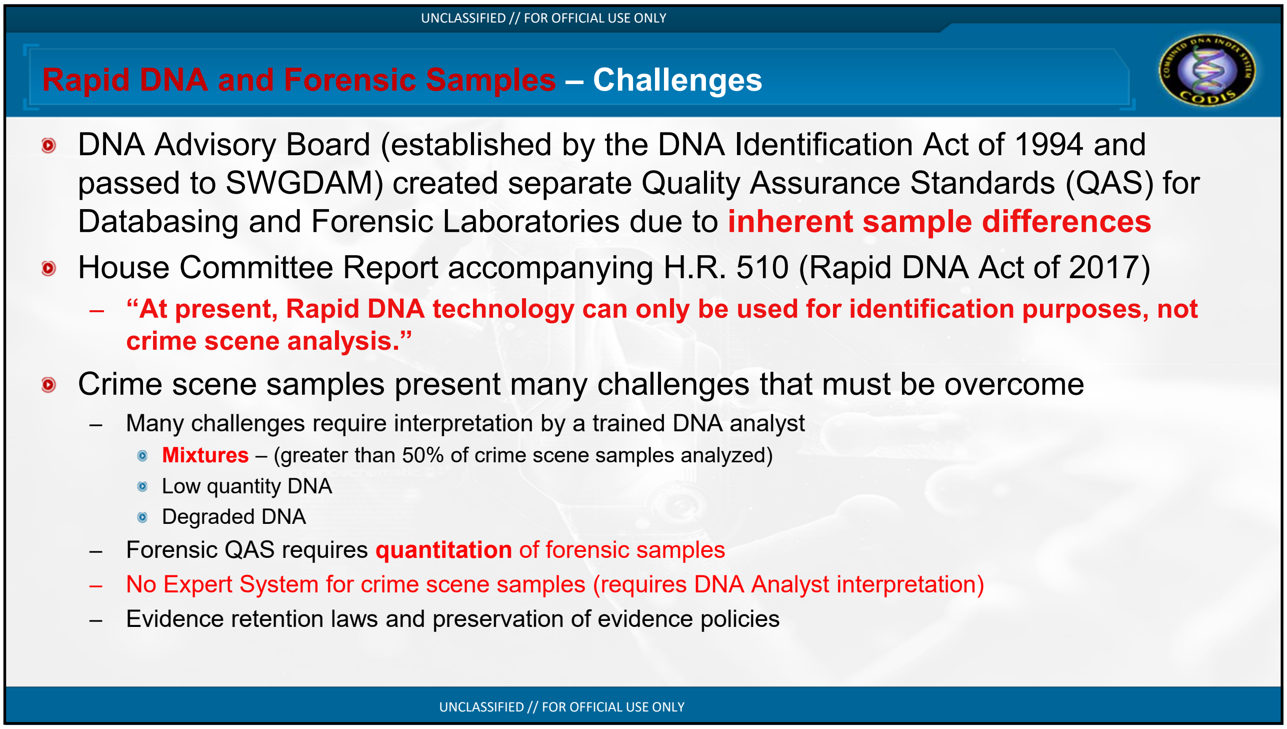
The investigating agency should immediately contact the booking agency to determine the status of the subject.

Booking Agency Information
Booking Agency ORI: FL037010A
Arresting Agency ORI: FL037010B

Arrestee SID: FL012345678

Livescan Unique Event ID: 20140624001
Fingerprint Date/Time: 2014-12-31T20:44:12
Arrest Date/Time: 2014-12-31T20:30:44
Booking Agency #: FLXYZ099
Arresting Agency #: FLABC099

Investigative Agency Information
Investigative Agency ORI: VA122015Z1
Investigative Case ID: GL19960712
Investigative Offense: Aggravated Assault
Statute of Limitations: 2030-07-12T00:00:00
Investigator Phone Number: 703-576-5555
Investigative Agency Contact Information: Detective XXX at the Criminal Investigative Division – Cold Case Unit of the Richmond Police Department. Department: Address: 9000 Jefferson Way, Richmond, VA 23240
Extradition Information:

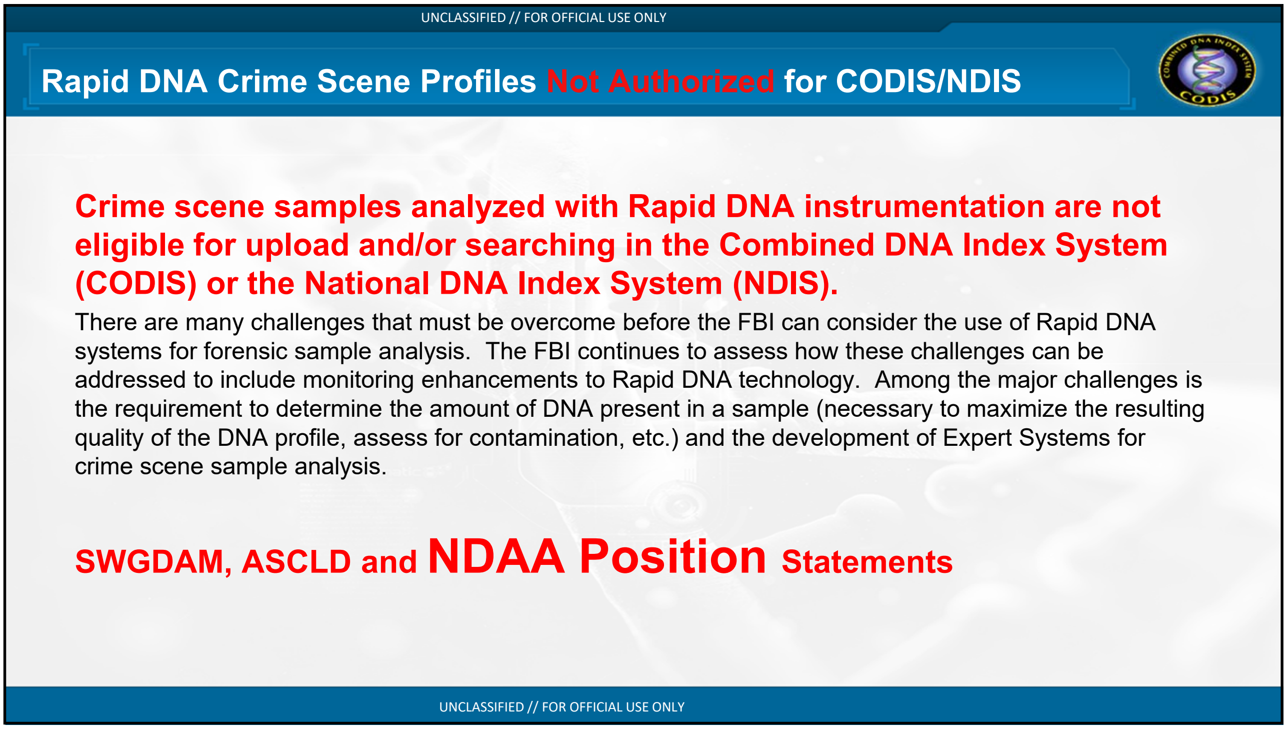


UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA and Forensic Samples – Challenges

- DNA Advisory Board (established by the DNA Identification Act of 1994 and passed to SWGDAM) created separate Quality Assurance Standards (QAS) for Databasing and Forensic Laboratories due to **inherent sample differences**
- House Committee Report accompanying H.R. 510 (Rapid DNA Act of 2017)
  - **"At present, Rapid DNA technology can only be used for identification purposes, not crime scene analysis."**
- Crime scene samples present many challenges that must be overcome
  - Many challenges require interpretation by a trained DNA analyst
    - **Mixtures** – (greater than 50% of crime scene samples analyzed)
    - Low quantity DNA
    - Degraded DNA
  - Forensic QAS requires **quantitation** of forensic samples
  - No Expert System for crime scene samples (requires DNA Analyst interpretation)
  - Evidence retention laws and preservation of evidence policies

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

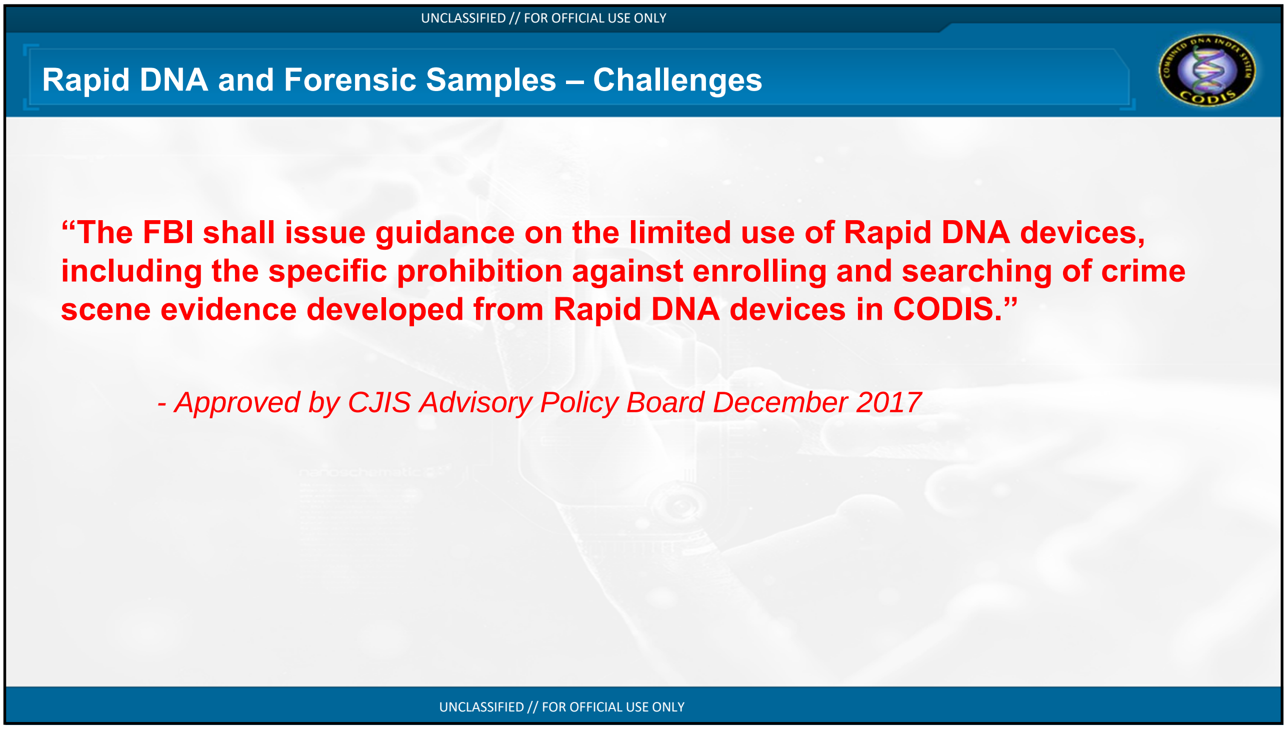
Rapid DNA Crime Scene Profiles Not Authorized for CODIS/NDIS

Crime scene samples analyzed with Rapid DNA instrumentation are not eligible for upload and/or searching in the Combined DNA Index System (CODIS) or the National DNA Index System (NDIS).

There are many challenges that must be overcome before the FBI can consider the use of Rapid DNA systems for forensic sample analysis. The FBI continues to assess how these challenges can be addressed to include monitoring enhancements to Rapid DNA technology. Among the major challenges is the requirement to determine the amount of DNA present in a sample (necessary to maximize the resulting quality of the DNA profile, assess for contamination, etc.) and the development of Expert Systems for crime scene sample analysis.

SWGDAM, ASCLD and NDAA Position Statements

UNCLASSIFIED // FOR OFFICIAL USE ONLY



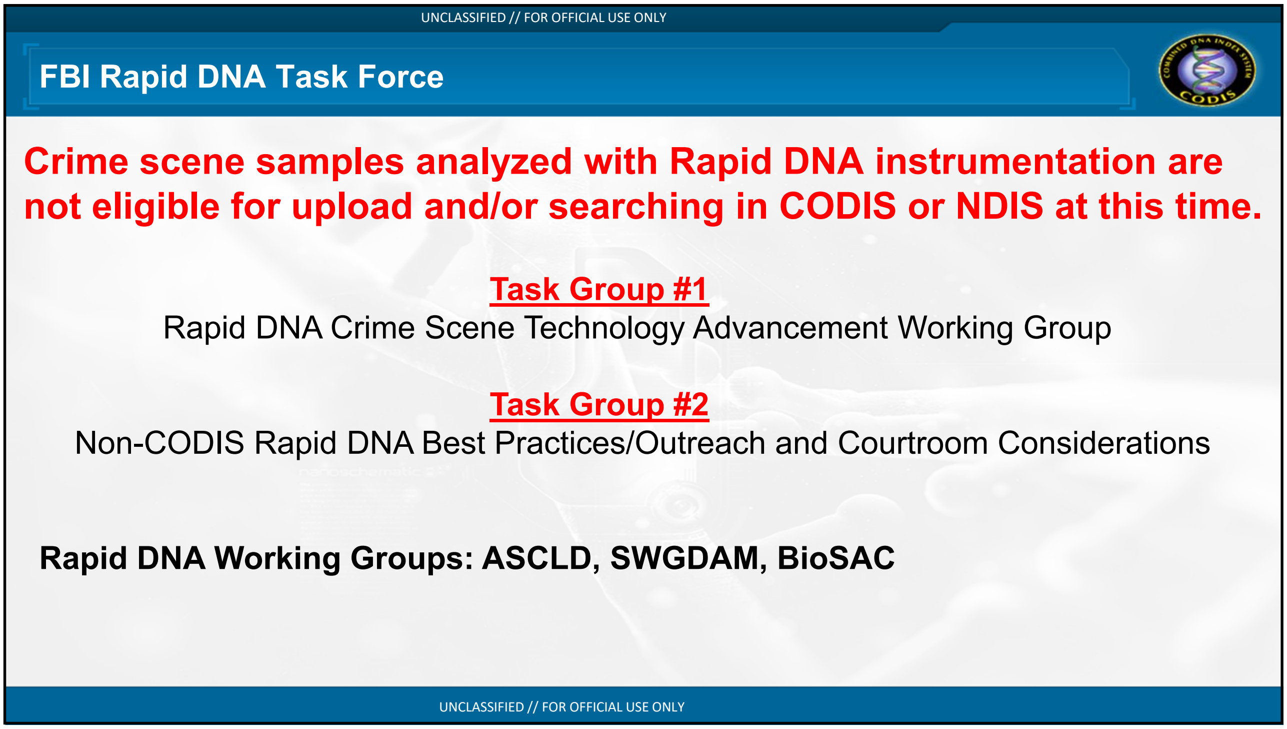
UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA and Forensic Samples – Challenges

"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."

- Approved by CJIS Advisory Policy Board December 2017

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

FBI Rapid DNA Task Force

Crime scene samples analyzed with Rapid DNA instrumentation are not eligible for upload and/or searching in CODIS or NDIS at this time.

Task Group #1

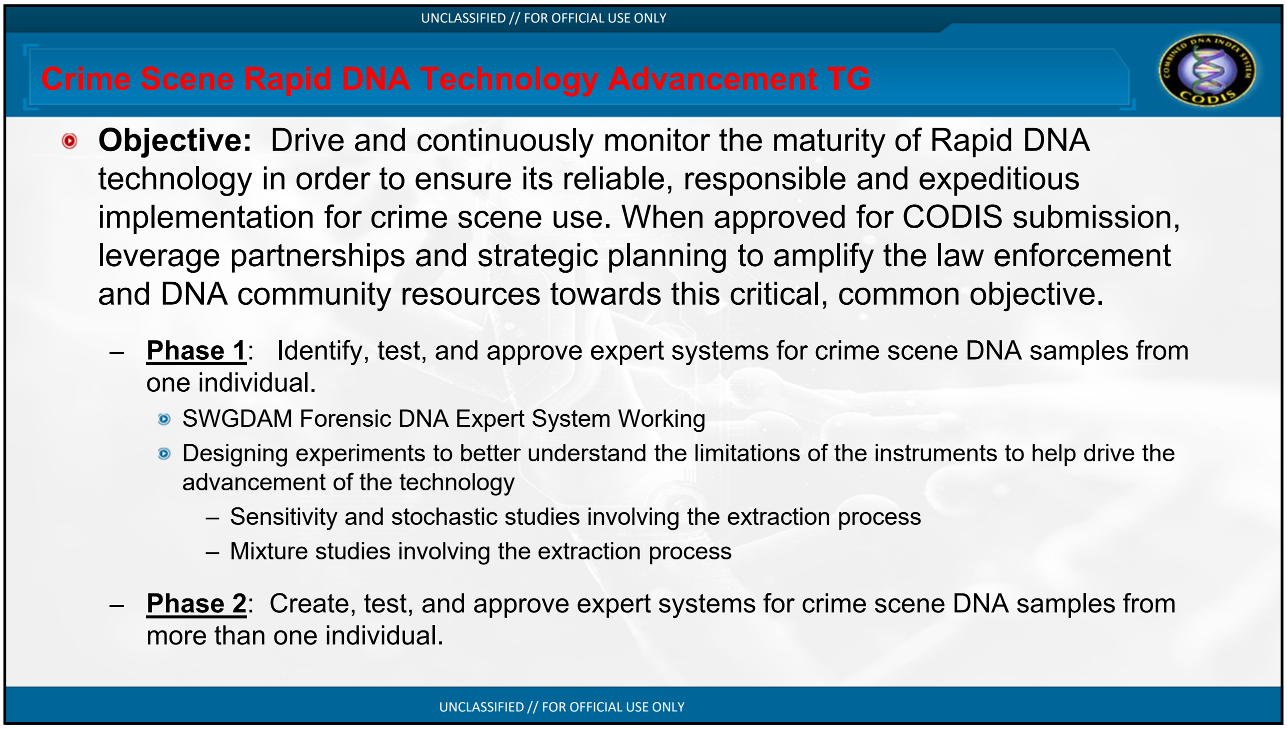
Rapid DNA Crime Scene Technology Advancement Working Group

Task Group #2

Non-CODIS Rapid DNA Best Practices/Outreach and Courtroom Considerations

Rapid DNA Working Groups: ASCLD, SWGDAM, BioSAC

UNCLASSIFIED // FOR OFFICIAL USE ONLY

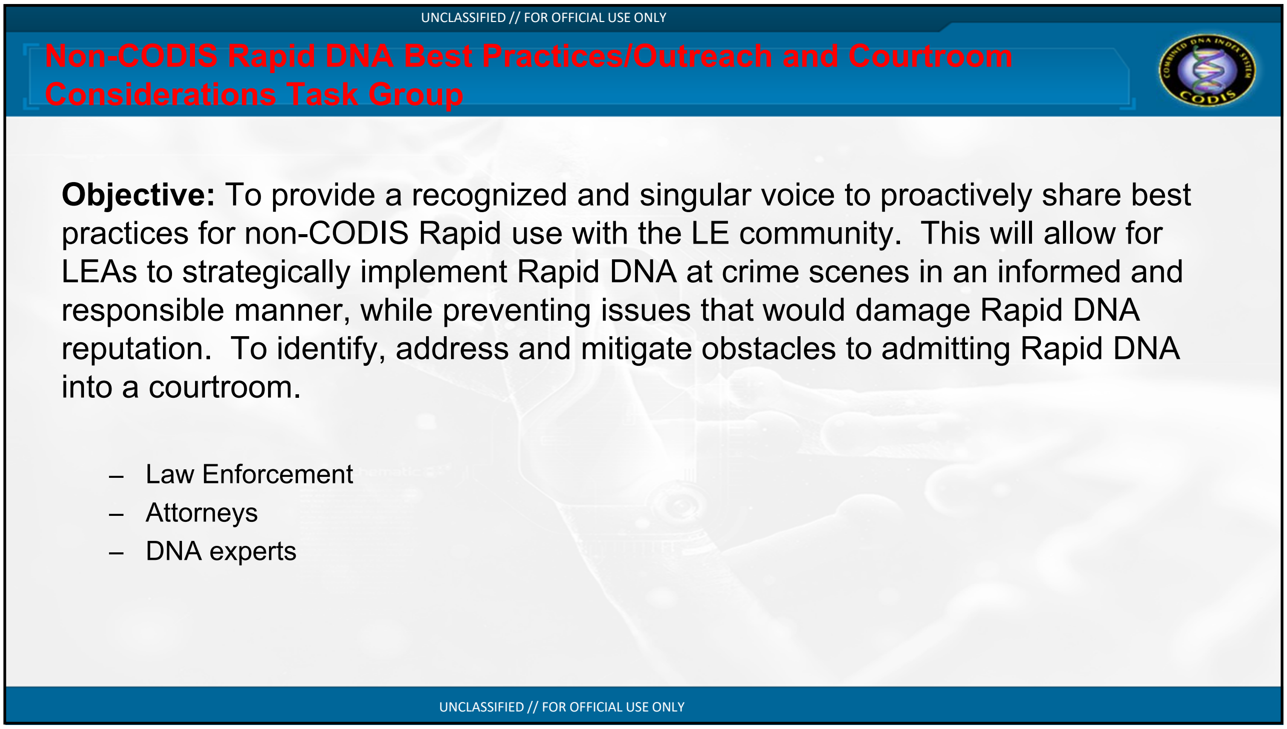


UNCLASSIFIED // FOR OFFICIAL USE ONLY

Crime Scene Rapid DNA Technology Advancement TG

- **Objective:** Drive and continuously monitor the maturity of Rapid DNA technology in order to ensure its reliable, responsible and expeditious implementation for crime scene use. When approved for CODIS submission, leverage partnerships and strategic planning to amplify the law enforcement and DNA community resources towards this critical, common objective.
  - **Phase 1**: Identify, test, and approve expert systems for crime scene DNA samples from one individual.
    - SWGDAM Forensic DNA Expert System Working
    - Designing experiments to better understand the limitations of the instruments to help drive the advancement of the technology
      - Sensitivity and stochastic studies involving the extraction process
      - Mixture studies involving the extraction process
  - **Phase 2**: Create, test, and approve expert systems for crime scene DNA samples from more than one individual.

UNCLASSIFIED // FOR OFFICIAL USE ONLY



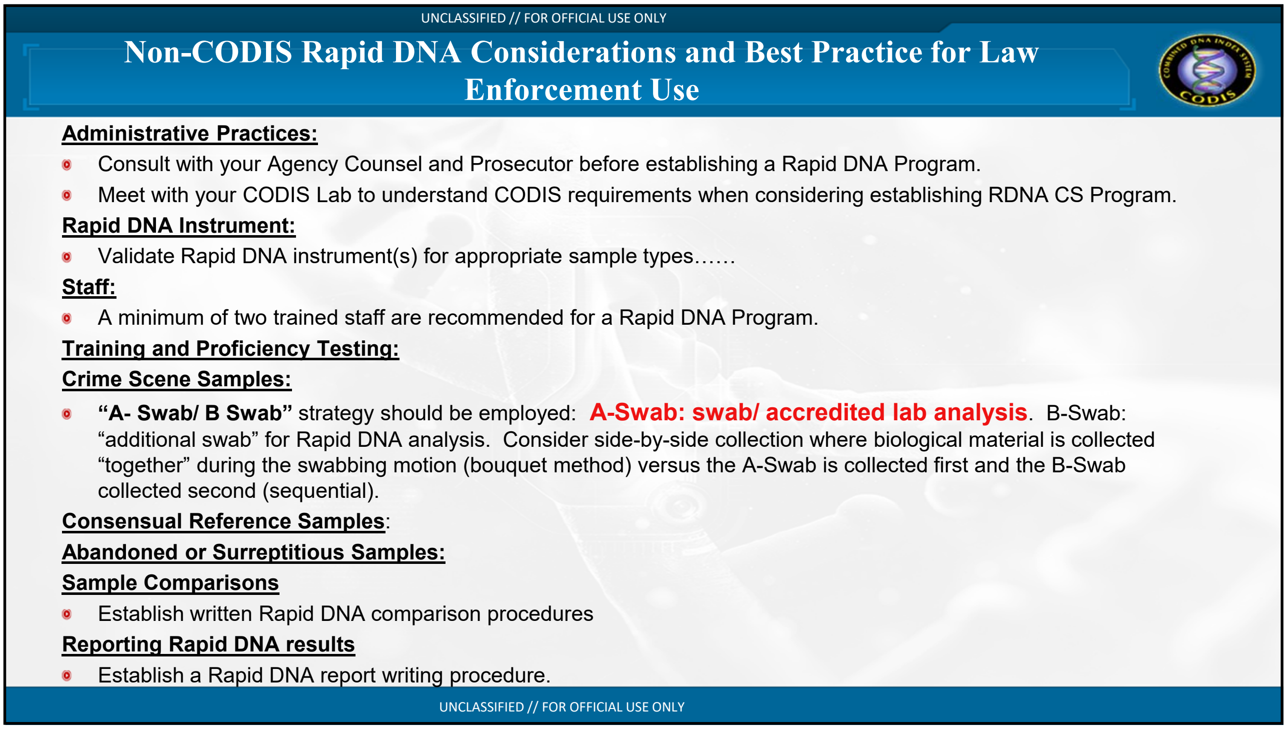
UNCLASSIFIED // FOR OFFICIAL USE ONLY

Non-CODIS Rapid DNA Best Practices/Outreach and Courtroom Considerations Task Group

Objective: To provide a recognized and singular voice to proactively share best practices for non-CODIS Rapid use with the LE community. This will allow for LEAs to strategically implement Rapid DNA at crime scenes in an informed and responsible manner, while preventing issues that would damage Rapid DNA reputation. To identify, address and mitigate obstacles to admitting Rapid DNA into a courtroom.

- Law Enforcement
- Attorneys
- DNA experts

UNCLASSIFIED // FOR OFFICIAL USE ONLY



UNCLASSIFIED // FOR OFFICIAL USE ONLY

Non-CODIS Rapid DNA Considerations and Best Practice for Law Enforcement Use

Administrative Practices:

- Consult with your Agency Counsel and Prosecutor before establishing a Rapid DNA Program.
- Meet with your CODIS Lab to understand CODIS requirements when considering establishing RDNA CS Program.

Rapid DNA Instrument:

- Validate Rapid DNA instrument(s) for appropriate sample types……

Staff:

- A minimum of two trained staff are recommended for a Rapid DNA Program.

Training and Proficiency Testing:

Crime Scene Samples:

- **"A- Swab/ B Swab"** strategy should be employed: **A-Swab: swab/ accredited lab analysis**. B-Swab: "additional swab" for Rapid DNA analysis. Consider side-by-side collection where biological material is collected "together" during the swabbing motion (bouquet method) versus the A-Swab is collected first and the B-Swab collected second (sequential).

Consensual Reference Samples:

Abandoned or Surreptitious Samples:

Sample Comparisons

- Establish written Rapid DNA comparison procedures

Reporting Rapid DNA results

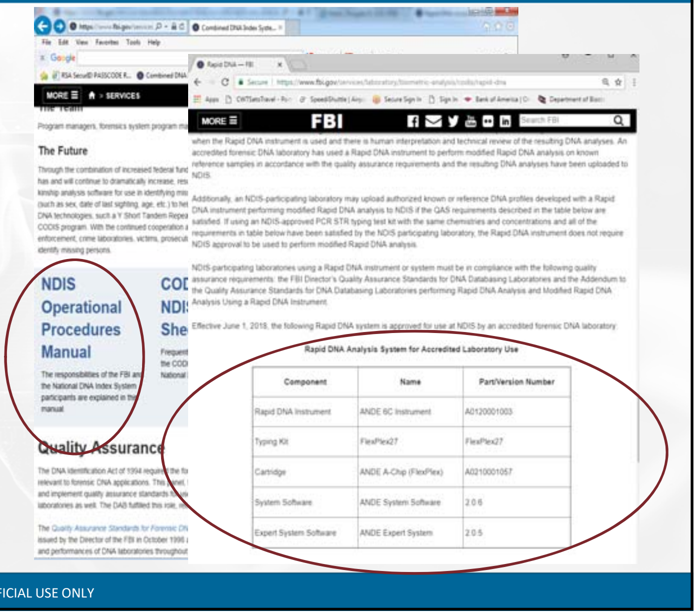
- Establish a Rapid DNA report writing procedure.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NDIS Procedures on Rapid DNA

- Rapid DNA System is a **fully automated** combination of
  - STR Kit/Rapid DNA Cartridge (chemistry)
  - Instrument (hands)
  - Expert System (brain)
    - **No Manual interpretation**
- NDIS approval of first Rapid DNA System for use in an **accredited laboratory** for **known reference buccal swabs** that contains the 20 CODIS core loci on June 1, 2018



MORE ☰
SERVICES
Rapid DNA — FBI
https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna
FBI
Search FBI

Program managers, forensics system program ma

The Future

Through the combination of increased federal fund has and will continue to dramatically increase, res kinship analysis software for use in identifying mis (such as sex, date of last sighting, age, etc.) to he DNA technologies, such a Y Short Tandem Repea CODIS program. With the continued cooperation a enforcement, crime laboratories, victims, prosecut identify missing persons.

NDIS Operational Procedures Manual

The responsibilities of the FBI and the National DNA Index System participants are explained in the manual.

Quality Assurance

The DNA Identification Act of 1994 required the fo relevant to forensic DNA applications. This panel, and implement quality assurance standards fo laboratories as well. The DAB fulfilled this role, re

The Quality Assurance Standards for Forensic DN issued by the Director of the FBI in October 1998 and performances of DNA laboratories throughout

when the Rapid DNA instrument is used and there is human interpretation and technical review of the resulting DNA analyses. An accredited forensic DNA laboratory has used a Rapid DNA instrument to perform modified Rapid DNA analysis on known reference samples in accordance with the quality assurance requirements and the resulting DNA analyses have been uploaded to NDIS.

Additionally, an NDIS-participating laboratory may upload authorized known or reference DNA profiles developed with a Rapid DNA instrument performing modified Rapid DNA analysis to NDIS if the QAS requirements described in the table below are satisfied. If using an NDIS-approved PCR STR typing test kit with the same chemistries and concentrations and all of the requirements in table below have been satisfied by the NDIS participating laboratory, the Rapid DNA instrument does not require NDIS approval to be used to perform modified Rapid DNA analysis.

NDIS-participating laboratories using a Rapid DNA instrument or system must be in compliance with the following quality assurance requirements: the FBI Director's Quality Assurance Standards for DNA Databasing Laboratories and the Addendum to the Quality Assurance Standards for DNA Databasing Laboratories performing Rapid DNA Analysis and Modified Rapid DNA Analysis Using a Rapid DNA Instrument.

Effective June 1, 2018, the following Rapid DNA system is approved for use at NDIS by an accredited forensic DNA laboratory.

Rapid DNA Analysis System for Accredited Laboratory Use

Component	Name	Part/Version Number
Rapid DNA Instrument	ANDE 6C Instrument	A0120001003
Typing Kit	FlexPlex27	FlexPlex27
Cartridge	ANDE A-Chip (FlexPlex)	A0210001057
System Software	ANDE System Software	2.0.6
Expert System Software	ANDE Expert System	2.0.5

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA Planning and Implementation Key Points

Crime scene samples analyzed with Rapid DNA instrumentation are not eligible for upload and/or searching in CODIS or NDIS at this time.

Step 1: RDNA System(s) Approved for Accredited NDIS Lab Use
Step 2: RDNA System(s) Approved for Booking Station Pilot Use
Step 3: RDNA System(s) Approved for Routine Booking Station CODIS/NDIS Use

Goals for FBI non-CODIS Rapid DNA Crime Scene Task Force:
Step 4: **Drive Development of Expert Systems for NDIS Lab Crime Scene Use**
Step 5: RDNA System(s) Approved for Accredited NDIS Lab Crime Scene Use
Step 6: RDNA System(s) Approved for Pilot Crime Scene Use
Step 7: RDNA System(s) Approved for Routine Crime Scene Use

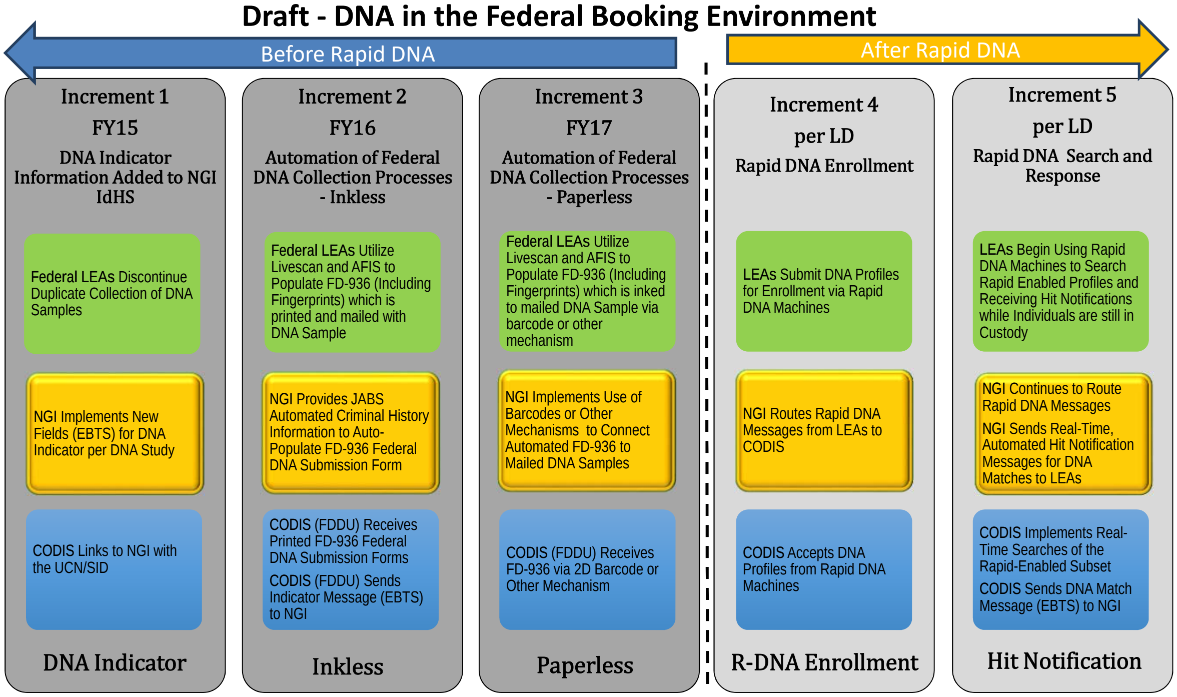
UNCLASSIFIED // FOR OFFICIAL USE ONLY

NGI DNA Indicator Study

Agency	Date of Visit
KY	4/28/2014
LA	5/01/2014
WV	5/05/2014
VA	5/20/2014
FL	5/28/2014
NV	6/03/2014
NM	6/04/2014

Agency	Date of Visit
CA	6/05/2014
TX	6/11/2014
OH	6/19/2014
MI	6/23/2014
ND	6/26/2014
IL	6/26/2014
Army/Navy/AF	7/16/2014

Draft - DNA in the Federal Booking Environment



Before Rapid DNA

After Rapid DNA

Increment 1
FY15
DNA Indicator Information Added to NGI IdHS

Federal LEAs Discontinue Duplicate Collection of DNA Samples

NGI Implements New Fields (EBTS) for DNA Indicator per DNA Study

CODIS Links to NGI with the UCN/SID

DNA Indicator

Increment 2
FY16
Automation of Federal DNA Collection Processes - Inkless

Federal LEAs Utilize Livescan and AFIS to Populate FD-936 (Including Fingerprints) which is printed and mailed with DNA Sample

NGI Provides JABS Automated Criminal History Information to Auto-Populate FD-936 Federal DNA Submission Form

CODIS (FDDU) Receives Printed FD-936 Federal DNA Submission Forms

CODIS (FDDU) Sends Indicator Message (EBTS) to NGI

Inkless

Increment 3
FY17
Automation of Federal DNA Collection Processes - Paperless

Federal LEAs Utilize Livescan and AFIS to Populate FD-936 (Including Fingerprints) which is inked to mailed DNA Sample via barcode or other mechanism

NGI Implements Use of Barcodes or Other Mechanisms to Connect Automated FD-936 to Mailed DNA Samples

CODIS (FDDU) Receives FD-936 via 2D Barcode or Other Mechanism

Paperless

Increment 4
per LD
Rapid DNA Enrollment

LEAs Submit DNA Profiles for Enrollment via Rapid DNA Machines

NGI Routes Rapid DNA Messages from LEAs to CODIS

CODIS Accepts DNA Profiles from Rapid DNA Machines

R-DNA Enrollment

Increment 5
per LD
Rapid DNA Search and Response

LEAs Begin Using Rapid DNA Machines to Search Rapid Enabled Profiles and Receiving Hit Notifications while Individuals are still in Custody

NGI Continues to Route Rapid DNA Messages

NGI Sends Real-Time, Automated Hit Notification Messages for DNA Matches to LEAs

CODIS Implements Real-Time Searches of the Rapid-Enabled Subset

CODIS Sends DNA Match Message (EBTS) to NGI

Hit Notification

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Booking Station Rapid DNA Major Developments

1. 2008 FBI & DoD interest lead to a DoD (DoD/DoJ/DHS) 2009 Development Contract
2. 2009 CJIS Advisory Policy Board Rapid DNA Task Force Recommendation (est. April 2010)
3. NetBio ANDE/DNAScan & IntegenX RapidHIT 200 delivered September 2012 (BCOE)
4. **Rapid DNA Act of 2017 enacted August 18, 2017**
5. 2017 FBI Rapid DNA Booking Station Pilot Steering Comm. (**AZ, CA, FL, LA & TX**)
6. FBI Position on Crime Scene Rapid DNA Analysis for CODIS (October 2017)
7. SWGDAM, ASCLD and NDAA Positions on Crime Scene Rapid DNA Analysis
8. CJIS Advisory Policy Board Dec ‘17: RDNA Crime Scene Education Recommendation to FBI
9. FBI Rapid DNA Symposium 3/’18, est. FBI non-CODIS Crime Scene RDNA Task Force
10. Completion of CODIS 8.0 Rapid DNA software, October 2018 deployment completed

September 2019: FBI WFO uses RDNA to upload and CODIS search of 6 Federal Arrestees

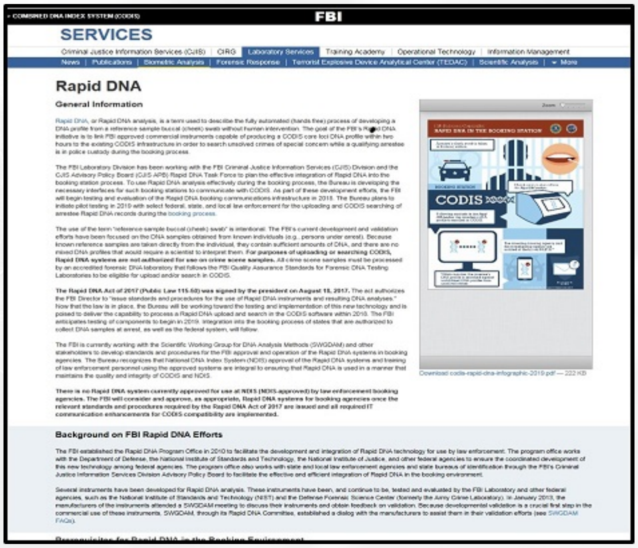
Collaborators: DOD, DHS, NIJ, CJIS APB, SWGDAM, CODIS Community, FBI STB, RDNA Co.’s

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Rapid DNA Webpage on FBI.gov

- Rapid DNA Webpage
- https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna
- RapidDNA@FBI.gov



COMBINED DNA INDEX SYSTEM (CODIS)
FBI
SERVICES
Criminal Justice Information Services (CJIS) | CIRG | Laboratory Services | Training Academy | Operational Technology | Information Management
News | Publications | Biometric Analysis | Forensic Response | Terrorist Explosive Device Analytical Center (TEDAC) | Scientific Analysis | More
Zoom
RAPID DNA IN THE BOOKING STATION
BOOKING STATION
CODIS

Rapid DNA

General Information

Rapid DNA, or Rapid DNA analysis, is a term used to describe the fully automated (hands free) process of developing a DNA profile from a reference sample buccal (cheek) swab without human intervention. The goal of the FBI's Rapid DNA initiative is to link FBI approved commercial instruments capable of producing a CODIS core loci DNA profile within two hours to the existing CODIS infrastructure in order to search unsolved crimes of special concern while a qualifying arrestee is in police custody during the booking process.

The FBI Laboratory Division has been working with the FBI Criminal Justice Information Services (CJIS) Division and the CJIS Advisory Policy Board (CJIS APB) Rapid DNA Task Force to plan the effective integration of Rapid DNA into the booking station process. To use Rapid DNA analysis effectively during the booking process, the Bureau is developing the necessary interfaces for such booking stations to communicate with CODIS. As part of these development efforts, the FBI will begin testing and evaluation of the Rapid DNA booking communications infrastructure in 2018. The Bureau plans to initiate pilot testing in 2019 with select federal, state, and local law enforcement for the uploading and CODIS searching of arrestee Rapid DNA records during the booking process.

The use of the term "reference sample buccal (cheek) swab" is intentional. The FBI's current development and validation efforts have been focused on the DNA samples obtained from known individuals (e.g., persons under arrest). Because known reference samples are taken directly from the individual, they contain sufficient amounts of DNA, and there are no mixed DNA profiles that would require a scientist to interpret them. **For purposes of uploading or searching CODIS, Rapid DNA systems are not authorized for use on crime scene samples.** All crime scene samples must be processed by an accredited forensic DNA laboratory that follows the FBI Quality Assurance Standards for Forensic DNA Testing Laboratories to be eligible for upload and/or search in CODIS.

The Rapid DNA Act of 2017 (Public Law 115-50) was signed by the president on August 18, 2017. The act authorizes the FBI Director to "issue standards and procedures for the use of Rapid DNA instruments and resulting DNA analyses." Now that the law is in place, the Bureau will be working toward the testing and implementation of this new technology and is poised to deliver the capability to process a Rapid DNA upload and search in the CODIS software within 2018. The FBI anticipates testing of components to begin in 2019. Integration into the booking process of states that are authorized to collect DNA samples at arrest, as well as the federal system, will follow.

The FBI is currently working with the Scientific Working Group for DNA Analysis Methods (SWGDAM) and other stakeholders to develop standards and procedures for the FBI approval and operation of the Rapid DNA systems in booking agencies. The Bureau recognizes that National DNA Index System (NDIS) approval of the Rapid DNA systems and training of law enforcement personnel using the approved systems are integral to ensuring that Rapid DNA is used in a manner that maintains the quality and integrity of CODIS and NDIS.

There is no Rapid DNA system currently approved for use at NDIS (NDIS-approved) by law enforcement booking agencies. The FBI will consider and approve, as appropriate, Rapid DNA systems for booking agencies once the relevant standards and procedures required by the Rapid DNA Act of 2017 are issued and all required IT communication enhancements for CODIS compatibility are implemented.

Download codis-rapid-dna-infographic-2019.pdf — 222 KB

Background on FBI Rapid DNA Efforts

The FBI established the Rapid DNA Program Office in 2010 to facilitate the development and integration of Rapid DNA technology for use by law enforcement. The program office works with the Department of Defense, the National Institute of Standards and Technology, the National Institute of Justice, and other federal agencies to ensure the coordinated development of this new technology among federal agencies. The program office also works with state and local law enforcement agencies and state bureaus of identification through the FBI's Criminal Justice Information Services Division Advisory Policy Board to facilitate the effective and efficient integration of Rapid DNA in the booking environment.

Several instruments have been developed for Rapid DNA analysis. These instruments have been, and continue to be, tested and evaluated by the FBI Laboratory and other federal agencies, such as the National Institute of Standards and Technology (NIST) and the Defense Forensic Science Center (formerly the Army Crime Laboratory). In January 2013, the manufacturers of the instruments attended a SWGDAM meeting to discuss their instruments and obtain feedback on validation. Because developmental validation is a crucial first step in the commercial use of these instruments, SWGDAM, through its Rapid DNA Committee, established a dialog with the manufacturers to assist them in their validation efforts (see SWGDAM FAQs).

Prerequisites for Rapid DNA in the Booking Environment

UNCLASSIFIED // FOR OFFICIAL USE ONLY

drhares@fbi.gov

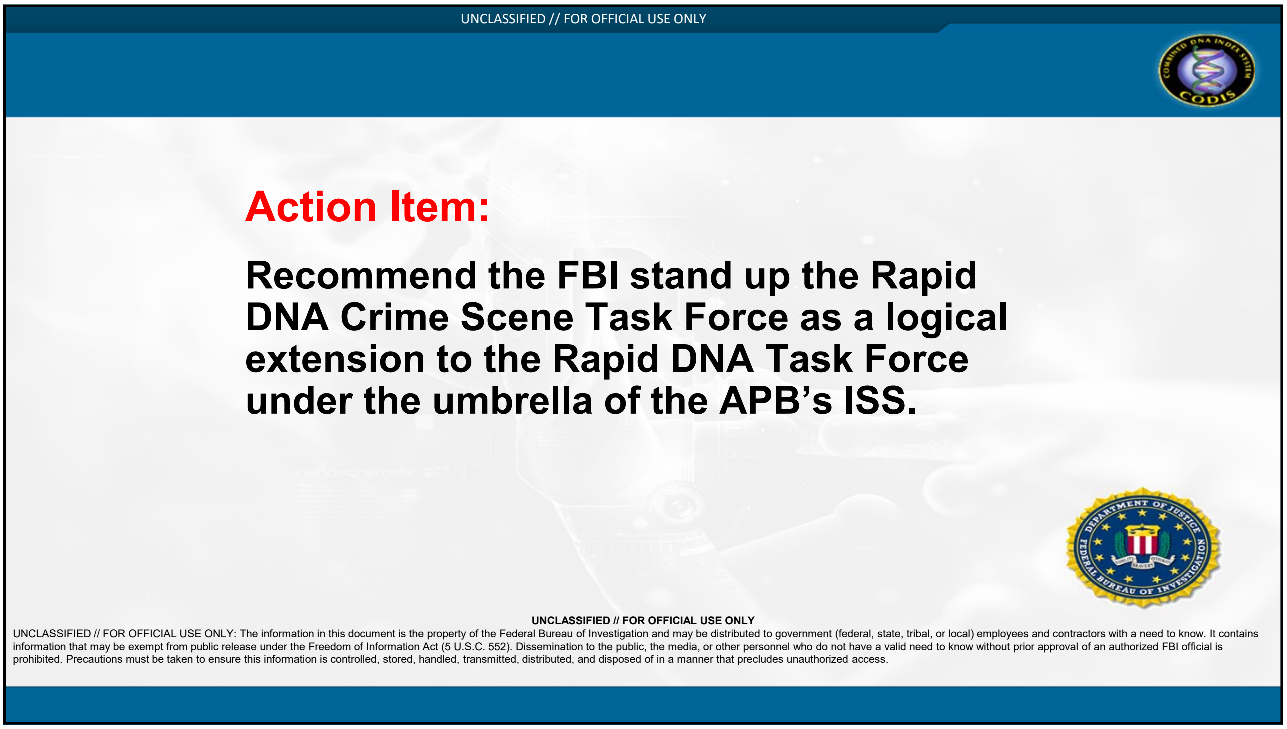
gcli@fbi.gov

tfcallaghan2@fbi.gov

RapidDNA@fbi.gov

UNCLASSIFIED // FOR OFFICIAL USE ONLY

53



UNCLASSIFIED // FOR OFFICIAL USE ONLY

Action Item:

Recommend the FBI stand up the Rapid DNA Crime Scene Task Force as a logical extension to the Rapid DNA Task Force under the umbrella of the APB's ISS.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

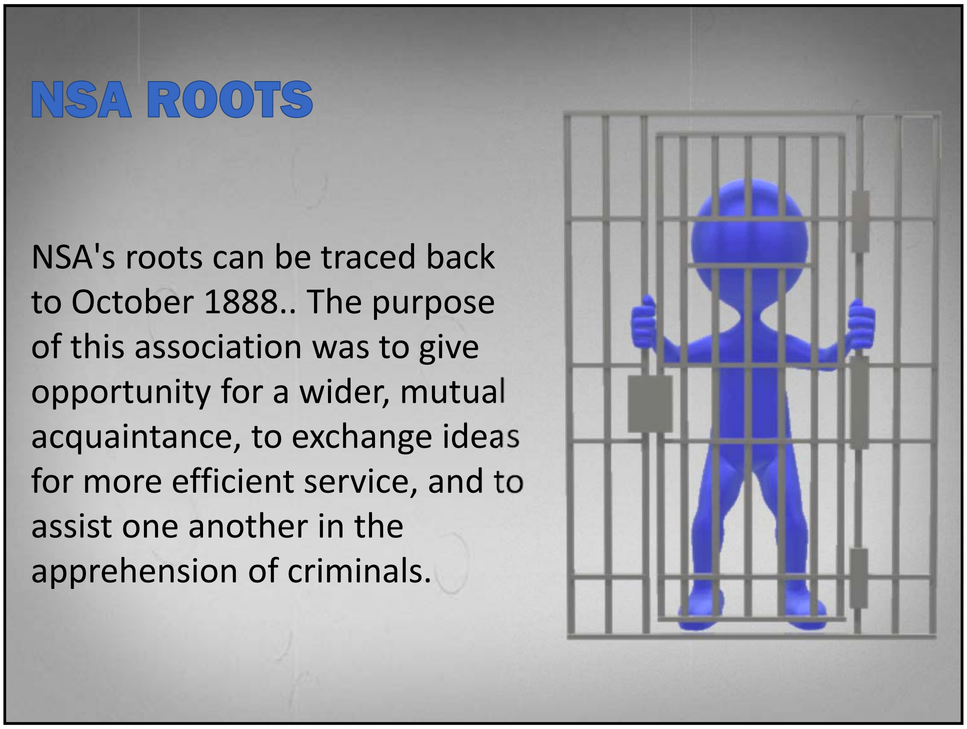
UNCLASSIFIED // FOR OFFICIAL USE ONLY: The information in this document is the property of the Federal Bureau of Investigation and may be distributed to government (federal, state, tribal, or local) employees and contractors with a need to know. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). Dissemination to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized FBI official is prohibited. Precautions must be taken to ensure this information is controlled, stored, handled, transmitted, distributed, and disposed of in a manner that precludes unauthorized access.

Intentionally Left Blank

National Sheriffs' Association

Origin

Chartered in 1940, the National Sheriffs' Association is a professional association dedicated to serving the Office of Sheriff and its affiliates through law enforcement education and training, and through the provision of general law enforcement informational resources.



NSA ROOTS

NSA's roots can be traced back to October 1888.. The purpose of this association was to give opportunity for a wider, mutual acquaintance, to exchange ideas for more efficient service, and to assist one another in the apprehension of criminals.

NIBRS

Mission

To precipitate a more robust law enforcement response to cybercrime.

Information Sharing Environment

Sustainable SAAS Transaction Platform for reporting cybercrime offenses and threat intel data and for sharing that information with federal partners.

UAS Sub-Committee

Newly formed for the purpose of establishing a direct line of communication with the FAA that will prepare law enforcement for the challenges ahead as it relates to the use of UAS

Intentionally Left Blank

AD	Assistant Director
ANDE	Accelerated Nuclear DNA Equipment
APB	Advisory Policy Board
ASCLD	American Society of Crime Laboratory Directors
ASUCRP	Association of State Uniform Crime Reporting Programs
ATF	Alcohol, Tabacco, and Firearms
BIA	Bureau of Indian Affairs
BJS	Bureau of Justice Statistics
BSS	Biometric Services Secton
CAU	CJIS Audit Unit
CCH	Computerized Criminal Histories
CE	Compliance Evaluation
CIO	Chief Information Officer
CJ	Criminal Justice
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CMF	Criminal Master File
CODIS	Combined DNA Index System
COPS	Community Oriented Policing Services
CPIC	Canadian Police Information Centre
CSMU	Crime Statistics Management Unit
CSO	CJIS System Officer
CSP	
DAD	Deputy Assistant Director
DCSA	Defense Counterintelligence and Security Agency
DDF	Disposition Document File
DFO	Designated Federal Officer
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DOD	Department of Defense
DOJ	Department of Justice
EBTS	Electronic Biometric Transmission Specifications
ERPOs	Extreme Risk Protection Orders
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FDLE	Florida Department of Law Enforcement
IAFIS	Integrated Automated Fingerprint Identification Systems
IAI	International Association for Identification
IAQ	Illegal Alien Query
IAR	Immigration Alien Response
ICE	Immigration and Customs Enforcement
IFFS	Identification for Firearm Sales

III	Interstate Identification Index
IS	Identification Services
ISCG	Identification Services Coordination Group
ISO	Information Security Officer
IT	Information Technology
ITMS	Information Technology Management Section
ITS	Information Technology Security
LEEP	Law Enforcement Enterprise Portal
MCC	Major City Chiefs
MCSA	Major County Sheriffs of America
MDM	Mobile Device Management
MOU	Memorandum of Understanding
N3G	NCIC Third Generation
NARIP	NICS Act Records Improvement Program
NCHIP	National Criminal History Improvement Program
NCIC	National Crime Information Center
NDAA	National District Attorneys Association
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
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
Nlets	International Justice and Public Safety Network
NSA	National Sheriffs' Association
NSOR	National Sex Offender Registry
NTOC	National Threat Operation Center
ORI	Originating Agency Identifier
OSAC	Overseas Security Advisory Council
P&I	Policy and Implementation
PO	Program Office
POC	Point of Contact
POF	Protection Order File
PRSU	Programs Research and Standards Unit
QAP	Quality Assurance Program
R-DNA	Rapid Deoxyribonucleic Acid
RISC	Repository for Individuals of Special Concern
SA	Security and Access
SEARCH	National Consortium for Justice Information and Statistics
SMART	Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking
SOR	Sex Offender Registration

SORNA	Sex Offender Registration Notification Act
SRS	
TAP	Tribal Access Program
THE	
TOTs	Type of Transactions
TTF	Tribal Task Force
TXDPS	Texas Department of Public Safety
UAS	Unmanned Aircraft System
UCN	Universal Control Number
UCR	Uniform Crime Reporting
ULF	Unsolved Latent File
UoF	Use of Force
USDOJ	United States Department of Justice
VCC	Virtual Command Centers
XML	Extensible Markup Language

Intentionally Left Blank