Criminal Justice Information Services (CJIS)
Advisory Policy Board
June 6-7, 2012
Buffalo, New York
Draft as of 05/31/12

Wednesday, June 6, 2012

8:30 a.m. - 8:40 a.m. -- **Board Convenes**

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

Roll Call
Colonel Steven F. Cumoletti
Chairman
CJIS Advisory Policy Board

8:40 a.m. - 8:50 a.m. -- **Introduction of Attendees and Special Guests**

Colonel Steven F. Cumoletti

8:50 a.m. - 9:00 a.m. -- **Welcoming Remarks**

Mr. Christopher M. Piehota
Special Agent in Charge
Buffalo Field Office
Federal Bureau of Investigation

Honorable Daniel Derenda
Commissioner
Buffalo Police Department
Buffalo, New York

Sheriff Timothy B. Howard
Erie County Sheriff's Department

9:00 a.m. - 9:30 a.m. -- **Item #1***
Executive Briefings

Mr. David Cuthbertson
Assistant Director
CJIS Division
Federal Bureau of Investigation

Ms. Erin Cozza
Executive Staff
Science and Technology Branch
Federal Bureau of Investigation

* No staff paper

CJIS Advisory Policy Board
Wednesday, June 6, 2012

9:30 a.m. - 9:45 a.m.	--	**Item #2*** **Department of Justice Chief Information Officer Update** Mr. Luke McCormack Chief Information Officer Department of Justice
9:45 a.m. - 10:00 a.m.	--	**Item #3** **Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee** Ms. Mary Rumple - **Chair** Director of Records Division Winston Salem Police Department Winston Salem, North Carolina
10:00 a.m. - 10:15 a.m.	--	**Item #4*** **UCR Redevelopment Program** Mr. Brian Griffith Program Manager, UCR Redevelopment CJIS Division Federal Bureau of Investigation
10:15 a.m. - 10:30 a.m.	--	**Break**
10:30 a.m. - 10:45 a.m.	--	**Item #5*** **Association of State Uniform Crime Reporting Programs (ASUCRP) Update** Mr. Daniel Bibel ASUCRP Representative to the APB Massachusetts State Police
10:45 a.m. - 11:05 a.m.	--	**Item #16** **Chairman's Report on the Security and Access (SA) Subcommittee** Captain William Tatun- **Chair** New York State Police

* No staff paper

CJIS Advisory Policy Board
Wednesday, June 6, 2012

11:05 a.m. - 11:20 a.m. -- **Item #7***
National Crime Prevention and Privacy Compact Council Report

Ms. Liane Moriyama - **Chair**
Compact Council
Administrator
Hawaii Criminal Justice Data Center

11:20 a.m. - 11:35 a.m. -- **Item #8***
Law Enforcement Coordination with Tribal Agencies

Ms. Michelle Klimt
Chief, Law Enforcement Support Section
CJIS Division
Federal Bureau of Investigation

11:35 a.m. - 11:55 p.m. -- **Item #9***
Law Enforcement National Data Exchange (N-DEx) Program Update/Time Line

Mr. Michael Haas
Chief, Law Enforcement National Data Exchange
CJIS Division
Federal Bureau of Investigation

11:55 p.m. - 12:15 p.m. -- **Item #10**
Chairman's Report on the Information Sharing (INSH) Subcommittee

Captain Scott Edson- **Chair**
Los Angeles County Sheriff's Department
Los Angeles, California

12:15 p.m. - 12:30 p.m. -- **Item #23****
Biometric Interoperability on Progress to Date

Ms. Lisa Vincent
Chief, Interoperability Initiatives Unit
CJIS Division
Federal Bureau of Investigation

12:30 p.m. - 1:45 p.m. -- **Lunch**

* No staff paper

CJIS Advisory Policy Board
Wednesday, June 6, 2012

1:45 p.m. - 2:05 p.m. -- **Item #11***
Next Generation Identification (NGI) Update

Mr. Kevin Reid
NGI Deputy Program Manager
CJIS Division
Federal Bureau of Investigation

Mr. Brian Edgell
Chief, Implementation and Transition Unit
CJIS Division
Federal Bureau of Investigation

2:05 p.m. - 2:20 p.m. -- **Item #12**
Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

Captain Thomas W. Turner - **Chair**
Division Commander
Virginia State Police

2:20 p.m. - 2:40 p.m. **Item #14***
Warrant Task Force Status Report

Mr. Michael McDonald - **Chair**
Director
Information Technology
Delaware State Police

2:40 p.m. - 2:55 p.m. -- **Item #13***
Terrorist Screening Center Presentation

Mr. Terry Cahill
Deputy Director
Terrorist Screening Center

Mr. Terrance Wyllie
Domestic Outreach Program

2:55 p.m. - 3:10 p.m. -- **Item #15***
Federal Bureau of Investigation Information Sharing

Dr. Elaine Cummins
Information Sharing Officer
Federal Bureau of Investigation

* No staff paper

CJIS Advisory Policy Board
Wednesday, June 6, 2012

3:10 p.m. - 3:25 p.m.	--	**Item #28*** **Secure Communities Update** Mr. Scott Kirby Secure Communities Immigration and Customs Enforcement Department of Homeland Security
3:25 p.m. - 3:45 p.m.	--	**Break**
3:45 p.m. - 4:05 p.m.	--	**Item #17*** **Cloud Computing and the CJIS Security Policy** Mr. George White Information Security Officer CJIS Division Federal Bureau of Investigation
4:05 p.m. - 4:20 p.m.	--	**Item #18*** **Law Enforcement Online (LEO) Update** Mr. Mark Phipps Chief, Law Enforcement Online Unit CJIS Division Federal Bureau of Investigation
4:20 p.m. - 4:35 p.m.	--	**Item #19*** **Chairman's Report on the Sanctions (SS) Subcommittee** Ms. Dawn Peck - **Chair** Manager Bureau of Criminal Identification Idaho State Police

* No staff paper

CJIS Advisory Policy Board
Thursday, June 7, 2012

8:30 a.m. - 8:50 a.m.	--	**Item #21** **Chairman's Report on the Identification Services (IS) Subcommittee** Mr. Michael Lesko - **Chair** Deputy Assistant Director Crime Records Service Texas Department of Public Safety
8:50 a.m. - 9:05 a.m.	--	**Item #22*** **NLETS, The International Justice and Public Safety Network Update** Mr. Steve Correll Executive Director
9:05 a.m. - 9:25 a.m.	--	**Item #24**** **National Instant Criminal Background Check System (NICS) Section Status Report** Mr. Paul Wysopal Chief, NICS Section CJIS Division Federal Bureau of Investigation
9:25a.m. - 9:40 a.m.	--	**Item #6** **Chairman's Report on the National Instant Criminal Background Check System (NICS) Subcommittee** Mr. Michael McDonald - **Chair** Director Information Technology Delaware State Police
9:40 a.m. - 10:00 a.m.	--	**Break**
10:00 a.m. - 10:15 a.m.	--	**Item #25*** **National Consortium for Justice Information and Statistics (SEARCH) Update** Mr. Ron Hawley Executive Director SEARCH

* No staff paper
** Staff paper delivered with the Information Only papers.

CJIS Advisory Policy Board
Thursday, June 7, 2012

10:15 a.m. - 10:30 a.m. -- **Item #26***
Federal Bureau of Investigation's
Biometric Center of Excellence

Ms. Margery Broadwater
Biometric Center of Excellence
CJIS Division
Federal Bureau of Investigation

10:30 a.m. - 10:45 a.m. -- **Item #27***
US-VISIT Update

Mr. Kenneth D. Gantt
Director
US-VISIT
Department of Homeland Security

10:45 a.m. - 11:00 a.m. -- **Item #20***
FBI CJIS Division Periodic Fee Review

Ms. Linda Patterson
CJIS Division
Federal Bureau of Investigation

11:00 a.m. - 11:15 a.m. -- **Item #29***
Individual Address to the APB:
Potential Impacts of Unconstrained Interoperability

Mr. Travis Hall
PhD Candidate
Department of Media, Culture and Communication
New York University

11:15 a.m. - 11:30 a.m. -- **Item #30***

Individual Address to the APB:
Secure Communities and the Impact of IAFIS and IDENT Interoperability on Community Policing

Ms. Sonia Lin
The Kathryn O. Greenberg Immigration Justice Clinic of the Benjamin N. Cardozo School of Law

11:30 a.m. - 11:45 a.m. -- **Other Business**

11:45 a.m. - 12:00 p.m. -- **Adjourn Advisory Policy Board**

* No staff paper

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
BUFFALO, NEW YORK
JUNE 6-7, 2012

STAFF PAPER

APB ITEM #3

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

The Uniform Crime Reporting (UCR) Subcommittee was called to order by Chair Mary Rumple on 04/19/2012, at 8:30 a.m. Mr. Gregory Scarbro, Criminal Justice Information Services (CJIS) Division, served as the Designated Federal Official. Ms. Leslie Underwood, FBI CJIS Division, documented the meeting proceedings.

Mr. Scarbro led the Pledge of Allegiance, Vice Chairman Stelma conducted roll call and Mr. Scarbro made the opening remarks and general housekeeping notes.

Members in attendance:

Mr. Daniel Bibel, Massachusetts State Police Department, Maynard, MA
Mr. Francis Bradley, Chief of Police, Hualapai Nation Police Department, Peach Springs, AZ
Lieutenant William Reed, Jr., Virginia State Police, Richmond, VA
Ms. Mary Rumple, Winston-Salem Police Department, Winston-Salem, NC
Deputy Director William Seibert, Jr., Missouri Gaming Commission, Jefferson City, MO
Mr. Stephen G. Shelow, Chief of Police, Pennsylvania State University, University Park, PA
Mr. Lawrence A. Stelma, Sheriff of Kent County, Grand Rapids, MI
Mr. Roberto Villasenor, Chief of Police, Tucson Police Department, Tucson, AZ
Mr. Michael C. Walker, John Jay College of Criminal Justice, Hawthorne, NJ

Additional meeting attendees:

Mr. Paul Barsalou, UCR Redevelopment Project (UCRRP) Contractor, CJIS, Clarksburg, WV
Ms. Nancy Carnes, FBI, CJIS, Clarksburg, WV
Mr. Steven F. Cumoletti, Deputy Superintendent, New York State Police, Albany, NY
Assistant Director David Cuthbertson, FBI, CJIS, Clarksburg, WV
Ms. Stacey Davis, FBI, CJIS, Clarksburg, WV

Ms. Kristi Donahue, FBI, CJIS, Clarksburg, WV
Mr. Pete Fagan, International Association of Chiefs of Police, Alexandria, VA
Ms. Joyce Humphrey, FBI, CJIS, Clarksburg, WV
Section Chief Michelle Klimt, FBI, CJIS, Clarksburg, WV
Mr. Darrin Moor, FBI, CJIS, Clarksburg, WV
Dr. James Noonan, FBI, CJIS, Clarksburg, WV
Deputy Assistant Director Jerome M. Pender, FBI, CJIS, Clarksburg, WV
Mr. Michael Roosa, Maryland State Police, Pikesville, MD
Mr. Gregory E. Scarbro, FBI, CJIS, Clarksburg, WV
Mr. William See, FBI, CJIS, Clarksburg, WV
Ms. Loretta Simmons, FBI, CJIS, Clarksburg, WV
Ms. Kimberly Smith, FBI, CJIS, Clarksburg, WV
Mr. John Strong, FBI, CJIS, Clarksburg, WV
Mr. Gregory Swanson, FBI, CJIS, Clarksburg, WV
Mr. Scott Trent, FBI, CJIS, Clarksburg, WV
Ms. Leslie Underwood, FBI, CJIS, Clarksburg, WV
Mr. Theodore Yoneda, FBI Office of the General Council, CJIS, Clarksburg, WV

UCR Issue #1
UCR Redevelopment Project (UCRRP) Update

Mr. Paul Barsalou provided an update regarding the new features and improvements to the UCR, which include the following:

Data Submission Options

Mr. Barsalou began by discussing the following submission options available for law enforcement for sending UCR data to the FBI. These include: Flat File, Information Exchange Package Documentation (IEPD), Online Data Entry, Microsoft Excel Forms Workbook, Microsoft Excel Tallybook, and the Law Enforcement National Data Exchange (N-DEx)-National Incident-Based Reporting System (NIBRS) extract. Mr. Barsalou then informed the Subcommittee that the FBI UCR Program is in the process of creating an Access database for State Programs to use so that they can leverage the spreadsheet option. Mr. Scarbro mentioned that the paperless mandate (by former Assistant Director Roberts) has served as the catalyst for the creation of the spreadsheet and Access database options.

Mr. Barsalou discussed that the N-DEx would continue testing with Tennessee for a NIBRS extract and plan to have it completed by the end of 2012 or early 2013. Mr. Scarbro stated that he wants to be transparent to the Subcommittee regarding the status of the N-DEx extract. He stated that a few states are relying heavily on that process and one state decommissioned their existing UCR reporting system in

hopes of using N-DEx as the vehicle to exchange data. With N-DEx's inability to provide this service this has created problems for the UCR Program with several states. Mr. Bibel expressed concern that there is a credibility issue with N-DEx because for a number of years, N-DEx has been saying that the capability will exist. Mr. Villasenor mentioned that he is a member of the "*Region IX Law Enforcement Information Sharing*" initiative. This Executive Leadership Council consists of senior law enforcement officials from California, Nevada, Arizona, and Hawaii. Mr. Villasenor mentioned that N-DEx wants to be involved in that project but everything they are promising is coming up short. Mr. Scarbro stated that under Section Chief Michelle Klimt's leadership he was confident that N-DEx would meet stated initiatives.

Paper Submission Options

Mr. Barsalou discussed the ingesting of paper submissions in the new UCR System and the need to move to electronic reporting methods. As of now, the UCR Program will allow for Optical Character Recognition (OCR) scanning of three of the most recently approved Office of Management and Budget (OMB) approved forms. The goal is to get paper-submitting agencies to stop using non-standard OMB approved forms by 07/01/2013. Mr. Scarbro stressed to the Subcommittee the significant impact the 07/01/2013 deadline will have on paper based agencies. Discussion followed on the FBI's position should agencies discontinue reporting because they are unable to move to a paperless format by the 07/01/2013 date. Concern was that the proposed date had not been vetted through the CJIS Working Groups. Other concerns centered on the view the Association of State Uniform Crime Reporting Programs (ASUCRP) would have at their meeting in Baltimore on 04/26-27/2012.

Further discussion was held regarding agencies having a "credible plan" in place to move to a paperless reporting format. Mr. Bibel asked if the Subcommittee could have guidance as to what constitutes a "credible plan." Motion #2 below supports that request.

UCR Subcommittee Action:

Motion #1: Mr. Bibel made a motion that the UCR subcommittee is in support of the 07/01/2013 date for when State UCR Programs and direct contributing agencies need to submit data electronically in a format acceptable by the FBI.
Second: Mr. Larry Stelma
Action: Motion carried.

Motion #2: Mr. Daniel Bibel made a motion that if a State UCR Program or direct contributing agency is not able to meet the timeframe of 07/01/2013, then they need to

present a credible plan to submit data electronically using a format as defined by the FBI's UCR Program. Further definition of what the criteria for a credible plan, should be developed and presented by the UCR Program to the CJIS Working Groups.
Second: Mr. Michael Walker
Action: Motion carried

Motion #3: Mr. Michael Walker made a motion that the FBI should publish NIBRS data at least annually to promote interest in NIBRS participation, demonstrate the benefit of the data in NIBRS, and recognize the efforts of current NIBRS contributors.
Second: Mr. Daniel Bibel
Action: Motion carried

Automated Data Quality Check & Responses

Mr. Barsalou continued his presentation by discussing the quality checks and business rules being developed in the UCRRP. Mr. Barsalou also discussed the process for returning system errors and warnings to State UCR Programs and direct contributors. He suggested that State UCR Programs may want to consider establishing a single e-mail address for response receipts. He also stated that business rules will be available for State UCR Programs to look at upon completion of the redevelopment efforts.

Mr. Reed discussed the parsing of errors and a bandwidth concern and asked if the plans are to send one e-mail back for each error per submission. The concern was raised because of limits on network distribution paths and e-mail mailbox sizes for attachments. Mr. Reed is requesting that the FBI look at sizes of files when sending back the errors prior to a final decision on the process. Mr. Reed also requested information on the format that will be made available.

Using the 9-Character National Crime Information Center (NCIC) Originating Agency Identifier (ORI)

Mr. Barsalou discussed the UCRRP's transition from the 7 to 9 digit ORIs. The FBI UCR Program will still process the 7-digit character ORI but will allow for the 9-character NCIC ORI. The 7-character ORI will be translated into the NCIC ORI before processing.

NIBRS Time Window

The FBI is eliminating the Time Window Submission but is not requiring agencies to change their system requirements. Mr. Barsalou explained that in the New UCR System, the FBI UCR Program will handle the Time Window Submission as a "modify" record. Written documentation on this process will be provided in the updated NIBRS Technical Specifications to be released this year.

Publication "Blackout" Period

Mr. Barsalou then discussed how the New UCR System will continue processing new submissions while keeping control over publication data. Discussion was held regarding the March 15 yearly cutoff for data to the FBI and if that deadline would changes based on the completion of the UCRRP. Mr. Scarbro stated that with the implementation of the UCRRP, the FBI will be providing data quality issues back to states in a much quicker timeframe than in past years. This process is going to create a change in the work process for State Programs who in the past have not had immediate turnaround on data quality issues. He stated that as we move through the process, there will be changes in publication dates and timelines and that the Subcommittee needs to be thinking about having an in-depth discussion later this year on this issue.

UCR External Data Query Tool

Mr. Barsalou then mentioned that all crime data, with the exception of personally identifiable information, will be available on the External Data Query Tool (EDQT) and will be pushed to the EDQT one month after the close of the prior reporting month. State Programs will have the capability to choose the frequency of the release of data.

Overall Project Status

Mr. Barsalou concluded with the timeline status for the UCRRP including an overview of the current Data Migration Status, System Development Timeline, Paperless Migration Status, and the Shared Management Concept Status. He discussed the shared management concept being designed and developed to support State UCR Programs, with the first trial effort focused on the South Carolina Law Enforcement Division's program and data. Mr. Scarbro mentioned that it will be up to each state's discretion to utilize this tool, but that it should be a win/win for everyone.

UCR Issue #12
Proposal to Create a Violent Offender File in NCIC

Ms. Kimberly Smith, NCIC Program Manager, discussed the creation of the Violent Person File within the NCIC. She stated that the files creation was based on the increase in officers killed in the line of duty. The purpose of the file is to provide a caveat in front of a record in NCIC stating if the individual is known to be violent but does not have a criminal history. Ms. Smith provided statistics on the importance of this file. The statistics are derived from the number of officers feloniously killed from 2001 – 2010 as found in the UCR Law Enforcement Officer Killed and Assaulted (LEOKA) Program. Between the years 2008 and 2010, the number of officers killed increased 36 percent. Ms.

Smith also stated that there was an analysis conducted regarding the criminal history of offenders identified in the killing of law enforcement officers and 44 percent of persons had a history of violent crimes while 39 percent had a history of a weapons violation. In addition, 23 percent had previous records for assaulting a police officer or resisting arrest. Furthermore, 4 percent had a murder conviction prior to the killing or assaulting of a law enforcement officer.

Ms. Mary Rumple discussed how "Sovereign Citizens" are bad individuals but now we can put them in this file and let others be aware that they have made past threats. Mr. Stelma asked if Violent Person File would go into the National Instant Criminal Background Check System (NICS). The answer provided was that it would be part of the NICS/NCIC relationship.

UCR Subcommittee Action:

This issue was accepted for information only.

UCR Issue #2
2013 Data Collections Initiatives

Ms. Nancy Carnes began by discussing each of the form changes that will be required for the new UCR System. These changes will be reflected in the new user manuals and technical specifications currently under development or awaiting release.

A lengthy discussion was held regarding the OMB role in the creation and modifications to UCR reporting forms. Mr. Scarbro mentioned that OMB has challenged the current hate crime form and hence delayed the collection of the new data on gender and gender identity.

Dr. Noonan then addressed the Subcommittee on the recent OMB meeting regarding the hate crime form. Dr. Noonan passed out form samples and discussed the specifics of the OMB required meeting to review the hate crime form's utility. Nine law enforcement cognitive interviews were conducted which allowed for individuals to discuss completing the form to identify potential problems. OMB had issue with the Anti-Bias section of the form but the interviewers didn't have a problem in that area. Minor issues were identified by participants in the field survey to include the lack of white space on the form, some confusion on which location codes to choose, and some missed filling out the ethnicity portion of the form. A brief discussion was held on the validity or significance of the location code data. For example, there is confusion as to when to use a school-college/university location and when to use field/woods of which many colleges and university have in abundance. Mr. Swanson noted that those types of questions are training issues as to which locations should be chosen. However the ORI would identify the agency as a college or university therefore field/wood would be the best location

choice. It was suggested by Mr. Roosa, that it may be worth considering an Oracle based form with business intelligence (e.g. Turbo Tax) to guide users in order to alleviate the questions. Mr. Stelma stated that the more complicated the form gets, officers are just going to say it was an assault so that they can go home.

Mr. Bibel continued the training discussion by recommending that more training materials need to get to agencies to get the new initiatives out to the user community. The FBI UCR Program needs to provide uniform national training standards.

Mr. Scarbro stated that work was ongoing with CTAP and the UCR Program to develop additional training resources.

UCR Subcommittee Action:

This issue was accepted for information only.

UCR Issue #5
NIBRS Technical Manual Update

Ms. Carnes provided an update on the status of the NIBRS Technical Manual. This new manual is going to address all of the new initiatives within the UCR Program and will replace the following: Volumes 1-4 NIBRS manuals, previous addendums, and state program bulletins. The NIBRS Technical Manual will hopefully be done by the end of the year. Mr. Bibel mentioned that he had seen the new draft document and it is a great piece of work.

UCR Subcommittee Action:

This issue was accepted for information only.

UCR Issue #6
NIBRS Publication Update

Mr. Scarbro started the topic by addressing that the FBI UCR Program tried to publish the NIBRS Sex Offense Reports and went through an extensive process using 2009 data. The problem was that these reports were created at the same time that the definition of forcible rape was being modified and FBI's Online Print Media Unit and the National Press Office (NPO) were reluctant to place the reports on its website. Mr. Scarbro further explained that it was even a problem getting the revised definition of rape on www.fbi.gov. A couple of issues raised by the NPO include the very young offenders contained in the NIBRS reports and concern about possible confusion by the general public with the recent change to the Summary Reporting System (SRS) definition of rape. The concerns

resulted in the reports not being released. The UCR Program is currently working on another NIBRS publication series and expanding it to other offenses using 2010 data. Mr. Scarbro stated that it would be made a priority with CJIS executive management to get those reports released. Larry Stelma then recommended that a motion should be placed at the end of the UCR Issue #1 in support of the release of NIBRS. (See Motion #3 in UCR Issue #1.)

After lunch, CJIS AD Cuthbertson welcomed the Subcommittee to CJIS and noted his appreciation of their work.

UCR Issue #3
Proposed Submission Procedures for Reporting Rape Data as it has been Redefined in the Uniform Crime Reporting Program's Summary Reporting System

Mr. Scarbro provided an update on the work completed to date in the implementation of the new rape definition. Mr. Scarbro stated that we have an established definition and buy in from the Advisory Policy Board (APB) and now need to decide how to collect it in the SRS. The first option is to capture the historical definition of rape along with the newly revised definition. The second option is to only collect data on the new definition and drop the historical data. No matter what option is chosen, any change made will need to go to OMB and be a lengthy delay. It was noted that in either SRS option there are not subcategories of sexual offense as it is reported in NIBRS.

Mr. Walker had concerns with just throwing out the historical definition and replacing it because it will result in a huge increase in the rape numbers and will be hard to explain what has led to this increase. Mr. Walkers' proposal was to have a checkbox if the rape would have been a rape under the historical definition. Mr. Bibel noted that because SRS is not incident based, the numbers would need to be tabulated and reported as totals. He made the recommendation for Option #1.

Mrs. Rumple mentioned that she talked to her state program manager and a major vendor and the consensus was that they would rather see Option #2. Mr. Scarbro then noted that by choosing Option #1, it would delay the redevelopment by about 3 months.

Mr. Cuthbertson also expressed concern that if we go with eliminating the historical data, we won't have the ability to verify what the breakdown is and back up the data.

Mr. Scarbro mentioned that it will be sometime before we see meaningful data. Mr. Moor followed that comment by stating that there are some agencies that had stated that they cannot and would not update to the new rape definition.

FBI UCR Program Action Item: Use NIBRS conversion to see what the impact would be to convert it both ways. The data based on old and new definition could be used to see if we could expect an X increase in crime.

Mr. Cuthbertson asked that the UCR Program have that information by the June APB meeting.

UCR Subcommittee Action:

Motion: Mr. Reed made the motion to recommend the adoption of Option 1 (The current UCR SRS Technical Specifications, as well as the electronic Tally Book and Electronic Forms Workbook, will be expanded to collect rape according to the newly established rape definition while also maintaining the reporting of the historical rape data).
Second: William Seibert
Action: Motion carried

UCR Issue #4
Nonforcible Sex Offenses: Statutory Rape and Incest

Mr. Scarbro began this topic by listing the various options brought forward from the CJIS Working Groups:

- Option1—Statutory Rape and Incest will be counted within Rape.
- Option 2—Statutory Rape and Incest will not be counted within Rape but will remain within their own category.
- Option 2a—Statutory Rape should be reported to the UCR Program for any nonforcible sexual intercourse with a person who is under the (state's) statutory age of consent.
- Option 2b—Statutory Rape should be reported to the UCR Program for any nonforcible sexual intercourse with a person who is under the age of 18. For UCR Program purposes, a juvenile is considered to be an individual under 18 years of age regardless of state definitions. Consequently, the FBI will identify the age of consent to be anyone under the age of 18.

Minor discussion was held regarding the clarification that Statutory Rape and Incest are gender neutral.

UCR Subcommittee Action:

Motion: Mr. Bibel made a motion to recommend Option 2 and 2a, that Statutory Rape and Incest will not be counted within Rape but will remain within their own category. Statutory Rape should be reported to the UCR Program for any nonforcible sexual intercourse with a person who is under the (state's) statutory age of consent.
Second: Michael Walker
Action: Motion carried

UCR Issue #9
Summary of Recently Conducted Uniform Crime Reporting (UCR) Quality Assurance Reviews (QARs)

Ms. Humphrey presented the summary of QARs for the following states: Alaska, Colorado, Idaho, Kansas, Maryland, Montana, Pennsylvania and Rhode Island. Ms. Humphrey requested that the Subcommittee review the information and authorize Letters of Interest to be sent to the respective CJIS Systems Officers and copies to be sent to the UCR Program Managers, and their respective agency heads.

UCR Subcommittee Action:
Motion: Mr. Michael Walker made a motion to send letter of interest to the CJIS Systems Officers, UCR Program Managers, and their respective heads for the state represented in the staff paper.
Second: Mr. Roberto Villasenor
Action: Motion carried

UCR Issue #8
Human Trafficking Status Report

Mr. See provided an update on Human Trafficking and provided a brief background regarding the laws and regulations approved through the CJIS advisory process. He discussed the changes to the UCR handbooks, specifications, and forms to allow for the new requirements. He also mentioned the work underway with FBI, Criminal Investigative Division, Civil Rights Unit (CRU). They have a proactive CRU Unit Chief who wants to create a Human Trafficking database and submit that data to the FBI UCR Program. Mr. See discussed the *Uniform Federal Crime Reporting Act of 1988* and the fact that there is appropriations money set aside for the submission of federal crime data. The kick-off meeting for CRU's requirements and development is set for the end of April. Mr. Cuthbertson discussed the relationship with data being fed into Sentinel and that we want to make sure we move into that area so that agents do not have to duplicate data entry.

UCR Subcommittee Action:

This issue was accepted for information only.

UCR Issue #10
Law Enforcement Officers Killed and Assaulted Update

Mr. Scarbro began by discussing a recent meeting with Bureau of Justice Assistance (BJA) and that the LEOKA Program has received $100,000 for the implementation of ambush study. The next step is the creation of the Memorandum of Understanding with BJA and then the LEOKA staff will begin vigorously interviewing offenders and victim officers on the topics of ambush and unprovoked attacks. Mr. Scarbro mentioned the recent retirement of Mr. Charles Miller and that his position had been posted on 04/18/2012. Mr. Scarbro noted that the individual selected will be responsible for that study as well as other initiatives. There is also recent attention on the fact that veterans have been involved as offenders, especially in the ambush situations. A meeting was held with the Veterans Administration on what data would be useful. Mr. Scarbro also noted that there had been regional training conducted to almost 18,000 law enforcement officers within the last calendar year.

Mr. Walker briefly discussed his study, *"An Investigation into the Murders of Law Enforcement Officers in the First 75 days of 2011 and those who Committed the Crimes"* and some of the findings based on the various offenders interviewed.

FBI UCR Program Action Item: It is requested that the FBI's UCR Program send Mike Walker's study to all Subcommittee Members. (**After review that process had already occurred.)**

Mr. Scarbro stated that the LEOKA Program needs to look at where the program can be expanded and improve research to the law enforcement community. Mr. Miller's replacement will be tasked with identifying areas to improve services.

FBI UCR Action Item: It is requested that the FBI's UCR Program review LEOKA policy as it relates to corrections officers, parole probation officers, and other special function roles that are serving in a law enforcement function when killed or assaulted, and report back to the UCR Subcommittee next round.

UCR Subcommittee Action:

This issue was accepted for information only.

Mr. Scarbro mentioned that the group was not going to discuss the N-DEx/ NIBRS IEPD

because it was discussed in UCR Issue #1 earlier in the day. Mr. Fagan did address the group and stated that N-DEx is trying to get the data sharing template working. Mr. Trent wanted to be sure that the topic was adequately covered and that all Subcommittee concerns were addressed. Mr. Scarbro mentioned that the UCR IEPD will continue to be developed but UCR was still looking at N-DEx to develop that capability.

UCR Issue #7
Hate Crime Document (Revised) Update

Mr. Scarbro discussed the recent Congressional letter that the UCR Program received regarding the addition of the Sikh religion to the hate crime database. Mr. Scarbro reminded Subcommittee members that this issue was addressed by the UCR Subcommittee in 2010 and that they chose to take no further action on the issue.

Ms. Carnes then provided an update on the Hate Crime document being updated. The document will include the new scenarios of the new biases as defined in the Matthew Shepherd/James Byrd law. The Washington DC chapter of the Anti-Defamation League and National Hate Crime Coalition has been reviewing our documents to be sure that what we are including is accurate and meets modern issues. For example, instead of homosexual, the correct terminology will be defined as lesbian and gay. Twenty-six examples will be included in the document to assist law enforcement in identifying these situations.

Additional Business

Mr. Scarbro passed out a draft UCR Subcommittee Mission Statement and current membership listing. It was requested that the Subcommittee members review the draft mission statement and membership list. If any changes to either are identified they should be sent to Mr. Scarbro's attention.

Motion to adjourn was made by Mr. Shelow.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
BUFFALO, NEW YORK
JUNE 6-7, 2012

STAFF PAPER

APB ITEM #6

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

The Criminal Justice Information Service (CJIS) Division's Advisory Policy Board (APB) National Instant Criminal Background Check System (NICS) Subcommittee meeting was held at the CJIS Division in Clarksburg, West Virginia on April 17, 2012. The meeting was called to order at 8:30 a.m. by the Chair of the Subcommittee, Michael McDonald. Ms. Jill Ann Montgomery, FBI/CJIS NICS Section, served as the Designated Federal Officer (DFO). John L. Howell, FBI/CJIS NICS Section served as the scribe.

DFO Montgomery led the attendees in the Pledge of Allegiance.

The roll was called by DFO Montgomery.

Chair McDonald asked all gallery attendees to introduce themselves.

DFO Montgomery shared general housekeeping notes.

Members in attendance were:

Mr. Michael McDonald, Delaware State Police, Dover, Delaware (Chair)
Ms. Terry D. Gibbons, Georgia Bureau of Investigation, Decatur, Georgia (Co-Chair)
Ms. Julie Basco, California Department of Justice, Sacramento, California
Ms. Marion L. Burrows, Bureau of Alcohol, Tobacco, Firearms and Explosives, Washington, D.C.
Ms. Diane Harrison, Washington State Patrol, Olympia, Washington
Captain Randy Moon, Kansas Highway Patrol, Topeka, Kansas
Mr. Jason O'Neil, Chickasaw Nation Lighthorse Police Department, Ada, Oklahoma
Ms. Lynn Rolin, South Carolina Law Enforcement Division, Columbia, South Carolina
Mr. Lawrence "Lance" T. Tyler, Utah Bureau of Criminal Identification, Salt Lake City, Utah
Ms. Kathy Witt, Fayette County Sheriff's Department, Lexington, Kentucky

Gallery attendees: CJIS Division Deputy Assistant Director Jerome M. Pender, NICS Section Chief Paul Wysopal, NICS Section's Liaison Unit Chief Amy C. Blasher, CJIS DFO Scott Trent, NICS Section employees included Joann Garrison, Melissa Heldreth, Teresa Henderson, Margaret Kisner, Walter G. Sparks, Garnet Tucker, Rebecca A. Vincent, Paul E. Wagner.

NICS Issue #1
Sharing Information from the NICS Waiting for Disposition (WFD) Statistics with Local, State, and Federal Law Enforcement Agencies to Improve Inadequacies with Disposition Reporting and Information Sharing

This topic was presented by David B. Tetrick, FBI CJIS Division's NICS Section.

The purpose of this paper was to share information on how the NICS Section collects WFD statistics, for what purpose and how the statistics are utilized. Additionally, Mr. Tetrick discussed how these statistics can not be taken at face value and do contain some inherent flaws.

Mr. Tetrick advised there were four areas that have the propensity to affect the validity of the statistics: 1) requires NICS Examiners to manually capture the receipt of responses in the NICS; 2) NICS personnel may request one piece of missing information from more than one agency at the same time. The NICS staff is instructed to capture responses from every agency regardless of the transaction's status, but cannot be guaranteed. 3) If an agency responds after the third business day, there is no way to currently capture the exact receipt of the response. The current system allows for the indication of the response within the three business days, after the three business days, or after 30 business days. 4) Finally, the statistics cannot determine at what point the request was issued during the life of the transaction, whether on day one or day three, and whether the receipt of such impacted the final determination of the pending eligibility decision.

Discussion: Mr. Lance Tyler asked if a state responded with a "no record" response, would the NICS Section consider that a response? The NICS Section does consider that to be a response and closes the request in WFD. Chair McDonald asked whether an administrative message could be sent to the courts requesting information.
Ms. Kathy Witt expressed concern over the NICS Section requesting information from multiple agencies in different counties, which creates unnecessary work on all agencies involved in the request. Others asked about the types of mechanisms utilized to make the requests for information and if the NICS Section works with the state bureau. Chair McDonald advised that even though there are some flaws with the current system, all was in agreement that the information would still be valuable.

Subcommittee Action Items:

1) Subcommittee to review the explanatory letter (that the NICS Section will draft) to state CSOs explaining WFD statistics and provide comments back to the NICS Section.

NICS Section Action Items from the Subcommittee:

1) The NICS Section will send WFD statistics annually to each CSO.
2) Recommend the NICS Section consider including all agencies being contacted relative to any request so that agencies may have the opportunity to coordinate efforts and avoid duplication.

NICS Section Action Items Based on Discussion:

1) Need to draft explanatory letter to be included with WFD statistics.
2) Need to consider drafting a topic paper for future NICS Subcommittee meetings to explain how the WFD will function under New NICS.

NICS Issue #2
Sharing Information about Difficulties Associated with Point-of-Contact (POC) States Failure to establish or Maintain an Adequate Appeals Process to Handle Denied Background Checks

This topic was presented by David B. Tetrick, FBI CJIS Division's NICS Section.

The purpose of this paper was to update the Subcommittee on some of the problems the NICS Section has identified with state POC agencies establishing and/or maintaining an adequate appeal process as defined in Title 28, Code of Federal Regulations, Section 25.10.

Mr. Tetrick gave an overview of Section 25.10 and the rights of the denied individual to be able to direct his/her appeal to the denying agency, whether that be the FBI or an agency serving as a POC. He also discussed that it is not enough for the POC to simply direct the denied individual to the NICS Section for furtherance of the appeal.

Discussion: Ms. Diane Harrison started the conversation by stating that the NICS Section may have been the catalyst for this issue by being so cooperative. In the beginning of NICS, the FBI offered to assist the state operations and were willing to take on appeal referrals. She also stated the policy allows for the POC states to direct the denied individuals to the NICS Section. Chair McDonald stated that if the arrest was in another state (for POC state denials) then the individual should be referred to the state where the arrest occurred. Mr. Lance Tyler advised in Utah they provide the individual the reason

for denial, and the individual has the burden to provide documentation to prove the denial was incorrect.

Subcommittee Action Items: No action items.

NICS Section Action Items from the Subcommittee:

1) Develop a model appeal process/definition of adequate appeal process.
2) Consider establishing an internal NICS POC for states to contact for appeal-related assistance and guidance.
3) Consider sending the Law Enforcement Guide to the NICS Subcommittee for review and comment (which will contain a section on assisting individuals appealing a NICS deny.)
4) After appeal guidelines are established and published, the NICS Section should send correspondence to the head of POC agencies that are not upholding responsibilities relative to an adequate appeal process.

NICS Section Action Items Based on Discussion: No action items.

NICS Issue #3
The Processing of Appeals Associated with a State-Entered NICS Index Record

This topic was presented by Angela D. Vandergrift, FBI CJIS Division's NICS Section.

The purpose of this paper was to let the states know how the NICS Section Appeal Services Team is now processing appeals denied on a state-entered NICS Index record.

Ms. Vandergrift gave an overview of the NICS Section's appeal process. She advised once the initial appeal request is received, the NICS Section has five business days to respond with the reason for denial to the individual, as well advise the appellant if the NICS Section requires any additional information to further process the appeal request.

Prior to October 2010, if a denial was on a record where fingerprints were not required (i.e., a NICS Index record), the NICS Section would forward the appeal request to the appeal queue, and it would be worked in the order received, often causing the appellant to wait extended periods of time for direction. In October 2010, a decision was made for transactions where the denial was based on a valid state-entered NICS Index record, the NICS Section would sustain the appeal immediately and forward the appellant back to the agency that entered the NICS Index record.

Discussion: Mr. Lance Tyler advised that very few individuals denied by Utah appeal to the NICS Section but if they do, the NICS Section always contacts him and upholds the decision. He also discussed the form Utah uses for appeals. Mr. Tyler also questioned

IFFS Flags on records. Discussion ensued about what type of documentation or direction would prove beneficial for the agency that the appellant is referred to, particularly if the agency may be unfamiliar with NICS and/or the NICS appeal process.

Subcommittee Action Items: No action items.

NICS Section Action Items from the Subcommittee: No action items.

NICS Section Action Items Based on Discussion:

1) The NICS Section will reach out to its state IFFS contacts and inquire if their contact information could be shared with the NICS POC agencies.
2) The NICS Section should obtain a copy of Utah's appeal form to consider developing a similar tool for appellants that could be provided to the ORI advising them on the problem/issue and how they may be able to assist the appellant.
3) The NICS Section may want to consider the feasibility of developing/recommending some type of code or specific data referral that could be added to the miscellaneous comments field of each state-entered NICS Index record that could be utilized by individuals initiating an appeal. This additional piece of information would be something that the entering agency could utilize to obtain additional descriptors/information to help make an identification decision relative to the appellant and the prohibiting record.

NICS Issue #4
Sharing Information about Individuals Denied a Firearm by the NICS with Local, State, Tribal, and Federal Law Enforcement Agencies for General Law Enforcement Purposes

This topic was presented by David B. Tetrick, FBI CJIS Division's NICS Section.

The purpose of this paper was to advise of implementation of the NICS Deny File on the NCIC in August 2012.

Mr. Tetrick advised the Committee that in August 2012, the NICS Section will begin putting six months worth of denials on NCIC, which will be able to queried by law enforcement agencies. The file will contain descriptive information of the denied person, including name, date of birth, place of birth, height, weight, sex, race and social security number (if available). It will also include the state of residence, state of purchase, date of the NICS denial, date of entry into NCIC, and the ATF-issued license number of the Federal Firearms Licensee. This information will be provided by the NICS to local, state, tribal and federal law enforcement agencies that conduct a search of this file. This information will be updated nightly.

Additionally, Mr. Tetrick advised that in July 2012, POC states will be required to set the Prohibited Category Code (PCA) on all state denied transactions. (Note: The reason for the denial will not be included as part of the NCIC record.)

Ms. Joann Garrison of the NICS Section spoke on the topic of the Law Enforcement Guide the NICS Section is developing. She discussed what is planned with the Guide and asked for the Committee's input on what information to include. She also advised the Guide could be added as part of training to the states.

Mr. Tetrick closed by adding this File adds a significant amount of public safety, and would request the Subcommittee provide input on the best means of educating the law enforcement community on the NICS Deny Transaction File, without delaying implementation in August 2012.

Discussion: The Subcommittee wanted to know if the reason for denial would be included in the file and discussion ensued about the decision to not include this information. While there would clearly be benefit to the officer to know such, the decision to not include this component generally focused around mental defective records. The sensitivity of these records and the agreements entered into by state agencies to share such within the NICS Index, inhibited many from divulging such. If included as part of the record, many states felt as if their mental defective records would need to be removed from the NICS Index. There was also discussion to include wording about "officer safety" within the caveat of the record's response but it was determined this was not necessary in every situation. The Subcommittee recommended the "NICS" be established within the caveat (as long as doing such did not delay implementation) since officers may not always be familiar with the acronym or what NICS is. The members of the Subcommittee were also interested in where a hit in this file would fall in the order of the NCIC response and other details relative to the plans for the file. Venetia Sims with the NCIC program visited the Subcommittee meeting and spoke briefly to members and answering questions relative to the new file. Ms. Sims advised that initially, the file would be available to be searched via a new query (QND-Query NICS Deny) but in the full term, would be included in the QW–Query Warrants search. There will be a caveat at the beginning of the record response and at the end. Ms. Sims advised the file would respond to a background search and also for an entry/edit function as well. The record will be last in the response. Diane Harrison expressed concerned that agencies likely won't notice the hit/response when conducting an entry because they aren't necessarily looking for any other records. This is a good recommendation or point to make within the NICS Law Enforcement Guide and also information on how users can obtain additional information on the hit/records as well.

Subcommittee Action Items: Proposal to define NICS in the caveat. Ms. Diane Harrison made the motion, and Mr. Lance Tyler seconded the motion; the vote was 10-0 in favor of this proposal. This has been completed.

NICS Section Action Items from the Subcommittee: No action items.

NICS Section Action Items Based on Discussion:

1) The NICS Section should seek to address the IACP Firearms Committee relative to the development of the Law Enforcement Guide. This group would be a good group to collect feedback and input from in the development of this tool.

NICS Issue #5
The Disposition of Firearms by Law Enforcement

This topic was presented by Mary Kay Paugh, FBI CJIS Division's NICS Section.

The purpose of this paper was to provide an update on the extended use of the NICS by criminal justice agencies to conduct NICS background checks when returning firearms in the possession of law enforcement.

Ms. Paugh reported in 2005, two motions were made to the CJIS APB Security and Access Subcommittee: 1) to request the U.S. DOJ amend the current federal regulation to allow access to the NICS for background checks performed by a criminal justice agency prior to the return of firearms in law enforcement possession; and 2) to model the release of firearms on existing procedures used by Federal Firearms Licensees. Motion One was approved; however, Motion Two prompted a request for an additional paper be prepared and presented at the 2005 Fall CJIS APB Working Groups. This paper outlined the technical requirements necessary to access the NICS; how access would be determined; and the policy requirements for access.

Ms. Paugh advised during the December 2005 CJIS APB Meeting in Orlando, Florida, Option Three of the aforementioned paper was approved. It stated: "If the state is currently acting as a Point of Contact (POC) on behalf of the FBI, the checks for those states, for the purpose of returning firearms in the possession of law enforcement, would also be conducted through the POC as the firearm and firearm-related permit checks currently are conducted. If the FBI currently conducts firearm background checks for the state, then checks for those states for the purpose of returning firearms in the possession of law enforcement would be conducted through the FBI."

Ms. Paugh also presented the NICS Subcommittee with a draft version of a form proposed for use by agencies when accessing NICS for this new purpose. She advised two separate law enforcement agencies, one in Bridgeport, West Virginia, and the other in Pittsburgh, Pennsylvania, had reviewed the form. Both agencies were very satisfied with the form. Ms. Paugh requested the Subcommittee's recommendations about the form.

Discussion: Ms. Harrison displayed her frustration that it has been since 2005 and this process has not been implemented yet, but other issues can come before the APB and be implemented immediately. Several members of the Subcommittee questioned if this form was mandatory, and Ms. Paugh advised it would not be mandatory, but was developed for audit purposes. In general, most members on the Subcommittee felt that the form would be a deterrent to agencies utilizing NICS for this purpose. It was not practical to expect officers would fill out a six-page form in lieu of a simpler alternative-simply running NCIC. Ms. Paugh advised that a NICS check would not required for this purpose, but rather provides officers and agencies another resource to utilize before releasing firearms. The Subcommittee questioned only being able to process three firearms per form; if more than three firearms are involved would another form be required or just an attachment? Ms. Paugh responded that an attachment would be sufficient. The Subcommittee asked how the forms would be available or distributed? Ms. Paugh responded that she believed they would be on-line. Chair McDonald commented about the purpose of the form to satisfy audit requirements. He discussed audit procedures relative to the NCIC and recommended the NICS Section look into this further before deploying with the proposed form. Captain Randy Moon stated he believed this change in NICS access would cause the need for training.

For those states to be serviced by the FBI, CJIS intends for those NICS inquiries to be initiated via E-Check. Ms. Paugh advised necessary changes to the E-Check are currently planned for Spring 2013.

Subcommittee Action Items: No action items.

NICS Section Action Items from the Subcommittee: No action items.

NICS Section Action Items Based on Discussion:

1) The NICS Section should evaluate the purpose of the form and if it is necessary.
2) The Subcommittee was interested in expressing its support of this initiative and the value/interest in it by law enforcement. They wanted to urge the appropriate parties to please support the expedited processing of this change.
3) The proposed form offers a telephone contact for assistance and questions. If this is the NICS customer service number, this will need to be coordinated with the NOU and the NICS training curriculum.
4) The NICS Section should evaluate E-Check for this initiative – should a new inquiry screen be developed under this purpose code? The Subcommittee advised that officers will not have access to all of the required fields/information for today's NICS check. The NICS Section should also evaluate the collection of a case file number, if the form is eliminated. During audit, the agency could easily locate the needed documents that would justify the search/access by the case file number.

NICS Issue #6
The NICS E-Check

This topic was presented by R. Marc Chamberlain, FBI CJIS Division's NICS Section.

The purpose of this paper was to highlight the benefits the NICS E-Check could offer state programs and to elicit input on how best to improve the current system and market this tool to state users. Mr. Chamberlain discussed current attributes of the NICS E-Check to the FFL community: 1) a more accurate search facilitated by the direct entry of descriptive data; 2) the ability to print completed NICS background check search requests; 3) the ability to print and save a daily log of all their transactions which supports organization and future auditing; 4) increased usability for the hearing and speech impaired; and 5) added customer protection against identity theft.

Mr. Chamberlain discussed the cost savings realized by the NICS Section from FFL usage of the E-Check. He speculated state programs could realize similar fiscal savings thru the use of the E-Check.

Discussion: The question was asked as to why only 15 percent of NICS transactions utilize E-Check. Mr. Walter Sparks discussed the current security measures in place with the E-Check via the issuance of a digital certificate. This process is cumbersome and has inhibited usage. Mr. Sparks further explained upcoming system enhancements to the NICS E-Check which will eliminate many of these concerns and complaints.

The Subcommittee also asked what the NICS Section has done to promote E-Check to the state POCs. Mr. Chamberlain advised that in 2005 a meeting was held at the CJIS Division with POC state representatives to discuss E-Check. Additionally, e-mails have been sent to the POC states gauging their interest in using the E-Check and this tool has been spotlighted on numerous occasions at the NICS annual User Conference with state users. To date, no state program has taken advantage of the NICS E-Check.

Finally, the Subcommittee asked what the benefit is to the NICS Section for states to utilize E-Check. Mr. Chamberlain responded that E-Check was altered to offer assistance to state programs. If the E-Check system could assist states in maintaining their POC status versus the FBI taking on that additional workload, the FBI would benefit greatly. Secondly, the FBI has invested resources in the enhancement of the E-Check for state use and it would be beneficial to see the tool being taken advantage of.

<u>Subcommittee Action Items</u>: No action items.

<u>NICS Section Action Items from the Subcommittee</u>:

1) The NICS Section may need to reconsider the current priority ranking of changes necessary to E-Check to accept ORIs.

NICS Section Action Items Based on Discussion: No action items.

NICS Issue #7
NICS Improvement Amendments Act of 2077 (NIAA) Update

This topic was presented by Tina B. Collins, FBI CJIS Division's NICS Section.

The purpose of this paper was to discuss actions taken thus far by the NICS Section to promote and support the opportunities presented with the passage of the NIAA and to elicit input and feedback from the Subcommittee relative to any ideas they may have for the NICS Section to consider in educating and promoting this legislation to groups or in areas not yet considered.

Ms. Tina Collins advised the group that the NIAA was signed into law on January 8, 2008, by the President of the United States as a result of the tragic shootings at Virginia Tech on April 16, 2007. The NIAA reinforced and enhanced the U.S. Attorney General's ability to acquire, for the NICS, information from federal agencies for people falling within one of the ten categories of federal firearms prohibitions contained in the Gun Control Act of 1968. Ms. Collins also reported the grant program developed under the NIAA to provide incentives for state agencies to do the same. Ms. Collins reported on specific activities of the NICS Section relative to the promotion of the NIAA. A few of these activities include sending correspondence to state and federal agencies regarding the minimum criteria required to establish a qualifying relief from disability program under the NIAA; sending correspondence to all federal agencies requesting a POC be identified to work with NICS Section to ensure information on individuals prohibited from purchasing a firearm is available to the NICS Section; conducting outreach to law enforcement agencies, as well as the mental health community regarding providing information pursuant to Title 18, United States Code, Section 922(g)(4) to the NICS Index; and recently, the NICS Section has held regional NIAA meetings in 2011 & 2012, in which 38 states have participated, allowing attendees to gain a better understanding of the NIAA and what resources are available to them. As a result of the NICS Section's efforts, Ms. Collins advised that over 786,000 criminal dispositions have been obtained and updated; the number of records in the NICS Index has increased by approximately 45 percent, and the number of mental health records has increased by approximately 171 percent. Ms. Collins concluded by asking the Subcommittee about any recommendations they felt the NICS Section should consider assisting agencies in contributing needed information.

Discussion: Chair McDonald advised that Delaware will be submitting their mental records by July. Ms. Terry Gibbons asked if any states have overcome mental agency concerns with sharing this type of information? Mr. Will Finch discussed Connecticut legislation where there is a mandate to report that these records to the CT Department of

Public Safety. The CT DHHS is seeking an exemption to this under HIPPA that would still allow them to provide the records to the NICS.

Subcommittee Action Items: No action items.

NICS Section Action Items from the Subcommittee:

1) Share examples and contacts with Terry Gibbons on states who have overcome obstacles in sharing mental health records.
2) Provide Chair McDonald the ATF checklist and examples of relief programs and legislation.

NICS Section Action Items Based on Discussion: No action items.

NICS Issue #8
Proposed Federal Regulation Changes for the NICS

This topic was presented by William Finch, FBI Office of General Counsel.

The purpose of this paper was to provide attendees with an overview of the current and future Notice of Proposed Rule Making (NPRM) that will affect Title 28, Code of Federal Regulations (C.F.R.), Part 25.

Mr. Will Finch discussed three current NICS Regulations which are being published for comment. Those proposed changes are:

1. To add tribal criminal justice agencies to those entities authorized to receive information in connection with the issuance of a firearm-related permit or license;

2. To authorize access for law enforcement and criminal justice agencies to the FBI-maintained NICS Index to permit background checks for the purpose of disposing of firearms in the possession of those agencies; and

3. To permit the NICS retain, in a separate database, its Audit Log records relating to denied transactions for the full record retention period approved by the National Archives and Records Administration. At present, that period is 110 years.

Mr. Finch also advised there are eight additional changes that will be proposed in the future. Those changes are:

1) To authorize access to the FBI-maintained NICS Index to permit the NICS to respond to inquiries from the United States Attorney General, or designee, in connection with identifying whether named individuals are restricted persons

pursuant to 42 U.S.C. § 262a (Enhanced Control of Dangerous Biological Agents and Toxins) and 18 U.S.C. § 175b (Biological Weapon-Select Agents);

2) To authorize access to the FBI-maintained NICS Index to permit the NICS to respond to inquiries from the ATF in connection with a civil or criminal law enforcement activity relating to the Importation, Manufacture, Distribution and Storage of Explosive Materials (18 U.S.C. Chapter 40);

3) To authorize access to the FBI-maintained NICS Index to permit the Nuclear Regulatory Commission to conduct background checks in connection with the clearance of its licensee and certificate holder-security personnel, as mandated by 42 U.S.C. § 2201a;

4) To authorize the retention of limited information from the NICS Audit Log records relating to denied transactions in a file created specifically for that purpose in the National Crime Information Center database where they will be electronically accessible to law enforcement agencies;

5) To modify the definition of the NICS Index found at 28 C.F.R. § 25.2 by inserting the words, "or state" between the words "Federal" and "law;" and;

6) To expand the non-Brady use of the NICS Index found at 28 C.F.R. § 25.6 (j)(1) for the additional purpose of providing information in connection with the issuance of explosive-related permits or licenses to possess or use explosives;

7) To correct a typographical error published in the regulation at 28 CFR § 25.9(b)(2)(i). The correct CFR cite in that subparagraph should read § 25.9(b)(1)(iii), not § 5.9(b)(1)(iii);

8) To update the security reference in 28 CFR 25.8(c) from the "the NCIC Security Policy of 1992" to something either generic without a date or the most current relevant security policy.

Discussion: Mr. Jason O'Neil advised that tribal law enforcement agencies are not exempted under GCA or the National Firearms Act. Mr. O'Neil also commented on the ability of tribal agencies to receive information in relation to issuance of a firearm permit or license; but questioned whether it was authorized for tribal law enforcement to receive conviction information and also submit to the NICS Index. Mr. Finch advised tribal law enforcement agencies could submit to the NICS Index under federal prohibitions, but not under the Prohibited Category (PCA) of J.

Subcommittee Action Items: No action items.

NICS Section Action Items from the Subcommittee: No action items.

NICS Section Action Items Based on Discussion: No action items.

NICS Issue #9
The Expansion of the NICS Index to Include Information Pertaining to Persons Prohibited from Purchasing/Possessing Firearms Based on State Law

This topic was presented by Diana Linn-Cook, FBI CJIS Division's NICS Section.

The purpose of this paper was to share information relating to the addition of the State Prohibited Persons File within the NICS Index which allows for the contribution and maintenance of information to the NICS Index pertaining to persons prohibited from purchasing/possessing firearms based on state law.

Ms. Diana Linn-Cook gave a historical view of NICS Index entries being based on federal prohibitions only; however in April 2012, entries will be able to be made using state prohibitions with a prohibited category code (PCA) of J. Ms. Linn-Cook advised these entries will only respond if the state of residence or state of purchase (SOP) matches the record's state of prohibition; or, if the transaction is for a firearm permit check, the applicant's SOP matches the record's state of prohibition.

Ms. Linn-Cook also presented several benefits of adding state prohibited records into the NICS Index. Several of these reasons include:

- A prompt indicator of a subject's disqualification based on state law and the ability to render an immediate deny decision;
- Greater efficiencies by reducing the need for the user to expend resources in conducting additional review or research in order to determine a final transaction status;
- Enhanced accuracy as the state-prohibiting records maintained in the NICS Index are predetermined to be state prohibiting for firearm possession (or state firearm permit eligibility) prior to entry into the database;
- Reduced need for a user to replicate previously conducted research and outreach when processing subsequent background checks for the same individual;
- Reduced resources expended by a user in determining the appropriate interpretation and application of another state's firearm-disqualifying laws;
- The availability of predetermined state-prohibiting information to the NICS users during the background check process;

- The ability to place state-prohibiting information, which is available through the III or the NCIC but is not readily or easily discernible as state prohibiting, in the NICS Index; and
- The ability to maintain information that may be subject to expungement within the III.

Discussion: Mr. Lance Tyler asked if an individual is in the NICS Index with a state prohibitor for a permit only, would that entry be returned for a background check for a firearm? Ms. Linn-Cook responded that entry would not return since the responses of the record are also triggered by the purpose ID for which the check was conducted. The Subcommittee suggested the NICS Section consider reaching out to state probation and parole offices to develop additional state prohibited category codes. Ms. Linn-Cook concluded by advising members when they are ready to start entering NICS Index records with a SPC of J, they can contact her for assistance.

Subcommittee Action Items: No action items.

NICS Section Action Items from the Subcommittee: No action items.

NICS Section Action Items Based on Discussion: No action items.

Additional Business:

Teresa Henderson of the NICS Section's Assessment Unit gave an overview of a paper that will be presented at the Working Group meetings in August. The topic of this paper will be how the NICS Section will send NICS Index entries to the states for validation. The request of the NICS Section will be to send the entries to the CJIS Systems Officers (CSOs) so they may coordinate their state's response to the self-validation audits. The Subcommittee recommended that this paper be brought as an action paper to allow the CSOs to vote on this request.

Chairman McDonald advised the group at the next meeting the members would be discussing and developing a mission statement as well as membership guidelines for this Subcommittee.

Closing Remarks:

Chairman McDonald thanked everyone for their hard work during the inaugural NICS Subcommittee meeting. The meeting was adjourned at 5:00 pm.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
BUFFALO, NEW YORK
JUNE 6-7, 2012

STAFF PAPER

APB ITEM #10

Chairman's Report on the Information Sharing (INSH) Subcommittee

The Information Sharing Subcommittee (INSH) meeting was called to order by Chairman Scott Edson at 8:30 a.m. Mr. Michael Hass, Law Enforcement National Data Exchange (N-DEx) Program Office, Criminal Justice Information Services (CJIS) Division, FBI served as the Designated Federal Officer (DFO). Ms. Jasmine Rutherford, N-DEx Program Office, CJIS Division, FBI served as the INSH Subcommittee scribe.

Chairman Edson welcomed the attendees, provided opening remarks, led the attendees in the Pledge of Allegiance and conducted roll call. Next, the gallery introduced themselves, followed by housekeeping notes provided by DFO Haas.

Members in attendance were:
Captain Scott Edson, Los Angeles County Sheriff's Department (Chairman)
Mr. Ronald P. Hawley, SEARCH (Vice-Chairman)
Mr. Francis X. Aumand, III, Division of Criminal Justice Service, Vermont Department of Public Safety
Mr. James W. Buckley, Jr., U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement
Colonel Steven F. Cumoletti, New York State Police
Mr. John K. Donohue, New York City Police Department
Ms. Carol A. Gibbs, Illinois State Police
Mr. Michael C. Lesko, Texas Department of Public Safety
Captain Ed Posey, Gainesville Police Department
Sheriff Lawrence A. Stelma, Kent County Sheriff's Office
Ms. Pamela Scanlon, Automated Regional Justice Information System
Mr. Michael Roosa, Maryland State Police
Mr. Justin Murphy, U.S. Department of Justice
Ms. Anne Roest, New York State Division of Criminal Justice

Members not attending but represented by proxy:
None

The following members were not present and not represented by a proxy:
Captain Michael Corwin, Kansas City Police Department
Mr. Mark A. Marshall, Isle of Wight Sheriff's Office

Gallery attendees:
Mr. Steve Ambrosini, Integrated Justice Information Sharing (IJIS) Institute
Mr. Christopher Brown, International Association of Chiefs of Police (IACP)
Mr. Mark Danna, FBI CJIS Division, Clarksburg, WV
Ms. Amber Fazzini, FBI CJIS Division, Clarksburg, WV
Mr. Patsy Felosa, FBI CJIS Division, Clarksburg, WV
Mr. Stephen Felosa, FBI CJIS Division, Clarksburg, WV
Ms. Jill Grant, FBI CJIS Division, Clarksburg, WV
Ms. Leslie Hoppey, FBI CJIS Division, Clarksburg, WV
Ms. Michelle Klimt, FBI, CJIS Division, Clarksburg, WV
Mr. Ronald C. Knight, FBI CJIS Division, Clarksburg, WV
Mr. William G. McKinsey, FBI CJIS Division, Clarksburg, WV
Mr. Jeffrey McMillen, FBI CJIS Division, Clarksburg, WV
Ms. Roxanne Panarella, FBI Office of General Counsel (OGC), Clarksburg, WV
Mr. Darrin A. Paul, FBI CJIS Division, Clarksburg, WV
Mr. Kshmendra Paul, Information Sharing Environment (ISE)
Mr. Mark Phipps, FBI CJIS Division, Clarksburg, WV
Ms. Jennie Rylands, FBI CJIS Division, Clarksburg, WV
Mr. Gregory Scarbro, FBI CJIS Division, Clarksburg, WV
Mr. William See, FBI CJIS Division, Clarksburg, WV
Ms. Sherri Shreves, FBI CJIS Division, Clarksburg, WV
Mr. John Strong, FBI CJIS Division, Clarksburg, WV
Mr. Roy James Travelstead, III, FBI CJIS Division, Clarksburg, WV
Mr. Scott Trent, FBI CJIS Division, Clarksburg, WV
Mr. Greg Trump, IJIS Institute
Mr. Sudhi Umarji, IJIS Institute
Mr. George White, FBI CJIS Division, Clarksburg, WV
Mr. Steve Williams, Florida Department of Highway Safety & Motor Vehicles
Mr. Brian Withers, FBI CJIS Division, Clarksburg, WV
Mr. Theodore K. Yoneda, FBI OGC, Clarksburg, WV

INSH Issue #1
Information Sharing and N-DEx Operations Task Force (ISNOTF) Update

Captain Ed Posey, Gainesville Police Department, provided an update on the recommendations and comments the task force provided INSH from the previous day's meeting. Captain Posey presented ISNOTF's recommendations during the appropriate issue areas.

INSH Subcommittee Action:
This issue was accepted for information only.

INSH Issue #2
Mr. Kshemendra Paul Public Safety Strategy

Mr. Kshmendra Paul, ISE discussed the information sharing model, endorsed by IACP. Responsible information sharing regarding weapons of mass destruction, terrorism, information sharing. There are five communities, Law Enforcement, Defense, Intel, Homeland Security and Diplomacy. The ISE vision is to remove barriers to information sharing as information is a national asset. Reusable interfaces are needed for efficiency and greater mission impact. The CJIS Advisory Policy Board (APB) has always had an interest in security, even though only sensitive data is handled, not classified. Security is especially important after such incidents like the wiki leaks when classified military documents were publicly released.

Mr. Paul went on to say we need to do a better job of interoperability between fusion centers, tasks forces, etc. A more holistic approach is required for collocation. A greater use of standards is required as they cross programmatic streams for integration. Mr. Paul continued to explain how that can be accomplished. The standards must be compatible, which currently is not the case. There is a great need to focus more on standards that are constrained and certified. Mr. Paul stated, we are ready to take the next steps but need to do so with state and local partners. The IJIS Institute can provide a standards test and certification format through their Springboard project. Mr. Paul suggests that distributing, decentralizing, and maintaining standards is important from the direction of top down, bottom up, and outside-in. Mr. Paul is committed to reaching out to develop other partnerships and collaborations. He believes CJIS is the crown jewel of Federal IT and as such, needs to be a catalyst. How does CJIS plug into the broader system? What's the roadmap for CJIS? CJIS needs to fit in more broadly and Mr. Paul would like to see specific ideas of pilot projects. He believes it is critical to put money behind those projects but agencies are at risk. Mr. Paul added, when we run out of money, we have to start thinking about standardization. In other words, we will really be forced to start "thinking," so pilot programs can be established in order to move the concept toward reality. Mr. Ron Hawley said the conversation on this is just beginning. Oversight must be institutionalized, so we can continue the open dialogue. We all need to come together, but there must be driving forces that keeps bringing everyone back to the table. Mr. Paul replied, that advocacy is important; however it's a messy process to get buy in. Mr. Paul stated he is not here to dictate the solutions but rather his purpose is to bring people together. Ms. Anne Roest stated support and guidance is needed but if overly controlled, it is prohibitive.

So what are some compelling infrastructure challenges? Mr. Paul stated that is for us to decide. N-DEx is how the Law Enforcement Information Sharing Program is going to be implemented. The Subcommittee appealed to Mr. Paul the need for his support and recommended that N-DEx should be the national standard for information sharing. Moving forward the Subcommittee would desire more of a collaborative effort to strengthen the position of N-DEx as the national information sharing platform.

INSH Subcommittee Action:

Motion: Mr. Michael C. Lesko moved to recommend to PM-ISE that they strengthen their support of the N-DEx System as the National Criminal Justice Investigative Information Sharing Platform.

Second: Mr. Ronald P. Hawley

Action: Motion carried.

INSH Issue #3
Law Enforcement National Data Exchange (N-DEx) Program Status

Mr. Michael Haas, FBI CJIS Division presented this issue and provided a PowerPoint presentation. Mr. Haas provided an update on the N-DEx Program concerning policy matters, program updates and data access and sharing. Mr. Haas's discussion included implementation issues and data owners setting rules for their data. Mr. Haas reiterated that criminal justice agencies will shortly be allowed to access N-DEx pending the full implementation of the Data Sharing Template. When that occurs, N-DEx will reissue the policy manual. It was conveyed to the members that colored restriction flags in the N-DEx system are being removed to dismiss confusion regarding accessibility to records. Mr. Haas also informed the subcommittee that computer based training has been placed on Law Enforcement Online (LEO). The N-DEx Program Office has created a new Public Resource Center (PRC) and has placed it on the FBI website to house rules, policies, FAQs, manuals, and materials. Mr. Haas then went on to explain the single sign-on access to N-DEx via UNet (the FBI's unclassified network) which is coming soon. This will greatly increase awareness and exposure of N-DEx throughout the FBI and as such, terminals with UNet will have a single sign on icon on their desktop. Mr. Haas also briefed a connectivity chart on the various ways to come into the N-DEx system, via the N-DEx portal and LEXS-SR.

Mr. Haas responded to concerns that the FBI has not contributed data to N-DEx since 2009. Internal policies hindered the ability of the FBI to do submit Electronic Case file (ECF) data into the system. The FBI did not have a process in place to conduct the necessary review of the information being submitted; due to that fact the FBI made the decision to cease submission until such a process could be developed. The other major hurdle is the fact that corporate policy regarding data submission needs to be updated. Once these hurdles are resolved, N-DEx plans to submit current data and where applicable and submit as much historical data as possible. Mr. Haas stressed

that it was still the FBI's intention to submit data and this initiative is one of the primary focuses of the N-DEx Program Office.

The committee understands such policy and technical issues arise, but felt as if the information was not conveyed to them. Being more transparent upon incurring such issues would have been preferred. After much discussion, the Subcommittee requested an explanation on how the FBI will move forward. Ms. Michelle Klimt, Section Chief, made it clear the N-DEx Program Office was not to blame, but rather the FBI as a whole should take responsibility for this matter. Mr. Ron Hawley stressed that it is important to focus on the solution and moving forward at this point.

INSH Subcommittee Action:

Motion: Mr. Francis X. Aumand, III moved the FBI shall provide a written detailed explanation prior to the June 2012 Advisory Policy Board Meeting to the Advisory Policy Board, Major City Chiefs, International Association of Chiefs of Police, National Sheriff's Association, and Major County Sheriffs as to why FBI data hasn't been ingested into N-DEx as agreed to prior to 2009, and a plan to address it, include a time line and regular updates to the Advisory Policy Board and more forthcoming in the future.

Second: Sheriff Lawrence A. Stelma

Action: Motion carried.

INSH Issue #4
N-DEx CSO Role

Mr. Darrin Paul, FBI CJIS Division presented the "CJIS Systems Officer (CSO) Administrator Role" concept for the N-DEx System. The concept of this role is being developed by the N-DEx Program Office to support CSOs with their responsibility of managing N-DEx users. Mr. Paul stated the CSO Administrator Role shall provide the CSOs the ability to manage users, audit, training, and delegate authority to N-DEx Agency Coordinators. Additionally, it shall provide the CSOs the necessary tools to oversee the N-DEx System within their areas of responsibility. The N-DEx Program Office has developed this concept in close collaboration with and confirmed by the CJIS Audit Unit, APB's Working Groups, and Direct Connect Task Force. Mr. Paul continued this concept had recently been briefed to CJIS and the purpose of briefing to the Subcommittee was for feedback.

Mr. Paul briefed a series of mock screen shots and illustrated to the Subcommittee the proposed capabilities. He reiterated the importance of collaboration with the CSOs and the fact the role could only be developed as fast as the CSO could provide the feedback. Utilizing the mock screen shots, he described to the subcommittee what a user possessing the CSO Administrator Role shall be able to access. A user possessing

the CSO Administrator Role would be able to click on the "CSO Admin" tab and access the role's capabilities. Within the CSO Administrator Role the user would be able to access three pages: User Management, Audit, and Training. Mr. Paul described this role as attribute driven and the tools are only as good as the information the user's system provides. He mentioned a group within the N-DEx Program Office will be submitting a topic paper to the Working Groups, which would outline the attributes necessary to efficiently participate with N-DEx. Additionally, Mr. Paul noted the N-DEx Program Office is identifying the feasibility to develop this role for users that access N-DEx data via the N-DEx Portal and LEXS-SR. The primary objective is to build one role to identify all users regardless of access method.

Mr. Paul included an approach which outlines the way ahead for developing this role. The described approach relied heavily on collaboration with the APB members. The N-DEx Program Office's goal is to provide the development document to the APB membership by early summer. The N-DEx Program Office shall then follow-up with an update to the Fall 2012 Working Groups.

Mr. Michael Haas stated the primary reason the N-DEx Program Office is examining the development of this role and tools is to mitigate CSOs' concerns when the N-DEx Program Office partners to connect regional systems and aggregators. He continued that CJIS would appreciate the Subcommittee's guidance on the process for connecting regional systems when the systems currently are not in full compliance with the CJIS Security Policy. Mr. George White stated the current process for major systems e.g. LInX, is to conduct a technical security assessment and identify if they meet CJIS security requirements. Mr. Ronald P. Hawley commented the difficult concept is these systems have operated with their own policies and governance boards for years and even if, they are willing to close the gaps that may exist with regards to policy, it will still take time to bring them into compliance. Mr. Hawley continued, the real question is does the system's current policies and technical ability comply enough so the N-DEx Program Office can connect while the system's agency meets the remaining security requirements. The Subcommittee discussed the possibility of identifying what concessions could be made if the agency is working toward CJIS requirements. The Subcommittee provided the N-DEx Program Office a recommendation on the way ahead for connecting partner systems.

INSH Subcommittee Action:

Motion: Mr. Ronald P. Hawley moved while the N-DEx Program Office is attempting to establish an information sharing relationship between N-DEx and a partner system that is governed by an established set of policies, it is authorized to recommend acceptance of those polices in lieu of the N-DEx policies provided the following criteria are met:

1. The partner system's governing body agrees to work toward complete reconciliation of policy statements within 24 months;
2. The partner system policies, as deemed by the effected CSAs and CJIS Information Security Officer, substantially address all existing CJIS Security and N-DEx policies; and
3. The partner system's governing body agrees to periodic assessment of their progress toward complete reconciliation.
4. The N-DEx Program Office will disable the partner system's NCIC/III query capability until all CJIS security and N-DEx policies are met.

The recommendation of the N-DEx Program Office shall be to the INSH who must in a timely manner fully vet their recommendation in determination of whether or not to recommend acceptance to the Executive Committee of the CJIS APB.

The Executive Committee of the APB is authorized to deny or accept the partner system's policies in lieu of the N-DEx policy. In those cases where the policy is accepted, the Chairman shall report the action at the next full meeting of the APB and that action shall include a recommendation for the sunset of their acceptance. The APB shall adopt the sunset date of the action.

Second: Mr. James W. Buckley, Jr.
Action: Motion carried.

INSH Issue #5
LEXS Task Force Update

Mr. James Gerst, FBI CJIS Division provided an update on the status of the LEXS Task Force. Mr. Gerst stated there is nothing at this time for the task force to review since the LEXS specification has not changed. Until the decision is made on who will manage the LEXS specification, there is no task force meeting scheduled at this time.

INSH Subcommittee Action:
This issue was accepted for information only.

INSH Issue #6
N-DEx Data Analysis

Mr. Patsy Felosa, FBI CJIS Division provided and update on the data analysis tool created by N-DEx Program Office in response to INSH's previous motions. The

Subcommittee provided the N-DEx Program Office direction in the form of two motions at the fall 2011 INSH meeting in Baltimore, MD.

- Moved to direct ISNOTF to partner with the N-DEx Program Office and IACP CJIS Committee to develop a process to incorporate data analysis into the on-boarding and existing process, whether and if so, how to provide a data analysis service to existing data contributors. Results provided to INSH.
- Moved to direct ISNOTF to work with the N-DEx Program Office and IACP CJIS Committee and report back to INSH the identified permissible analytics for data quality for the purposes of improving the N-DEx system.

As a result of the motions the N-DEx Program Office partnered with the IACP in support of their Data Analysis Project. The project has focused on incidents, arrests, and service calls and providing statistical reports regarding the completeness of data fields as selected by the IACP CJIS Committee. All of the data analysis concerning N-DEx was at the national level. No individual data submitter information was analyzed or disclosed. The IACP assured the N-DEx Program Office and INSH, they will supply an advanced copy of report before providing overall findings at an upcoming IACP Conference.

Mr. Felosa continued, through this project, the N-DEx Program Office identified business practices to enhance data submissions. These best practices include data contribution checklist, pre-ingestion data analysis and data submission frequency reports. The N-DEx Program Office at the agency's request can generate activity reports to help agencies understand the richness and robustness of their data contributions.

As part of the Data Analysis issue, the Subcommittee held a brief discussion on the process for releasing the *N-DEx Policy and Operating Manual* following an update of the language. The Subcommittee at the request of Colonel Steven F. Cumoletti, APB Chair, provided the N-DEx Program Office with two forms of guidance regarding the release of the *N-DEx Policy and Operating Manual*. Colonel Cumoletti stated he would like ISNOTF and INSH to review the *N-DEx Policy and Operating Manual* prior to being released. This is to reaffirm the APB approved language, concentrating specifically on the policy allowing the criminal justice community access to N-DEx. The Subcommittee concurred, the ISNOTF should be the body that reviews the *N-DEx Policy and Operating Manual* then provides a recommendation to INSH for their endorsement. They recommended the N-DEx Program Office develop an overview page that highlights what changes occurred within the *N-DEx Policy and Operating Manual*. The detailed process for the *N-DEx Policy and Operating Manual* shall be for the ISNOTF to review the manual and make recommendations to the INSH chair. The INSH chair shall review the manual and subsequently direct the N-DEx Program

Office to release the manual, once the criminal justice community is permitted access to N-DEx.

Mr. Michael Haas requested direction on how INSH wants the N-DEx Program Office to handle any additional small changes e.g., language cleanup, tweaks to the *N-DEx Policy and Operating Manual.* The Subcommittee stated if the changes are a reflection of the pre-approved APB language, the N-DEx Program Office shall make the revisions and provide the revised manual to ISNOTF to verify and endorse. ISNOTF shall then provide the manual to the INSH chair to endorse and direct the N-DEx Program Office to publish. The Subcommittee directed, if the language changes significantly from what were originally approved by the APB, then the manual will need to be reviewed by INSH and passed to the Executive Committee for their approval.

INSH Subcommittee Action:

Motion: Captain Ed Posey moved the N-DEx Program Office shall provide detailed data submission reports, when requested by the data owner, data submitter or CSO.
Second: Mr. James W. Buckley, Jr.
Action: Motion carried.

Motion: Mr. James W. Buckley, Jr. moved the N-DEx Program Office shall explore and report back to Working Groups the level of effort required for N-DEx to support email notification capabilities and solicit from Working Groups uses of the email notifications and prioritization.
Second: Mr. Michael Roosa
Action: Motion carried.

Motion: Captain Ed Posey moved the N-DEx Program Office shall provide a notification to the record submitting agency and as appropriate, record-owning agency, and CSO, if the record submission/update to N-DEx doesn't occur within 30 days by the record-owning agency.
Second: Ms. Pamela Scanlon
Action: Motion carried.

INSH Issue #7
Relationship between N-DEx and UCR

Mr. Michael Haas, FBI CJIS Division provided an update as a result of a previous motion from the Fall 2011 INSH Meeting. The motion stated:

- To request CJIS, N-DEx Program Office, UCR Program Office, UCR Subcommittee, and INSH Subcommittee to determine the options, policies, and

implementations to use one IEPD for both N-DEx and UCR submissions that may remain separate at the discretion of each agency.

Mr. Haas briefed there are currently four agencies directly submitting their National Incident-Based Reporting System information via the Flat File to CJIS. The remaining agencies submit indirectly via their State Crime Reporting Programs. CJIS proposes three submission methods that agencies may choose for crime reporting:

- Traditional NIBRS Flat-file submission
- N-DEx Incident/Arrest IEPD
- UCR Crime Report XML IEPD

INSH Subcommittee Action:
This issue was accepted for information only.

INSH Issue #8
CJIS Audit Unit Update

Mr. Jeffrey McMillen, FBI CJIS Division presented this issue and answered questions concerning the N-DEx audit. Regarding the audit findings, Mr. McMillen commented they have not found any new issues with the agencies they have audited. Additionally Mr. McMillen stated, the level of N-DEx knowledge continues to increase and the audits are still being conducted telephonically. The CJIS Audit tools are currently available on LEO.

INSH Subcommittee Action:
This issue was accepted for information only.

INSH Issue #9
Law Enforcement Online Enterprise Portal Update (LEO-EP)

Mr. Mark Phipps, FBI CJIS Division provided an update on the status of the LEO-EP. The portal meets global standards and was built utilizing the CJIS trusted broker in an effort to provide a single sign on environment. Identity providers (IdP) can securely assert identities to access services based on attributes. This access improves information sharing and streamlines vetting. In order to operate, SAML (Security Assertion Markup Language) and XML are required in addition to Global Federated Identify and Privilege Management attributes. The user shall have an icon located on their computer desktop to navigate to the LEO-EP, so a user is never prompted for a log-in. The LEO-EP shall provide the user access to multiple service providers. The CSO is only required to manage the users and services under the CJIS User Agreement. Through future enhancements, the LEO-EP and LEO shall be merged into one interface. Utilizing this transition, a user shall be able to log-in through LEO or come in as a federated IdP and access the LEO-EP and LEO services. Currently, LEO

has the Virtual Command Center, Special Interest Groups, and many other services available. LEO email shall be significantly upgraded through these enhancements and optional to users, while still permitting access to services. The LEO application process shall be electronic for those who want to use it as an IdP. At this time LEO is enabling interested agencies to access the LEO-EP. By accessing services through the LEO-EP, a user does not have to change their existing account. The LEO-EP simply utilizes the existing information provided and directs the user to the provided services. To obtain the LEO-EP service contact the LEO Operations Unit by LEOportal@leo.gov.

INSH Subcommittee Action:
This issue was accepted for information only.

INSH Issue #10
Integrated Justice Information Systems (IJIS) Update

Mr. Steve Ambrosini presented an update on the Global Standards Council from the previous week. IJIS in interested in the full interoperability spectrum. IJIS is engaged in national information sharing and working to have N-DEx standards adopted by Industry. We are working to acquire common and broader interoperability, so adopting agencies can more efficiently exchange information with each other. This should not still be an issue in 5-10 years as it should be fully part of the system by that point.

Springboard is a venue for industry and government to come in and evaluate standards as they are available. Test facilities are being designed for the *Springboard* project.

Mr. Steve Felosa, FBI CJIS Division stated that he and Mr. Bob Gooden comprise the Vendor Outreach Liaison Team which looks at agencies that don't have a state or regional sharing system in place and cannot access N-DEx. Funding for small agencies must be found via grants to permit an N-DEx adapter to be added to their Record Management Systems. N-DEx attempts to target the larger agencies in Major Metropolitan areas who may have larger amounts of data to submit if the mapping is to be completed by the N-DEx Data Integration Team. We have found from Industry that requests for N-DEx access or capability are not common. The N-DEx Program Office must create awareness and utilize vendors to communicate to their clients. This is accomplished through relationships with IJIS and hosting of summits to bring Industry together with CJIS to create further awareness. N-DEx leverages IJIS to keep a level playing field because of their information sharing knowledge and their connections with Industry.

N-DEx needs Probation and Parole agencies to participate in IBP2 IEPD testing. A follow-on full Corrections summit is planned for late summer to get stakeholder input

to enhance IBP2 IEPD and provide an update on progress with the Probation and Parole candidates. IJIS is highly focused on the partnership initiative, working with associations and identifying high priorities.

IJIS is also in the very early stages of developing services specifications pipeline. Still requested is the global standards process.

INSH Subcommittee Action:
This issue was accepted for information only.

Chairman Edson adjourned the meeting at 4:45 p.m.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
BUFFALO, NEW YORK
JUNE 6-7, 2012

STAFF PAPER

APB ITEM #12

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

The National Crime Information Center (NCIC) Subcommittee meeting was called to order by Chairman Captain Thomas W. Turner at 8:30 a.m., Wednesday, April 18, 2012. Chairman Turner welcomed attendees to the spring meeting. Ms. Stephanie L. Louk of the Law Enforcement Support Section, NCIC Operations and Policy Unit, FBI CJIS Division, served as the Designated Federal Officer (DFO). Ms. Joyce R. Wilkerson, also of the NCIC Operations and Policy Unit, FBI CJIS Division, documented the meeting proceedings. DFO Louk led the NCIC Subcommittee in the Pledge of Allegiance. Following the pledge, Chairman Turner called the roll.

The following NCIC Subcommittee members were in attendance:
Lieutenant Colonel Brad Bates, Kentucky State Police
Ms. Wendy L. Brinkley, North Carolina State Bureau of Investigation
Sheriff Clifford D. Brophy, Stillwater County Sheriff's Office
Lieutenant Colonel John W. Clawson, Indiana State Police
Mr. Michael McDonald, Delaware State Police (**Vice Chairman**)
Mr. Walt Neverman, Wisconsin Department of Justice
Captain Thomas W. Turner, Virginia State Police (**Chairman**)
Mr. James G. Weaving, Charlotte-Mecklenburg Police Department
Mr. Carl Wicklund, American Probation and Parole Association

The following NCIC Subcommittee members were not in attendance but represented by a proxy:
Mr. Andrew Black served as proxy for Mr. Thomas Kane, Federal Bureau of Prisons

The following NCIC members were not in attendance and not represented by a proxy:
Chief William J. Kilfoil, Port Washington Police District
Sheriff John J. Nye, Henry County Sheriff's Office

Meeting attendees in the gallery introduced themselves and the agency they represented as follows:
Mr. Thomas G. Aldridge, Federal Bureau of Investigation
Ms. Michelle S. Klimt, Federal Bureau of Investigation
Ms. Linda S. Click, Federal Bureau of Investigation
Mr. James Robert Gerst, Federal Bureau of Investigation
Ms. Dixie Sue Hornick, Federal Bureau of Investigation
Ms. Cynthia Johnston, Federal Bureau of Investigation
Ms. Krista L. Koch, Federal Bureau of Investigation
Ms. Kimberly Kay Lough, Federal Bureau of Investigation
Ms. Roxane Panarella, Federal Bureau of Investigation
Mr. Kshemendra Paul, Office of Director for National Intelligence
Mr. Patsy T. Sabatelli, Federal Bureau of Investigation
Ms. Kimberly K. Smith, Federal Bureau of Investigation
Mr. R. Scott Trent, Federal Bureau of Investigation

DFO Louk discussed the house keeping items and reminded the members of the process in which the motions would be displayed on the screen prior to the voting. Agenda items were then addressed.

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

Mr. Patsy T. Sabatelli, FBI CJIS Division, presented this issue. The purpose of this issue was to determine if the current MOU between the FBI and NICB should be modified to expand NICB's "Authorized Use" of the NCIC data to include heavy equipment fleet owners who are self-insured and heavy equipment rental companies. In 1994, the CJIS Advisory Policy Board (APB) voted to give the NICB the capability to access the NCIC Vehicle File via a "mirror image file" to be updated automatically and simultaneously via a direct link to NCIC. The NICB use of the NCIC Vehicle "mirror image file" is currently regulated by an MOU between the FBI and NICB and outlines the following uses, access, and services made available to the NICB through their NCIC Vehicle "mirror image file." In 2006, the APB authorized the expansion of the MOU to include the vehicle finance industry in order to more effectively combat vehicle theft. The NICB requested to expand its authorized use of NCIC data to include heavy equipment fleet owners who are self-insured and heavy equipment rental companies in order to combat vehicle theft. If approved, the "Authorized Use" section of the current MOU would be modified to specifically include heavy equipment rental companies and heavy equipment fleet owners who are self-insured.

Discussion: The Subcommittee members stated that all five Working Groups endorsed the expansion. However, they requested clarification as to why nine members of the Western Working Group opposed the expanded access. It was thought that the Western Working Group members felt that NICB would continue to request additional access or other entities.

FBI Action Item: In future cases in which similarly situated entities are requesting expanded NCIC access authorization, the FBI should forward the requests through the Advisory Process consent agenda formality.

NCIC Subcommittee Action:

Motion: Mr. Michael McDonald moved to endorse Option 1: Expand the Authorized Use of NCIC data by NICB to include heavy equipment fleet owners who are
self-insured and heavy equipment rental companies.

Second: Ms. Wendy L. Brinkley

Action: Motion carried.

NCIC Issue #2
Proposal to Allow Expired License Year Data to be Entered in Felony Vehicle Records in the National Crime Information Center (NCIC) Vehicle File

This issue was presented by DFO Louk, FBI CJIS Division. The purpose of this item was to present Washington State Patrol's proposal to allow expired License Plate Year of Expiration (LIY) data to be entered in felony vehicle records in the NCIC Vehicle File. In December 2000, the APB approved to allow entry of expired license plate/registration data in the Vehicle File where license plate data is being entered. However, the APB's motion was specific to stolen vehicle records. In addition to the December 2000 request, in December 2003, the APB approved allowing retention of expired license plate/registration data in the Boat, License Plate, and Person Files as well. Currently, felony vehicle records entered into NCIC with a vehicle license expired beyond one year are rejected. DFO Louk indicated that this issue was a consent agenda item. All five Working Groups endorsed the approval to allow the entry of expired license beyond one year in the LIY field for felony vehicle records in the Vehicle File.

Discussion: The Subcommittee members did not discuss the issue.

NCIC Subcommittee Action:

Motion: Ms. Wendy L. Brinkley moved to endorse Option 1 - Allow entry of expired license beyond one year in the LIY field for felony vehicle records in the Vehicle File. A priority of 4M was set.

Second: Mr. James G. Weaving

Action: Motion carried.

NCIC Issue #3
Proposal to Create a New Extradition Field (EXT) Code to Indicate "Pick-up Intrastate" in the Locate Message for the NCIC Wanted Person File

This issue was presented by Ms. Dixie Sue Hornick, FBI CJIS Division. The purpose of this paper was to present a proposal to create a new Extradition (EXT) Field Code for Locate Messages to indicate that a subject of a wanted person record has been picked up within the state. At the June 2008 APB meeting, the CJIS Division requested that procedures for instate pick-ups be developed. The CJIS Division had determined that oftentimes when an intrastate pick-up occurred, the locate transaction included EXT/NOEX (No Extradition). The APB was provided two options that would change the procedures. Option one included the addition of a new EXT Field Code of INSP for Intrastate Pick-up. If this option was chosen, it was recommended that EXT/INSP could only be used when the locating Originating Agency Identifier (ORI) is from the same state as the entering ORI. However, the APB accepted option two which was to modify the conditions of when to use EXT/EXTR in the locate transaction. EXT/EXTR now means that the agency that entered the record advised that the apprehended/located person will be extradited or **picked up intrastate**, or that the person is wanted by a federal agency and has been apprehended/located by state or local authorities.

Mr. Brad Truitt, Tennessee Bureau of Investigation, submitted a suggestion to create a new EXT Field code in the locate message to indicate "pick-up intrastate." According to Mr. Truitt, agencies become confused when placing a locate on wanted person records when the subject is picked up within the state. Instead of the agency entering EXTR in the EXT Field, many are entering NOEX since they are not extraditing the subject (out of state). The creation of an additional EXT Field code of INPU to indicate "pick-up intrastate" may help eliminate the confusion for agencies when placing a locate on a wanted person record wherein the subject was located within the same state. If a new code is recommended, it was requested that the Subcommittee provide direction on how a located record with a code indicating instate pick-up should be processed in the system. For EXT Field codes EXTR and DETN, the record is maintained in located status for five days and detainer information can be appended (otherwise it is purged). For EXT Field code NOEX, the record remains active until a second locate is placed on the record. Detainer information cannot be appended to these records. Should the record be processed like EXTR/DETN records or NOEX records, or follow a unique set of rules?

Ms. Hornick noted that the change in policy documenting the use of EXTR for instate pick-up was implemented in 2009. Since this policy has been in place for only 2 years, it may be more productive to consider if the CJIS System Agencies (CSAs) have had ample opportunity to train their users on the proper use of the EXT Field codes. If a new code is created, all CSAs wanting to use the code would need to program and the EXTR would no longer be valid for instate pick-ups.

Ms. Hornick informed the Subcommittee members that four of the Working Groups moved for no change while one Working Group moved that the topic be forwarded to the Warrant Task Force for discussion.

Discussion: The NCIC Subcommittee members discussed this creation of the new EXT/INPU and determined there may be a training and awareness issue on the modified definition to the EXT/EXTR code that was endorsed by the APB in 2008. However, the members felt that since this topic had not yet been discussed by the Warrant Task Force, that group should have the opportunity to discuss and make a recommendation to the NCIC Subcommittee.

NCIC Subcommittee Action:

Motion: Ms. Wendy L. Brinkley moved to forward this topic to the Warrant Task Force for further evaluation.
Second: Lieutenant Colonel Brad Bates
Action: Motion carried.

NCIC Issue #4
Proposal to Modify the NCIC Validation Policy and Second-Party Check Requirement

This issue was presented by Ms. Kimberly Kay Lough, FBI CJIS Division. The purpose of this issue was to present a proposal to modify the NCIC validation policy and second-party check requirement. The intent of record validation is to ensure that records entered into the NCIC System are complete, accurate, and still outstanding or active, as cited in the policy. In order to validate according to policy, agencies must review the entry and supporting documentation and consult with the appropriate complainant, court, source, etc. The NCIC System pulls records for validation based on the date of entry. A record entered January 14, 2011, will be pulled for the initial 60-90 day validation in April 2011. As long as that record remains in NCIC, it will be subject to being pulled for the April validation each year after. The June 2010 APB approved changing the validation policy to only require a full validation on the initial 60-90 day validation followed by a source re-contact for each year after. Current second-party check procedures help to ensure the accuracy of NCIC records after entry into NCIC. The accuracy of a record must be double-checked by a second party, someone other than the individual that entered the record. Ms. Lough indicated that the Colorado Bureau of Investigation (CBI) requested the APB explore solutions to eliminate the second-party check and use the validation

process itself to assure record quality. Specifically, CBI's suggestion included keeping the second-party check as a best practice and moving the validation cycle from 60-90 days after entry to up to a month after entry, followed by annual validation each year after. The CBI proposed that the change in this procedure would balance the current budgetary and staffing constraints experienced by agencies to have a secondary check performed and replace it with a validation process to assist in insuring relevant and accurate information is entered into the NCIC database. The CBI stated that the NCIC System does not have a field to indicate that the second-party check process has been completed; whereas the validation process has the Name of Validator Field. Other than through state/local agency developed methods, there is no means to indicate completion of the second-party check. CBI also believed there are agencies not entering records into the NCIC system in order to avoid the additional required quality control checks. In addition, CBI stated that the validation cycle offset of three months is cumbersome to remember and that the penalty for making an error in validation may be the removal of records which itself can create a public safety issue. Ms. Lough reminded the members that the NCIC System generates a $.F.Failure to Validate Notification to CJIS Systems Agencies when records due for validation have not been validated after 30 days.

The Subcommittee was requested to make a recommendation on two issues:
1) removing the Second Party Check Requirement and 2) modifying the validation policy. Subcommittee members were reminded that four of the five Working Groups recommended no change to both proposals. The only Working Group to endorse the change was the Western Working Group, which is the region where the request originated.

Discussion: This topic did not generate discussion from the Subcommittee members.

SECOND PARTY CHECK ISSUE

NCIC Subcommittee Action:

Motion : Ms. Wendy L. Brinkley moved to endorse Option 2b - No change.
Second: Lieutenant Colonel John W. Clawson
Action: Motion carried. One opposed.

VALIDATION ISSUE

NCIC Subcommittee Action:

Motion: Ms. Wendy L. Brinkley moved to endorse Option 2 - No change to validation.
Second: Lieutenant Colonel John W. Clawson
Action: Motion carried.

NCIC Issue #5

Proposal to Modify the Validation Period for NCIC Known or Appropriately Suspected Terrorist (KST) File Records to a Minimum of Three Years from the Date of Last Review

This topic was removed from the agenda based on a request from the Terrorist Screening Center (TSC). The TSC felt the new validation policy would meet their needs.

NCIC Issue #6
Ordinance Warrants Maintained Within a CJIS System

Ms. Kimberly Kay Lough, FBI CJIS Division, presented this issue. The purpose of this issue was to present a proposal to develop access to Ordinance Warrants that do not meet the criteria for entry into a CJIS System by the individual state's definition. The APB formed the Warrant Task Force to review and discuss issues related to the entry of Wanted Person File records into the NCIC. The purpose of the task force is to identify ways to increase the number of warrants being entered into the NCIC. The December 2011 Warrant Task Force discussed state systems containing additional warrants that were not maintained within the NCIC. One of the reasons identified for the discrepancies is state systems contain ordinance warrants that do not meet current entry criteria by the individual state's definition for entry into the NCIC. The Warrant Task Force recommended that the Subcommittee discuss a method to maintain ordinance warrants in a CJIS system.

Discussion: Warrant Task Force Chairman McDonald stated that the Warrant Task Force discussed this issue and task force members felt that the severity of a warrant should not be a factor as to whether a warrant should be entered in NCIC and available for police officers. He continued to state that the knowledge of any warrant, regardless of the severity, would be an advantage for any police officer encountering an individual as an intelligence lead policing strategy across the nation. He further stated that this type of warrant entry would be voluntary and each state could set its own filters as to whether these warrants were hit on. He further stated that the Warrant Task Force is not endorsing the proposal, but rather they are requesting the NCIC Subcommittee's level of interest in the proposal.

The Subcommittee discussed the various Working Group motions. Two Working Groups requested that CJIS Division staff explore the development and implementation of a new or expanded file for ordinance warrants into a CJIS System and that CJIS Division staff should begin by canvassing all CSAs to determine level of interest and number of additional warrants for entry. Three of the Working Groups did not recommend researching the development of a new file or expanding the current file.

The NCIC Subcommittee members recommended that states should leverage the International Justice and Public Safety Network, an existing system, were the functionality is already in place that could maintain ordinance warrants. However, one Subcommittee member did voice that states like "one-stop shopping" rather than using multiple systems to obtain the requested information. In addition, the Subcommittee recommended that states utilize the SQW.

NCIC Subcommittee Action:
Motion: Mr. Carl Wicklund moved for Option 2 - No change.
Second: Sheriff Clifford Brophy
Action: Motion carried.

NCIC Issue #7
NCIC Wanted Person File: Wanted Person vs. Warrant Entry

Ms. Kimberly Kay Lough, FBI CJIS Division, presented this issue. The purpose of this issue was to present a proposal to allow an agency the capability to enter multiple wanted person records for the same subject into the NCIC Wanted Person File. NCIC now accepts federal, felony, serious and non serious misdemeanors, as well as temporary warrants with or without extradition finalized. Proposals to allow the entry of multiple warrants into the NCIC Wanted Person File by the same ORI have been discussed several times in the past by the APB. After the latest APB approved enhancement to NCIC of adding the Additional Offense (ADO) Field, NCIC policy remains that when a warrant issued for a subject contains multiple charges or additional warrants are issued for the same entering agency, the code for the more serious charge should be entered in the Offense Code (OFF) Field with the additional charges shown in the Miscellaneous (MIS) Field and can be flagged with a Y or N in the ADO Field in November 2011. However, the Warrant Task Force once again pursued the enhancement to the NCIC Wanted Person File because they believe this may assist CSAs in contributing additional warrants on existing wanted persons to the NCIC Wanted Person File.

The purpose of the Warrant Task Force is to identify ways to increase the number of warrants being entered into NCIC. It was identified by task force members that their state system is capable of accepting multiple entries for the same subject by the same ORI. Currently, the NCIC System has edits in place to reject duplicate entries in the Wanted Person File. The current NCIC Wanted Person File is person based. When the entering agency has several warrants/charges on the subject, they enter one record with the most serious charge in the OFF Field and the remaining charges can be detailed in the MIS Field. Because the task force felt it needed to preserve the Wanted Person File as a true "person file," previous suggestions that were offered to allow multiple warrants to be accepted and displayed into the NCIC Wanted Person File usually created barriers to

implementation because of the "person centric" nature of the file. While the suggestions were attractive and of interest, they were not feasible unless the file was changed to be "warrant centric" rather than "person centric."

Ms. Lough advised that when the Warrant Task Force met on December 5, 2011, much of their discussion focused on ways to increase the number of warrants entered into the NCIC. After much deliberation, the Task Force revisited the entry of multiple warrants in NCIC and support the concept to allow a single ORI the capability to enter multiple warrants for the same subject and requested that CJIS Division staff to explore and analyze an implementation plan for policy and technical requirements.

Discussion: The NCIC Subcommittee members explained that some state systems have the functionality to enter multiple warrants and the validation process would be a one to one comparison and much easier to perform under the warrant entry proposal. Some members urged the Subcommittee to support the concept, let the CJIS Division develop the implementation plan for technical and policy requirements, then analyze it. It was noted that all the Working Groups endorsed the concept but two of the Working Groups also requested the implementation plan be vetted through the Advisory Process. It was also noted that if multiple warrant were entered into NCIC, consideration should be given to linking the warrants.

NCIC Subcommittee Action:

Motion: Mr. Carl Wicklund moved to support the concept to allow a single ORI the capability to enter multiple warrants for the same subject. Request CJIS staff to explore and analyze an implementation plan for policy and technical requirements and then bring it back through the Advisory Process.

Second: Lieutenant Colonel John W. Clawson

Action: Motion carried.

NCIC Issue #8
Placing a Locate by the Originating Agency Identifier (ORI) of Record

Ms. Kimberly Kay Lough, FBI CJIS Division, presented this issue. The purpose of this issue was to present a proposal to allow the entering agency the capability to locate its own record. During the December 2011 Warrant Task Force meeting, task force members continued to explore ways to increase the entry of NCIC Wanted Person File records. In addition, the members discussed the locate and hit confirmation process, specifically improperly placed locates. Task Force members expressed their continued frustration with the locate and detainer process. The following two issues were identified: 1) agencies not placing locates when required by NCIC policy and confirmed by the entering agency, and 2) not placing the correct locate code as the situation presents.

Current policy and NCIC System edits allow the locating/apprehending agency within extradition limitations to place a locate on a positively identified record. When agencies contact and verify the identity of the subject or property, the owning agency is asking for the locating agency to place a locate with EXTR or DETN as policy indicates. The locating agency either refuses to place a locate or is improperly placing NOEX in the locate message. CSAs have attempted to resolve the disconnect by contacting the local agency and/or the other respective CSAs. Even though some agencies have corrected their procedures and completed the locate process according to policy, the problem still continues. The Warrant Task Force recommended that the owning agency be able to locate its own warrant after the locating agency refuses to complete the process or locates the record incorrectly. By allowing the owning agency the ability to locate their own record in instances where the locating agency either does not locate the record or incorrectly locates it, the system change would further allow the owning agency to append a detainer to the record as needed. By appending the detainer, the record would remain in NCIC to accurately reflect the subject's detainment at another facility and more importantly, provide notification prior to release that a detainer has been lodged by another jurisdiction and the subject should be held on that detainer thereby preventing their release prior to being returned to the jurisdiction that lodged the detainer.

Ms. Lough noted that the Working Groups provided a few different suggestions on how to allow the entering/owning agency the capability to submit a locate on its own record in absence of the located being placed or being placed incorrectly by the locating/apprehending agency. Ms. Lough provided that two of the Working Groups suggested using the locate transaction, one of the Working Groups suggested using the Clear transaction, while the remaining two Working Groups suggested that the CJIS Division remove the edit from NCIC detainer process that requires the record to be to be in located status, which will allow a detainer to be placed on a record located with NOEX.

Discussion: The NCIC Subcommittee suggested that even though all of the Working Groups did not recommend the CJIS Division remove the edits, that was a reasonable approach to resolving this issue and probably was not thought of by the other Working Groups. The Subcommittee members were reminded that the Warrant Task Force recommendation was not intended to modify the normal business practices if the locating agency would place the locate according to policy. However, if the locating agency refused to place the locate or incorrectly placds it, then the owning agency should have the capability to do so to preserve the quality of the record. The Warrant Task Force Chairman McDonald suggested that lifting the edits would be a reasonable and acceptable solution. A copy of a record response was provided for the members to review.

Mr. Walt Neverman provided the North Central Working Group's position in that if the real issue lies in the detainer process, then that should be addressed. Therefore, the North Central Working Group's recommendation requested the CJIS Division to remove the

edits from the NCIC detainer process. NCIC Subcommittee felt this solution addressed all the issues.

NCIC Subcommittee Action:

Motion: Ms. Wendy Brinkley moved to suggested that the CJIS Division remove the edit from NCIC detainer process that requires the record to be in located status which will allow a detainer to be placed on a record located with NOEX.

Second: Mr. Carl Wicklund

Action: Motion carried.

NCIC Subcommittee Action:

Motion: Mr. Carl Wicklund made a friendly amendment to the original motion:
Allow detainer to be appended to a record that is in active status.
Allow a detainer to be appended to a record that is in located status regardless of the EXT value.

Second: Lieutenant Colonel John W. Clawson

Action: Motion carried.

NCIC Subcommittee Action:

Motion: Lieutenant Colonel John W. Clawson moved to set a priority of 2H.

Second: Mr. Michael McDonald

Action: Motion carried.

NCIC Issue #9
Proposal to Modify the Query Tenprint (QTP) Process

This issue was presented by DFO Louk, FBI CJIS Division. The purpose of this issue was to present a proposal to modify the QTP process. DFO Louk first reminded the Subcommittee members of the current QTP processes. For each tenprint criminal and civil submission, the Integrated Automated Fingerprint Identification System (IAFIS) sends an inquiry to NCIC. NCIC searches the Wanted Person File and the terrorist records of the former Violent Gang and Terrorist Organization File. The NCIC inquiry is generated using name, date of birth (DOB), sex, and race from the fingerprint submission. Additional inquiries are generated using: FBI number, up to ten aliases, five additional DOBs, four miscellaneous numbers, and four social security numbers, if provided on the tenprint submission. The DOB included in the inquiry message must match the NCIC record's DOB exactly to return an NCIC record as a possible match. Hit notification is sent to the owner of the NCIC record as an Nlets Administrative Message. Pertinent information from the fingerprint submission, particularly the identity of the contributor, as well as the NCIC record, is included in the Nlets message. The NCIC record holder is

advised to contact the fingerprint contributor as necessary to verify the validity of the hit.

Currently there are other pending enhancements to the QTP process that will be incorporated post Next Generation IAFIS (NGI). Phase Two functionality will include notifying the fingerprint contributor of a possible match generated by the automatic NCIC search. Phase Three will include the expansion of the NCIC search to all NCIC persons files for criminal submissions. It was determined by the June 2008 APB, that when Phase Two is implemented, for civil submissions, the QTP will only provide responses to the fingerprint contributor when the match is generated from the Wanted Person and Protection Order Files and the National Sex Offender Registry. Hits generated on civil submissions will produce a caveat to the civil fingerprint contributor to contact the ORI of the NCIC record.

The June 2010 APB approved the recommendation to exclude the hits when the FBI numbers in the NCIC record and the IAFIS submission do not match. In addition, the APB recommended that a task group be created to further refine the process. Subsequent to the APB recommendation, a QTP Notification Task Group was formed. The Task Group met on August 17, 2011, in Pittsburgh, Pennsylvania. The following issues were discussed during the meeting: name search used for QTP, NCIC Files searched, Protected Person Data, SOC Field all nines, and previously approved enhancements. Three of the discussion points were presented to the NCIC Subcommittee for recommendations.

ISSUE 1 - NAME SEARCH

QTP searches are conducted using the same name search algorithm as conventional NCIC searches (New York State Identification and Intelligence System). One exception is the KST record searches are based on the exact last name and first three characters of the first name. The QTP searches are generating an overwhelming number of false hits based on the name search currently used. One alternative for modifying the QTP name search algorithm is to mirror the search used for the KST records. All QTP searches could be based on the exact last name and first three characters of the first name criteria. Another alternative is to establish the search on exact last name using the current criteria for the first name. The Subcommittee members were asked to determine if the name search algorithm currently used for the QTP searches should be modified.

Discussion: DFO Louk indicated that the Working Groups were split on this issue. Three Working Groups endorsed Option 1: Modify the QTP search criteria to the exact last name search while the other two Working Groups optioned for Option 2: Modify the name search to mirror the search used for KST (exact last name and first three characters of the first name.) Subcommittee members discussed the Northeastern Working Group's motion to accept Option 2. Mr. McDonald noted that he felt the Working Group accepted this option based on the amount of hits that would be generated using the same search used for the KST, and felt it made more sense. He requested input from the other

Subcommittee Members who represented a regional Working Group. Mr. Walt Neverman provided that all the Working Groups were in agreement that the search needed redefined and that it was probably a "hit and miss" to determine the criteria. Ms. Krista L. Koch provided that there was not a difference in the technical impact between Option 1 and Option 2 and an analysis could not be conducted to determine the difference in the two search results. The NCIC Subcommittee discussed the available options to narrow the search, without narrowing the search too much and possibly missing a hit. The Subcommittee members determined that it may best to modify the search to the exact last name, then re-evaluate if the concern still exists that too many false-negative hits were being generated.

NCIC Subcommittee Action:

Motion: Ms. Wendy Brinkley moved to endorse Option 1 - Modify the QTP search criteria to the exact last name match with a priority of 3M.
Second: Sheriff Clifford Brophy
Action: Motion carried.

ISSUE 2 - NCIC FILES SEARCHED

DFO Louk stated that during Phase Two implementation, when the fingerprint contributor begins receiving QTP notifications, the QTP will only return responses to the fingerprint contributor when the search is generated from the NCIC Wanted Person and Protection Order Files and the National Sex Offender Registry for civil submissions. Statistics were analyzed on the number of QTP notifications that are generated based on hits from each specific file. Although, there were files that the Task Group did not determine to be beneficial to law enforcement, the number of QTP notifications generated from those files were minimal. Therefore, it was determined that excluding those files from the QTP search would provide little to no impact on the number of notifications generated. The Subcommittee members were asked to determine if a QTP search for each specific file provided benefit to law enforcement.

Discussion: DFO Louk indicated that all five Working Groups endorsed no change. No further discussion was generated from the members.

NCIC Subcommittee Action:

Motion: Ms. Wendy Brinkley moved to endorse Option 2 - No change. The QTP process will continue searching all persons files.
Second: Sheriff Clifford Brophy
Action: Motion carried.

ISSUE 3 - PROTECTED PERSON DATA

DFO Louk stated that the NCIC Files search was expanded in 2010 to include all persons

files. In analyzing QTP notifications, it was determined that QTP hits were being generated from matches on the Protection Order File for both the subject's name and the protected person's name. The Task Group recommended that the protected person data (including name, sex, race, DOB, and SOC) be excluded from the QTP search. The group opined that generating hits based on data of the protected person provides no benefit to the law enforcement agency. The Subcommittee was asked to discuss this opinion and provide guidance on whether to exclude those fields from the QTP search. Analysis conducted by CJIS Division staff determined that approximately seven percent of the hits reviewed were generated based on the protected person name.

Discussion: DFO Louk provided clarification on the current process, in that protected person data is included in the searches. She further stated that all five Working Groups moved for Option 1- Protected Person data will be excluded from the QTP searches.

NCIC Subcommittee Action:

Motion: Mr. Carl Wicklund moved to endorse Option 1 - Protected Person data will be excluded from the QTP searches with a priority set at 3M.
Second: Mr. James G. Weaving
Action: Motion carried.

DFO Louk indicated that the NCIC Subcommittee members were requested to discuss two additional issues based on the results of the Southern and Federal Working Group's motions. The motions are listed below.

NEW ISSUE 4
FEDERAL WORKING GROUP ACTION:

Motion: Ms. Karyn Becker made a motion to adopt new Issue 4: Revisit the 2008 recommendation to only return hits for 2 NCIC Files to noncriminal justice fingerprint agencies.
Second: Mr. William Marosy
Action: Motion carried.

SOUTHERN WORKING GROUP ACTION:

Motion: Ms. Donna Uzzell made a motion to revisit the 2008 recommendation to only return hits for 2 NCIC Files to noncriminal justice fingerprint agencies.
Second: Ms. Kathy Witt
Action: Motion carried.

NEW ISSUE 5
SOUTHERN WORKING GROUP ACTION:

Motion: Ms. Donna Uzzell made a motion that in Phase 1, look at including Persons with Information data in the QTP search and generating notifications to the NCIC entering agency.
Second: Ms. Deborah Beckner
Action: Motion carried.

Discussion: NCIC Subcommittee members discussed both issues and opined that the recommendations were unclear and the Working Group should discuss them in further detail prior to the NCIC Subcommittee discussing and forwarding recommendations to the APB.

NCIC Action:
Motion: Mr. Walt Neverman moved that NEW ISSUE 4 and NEW ISSUE 5 should be revetted through the Working Groups for further discussion with guidance from the NCIC Subcommittee.
Second: Mr. Carl Wicklund
Action: Motion carried.

NCIC Issue #10
Criminal Justice Information Services (CJIS) Division National Crime Information Center (NCIC) Enhancements Status

This issue was presented by Ms. Cynthia Johnston, FBI CJIS Division.
Ms. Johnston provided Subcommittee members with a current list of the NCIC enhancements and a copy of the Build schedule. Subcommittee members were requested to review the enhancements and if they believed a priority level needed to be changed or an enhancement should be removed, provide that input to the APB. In addition, Ms. Johnson provided updated implementation dates to specific enhancements. She also noted that Build 14 is scheduled for August 2013.

Based on a request that generated during the fall 2011 NCIC Subcommittee meeting, Ms. Johnston provided the Subcommittee members with information on the recently implemented NCIC enhancements. The information included a brief description of the enhancement, the date the APB provided approval, the implementation date, and the status of the enhancement, meaning the number of states that have implemented the enhancement and the number of records maintained in the file as a direct result of the enhancement. Ms. Johnston stated that the purpose of providing this information was to monitor the utility of the enhancements.

Discussion: The Subcommittee members reviewed the enhancement list, however provided no recommendation to APB. Ms. Krista K. Koch explained the CJIS Division

Build schedules. Subcommittee members did voice their opinion that the status of the implemented enhancements was very beneficial and recommend continuing to provide that type of information.

NCIC Subcommittee Action:
This issue was accepted for information only.

NCIC Issue #11
National Crime Information Center (NCIC) 2000 Header Requirement

This issue was presented by Ms. Kimberly Kay Lough, FBI CJIS Division. The purpose of this paper was to provide a status of state, federal, and tribal agency compliance with the 1N01 Header requirement. In order for states to become compliant with the NCIC 2000 full operating capabilities (FOC), CSAs must migrate all NCIC transactions to NCIC 2000 (1N01 header) format by July 1, 2012.

Ms. Lough provided a more recent update to the information than was provided in the staff paper. She indicated that as of March 1, 2012, California, Mississippi, Nebraska, New Mexico, Oklahoma, U.S. Army, U.S. Air Force, U.S. Secret Service, Royal Canadian Mounted Police, and INTERPOL still use the legacy header.

Ms. Lough reiterated that if a CSA cannot meet the compliance deadline of July 1, 2012, they may request an extension through a process similar to the FOC compliance extension request. Arizona and Pennsylvania both have submitted extension requests, however it appears both states are in compliance. Massachusetts submitted a 2-month extension request. Ms. Lough also advised that in the future this update would be included in the NCIC Readiness Update.

NCIC Subcommittee Action:
This issue was accepted for information only.

NCIC Issue #12
Warrant Task Force Status Report

This issue was presented by Ms. Kimberly Kay Lough, FBI CJIS Division. The most recent meeting of the Warrant Task Force took place on December 5, 2012, in Albuquerque, New Mexico. The following issues were discussed by the task force: Legislation Update (S 3120 & S 306), Outreach by Warrant Task Force to Criminal Justice Organizations, Court Cases involving Warrants, Multiple Warrants in NCIC, Improperly Placed Locates, Automated Warrant Management Systems, National Center for State Courts and SEARCH Projects. The Warrant Task Force revisited past meeting recommendations that developed into system and policy enhancements. The list below details the significant changes that have been or are scheduled to be implemented into the NCIC System: Allow multiple warrants on the same individual to be indicated by a flag in the Additional Offense Field, expand the Hot Check to include all person files, self assessment tool provided every 6 months, add additional timely entry "exception" to include investigatory discretion, amend the completeness policy for audit assessments, amend the validation policy, flag misdemeanors in IAFIS – post NGI, include additional codes for extradition at the time of entry, change all address fields to optional for entry and define them as non-critical for completeness for audit assessments, require the Extradition Limitation Field be a mandatory field, and address critical field determinations for Persons With Information dataset.

Ms. Lough indicated the Warrant Task Force continues to monitor two pieces of legislation relating to warrant entry and maintenance. The first, Senate Bill 306, the National Criminal Justice Commission Act of 2011, was reintroduced into the 112th Senate. The Act was read twice and referred to the committee on the Judiciary on February 8, 2011. At this time, there is no further action to report. The second, Senate Bill 3120, the Fugitive Information Networked Database Act of 2010 (FIND Act) was referred to the Senate committee on March 16, 2010, read twice and referred to the Committee on the Judiciary. At this time, no further action has been taken.

Ms. Lough stated the task force will be creating of a sound practice document for warrant entry. The document will be maintained on Law Enforcement Online. The site will contain information on model systems, automation, intrastate extradition, the NCIC System locate process, etc. It was also noted that Wisconsin's system should be referenced as a model system.

Ms. Lough provided that the topics to be discussed at the next meeting in

June 2012 include: John Doe warrants for DNA, warrant automation, and pending legislation. Ms. Lough indicated that the Proposal to Create a New Extradition Field Code to Indicate "Pick-up Intrastate" in the Located Message for the NCIC Wanted Person File topic will also be discussed.

Discussion: Subcommittee members asked which membership groups have been contacted to support this legislation. It was noted that reaching out to membership organizations such as the International Association of Chiefs of Police and the National Sheriff's Association for their endorsement may be beneficial in promoting the legislation. Mr. Mike McDonald stated that he would reach out to Mr. Bart Johnson and Mr. Jim McMahon for support. Subcommittee members stated that issue may be that federal agencies won't align unless the administration forces them to do so. The members further discussed reaching out to Congress again for support.

In closing, members briefly discussed Ms. Donna Uzzell's request for all warrant topics to be vetted through the Warrant Task Force for discussion and recommendation prior to vetting through the Working Groups and Subcommittee(s).

NCIC Subcommittee Action:

Motion: Lieutenant Colonel Brad Bates moved any warrant related topics should be vetted through the Warrant Task Force (while in existence) prior to forwarding to the Working Groups.
Second: Mr. Andrew Black
Action: Motion carried.

NCIC Issue #13
White Paper on Public Safety

Mr. Kshemendra Paul, Office of Director for National Intelligence, presented this issue. Mr. Paul is the Program Manager of the Information Sharing Environment (ISE). He provided a PowerPoint presentation entitled "Responsible Information Sharing." The presentation included the ISE's mission and vision, as well the following discussion points: principles of information sharing, information is a national asset, information must be shared and safe guarded, information sharing to inform decisions, information interoperability, and how to get involved.

Discussion: The Subcommittee members provided Mr. Paul with some thoughts on information sharing. Those thoughts included: enforce federal compliance with information sharing, use the APB process to collaborate with the states and federal agencies, and use the CJIS Wide Area Network and the Nlets as means of information sharing.

NCIC Subcommittee Action:
Motion: This issue was accepted for information only.

NCIC Issue #14
Proposal to Create a Violent Offender File in the National Crime Information Center (NCIC)

Ms. Kimberly K. Smith, FBI CJIS Division presented this issue. The purpose of the issue was to present a proposal to create an NCIC Violent Offender File. Ms. Smith first highlighted some statistical references as noted in the staff paper. Currently, 50,000 law enforcement officers are assaulted in the United States each year while on duty. Between the years 2008 and 2010, the number of officers killed increased 36 percent. An analysis was conducted regarding the criminal history of offenders identified in the killing of law enforcement officers. It was determined that 44 percent of persons had a history of violent crimes while 39 percent had a history of a weapons violation. In addition, 23 percent had previous records for assaulting a police officer or resisting arrest. Furthermore, 4 percent had a murder conviction prior to the killing or assaulting of a law enforcement officer.

During the 1990's, an NCIC file existed that contained data on violent felons. The file was created to assist the Bureau of Alcohol, Tobacco, and Firearms (ATF), in enforcing a U.S. Code that prohibited certain felons from possessing firearms. Although, the ATF Violent Felon File records were maintained solely by the ATF (entries, modifies, etc.), the file served to enhance officer safety for the entire law enforcement community. An officer receiving a hit on the file would automatically be notified of the violent offender encountered. In 1998, the file was discontinued at the request of the ATF. The primary justification pertained to the passage of laws requiring longer mandatory incarceration of armed criminals. The request to discontinue the file was subsequently approved by the June 1998 APB.

Ms. Smith stated that it has been requested that a Violent Offender File be created in NCIC. Statistics provided by Law Enforcement Officers Killed and Assaulted (LEOKA) indicate that nearly 20 percent of the officers feloniously killed in the line of duty from 2000 - 2009 were during routine traffic stops or pursuits. The Violent Offender File will increase officer safety by providing timely information on a subject deemed to be a violent offender.

The request has been endorsed by both the IACP and the NSA. The Concept of Operations for the Violent Offender File was provided as an attachment to the paper. Ms. Smith noted that the file would mirror the NCIC Protective Interest File.

Discussion: The Subcommittee members discussed the creation of the file in great length. It was suggested that renaming the file to Violent Person File should be considered as the word "offender" may imply the person was convicted. The criteria for entry was a focal point of the discussions. Subcommittee members voiced their concerns regarding the constraints on the criteria for entry. Members stated they felt the entry criteria NCIC Gang File records was a major constraint for utilization. DFO Louk indicated that the NCIC Gang File was being analyzed.

Ms. Smith noted that the Western Working Group suggested that the Identification Services Subcommittee should also discuss the creation of the file and make a recommendation to the APB.

FBI Action Item: It was recommended that the FBI create suggested guidelines for entry.

NCIC Subcommittee Action:

Motion: Mr. Carl Wicklund moved to endorse Option 1 - Endorse the creation of the NCIC Violent Offender File with specified changes. A priority of 2H was set.

1. Change the name of the File to Violent Person File.
2. Modify 1.2.2.1 Criteria for Entry to read: (changes are highlighted and struck out)

1.2.2.1 Criteria for Entry

Each record in the Violent ~~Offender~~ Person File must be supported by one of the following criteria:

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 ~~on crimes~~ of violent offense against a person to include homicide and attempted homicide ~~where a firearm or weapon was used~~.

3. Offender has been convicted of violent offense against a person where a firearm or weapon was used.

~~3~~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.

Second: Mr. Walt Neverman

Action: Motion carried.

NCIC Issue #15

National Crime Information Center (NCIC) 2000 Readiness Update

Ms. Kimberly Kay Lough, FBI CJIS Division, presented this issue.
Ms. Lough provided a status of state/federal agencies readiness for NCIC 2000 full operating capability. Illinois is currently the only state that has an active 6-month readiness extension request. It was thought there were political and funding issues that prohibit Illinois' migration toward NCIC 2000 FOC.

Discussion: The Subcommittee members discussed whether non-compliant states were forwarded to the Sanctions Committee for action. FBI staff clarified that the Sanctions Committee did not have the authority to review and impose sanctions, and furthermore that the purpose of the update was to track the process in which states are working toward NCIC 2000 FOC. Submitting extension request letters was part of the process that has been outlined by the CJIS Division.

The Subcommittee members discussed that it may be beneficial to reach out to the non-compliant states to encourage the implementation of the NCIC 2000 FOC. It was thought that in many cases, the high ranking authorities within the states are not aware of the non-compliance issue.

NCIC Subcommittee Action:
This issue was accepted for information only.

NCIC Issue #16
Update - Assessment of National Crime Information Center (NCIC) Policies at Agencies Using Electronic Records Management Systems (ERMSs)

Ms. Linda S. Click, FBI CJIS Division presented this issue. During the spring and fall 2008 APB meetings, the APB approved all portions of the staff paper regarding "Assessment of NCIC Policies at Agencies Using Electronic Records Management Systems." Since then, the policy guidance in that staff paper has been the official source for policy assessment of agencies using ERMSs. The purpose of this staff paper was to present language modifications to the original document on ERMSs without changing the policies or requirements for agencies using ERMSs. It only provided language clarification on issues through additional wording or re-sequencing of information. The following is a summary of the language modifications made:

1. Stated that technical staff are permitted to resolve data quality discrepancies identified through the electronic synchronization processes for second-party checks and validation.
2. Moved the ERMS qualifying criteria, as previously approved by the

APB, from the latter to the beginning part of the document, as it is the key starting point for determining whether the remaining portions of the paper are applicable.

3. Added language to note that an electronic synchronization for the second-party check and validation processes must include both "record-to-record" and "field-to-field" comparisons.

4. Added a notation to the qualifying criteria for ERMSs, scenarios 2 and 3, that as long as the second-party check is completed from the **original hard copy source document** (prior to destroying/placing in storage) against the **NCIC record**, it will eliminate the need for two second-party checks and will suffice for NCIC policy compliance.

Attachment A "Assessment of NCIC Policies at Agencies Using Electronic Records Management Systems (EMRSs)" was provided and included the updates as described above.

Discussion: Subcommittee members requested clarification as to whether a manual comparison **or** a file synchronization may be conducted. Ms. Click confirmed either could be conducted and further advised that a file synchronization was not required, however it may be more efficient. Subcommittee members then applied the policies to case scenarios for better clarification.

NCIC Subcommittee Action:
Motion: This issue was accepted for information only.

Chairman Turner adjourned the meeting.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
BUFFALO, NEW YORK
JUNE 6-7, 2012

STAFF PAPER

APB Item #16

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

The Security and Access Subcommittee Meeting was called to order at 8:30 a.m.by Chairman William Tatun, Captain, New York State Police. Ms. Lora England, FBI CJIS Division, served as designated Federal Officer for the meeting. Mrs. Margery Broadwater, Biometric Services Section, documented the meeting proceedings. Ms. England led the group in the Pledge of Allegiance.

Roll call was conducted by Chairman Tatun with the following members present: Ms. Brenda Abaya, Hawaii Criminal Justice Data Center; Mr. Larry Coffee, Florida Department of Law Enforcement; Mr. Joe Dominic, California Department of Justice; Mr. Alan Ferretti, Texas Department of Public Safety; Mr. Blaine Koops, Sheriff of Allegan County, Allegan, Michigan; Mr. Jeff Matthews, Alabama Criminal Justice Information Center; Mr. Terrill O'Connell, Oregon State Police; Mr. Bill Phillips, International Justice and Public Safety Information Sharing Network (Nlets); Sergeant T.J. Smith, Los Angeles County Sheriff's Department; Mr. Delton Tipton, South Dakota Law Enforcement Telecommunications System and Mr. Brad Truitt, Tennessee Bureau of Investigation.

Also in attendance were: Mr. Robert Turner, Integrated Justice Information System (IJIS) Institute/CommSys Incorporated; Mr. Justin Murphy, Department of Justice; Mr. Jerome Pender, Mr. John Strong, Mr. R. Scott Trent, Mr. James Gerst, Mr. James Loudermilk, Mr. William McKinsey, Mr. J. Abbott, Mr. Jeffrey Lindsey, Mr. Thomas Aldridge, Ms. Roxane Panarella, Mr. Mark Danna, Mr. George White, Mr. Jeffrey Campbell, Mr. Stephen Exley, Mr. Michael McIntyre, Mr. Brandon Morris, Ms. Dorothy Riddle, and Ms. Diane Shaffer, FBI CJIS.

Mr. John Strong, Deputy Assistant Director, FBI CJIS, welcomed the group to Clarksburg, West Virginia. He thanked the Subcommittee members for their time and support and offered assistance, if needed, during the member's stay in Clarksburg.

SA Issue #1
White Paper – Public Safety Strategy

The issue was provided previously to the Subcommittee members for information only and was not discussed at the meeting.

ACTION ITEM: Ms. Brenda Abaya requested access to the videos referred to in the White Paper. Mr. George White, CJIS Information Security Officer (ISO) to follow up on the request.

Security Access Subcommittee Action
Motion: Mr. Alan Ferretti moved to accept for information only.
Second: Mr. Jeff Matthews
Action: Motion carried.

SA Issue #2
Law Enforcement National Data Exchange (N-DEx) CJIS Systems Officer's (CSO's) Role

The issue was presented by Mr. Darrin A. Paul, Principal Consultant, N-DEx contractor. Mr. Paul updated the members on the development of the CSO Administrator Role within N-DEx. The development of a CSO Administrator Role within the N-DEx System would enable CSOs the ability to manage users, audit, training, and delegate authority to point of contacts at state, local, federal, and tribal agencies. This role will provide the CSOs the necessary tools to cover the N-DEx System within their areas of responsibility. The following policy foundations were used when outlining the proposed requirements for the CSO Administrator role: CSO's decision supersedes all authority within his/her area of responsibility and the CSO can delegate to an N-DEx Agency Coordinator.

Mr. Paul provided a high level briefing on several options of proposed functionalities that will help the CSOs, including:

User Manager Tab – will provide the CSOs the ability to manage the users that fall under their area of responsibility.

Auditor/Security Administrator Tab – will provide the CSOs the ability to manage the audit process for their agencies and audit the actions of those users of which the CSO has responsibility.

Training Administrator Tab – will provide the CSOs the ability to manage the N-DEx training and re-certification process for those users from state, local, federal, and tribal criminal justice agencies of which the CSO has user training responsibility.

Delegation of Authority Tab – will provide CSOs the ability to delegate the management of a specific predefined Originating Agency Identifier (ORI) set of users to an N-DEx Agency Coordinator.

"Screens" and documents will be forwarded to Subcommittee members to review and provide feedback to the N-DEx Program Office. Mr. Paul stressed the goal is to provide a quality tool to law enforcement and ensure that N-DEx is user friendly.

Security Access Subcommittee Action:
Motion: Mr. Blaine Koops moved to accept for information only.
Second: Mr. Terrill O'Connell
Action: Motion carried

SA Issue #3
FBI CJIS Division Annual Information Technology Security Audit (ITSA) Findings Briefing

The issue was presented by Mr. Michael McIntyre, FBI CJIS. Between March 2011 and February 2012, twenty-three CJIS Systems Agencies (CSAs) were audited to include 8 federal agencies and 15 states. 180 local agencies were audited as part of the overall audit process.

Of the total 23 CSAs audited, the top noncompliance findings/percentages were:

#1	Private Contractor Security Addendums	(26.1%)
#2	Authentication (Passwords)	(21.7%)
#3	Security Awareness Training	(17.4%)
#4	Security Audits	(8.7%)
#4	Personal Firewalls	(8.7%)
#4	Personnel Security Record Checks	(8.7%)
#5	Management Control Agreements	(4.3%)
#5	Encryption	(4.3%)
#5	Media Protection (Media Sanitization/Destruction Policy	(4.3%)
#5	Advanced Authentication	(4.3%)
#5	Malicious Code (Virus Protection)	(4.3%)

Of the total 180 local agencies audited, the top noncompliance findings/percentages were:

#1	Authentication (Passwords)	(35.0%)
#2	Security Awareness Training	(33.9%)
#3	Management Control Agreements	(22.8%)
#4	Personnel Security – Record Checks	(21.1%)
#5	Private Contractor Security Addendums	(20.6%)
#6	Encryption	(17.2%)
#7	Personal Firewalls	(12.8%)
#8	Malicious Code (Virus Protection)	(8.9%)

Starting October 1, 2011, new policy requirements implemented in the CJIS Security Policy, Version 5.0, were added to the ITSA according to the "required by year." These requirements are not sanctionable at this time.

Since the start of the zero cycle, six CSAs were audited on new policy to include 0 federal agencies and six states. 72 local agencies were audited as part of the overall audit process.

Of the total six CSAs audited, the top new policy noncompliance findings/percentages were:

#1	Media Destruction	(66.7%)
#2	Media Protection (@rest)	(33.3%)
#3	Visitor Logs	(17%)
#4	Media Transport	(17%)

Of the total 72 local agencies audited, the top new policy noncompliance findings/percentages were:

#1	Visitor Authentication/Visitor Logs	(51.4%)
#2	Media Destruction	(41.7%)
#3	Media Protection (@ rest)	(26.4%)
#4	Malicious Code (Virus Protection)	(8.3%)
#5	Media Transport	(2.8%)
#5	Boundary Protection (Firewall)	(2.8%)
#6	Event Logging	(1.4%)
#6	Personally Owned Information Systems	(1.4%)

Security Access Subcommittee Action:
Motion: Mr. Alan Ferretti moved to accept for information only.
Second: Mr. T.J. Smith
Action: Motion carried.

SA Issue #4
ISO Program Update

The issue was presented by Mr. George White, FBI CJIS. Mr. White introduced Mr. Stephen Exley of the ISO Program office staff and Mr. Jeffrey Campbell, who is the Assistant CJIS ISO. Mr. White also provided the following information:

- There has been discussion about partnering with the STARS conference for the ISO Symposium.
- The next iteration of the *CJIS Security Policy,* Version 5.1 should be released within the next 90 days. It will include all Advisory Policy Board actions (June and December 2011) which have been approved by the FBI Director.

- ISO Information
  Law Enforcement Online (LEO) homepage adjustments
  Frequently Asked Questions will be posted on-line
  ISO Chat recently hosted on LEO
- ISO Program Office continues to attend conferences/meetings
  Automated Fingerprint Identification System User's Group
  Florida Department of Law Enforcement
  Guam Visit
  IJIS Board

Security Access Subcommittee Action:
Motion: Mr. Alan Ferretti moved to accept for information only.
Second: Mr. Blaine Koops
Action: Motion carried.

SA Issue #5
Re-scope of Criminal Justice Information (CJI) Definition

This issue was presented by Mr. George White, FBI CJIS. Mr. White noted that during the past 12 months, there has been a growing sense within the CJIS community that the CJI definition is too broad and should be revisited. The States of Florida and Texas requested that the CJIS ISO take forward a topic paper to exempt ORIs from the CJI definition. There were various reasons but one reason in particular was to facilitate the transport of License Plate Reader (LPR) information. The proposed LPR process leveraged a stolen vehicle file extract that included ORIs for the purposes of identifying the agency associated with the stolen vehicle. By policy, ORIs are within the scope of the CJI definition and therefore require all the normal protections described within the policy.

The Subcommittee requested that the CJIS ISO develop alternatives to the current CJI definition; provide them to members during ad hoc teleconferences; and to bring recommendations based on those teleconferences to the spring 2012 Security Access Subcommittee meeting.

The following options were presented to the Subcommittee:

1. Make no changes to the *CJIS Security Policy*
2. Make changes to "Section 4.1 Criminal Justice Information" and "Appendix A Terms and Definitions" as indicated.

Security Access Subcommittee Action:
Motion #1: Mr. Alan Ferretti moved to make changes to "Section 4.1 Criminal Justice Information" and "Appendix A Terms and Definitions" as indicated below (italicized and bold font):

4.1 Criminal Justice Information (CJI)
Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. **Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

2. **Identity History Data**—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

3. **Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. **Property Data**—information about vehicles and property ***when*** associated with ***an individual***.

5. **Case/Incident History**—information about the history of criminal incidents.

The following types of data are exempted from the protection levels required for CJI:
1. ORI numbers when NOT associated with an individual
2. National Crime Information Center numbers (NIC) when NOT associated with an individual

NOTE: This exempted data should still be used for official purposes only and that the information that is linkable to an individual may require privacy protection(s).

The intent of the *CJIS Security Policy* is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g., within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules. ***In the interest of public safety due to the threat of physical harm, CJI may be released and that release documented for audit purposes.***

Appendix A Terms and Definitions

Criminal Justice Information (CJI) – Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property ***(when associated with an individual)***, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including but not limited to data used to make hiring decisions. ***The following types of data are exempted from the protection levels required for CJI:***
1. ORI numbers when NOT associated with an individual
2. NIC numbers when NOT associated with an individual

Second: Mr. Larry Coffee
Action: Motion carried.

Motion #2: Mr. Alan Ferretti moved that the proposed changes be vetted through the fall 2012 CJIS Working Group meetings.
Second: Mr. Larry Coffee
Action: Motion carried.

NOTE: There was additional discussion concerning other transaction type numbers that could fit into the same category as ORI and NIC numbers. Although the motion to make the requested changes passed, the Subcommittee expressed a desire for the ISO to take another look at the ORI and NIC exemptions and see if other types of transaction number should be included in the exemption

SA Issue #6
Noncriminal Justice Agency (NCJA) User Agreements and the *CJIS Security Policy*

This issue was presented by Mr. George White, FBI CJIS. One of the evolutionary changes in Version 5.0 of the *CJIS Security Policy* was the inclusion of the NCJA community. Feedback has been positive however, areas requiring further clarification have been noted. Specifically, the Subcommittee requested a better description of information exchange agreements and/or addendums needed for NCJA functions.

There was additional discussion on using the title "Chief Administrator." Jeff Mathews argued that this position is a technical appointment in the State of Arkansas and is a totally different role than their "Repository Manager." The title was used here in an attempt to blend *CJIS Security Policy* language with the Outsourcing Standard.

The title "authorized recipient" was also used but was not acceptable to the Subcommittee so it was dropped.

The following options were presented to the Subcommittee:

1. Make no changes to the *CJIS Security Policy*
2. Modify the current *CJIS Security Policy* language regarding NCJA user agreements with the proposed changes (as detailed below in italicized and bold font) in 2a, 2b, 2c, 2d

2a Current:
5.1.1.7 Security and Management Control Outsourcing Standard

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

2a. Proposed:
5.1.1.7 Outsourcing Standard for Channelers

Channelers designated to request civil fingerprint-based background checks on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Channelers. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standard for Non-Channelers
Contractors designated to perform noncriminal justice ancillary functions on

behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

2b. Current:

5.1.1.6 Agency User Agreements
A NCJA (public)…
A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. An NCJA (private) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (private) is a local bank.
All NCJAs accessing…

2b. Proposed:

5.1.1.6 Agency User Agreements
A NCJA (public) ……
A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. ***A NCJA (private) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access.*** *An example of a NCJA (private) is a local bank.*
All NCJAs accessing…..

2c. Current:

5.1.2 Monitoring, Review, and Delivery of Services
As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.

2c. Proposed:

5.1.2 Monitoring, Review, and Delivery of Services
*As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA**, authorized agency, and/or FBI** shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.*

2d. Current:

5.1.2.1 Managing Changes to Service Providers
Any changes to services provided by a service provider shall be managed by the CJA. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

2d. Proposed:

5.1.2.1 Managing Changes to Service Providers
*Any changes to services provided by a service provider shall be managed by the CJA**, authorized agency, and/or FBI**. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.*

Security Access Subcommittee Action:
Motion: Mr. Alan Ferretti moved to modify the current *CJIS Security Policy* language regarding NCJA user agreements with proposed changes as detailed below in 2a, 2b, 2c, and 2d (changes/additions/strikeouts are in bold font).

2a. Proposed:
5.1.1.7 Outsourcing Standard for Channelers

Channelers designated to request civil fingerprint-based background checks on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Channelers. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standard for Non-Channelers
Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

2b. Proposed:

5.1.1.6 Agency User Agreements
A NCJA (public) ……
A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. ***A NCJA (private) receiving***

access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. *An example of a NCJA (private) is a local bank.*
All NCJAs accessing…..

2c. Proposed:

5.1.2 Monitoring, Review, and Delivery of Services
*As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA**, authorized agency, and/or FBI** shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.*

2d. Proposed:

5.1.2.1 Managing Changes to Service Providers
*Any changes to services provided by a service provider shall be managed by the CJA**, authorized agency, and/or FBI**. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.*

Second: Mr. Charles "Jeff" Matthews
Action: Motion carried.

SA Issue #7
Cloud Computing White Paper and Proposed *CJIS Security Policy* Language

This issue was presented by Mr. George White and Mr. Stephen Exley, FBI CJIS.
Whether driven by economic efficiencies or technological improvements, increasing numbers of organizations in the CJIS community are considering transitioning to a cloud environment. The Subcommittee recognized this and asked the CJIS ISO Program to study the issue and report back with a White Paper and recommendations for identifying a common reference for discussing clouds and identifying vulnerabilities and best practices. Members were provided with a copy of the White Paper on Cloud Computing. Mr. Exley discussed the proposed cloud computing verbiage for the *CJIS Security Policy,* as outlined below:

5.10.1.5 Cloud Computing
Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing White Paper (Appendix G.3), National Institute of Standards and Technology (NIST) SP 800-146, and the cloud provider's policies and capabilities, will enable organizations to make informed decisions on whether or not the cloud provider can provide the service and be compliant with the requirements of the *CJIS Security Policy*. When the cloud provider is a private contractor it is subject to the same requirements as other private contractors, e.g., signed Security Addendum (5.1.1.5), personnel screening (5.12.1.2), and audits (5.11.2).

Add Following Definitions to Appendix A:

Cloud Computing – A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud subscriber – A person or organization that is a customer of a cloud.

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber.

Cloud provider – An organization that provides cloud services.

Add the following to Appendix I (References):

NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing
NIST SP 800-145, the NIST Definition of Cloud Computing
NIST SP 800-146 (DRAFT), Cloud Computing Synopsis and Recommendations

Additional discussion included the differentiation between distributed and non-distributed cloud computing. The Subcommittee also urged that this section be related back to the other policy areas.

Security Access Subcommittee Action:
Motion: Mr. Alan Ferretti moved to circle back to the subject and add specificity to the aspects unique to cloud computing's differing models. In addition, reduce the amount of information that is repeated from NIST references to a manageable level and specific to policy. Ensure the language emulates that found in the virtualization section (of the *CJIS Security Policy)*.
Second: Mr. Bill Phillips
Action: Motion carried.

SA Issue #8
Advanced Authentication (AA) Use Cases

This issue was presented by Mr. Stephen Exley, FBI CJIS. The CJIS ISO Program receives regular inquiries regarding the AA requirement. Most of the guidance provided references the proper implementation of AA. The CJIS ISO Program has created a number of use case scenarios in order to offer additional guidance regarding the implementation of AA within compliance of the *CJIS Security Policy.*

The following options were presented to the Subcommittee:

a. Approve the Advanced Authentication Use Case scenarios for inclusion in the upcoming CJIS ISO Frequently Asked Questions Website as detailed in Attachment #1.
b. Approve the Advanced Authentication Use Case scenarios for inclusion in the *CJIS Security Policy* as detailed in Attachment #2.

Security Access Subcommittee Action:
Motion #1: Mr. T.J. Smith moved to accept recommendations a and b:

a. approve the Advanced Authentication Use Case scenarios for inclusion in the upcoming CJIS ISO FAQ Website as detailed in Attachment #1.

b. Approve the Advanced Authentication Use Case scenarios for inclusion in the *CJIS Security Policy*, as detailed in Attachment #2.

Attachment #1
Advanced Authentication (AA) Use Cases for Inclusion into the upcoming CJIS ISO FAQ Website

Request the Advanced Authentication Use Case scenarios seen in this attachment be made publically available via the upcoming CJIS ISO FAQ website as detailed in the following examples:

Advanced Authentication Use Case Scenarios:
Use Case 1 - A Local Police Department's Authentication Controls
During the course of an investigation, a detective accessed CJI from a hotel room using an agency issued mobile broadband card. To gain access, the detective first established the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption), then was challenged to enter both password and the value from a hardware token (satisfying the requirement for advanced authentication). Once the detective's credentials were validated, his identity was asserted by the infrastructure to all authorized applications needed to complete his investigation.

Use Case 2 – Smart Card
A user has been issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects the application, enters the proper username (identification), a password ("something you know"). Once challenged,

the user connects the smart card ("something you have") to the terminal. The user will then be prompted to enter a user pin number to unlock the smart card. Once unlocked, the smart card will send the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates presented from are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based
A user has been issued a laptop and connects to the agency network via an agency issued mobile broadband card and an encrypted VPN tunnel. As part of an on-going investigation, the user initiates an application that will permit access to CJI from the agency-issued laptop. The user is then prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a text message containing a One-Time Password (OTP) is sent (out of band) to the user's agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user then enters the OTP ("something you have") received via text. The username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Risk-based Authentication (RBA)
A user has just moved office locations and requires email access (containing CJI) via an Outlook Web Access (OWA) client that has a Risk-based Authentication solution implemented. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user and is not listed under the user's profile. The user is then prompted to answer the high-risk challenge/response questions. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, RBA solution logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. The CSP requirements for an acceptable RBA solution have been satisfied.

Use Case 5 – Biometrics (fingerprint)
A user requires access to CJI from a laptop while in the field processing data. The user requests a remote session back to the local agency, enters a username (identification), enters a password ("something you know"), then swipes his/her fingerprint ("something you are") using an attached fingerprint reader. The software associated with the reader collects and sends the fingerprint attributes to software that asserts the fingerprint attributes to the authentication solution at the local agency (satisfies the requirement that an individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level) along with the asserted username and password. The authentication solution accepts the asserted attributes and interrogates the database to verify the asserted attributes matches. The username, password, and asserted fingerprint attribute are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 6– Hardware Token OTP – Blackberry Mobile phone-based
A user has been issued a Blackberry and a hardware token that displays a One-Time Password (OTP) and generates a new OTP every 60 seconds. The user initiates an application that connects to the CSA and will allow for CJI processing from the

Blackberry. The user is challenged for a username (identification), password ("something you know"), and the OTP ("something you have") from the hardware token. The username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Attachment #2
Advanced Authentication (AA) Use Cases for CJIS Security Policy Inclusion

Request the Advanced Authentication Use Case scenarios seen in this attachment are made publically available via inclusion in the *CJIS Security Policy* as detailed in the following examples:

Current language:
Figure 7 - A Local Police Department's Authentication Controls
During the course of an investigation, a detective accessed CJI from a hotel room using an agency issued mobile broadband card. To gain access, the detective first established the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption), then was challenged to enter both password and the value from a hardware token (satisfying the requirement for advanced authentication). Once the detective's credentials were validated, his identity was asserted by the infrastructure to all authorized applications needed to complete his investigation.

Proposed language:
Figure 7 – Advanced Authentication Use Cases
Use Case 1 - A Local Police Department's Authentication Controls
During the course of an investigation, a detective accessed CJI from a hotel room using an agency issued mobile broadband card. To gain access, the detective first established the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption), then was challenged to enter both password and the value from a hardware token (satisfying the requirement for advanced authentication). Once the detective's credentials were validated, his identity was asserted by the infrastructure to all authorized applications needed to complete his investigation.

Use Case 2 – Smart Card
A user has been issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects the application, enters the proper username (identification), a password ("something you know"). Once challenged, the user connects the smart card ("something you have") to the terminal. The user will then be prompted to enter a user pin number to unlock the smart card. Once unlocked, the smart card will send the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates presented from are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based
A user has been issued a laptop and connects to the agency network via an agency issued mobile broadband card and an encrypted VPN tunnel. As part of an on-going

investigation, the user initiates an application that will permit access to CJI from the agency-issued laptop. The user is then prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a text message containing a One-Time Password (OTP) is sent (out of band) to the user's agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user then enters the OTP ("something you have") received via text. The username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Risk-based Authentication (RBA)
A user has just moved office locations and requires email access (containing CJI) via an Outlook Web Access (OWA) client that has a Risk-based Authentication solution implemented. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user and is not listed under the user's profile. The user is then prompted to answer the high-risk challenge/response questions. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, RBA solution logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. The CSP requirements for an acceptable RBA solution have been satisfied.

Second: Ms. Brenda Abaya
Action: Motion carried.

Motion #2: Mr. T.J. Smith moved to generate and include use cases that depict negative scenarios.
Second: Ms. Brenda Abaya
Action: Motion carried.

SA Issue #9
Non-Standard Requests and Dissemination of Criminal Justice Information

This issue was presented by Mr. Jeffrey Campbell, FBI CJIS. The *CJIS Security Policy* defines social engineering as:

The act of manipulating people to perform action or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

The threat to CJI from social engineering was discussed at the fall 2011 Subcommittee meeting. Many members were concerned about the ease of accessing CJI through social engineering and asked the CJIS ISO Program to review the issue and develop recommended addition(s) to the *CJIS Security Policy* to address the threat more comprehensively.

The following options were presented to the Subcommittee:

1. Accept recommendations 1a, 1b, and 1c
2. Make no changes to the *CJIS Security Policy*

Security Access Subcommittee Action:
Motion: Mr. Terrence O'Connell moved to accept recommendations 1a, 1b, and 1c:

1a. Add a requirement for a local policy to identify an individual requesting CJI outside the agency's formal, established channels (e.g., telephone, fax, in-person outside office environment): Law enforcement and civil agencies shall have a local policy stating the requirement to validate a requestor of CJI as an authorized recipient before disseminating CJI.

Current *CJIS Security Policy Language with recommended addition in bold:*

5.1.1 Information Exchange
Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI. Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. See Section 5.1.3 for secondary dissemination guidance. ***Law enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.***

1b. Adding section 5.1.4 Secondary Dissemination of Non-CHRI CJI to the *CJIS Security Policy* to clarify this dissemination requirement and re-number current section 5.1.4 References/Citations/Directives to 5.1.5

Current *CJIS Security Policy* Language:

5.1.3 Secondary Dissemination
If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 References/Citations/Directives
Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

Proposed *CJIS Security Policy* Language with Recommended Addition in Bold:

5.1.4 Secondary Dissemination of Non-CHRI CJI
If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as a member of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

5.1.5 References/Citations/Directives
Appendix I contains all of the references used in this policy and may contain additional sources that apply to this section.

1c. Remove topic 7, Social Engineering from 5.2.1.2, Personnel with Physical and Logical Access, and add the social engineering security awareness training topic to 5.2.1.1, All Personnel, as topic 9. This will result in all authorized personnel with access to CJI to receive this training. Following is what the new 5.2.1.1 will look like after the Social Engineering topic is removed from 5.2.1.2:

5.2.1.1 All Personnel

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI::

1. *Rules that describe responsibilities and expected behavior with regard to CJI usage.*
2. *Implications of noncompliance.*
3. *Incident response (Points of contact; Individual actions).*
4. *Media protection.*
5. *Visitor control and physical access to spaces-discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.*
6. *Protect information subject to confidentiality concerns – hardcopy through destruction.*
7. *Proper handling and marking of CJI.*

8. *Threats, vulnerabilities, and risks associated with handling of CJI.*
9. ***Social Engineering.***
10. *Dissemination and destruction.*

Second: Mr. Bill Phillips
Action: Motion carried.

SA Issue #10
Visitor Log Record Requirements for Physically Secure Locations

This issue was presented by Mr. George White, FBI CJIS. The requirement for tracking all visitors to physically secure locations has not only been a longstanding basic requirement from a physical security perspective but has also been a specific requirement outlined in the *CJIS Security Policy* for many years.

The current requirements are outlined in paragraph 5.9.1.8 of the *CJIS Security Policy.*
(Note: the fall 2011 APB approved removing the requirement for "signature of visitor" from the bulleted list of access record requirements.)

5.9.1.8 Access Records

The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publically accessible) that includes:

1. *Name and agency of the visitor*
2. *Form of identification*
3. *Date of access*
4. *Time of entry and departure*
5. *Purpose of visit*
6. *Name and agency of person visited*

The visitor access records shall be maintained for a minimum of one year. Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.

The CJIS ISO received a written request from the Amarillo Police Department to abandon the requirement in the *CJIS Security Policy,* Version 5.0, for agencies to maintain access records of visitors to physically secure locations. Amarillo Police Department's detective division and many administrative offices are located within the boundaries of physically secure locations and there is great concern that requiring visitors, victims, witnesses, or persons of interest, etc., to log in and out will "have a chilling effect on their willingness to come to the police department." Visitors to these areas are always escorted and their presence is generally noted in a police report or detective's case file.

Mr. White noted that the FBI/CJIS Office of General Counsel Privacy Officer "does not recommend an exception or deletion of this security policy requirement."

The following options were presented to the Subcommittee:

1. Make no changes to the *CJIS Security Policy*.

2. Delete paragraph 5.9.1.8, Access Records from the *CJIS Security Policy.*

Proposed deletion:

~~***5.9.1.8 Access Records***~~
~~*The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publically accessible) that includes:*~~

~~*1. Name and agency of the visitor.*~~
~~*2. Form of identification*~~
~~*3. Date of access.*~~
~~*4. Time of entry and departure.*~~
~~*5. Purpose of visit.*~~
~~*6. Name and agency of person visited.*~~
~~*The visitor access records shall be maintained for a minimum of one year.*~~
~~*Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.*~~

3. Approve the following modification to the verbiage in paragraph 5.9.1.8 of the *CJIS Security Policy*:

5.9.1.8 Access Records (Current)
The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publically accessible) that includes:

1. *Name and agency of the visitor.*
2. *Form of identification*
3. *Date of access.*
4. *Time of entry and departure.*
5. *Purpose of visit.*
6. *Name and agency of person visited.*

The visitor access records shall be maintained for a minimum of one year. Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.

5.9.1.8 Access Records (Proposed)

The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publically accessible) that includes:

1. *Name and agency of the visitor.*
2. *Form of identification*
3. *Date of access.*
4. *Time of entry and departure.*
5. *Purpose of visit.*
6. *Name and agency of person visited.*

Individuals whose visit is recorded in a police report, investigative file, or similar documentation are exempt from these requirements.

The visitor access records shall be maintained for a minimum of one year. Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.

Discussion: This issue generated a great deal of discussion from the membership. Previously, the Working Groups had voted to make no change to the current policy. Mr. Alan Ferretti noted that by telling chiefs and sheriffs what to do in their offices and by forcing the issue – "we are imposing on them something that is not any of our business." Mr. Terrill O'Connell noted that part of the argument is that the individuals are being logged elsewhere - in other places within the building. Discussion also revolved around defining "visitor" and how to protect confidential informants.

Security Access Subcommittee Action:
Motion #1: Mr. Joe Dominic moved to make no change to the *CJIS Security Policy.*
Second: Mr. Terrill O'Connell
Action: Motion carried by a vote of 7-4.
The following members voted to make no change: O'Connell,Truitt, Abaya, Dominic, Tipton, Phillips, Matthews. Motion opposed by the following members: Ferretti, Coffee, Koops, Smith.

Motion #2: Mr. T.J. Smith moved to research and develop a definition for "visitor" for the purpose of determining whether the term today, without associated definition, places too high of a burden on agencies with respect to visitor sign-in.
Second: Mr. Alan Ferretti
Action: Motion carried.

SA Issue #11
CSO Latitude for Accepting Background Checks Previously Conducted in CSO's Jurisdiction

This issue was presented by Mr. George White, FBI CJIS. There have been questions raised about whether the CSO has the latitude to accept background checks conducted previously by other agencies within the CSO's jurisdiction. While this has been an accepted practice it has been proposed to formalize it with language stating such in the *CJIS Security Policy.* The intent of the policy is to ensure contractors/vendors with criminal records consisting of felony conviction(s) and other disqualifying factors are not granted access to CJI. The formal acknowledgement of the CSO's latitude to accept background checks conducted previously by other agencies within the CSO's jurisdiction will allow business to be conducted in an efficient and timely fashion for the CSO and the vendor/contractor.

Because the effectiveness of a background check decreases with age, the recommendation states a CSO may not accept background checks that are more than 12 months old.

The following options were provided to the Subcommittee:

1. Make no change to the *CJIS Security Policy*

2. Accept the following addition (in bold font) to the *CJIS Security Policy* as new paragraph 5.12.1.1(10), Minimum Screening Requirements for Individuals Requiring Access to CJI:

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:
1. To verify identification, a state or residency and national fingerprint-based record checks shall be conducted…

9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject…

10.The CSO has the latitude to accept favorably adjudicated background checks within their jurisdiction that are not more than 12 months old.

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

Security Access Subcommittee Action:
Motion: Mr. Joe Dominic moved to accept the following addition (in bold font) to the *CJIS Security Policy* as new paragraph 5.12.1.1(10) Minimum Screening requirements for Individuals Requiring Access to CJI:

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI

10. The CSO has the latitude to ~~accept~~ allow acceptance of favorably adjudicated background checks within their jurisdiction that are not more than 12 months old.
Second: Mr. Brad Truitt
Action: Motion carried.

SA Issue #12
Mobile Device CJIS Security Matrix and White Paper

This issue was presented by Mr. Jeffrey Campbell, FBI CJIS. There is increasing interest in deploying mobile devices, specifically cell phones and tablets, throughout the national CJIS community. Securing these devices is critical in protecting criminal justice information. Many agencies are looking for guidance on how to successfully integrate these devices into their network while maintaining compliance with the *CJIS Security Policy*. Members were provided additional information in two attachments: Mobile Device Security and Mobile Device Compatibility Matrix.

Security Access Subcommittee Action:
Motion: Mr. Alan Ferretti moved to develop policy language to move toward a Blackberry Enterprise Server-like standard for mobile devices. An ad-hoc task force will work on and fast track the proposal to the fall 2012 Working Groups.
Second: Mr. Brad Truitt
Action: Motion carried.

SA Ad Hoc Issue #1
Non-US Citizen Access to CJI

The discussion revolved around consulting firms located in the United States who subcontract IT work to non-US Citizens. Mr. Joe Dominic noted it is difficult to find US citizens to do this type of work as they do not have the expertise that is available from non-US citizens in China, Russia, India and Canada. There was also discussion about maintenance updates that are handled "remotely" by these contractors.

Mr. White pointed out that DOJ 2640.2F does not apply to the states. Additional discussion Centered on the use of the term "legal ability to work" versus "green card" holders within the scope of the topic. For those with remote access into a system that processes CJI, managing or monitoring that access should be accomplished.

Other thoughts included excluding the "Five I" countries (United States, United Kingdom, Australia, New Zealand and Canada). This was favorably received by the Subcommittee but they also felt that India should be included as there are many people regularly employed from that country.

Security Access Subcommittee Action:

ACTION ITEM: The ISO Program office staff was asked to research and provide some guidance as to what countries would be allowed access; what type of access; and how the access could be managed.

SA Ad Hoc Issue #2
Next Generation Identification (NGI) Update

This issue was provided by Mr. Brian Edgell, FBI CJIS. Mr. Edgell provided a high level briefing on the status of NGI and the implementation schedule, as outlined below:

Increment 0 – Complete
Advanced Technology Workstations

Increment 1 – Complete
Initial Operational Capability

Increment 2 – Complete
Repository for Individuals of Special Concern and Initial NGI Infrastructure

Increment 3 – In progress
Palms and Latents

Increment 4 – In progress
Rap Back, Facial, Photo/Scars, Marks, Tattoos Search Capabilities

Increment 5 – In progress
Iris Pilot

Increment 6 – Technology Refreshment

Security Access Subcommittee Action:
Accepted for information only.

SA Ad Hoc Issue #3
NCJA Audit Requirements from *CJIS Security Policy Appendix J*

Mr. Larry Coffee expressed concerns about NCJA Audit Requirements as outlined in Appendix J of the policy. NCJAs are required to retain audit records but the policy does not reference that there is a requirement to create audit logs. Mr. George White explained that auditing varies greatly between NCJAs based on their roles and it should be left to the locals to decide specific requirements.

Security Access Subcommittee Action:

Action Item: The ISO Program Office to review Appendix J and determine if any changes are necessary.

Future Compact Council and Advisory Process-related meetings were announced:

Compact Council Meeting
May 15-17, 2012
San Antonio, Texas

Advisory Policy Board Meeting
June 5-7, 2012
Buffalo, New York

CJIS Working Group Meetings
NGI User Conference
August 14-17, 2012
Atlanta, Georgia

There being no further business, the meeting adjourned at 5:00 p.m.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
ADVISORY POLICY BOARD (APB)
BUFFALO, NEW YORK
JUNE 6-7, 2012

STAFF PAPER

APB ITEM #21

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

The Identification Services (IS) Subcommittee was called to order by Chairman Michael Lesko on April 18th, 2012, at 1:00 p.m.

Mr. Nicky J. Megna, Next Generation Identification (NGI) Program Office (NGIPO), Criminal Justice Information Services (CJIS) Division, served as Designated Federal Officer for the meeting.

The Pledge of Allegiance was recited and the meeting commenced.

IS Subcommittee roll call was called by Vice Chairman Charles Schaeffer.

Mr. Lesko went over housekeeping notes for the meeting.

The following members were present:
Mr. Louis Assaro, U.S. Citizenship and Immigration Services, Clarksburg, WV
Mr. Kenneth Bischoff, Western Identification Network, Inc., Rancho Cordova, CA
Mr. James Buckley, Jr., Immigration and Customs Enforcement, Clarksburg, WV
Mr. Thomas F. Callaghan, Federal Bureau of Investigation, Washington, DC
Ms. Terry D. Gibbons, Georgia Bureau of Investigation, Decatur, GA
Lt. Gabriel Keown, Philadelphia Police Department, Philadelphia, PA
Mr. Michael C. Lesko, Texas Department of Public Safety, Austin, TX
Mr. Joseph N. Morrissey, New York State Division of Criminal Justice Services, Albany, NY
Mr. Brian Pittack, Department of Homeland Security, Arlington, VA
Mr. Charles Schaeffer, Florida Department of Law Enforcement, Tallahassee, FL

Members not attending but represented by proxy:
Ms. Allison Miller served as proxy for Ms. Lauren Cooney, US Army Biometrics Identity Management Agency, Clarksburg, WV
Mr. Ed German served as proxy for Ms. Keri Moorefield, U.S. Government, Washington, DC

Gallery Attendees:
Ms. Chasity Anderson, FBI CJIS Division, Clarksburg, WV
Mr. Gary Barron, FBI CJIS Division, Clarksburg, WV
Mr. William Casey, FBI CJIS Division, Clarksburg, WV
Mr. Leslie Cavis, FBI CJIS Division, Clarksburg, WV
Ms. Shelley Dolf, FBI CJIS Division, Clarksburg, WV
Mr. Brian Edgell, FBI CJIS Division, Clarksburg, WV
Mr. Patrick Fagan, III, SAVA Workforce Solutions, Richmond, VA
Ms. Trudy Ford, FBI CJIS Division, Clarksburg, WV
Mr. Michael Gannon, Department of Homeland Security, Arlington, VA
Mr. David Gavin, SAVA Workforce Solutions, Austin, TX
Mr. James Gerst, FBI CJIS Division, Clarksburg, WV
Ms. Natalie Givan, FBI CJIS Division, Clarksburg, WV
Mr. John Kane, FBI CJIS Division, Clarksburg, WV
Ms. Christy Kirkwood, FBI CJIS Division, Clarksburg, WV
Mr. James Loudermilk, FBI Headquarters, Washington, DC
Mr. Jerry Marco, FBI CJIS Division, Clarksburg, WV
Mr. Allen Nash, FBI CJIS Division, Clarksburg, WV
Mr. William G. McKinsey, FBI CJIS Division, Clarksburg, WV
Mr. James Mills, FBI CJIS Division, Clarksburg, WV
Ms. Beth Owens, Franklin County, OH
Mr. Scott Phillips, FBI CJIS Division, Clarksburg, WV
Mr. Jon Kevin Reid, FBI CJIS Division, Clarksburg, WV
Mr. William Reindollar, Department of Homeland Security, Arlington, VA
Mr. Tadgh Smith, Department of Homeland Security, Washington, DC
Ms. Jennifer Stathakis, FBI CJIS Division, Clarksburg, WV
Mr. Brian Stump, FBI CJIS Division, Clarksburg, WV
Ms. Laura Sudkamp, Kentucky State Police Forensic Laboratories, Frankfort, KY
Mr. Scott Trent, FBI CJIS Division, Clarksburg, WV
Ms. Rachel Tucker, FBI CJIS Division, Clarksburg, WV
Mr. Sudhindra Umarji, Trusted Federal Systems, Inc., Rockville, MD
Ms. Christina Wolverton, FBI CJIS Division, Clarksburg, WV
Mr. Steve Wilkins, Pierce County Sheriff's Office, Pierce County, WA
Mr. Gary Williams, FBI CJIS Division, Clarksburg, WV

(Minutes will be reported in the order according to the agenda.)

IS Issue #1
White Paper – Public Safety Strategies

Mr. Kshemendra Paul, Program Manager of the Information Sharing Environment (ISE), presented Responsible Information Sharing. The goal is to improve information sharing across the government communities and mission partners. Information is a national asset, must be shared and safeguarded, and informs proactive decisions. Mr. Paul spoke to the need to expand our focus beyond the Systems Development Lifecycle, to consider information integration throughout each phase; information management first, system development second. Standards are the key to information interoperability, providing the foundation for consistent procurement language and tool development. The drive is for an information interoperability eco system. Mr. Paul also recognized that technical and policy barriers exist and that the current financial situation is driving decisions. The ISE is currently working with the International Association of Chiefs of Police and Global Justice, and now looking to the APB to support standards definition. They are also looking to identify additional pilot projects opportunities.

Discussion: Mr. McKinsey questioned if this has any relation to the White House initiative that requires agencies to name one service (by August) that we are willing to do for the government as a whole, and have it in place by December. Mr. Paul answered this could be a way to do that. He stated it was obvious the CJIS Division is a shared service organization. Mr. Assaro asked if Mr. Paul's office has to deal with the fallout from rushed initiatives gone wrong. Mr. Paul replied that they try to be more proactive, move forward. One success from his office was Sensitive But Unclassified Network Interoperability, responding to state and local concerns about a lack of interoperability across government networks. Mr. Edgell stated CJIS is working with Integrated Justice Information Systems (IJIS) and the major police associations. This subcommittee body aligned with IJIS last fall as a trusted partner. Mr. Edgell followed asking who from your vantage point is best suited to represent industry, and more specifically biometrics. Mr. Paul responded that he was reluctant to endorse any, but rather just inform who they were working with. They are working with IJIS closely on the spring board initiative. Certification of standards conformance and compliance is a key issue. They are working with OASIS for identify management. Object Management Group, model driven architectures, UML. IJIS isn't a standards organization, but an active vendor association in the space we operate in. ACT-IAC is writing a whitepaper on standards based procurement. Mr. Paul stated they are asking industry to change their business model, trying to realize efficiencies in procurement. Mr. Paul asked if there were other groups they should be reaching out to? Mr. Edgell stated he shared the same concern, does IJIS represent the true vendor community. Mr. Paul noted that the IJIS view is focused on Justice and public safety, questioning the access to product managers in Oracle or Microsoft. ISE can reach these folks through OASIS. Mr. Schaeffer commented on the ISE vision statement, agreeing it is where we are. Mr. Schaeffer continued, what's

missing is how do we get there? Is there some consideration in your organization to create a road map? A lot of folks are willing to go down a road if they know how to get there, but if you lay out a vision and we don't have a path to get there, it remains just a goal. Is there someone working on laying that out? Mr. Paul responded that it is his office's responsibility to catalyze that process; one is a standards way forward document, technical standards and business process standards, with support across stakeholders to move out on. It's not as strategic as it could be, based on where they have the coalition of the willing. Mr. Paul continued the other thing is the transformation initiative, work that was catalyzed last year, looking now at how we do this. It's not a step A-B-C roadmap, but principles under an umbrella vision. Mr. Paul is not looking to create yet another body, but to better cross latch existing organizations, use that to drive the details. Mr. Lesko stated that we have seen various iterations of this thought piece from this group before. They've been shared and the IS Subcommittee has made comments, but have not seen their comments reflected in the Global document. Mr. Lesko continued, that getting buy in requires all parties buying in to have appropriate input into this design, else we leave it as Global is the driver. Mr. Paul responded that through his leadership function and based on his preference to work through existing structures, he will work to identify how to better cross link APB and Global. Mr. Paul would like to see the feedback directly, stating it pains him to know that work was done and not reflected. The request was heard loud and clear and he will take as an action item. Mr. Megna noted, the National Institute of Standards and Technology (NIST) have played a critical role in the identification and development of standards enabling interoperability, resulting in thousands of state/local/federal agencies submitting transaction electronically every day. They've now shifted focus to trying to get private industry on board to build the things needed right now. Mr. Fagan added, adoption of standards is still the number one inhibitor for agencies to move forward. Working for NGI he's hearing agencies state they don't have the financial resources to migrate to the new standards. He asked Mr. Paul if he had insight into funding sources for this adoption. Mr. Paul replied he feels we are way too timid in leveraging special condition languages on grants and acquisition regulations; we need to make sure you are going through a collaborative process with state and local, industry, not just government standards. We have a process driving this balance right now. Mr. Paul is asking the APB to help inform what we do with procurement language. Mr. Buckley stated that the Department of Homeland Security (DHS) has already starting leveraging grant money on special conditions. Mr. Bischoff stated that preconditions on grants are ok as long as you recognize the unique circumstance of each state and local. Local agencies can often be further along than the state, so these caveats become pretty arbitrary if agencies are not in sync. Mr. Lesko closed with wanting to make sure it's bottom up with stakeholder involvement for standards development.

IS Issue #2
Identification Services Coordination Group Update

Mr. Charles Schaeffer presented this issue. The purpose of this issue was to provide an update on the current Identification Services Coordination Group (ISCG) activities, including action items that resulted from the previous days face-to-face meetings.

- **Topic 1 – NGI Readiness Assessment**
  - *Action Item 1: CJIS establish a common definition of Palm, and best practices for its capture and usage, to be disseminated in a more user friendly type of communication at the NGI User Conference.*
  - *Action Item 2: The ISCG will continue to discuss and document best practices for establishing policies for collecting biometrics at the local and state level.*
  - *Action Item 3: The NGIPO will prepare a chart depicting which version of the Electronic Biometric Transmission Specification (EBTS) each state is currently using and will prepare a timeline for when each state plans to migrate to the EBTS v9.0 or higher.*
- **Topic 2 -- NIST Study Regarding 1000 ppi and 500 ppi Images**
  - *Action Item: CJIS quantify the difference between 500 ppi and 1000 ppi capture and storage for latent services prior to setting 1000 ppi as the final goal.*
- **Topic 3-- Latent Interoperability Transmission Specification (LITS)**
  - *Action Item: The ISCG will review the special publication of the LITS and provide comments to the NGIPO for review during the fall CJIS APB process.*
- **Topic 5 --Unsolved Latent File (ULF) Maintenance Issues**
  - *Action Item 1: The ISCG will work in collaboration with the Latent Services Steering Committee to identify deletion strategies and provide recommendations to the FBI and the IS Subcommittee.*

Mr. Buckley asked what had happened to previous recommendations from the working groups from previous years. Mr. Schaeffer responded that work has progressed and records had been deleted, but strategies need to continue to be evaluated. Previous suggestions to apply statutes of limitations and seriousness of crime were not available based on the contributor knowledge that if they selected homicide they would get their results faster; therefore it's estimated that 90% of the records are marked homicide. Asking the agencies to validate their records would be a hefty request. Mr. German asked if we'd approached the White House for funds to help with the current problem of the ULF. The White House has demonstrated a significant interest in Latent Interoperability initiatives and may be responsive to this request. Mr. Edgell responded that it would be premature to provide a number at this point because NGI has yet to deploy Increment 3 and has not had the opportunity to evaluate the performance and to understand what tradeoffs between performance/storage/accuracy are available. Once

performance data has been developed a cost for ULF increase number could be developed. Mr. Lesko added that First-In-First-Out should not be an option and a better solution needs to be developed. Additionally, with a major national focus on latent interoperability, it appears that ULF activity will increase significantly.

  - *Action Item 2: The FBI will develop a best practice document on how to search the ULF and how to determine what images should be deposited in the ULF.*
  - *Action Item 3: The FBI will identify the top end number of the image features that can be stored in the ULF and try to identify the optimal number of features that are needed to make an identification.*
- **Topic 6 -- Expansion of the Repository for Individuals of Special Concern (RISC) Searches to Additional Repositories Including the Criminal Master File (CMF)**
  - *Action Item: The NGIPO will prepare a discussion paper on the future RISC services for the review of the CJIS APB.*
- **Topic 8 -- FBI/NIST Study on the Image Quality of Fingerprint Acquisition Profile (FAP) 10 and FAP 30 Mobile ID Devices**
  - *Action Item: That the FBI CJIS Division, in collaboration with the NIST conduct a study to compare the quality level of the FAP 10 and FAP 30 devices, and provide the results of the study to the ISCG.*

The subcommittee gave the ISCG and additional Action Item to look into information regarding the use of tattoos in a law enforcement capacity.

Motion: Mr. James Buckley, Jr. moved to endorse the recommendation by the ISCG, which recommends the IS Subcommittee allow the removal of the Tenprint Fingerprint Features Search Type of Transaction from the EBTS.
Second: Mr. Kenneth Bischoff
Action: Motion passed

IS Issue #3
Proposal to Modify Query Tenprint (QTP)

Ms. Buffy Bonafield, FBI CJIS Division, presented this issue. The purpose of this issue was to present further options to refine the QTP process based on an APB recommendation, and form a task group to conduct this work. The QTP Task Group was formed and at the August 17, 2011 meeting in Pittsburgh, Pennsylvania, they discussed the issues that are addressed in the paper.

Motion: For Issue 1, Mr. Kenneth Bischoff moved to accept Option 1, To modify the QTP search criteria to the exact last name match. Priority set to 3M.

Second: Mr. James Buckley, Jr.
Action: Motion passed

Motion: For Issue 2, Mr. James Buckley, Jr. moved to accept Option 2, No change. The QTP process will continue searching all persons files.
Second: Mr. Kenneth Bischoff
Action: Motion passed

Motion: For Issue 3, Mr. Kenneth Bischoff moved to accept Option 1, Protected Person data will be excluded from the QTP searches. Priority set to 3M.
Second: Mr. James Buckley, Jr.
Action: Motion passed

Motion: For Issue 4, Mr. Kenneth Bischoff moved to request that prior to implementation of Phase II revisit the 2008 recommendation to only return hits for 2 files to noncriminal justice agencies during Phase II.
Second: Mr. Joseph N. Morrissey
Action: Motion passed

Motion: For Issue 5, Mr. Charles Schaeffer moved to request research adding the Persons with Information data to the QTP search for Phase I.
Priority – 3M
Second: Mr. James Buckley, Jr.
Action: Motion passed

IS Issue #4
NGI Implementation and Transition Update

Mr. Brian Edgell, FBI CJIS Division, presented this issue. The purpose of this issue was to provide a high-level overview of the NGI Program implementation and transition efforts. Mr. Edgell started by stating that with the current focus on Rap Back, the NGIPO did not present a general NGI update to the working groups, but wanted to take some time and speak to it here. The NGI Program is halfway through its development phase. Mr. Edgell gave a quick recap of the deployments of increments 0 and 1 and associated successes. He stated we currently have over 500 agencies searching the RISC repository (Increment 2). We are adding the Immigration Violator File (IVF), into the wanted set of data, to be included in the next build. The enhanced latent functionality and the National Palm Print System are a year out from deployment. We are currently building training strategies and preparing for the new rollout of Universal Latent Workstation software. We have an internal working group with CJIS stakeholders to support the Increment 3 deployment. For new latent search accuracy we're seeing numbers in the mid 80s. The

Customs and Border Protection rapid response is currently being met today within IAFIS; NGI is building to support over 200,000 a day.

Discussion: Mr. German asked, for palms and latents, what does an investigative search mean? Mr. Edgell responded it's like a latent print search. Palms will be searched as they come in against known and unknown data sets. NGI will now search all of the events, not just the composite. CJIS has collected roughly 4 million palms to date, from 29 states. We have a Memorandum of Understanding (MOU) that's approved and ready to go, to gather additional palm prints from states repositories. Mr. Smith asked if this included searching against DHS latent repositories. Mr. Edgell responded, today we're searching their tenprint repositories and in increment 4 we will be able to use the Name of Designated Repository field to search latent repositories. Increment 4 is a compilation of new services. We're using biometrics as investigation enablers, using them earlier to aid investigations. Facial Recognition and Rap Back will be two new services that we don't have today, and we will do a pilot for each. Starting with facial recognition, we have a pilot that is operational today with have a repository of 12 million usable images. The state of Michigan is using this pilot now. The Biometric Services Section Face Team is waiting on interface and in August we'll deploy the Universal Face Workstation software. Again, there exist large quantities of data residing in state and local repositories on the order of 30 million. We have MOUs ready to go to gather that data. Mr. Edgell continued he would like to eliminate the MOU to move data, and make a policy to address it as part of the user agreement. The Rap Back Pilot will be available in May, starting with federal partners, and expanding to state and locals, once we evaluate the authority to retain civil fingerprints. Mr. Bischoff stated the existence of a pilot implies to the existence tag fields defined for the EBTS to populate the record. Mr. Bischoff is in the middle of detailed design with his vendor and cannot wait for the official EBTS next fall. Mr. Bischoff has eight states ready to go, and does not want to miss this opportunity. Mr. Edgell responded that for the pilot we are not using new fields, but reusing existing. Mr. Megna added, the NGI integrator feeds into the implementation of the EBTS specification. There also exists an EBTS working group, that we can extend you an invitation, if one has not been extended already. This is the earliest insight into what the changes are looking like that we can offer, but they still require the approval of the IS Subcommittee before it is recommend they be built against. Mr. Edgell added; the requirements are baked into the design, so we can help you anticipate some of those changes. The administrative burden of privacy and policy is where we are focusing. We appreciate your situation and understand your concern. Mr. Reid noted he wants to make sure it's understood that the policy issues are the show stopper here, not the technical. The Compact Council needs the support of this committee to really drive that effort. Mr. Bischoff stated the mechanical delivery mechanisms have to be there and are not dependent on policy. Mr. Reid stated that he disagrees; there are some policy issues that can change some of the technical interfaces significantly.

IS Issue #5
NGI Expansion of Repository for Individuals of Special Concern (RISC) Service to Include Additional Repositories

Mr. Brian Edgell, FBI CJIS Division, presented this issue. The purpose of this issue was to provide a response to an Action Item from the Fall, 2011 IS Subcommittee meetings. Mr. Edgell stated that the NGIPO had met with several federal mobility projects. NGI will pilot and expanded rapid search capability to include the entire CMF for six to eight FBI Field Offices, Task Force members and SWAT teams. The NGIPO will evaluate the tradeoffs and determine if it's feasible to search the entire CMF from a roadside situation without impacting current performance. This is also a mechanism to evaluate connecting strategies for federal law enforcement agencies. The NGIPO are responding to the action item.

Mr. Pender stopped in to address the group. He thanked everyone for coming, appreciate the effort it takes to get here. We are very happy to have you here; the APB is such a key part of our process.

IS Issue #6
NGI Rap Back Business Process Concept of Operations

Mr. David Gavin, FBI CJIS Division, presented this issue. This was a discussion topic that has gone through the working groups. First Mr. Gavin defined Rap Back as the FBI retains the fingerprints for civil events. Future incoming fingerprints will be searched against those and if there's a hit, then the subscribing agency(s) will be notified. The states have been doing this for some time, and now NGI will deliver this on a national level. This has been mostly driven by Compact Council because its dedication to noncriminal justice services, but there is a criminal component that will require the input of the APB, being vetted through the ISCG and the IS Subcommittee. Mr. Gavin gave some history of how the Rap Back Focus Group came to being, and the various levels of involvement in the definition of the NGI system requirements. He then reiterated that the Rap Back Business CONOPS is not a technical document, but a living process document. It's an attempt to describe the national Rap Back service. Any comments can be provided to Rachel Tucker. Rachel Tucker and John Kane are the engines driving the project. This current document does focus on the State Identification Bureaus, but there will be federal representation in the document in future versions. Mr. Gavin stated the NGIPO is requesting feedback on any and all areas. This document has come through the Rap Back Focus Group, SEARCH, APB Working Groups and Compact Council Standards and Policy Subcommittee. The privacy work is in the critical path right now so we'll look a little deeper here, starting with:

Feedback Area #1 Criminal Justice – The NGIPO has received unanimous agreement on the application of Rap Back for supervision, Sex Offender Registry (SOR), probation, and parolee subjects. This discussion centers on parameters for criminal justice purposes. For an Investigative use, if the detective is in a situation where they'd run a QH or QR, that would be a good candidate case to compare how Rap Back could be used. Concern surrounds scope creep of use and non removal of the Rap Back after it was no longer needed. This enhances the need to clearly communicate the use, Administration of Criminal Justice purpose only. Additionally, an expiration date to Rap Back subscriptions is being considered. To date the NGIPO has had a very broad endorsement for the use of Rap Back for criminal justice purposes.

Discussion: Mr. Schaeffer suggested considering a missing person as a new scenario, which Florida handles as an open investigation. Ms. Tucker stated this is something we can already do. Mr. Schaeffer furthered explained, if a nurse goes missing, could a detective promote that into a Rap Back? Mr. Edgell agreed that scenario is treated as an open investigation and we will look into it. Mr. Gavin again asked, if the group agrees that the QH, QR is a valid comparison for use? The group replied yes.

Feedback Area #2 Triggering events – These are the events that could be used to trigger a notification for activity on that Rap Back. Additionally, the Office of General Council (OCG is looking into activity on external data bases for inclusion as a trigger event. Triggering events are inclusive; the subscriber can choose any event.

Discussion: Disposition generated significant discussion. National Fingerprint File states do not send dispositions to CJIS and disposition reporting rates are low to begin with. Concern was generated about interim dispositions notices, on events not relevant to the disqualification potential. Mr. Gavin reiterated, you can choose what triggering events suit your needs. Mr. Gavin then posed a question to the group, do you see a unique criminal justice value to dispositions. Mr. Schaeffer noted a disposition is not a discrete event and therefore could result in many useless notifications.

Feedback Area #3 Linking Fields – Rap Back notifications will result in a new transaction between NGI and the states, in an unsolicited message. The appropriate information needs to be included in that notification to help trace back to the original subscription. The working groups discussed adding additional fields. Also create a number of user defined fields that the states could use consistently to work within their existing process.

Discussion: Mr. Smith stated that dispositions are a high value item for Immigration and Customs Enforcement (ICE). A disposition can change a visitor's status to criminal, which is valuable for ICE. Mr. Schaeffer noted again, an additional scenario would help for criminal justice business case for support. It was also asked if Concealed Carry

Weapons permit holders could be included in Rap Back, right now it's done based on name in some states. Mr. Edgell responded it would depend on the state statutes. Mr. Schaeffer inquired if multiple agencies are watching the same individual would they be notified of each other's interest? Mr. Edgell took that as something to look into.

Feedback Area #5 Conceptual services – For states without Rap Back programs could there be some function and service provided by NGI and CJIS to handle the notifications as they extend past the State Identification Bureaus (SIB). This is a post NGI concept, and completely optional. The Rap Back Focus Group was not enthusiastic about it, stating concern with CJIS going directly to an end user. Conversely, many states without existing Rap Back services expressed great interest. Mr. Gavin asked if this group request we further develop this conceptual service capability for criminal and civil capacities. The group replied yes.

Feedback Area #4 Privacy – Mr. Gavin started with a key statement, Rap Back doesn't give any new authority or access to criminal justice information. The following are tools for mitigating the risk of dissemination of criminal history information and Personally Identifiable Information to an unauthorized recipient; auditing and training, pre notification, validation, expiration, notice to the applicant OGC stated their recommendation is that all Rap Back subscriptions have to have pre notification, and 3 year validation or expiration. The problem is that in all user forums, alternately the users will say validation is a problem and pre notification is a problem.

Discussion: Mr. McKinsey inquired as to where the three years originated? Mr. Edgell commented that right now we have a policy approved by the APB for two years, because that was our best understanding four years ago. Now we've matured our understanding. Each of these are mitigations, no one solution fits all states and agencies. Mr. McKinsey asked if states will have the ability to choose which mitigations they will implement. Mr. Edgell replied the NGI solution supports all of these, technically, since one size does not fit all. Mr. Edgell was then asked to evaluate the resources required to perform record validation. Mr. Lesko stated in addition to the notice to the applicant of what will happen with their record, we should also provide notice to them with the process for removing their information upon termination of the employment or association. Additionally we should form agreements with the entity subscribing to that Rap Back requiring them to pull that record out, following up this agreement with an audit scenario. Mr. Loudermilk agreed that notice to the applicant about the removal of their information is a good strategy and should be pursued. Ms. Anderson noted we internally talked with audit on the agreement between agency and entity, and their request was "timely manner" is not an acceptable measure for audit. Mr. Lesko noted this is something we haven't agreed to and agrees it is something to establish. Mr. Schaeffer added we need to identify a consistent form for this notification so it can be audited. Mr. Lesko stated this resembles the relief from disabilities for NCIC. Mr. McKinsey requested a walk through how the

pre-notification makes it way to the entity. Mr. Lesko responded; in Texas, the event happens, then they send an email to the entity that has oversight of the individual notifying them of activity on one of their records. The entity then logs into a portal and views the name of the individual. The portal requests they validate their authority to receive the remaining information. Mr. Loudermilk questioned how the information within a pre notification, when the receiving entity no longer has an interest in the record, isn't a violation of the privacy act in and of itself. Mr. Edgell replied that is part of our dilemma in the accommodation of OGC and Privacy concerns, and the reason we've come up with the additional strategies.

IS Issue #7
Implementation of the NGI Enhanced Repository

Mr. Brian Edgell, FBI CJIS Division, presented this issue. The purpose of this issue was to single out a significant change to the way NGI will store information, particularly how an identity record will establish its "Master Name." Mr. Edgell stated that when a civil submission is the first submission, that name establishes the identity, regardless of any subsequent criminal activity. Previously, if a criminal submission happened after a civil name was established, the criminal name would replace the civil as the "Master Name."

Discussion: Mr. Morrissey asked if there was no longer a vested interest in the civil applicant, then the criminal name would be the master. Mr. Edgell replied we would take the Rap Back away, but we'd continue to hold the record, unless an expungement was initiated or something to that degree. We will hold that record until we no longer have the authority to retain it. It all depends on how the state law applies to CJIS civil retention. Ms. Tucker added, we are already looking at the varying state and local laws that will not permit their civil records to have latent transactions cascaded.

IS Issue #8
NGI Message State when a Shareable Link is Established in an External System

Mr. Robert Holman, FBI CJIS Division, presented this issue. The purpose of this issue was to respond to a contributor request for the CJIS Division to evaluate the possibility for NGI to send a notification to SIBs, who have an established State Identification Number (SID), when a search of NGI or the DHS IDENT results in the establishment of a record link. This functionality does not currently exist within the NGI development effort. It was noted that four of the Working Groups selected Option 2.

Motion: Mr. Kenneth Bischoff moved to accept Option 2; provide an automatic notification to the states that have an established SID on a criminal history record when a CJIS Division customer's search of NGI or an external system results in the establishment of a shareable record link and when a record link has been removed.

Second: Mr. Edward German
Action: Motion passed

IS Issue #9
Implementation Allowable Transmission Resolutions for the NGI Fingerprint/Palmprint Images Originally Captured at 1000 ppi

Mr. Nicky Megna, FBI CJIS Division, presented this issue. The purpose of this issue was respond to a Western Identification Network (WIN) request for CJIS to evaluate the current mandate requiring agencies to transmit images at 1000 ppi if they are captured at 1000 ppi. WIN is requesting that we allow agencies to submit downsampled images at 500 ppi that were captured at 1000 ppi. WIN had concerns with the infrastructure between WIN and its users being able to support the transmission and storage of the larger file sized images. It's known that this downsampling practice is going on today. The Federal Working Group was the only one in support of keeping with the current mandate. All other working groups supported relaxing the mandate while NIST worked to identify a way to regulate the practice.

Discussion: Mr. Bischoff added that CJIS previously had an approved downsampling policy that is in use today. Now it appears that contributors are no longer allowed to use previously certified CJIS downsampling protocol. He added he's happy to see the working groups supporting his concern. He's asking to continue using the previously approved method while CJIS and NIST identify a new acceptable approach.
Mr. Megna stated that CJIS had consulted with NIST, and they advised that it would be a good idea for additional testing to be performed. Mr. Justin Smith added the difference between Option 1 and 2 is if you want CJIS to look at alternate methods, because technologies have improved, and provide feedback on our findings. Mr. German, added, the SWIGFAST position on these same issues is that even though 1000 ppi is a burden now, don't close the door. Technology chances and prices decrease. Mr. Bischoff clarified that his downsampling will be necessary only in small pockets of his agency. Mr. Schaeffer stated it's not just an upstream submission of tenprint; a candidate list full of 1000 ppi images is a network burden as well. Mr. Lesko asked that relating to bandwidth, has CJIS looked at the impact of a downsampled image on matches. That seems more important than the bandwidth issue. Mr. Megna stated all five methods will be evaluated. Mr. Lesko asked what the impetus to the change the policy was. Mr. Megna responded the change wasn't called out specifically, but it was approved by this subcommittee, through the EBTS Working Group. Mr. Edgell noted any results from our studies and evaluations will be brought back to this group, prior to being put into EBTS.

Motion: Mr. Charles Schaeffer moved to accept Option 2 with changes; Permit downsampling of images captured at 1000 ppi to 500 ppi utilizing previously approved methodologies to allow for operational considerations, while expressing preference for

transmission of images at 1000 ppi. CJIS in collaboration with NIST will investigate best practices for downsampling and report back to the Working Groups the results of their research.
Second: Mr. Edward German
Action: Motion passed

IS Issue #10
National Iris Service

Mr. Justin Smith, FBI CJIS Division, presented this issue. The purpose of this issue was to provide a response to the IS Subcommittee documenting the CJIS commitment to not let work for the Iris pilot impact the NGI deployment of other initiatives. Mr. Justin Smith stated it will not impact other NGI capabilities. It's being developed on existing hardware and the privacy and policy work will be minimal. For the Trade study NGI used the NIST IREX III test, while Lockheed developed the business cases. L1/MorphoTrust provided the best value solution overall. Why Iris? Iris is very accurate, an excellent candidate for "Lights out" operations. The hardware footprint is also very small do to the size of the Iris image. Supervised Release/Corrections are candidates for the pilot, being that many already have the capability in place. The additional goal is to start to build an Iris repository. CJIS also plans to have some form of device certification in place, to avoid the FAP 10, FAP 30 issue with Iris.

IS Issue #11
Biometric Interoperability Update to include Federal and State Agency Participation in Automated Identification System (IDENT) IAFIS Interoperability

Ms. Lisa Vincent, FBI CJIS Division, presented this issue. The purpose of this issue was to provide information regarding the implementation of biometric-based interoperability between the FBI CJIS Division and other federal and international agencies including the DHS and the Department of Defense (DoD). It was stated that the Secure Communities initiative is now receiving CAR transactions from 47 states, with 37 states having statewide CAR transactions searched by IDENT. On April, 18, 2012, DoD ABIS users started searching IDENT through IAFIS Shared Services. Within the first ten transactions they received a hit on a Known or Appropriately Suspected Terrorist record. Mr. Buckley stated he's pushing for blanket coverage to have all CAR transactions coming into IAFIS searched against IDENT. He's working on education and verbiage to ensure DHS components completely understand the intent. Mr. Buckley also is evaluating providing a RISC like search of their Rules Based Watchlist. Ms. Anderson asked what the difference was between these records and the IVF records to be included within RISC. Mr. Buckley responded that the IVF is not complete; it does not contain some outstanding warrants and cases for failure to appear for deportation. These may be revisited; originally the APB did not want to handle immigration matters.

IS Issue #12
Biometric Interoperability Data Protection Strategies

Ms. Lisa Vincent presented this issue. The purpose of this issue was to respond to an APB request to re-evaluate of all previously approved Data Protection Strategies. Each of the nine strategies was discussed resulting in the following motions.

Motion: Mr. Kenneth Bischoff moved to recommend the data protection strategies apply to all participating databases rather than singling out IDENT and IAFIS. Request the FBI CJIS Division review the data protection strategies to modify the existing language to apply to all participating databases.
Second: Mr. James Buckley, Jr.
Action: Motion passed

Motion: Mr. Charles Schaeffer moved to recommend the FBI CJIS Division review the data protection strategies every 3 years and report to the IS Subcommittee.
Second: Mr. Kenneth Bischoff
Action: Motion fails
Motion restated: Mr. Charles Schaeffer moved to recommend the IS Subcommittee review the data protection strategies every 3 years and report to the APB.
Second: Mr. Kenneth Bischoff
Action: Motion passed

IS Issue #13
Disposition Task Force Update

Ms. Julia Wilson, FBI CJIS Division, presented this issue. The purpose of this issue was to update the IS Subcommittee on recent activities of the task force. Ms. Wilson spoke about the broad spectrum of agencies that make up the task force. The 3/5/2012 meeting in Columbus, Ohio resulted in the establishment of a mission and vision statement, and specific goals. They anticipate at the next task force meeting, establishing objectives to accomplish the goals. The disposition calculation rate needs to be consistent between what states have and what is available in IAFIS. What is the picture of missing dispositions? Establishing a baseline calculation for missing disposition is a driver to the direction to the task force.

Discussion: Mr. Schaeffer noted that large portions of Florida's missing dispositions are criminal traffic arrests that are pled down to civil penalty, and therefore the adjudications will never come in. This is a national problem and requires a national best practice to leverage, for decisions on when to provide dispositions. Mr. Lesko stated that Texas has attached funding to courts meeting their goal of 90% disposition compliance, which has

increased the overall compliance within the State. Mr. Lesko asked how many states are involved with the III Message Key. Texas is now testing. Ms. Wilson responded that six states and one federal agency. Mr. Trent stated that since this is an IS Subcommittee task force, are they doing what you are looking for? Mr. Buckley added that he hadn't heard of anything that had come out of the task force yet, and has not seen output to demonstrate the return on investment. Mr. Schaeffer responded that we've used the task force to help define disposition. Based on inconsistency between states, the task force helped craft the definition of Disposition for the rap sheet and has been very helpful. Ms. Gibbons added that the current work products have been presented; the mission, vision, and goals are a product. She clarified that Mr. Trent is asking are we in agreement that these are what we want. Mr. Edgell stated that disposition improvement is one of the tenants of NGI. He's concerned that the meetings have occurred and he's not seen a benefit relative to NGI. Mr. Edgell feels the Program Office should work a little closer with the task force to get beyond the goals and see the impacts of what's happened. Ms. Wilson stated that the disparate backgrounds of the individuals involved have resulted in a longer learning period regarding the APB process.

Mr. Edgell is looking to define measurable tasks to be assigned and returned. Disposition is an issue that affects multiple components within NGI. Mr. Buckley asked why the task force was formed in the first place. Mr. Edgell asked if someone is being placed on parole, is that considered a disposition. Mr. Schaeffer replied it was a sentence. A disposition is a fluid event, a court event, which could result in many unimportant notifications. Mr. Edgell stated that clearly there is more work to be done with the incorporating Disposition into NGI components. The NGIPO can take the action to use the task force to address current issues with wording and definition. Mr. Lesko asked if the subcommittee agrees that this is the direction the task force should go. It was decided that an Action Item will be used to monitor the progress of the task force toward these goals.

IS Issue #14
Proposal to Create a Violent Offender File in the NCIC

Ms. Kim Smith, FBI CJIS Division, presented this issue. The purpose of this issue was to request Subcommittees recommendations as to the creation of a Violent Offender File within NCIC. Ms. Smith stated the Law Enforcement Officers Killed and Assaulted program statistics are driving the development of further classification of NCIC data. A CONOPS has been created describing the "Entry Criteria" and the extra field criteria. Ms. Smith informed the IS of the feedback received from the NCIC Subcommittee and had incorporated it into this discussion. Ms. Smith then detailed the changes request by the NCIC Subcommittee.

Discussion: Mr. McKinsey noted that options one through three were based on convictions and number four based on perceived or stated threats against law enforcement. Mr. German inquired as to what type of oversight would guide the decision to place someone in as a four. Ms. Smith stated that the Privacy Impact Assessment is under review. The onus will be on the agency for category four, and the records will be validated, they will have to have a cross check in place.

Motion: Mr. James Buckley, Jr. moved to accept Option 1; endorse the creation of the NCIC Violent Offender File with changes specified by the NCIC Subcommittee.
Second: Mr. Kenneth Bischoff
Action: Motion passed

IS Issue #15
Extension of UK Visa to Include Individuals Fingerprinted in Jamaica

Mr. Michael Gannon and Mr. Brian Pittack, DHS US-VISIT, presented this issue. The purpose of this issue was to request the APB's approval to expand the United Kingdom Border Agency data sharing agreement to include collection sites located in Jamaica. During the presentation it was stated that as of April 4, 2012, US-VISIT had finished cleanup of all the mis-linked FBI records in IDENT. Additionally, DHS unofficially presented some possible scenarios of future data sharing processes. Several of these scenarios raised concern from the Subcommittee members in that the future scenarios depicted the FBI Number being provided as part of the response, and being disseminated to foreign non law enforcement agencies. The scenarios depicted information sharing that was outside the scope of "Red light Green light" that was originally approved.

Motion: Mr. James Buckley, Jr. moved to approve the Extension of UK Visa to include individuals fingerprinted in Jamaica
Second: Mr. Kenneth Bischoff
Action: Motion passed

Motion: Mr. Charles Schaeffer moved to request DHS formalize the presentation to be provided to the working groups and Compact Council explaining the path forward for expansion beyond the UK.
Second: Mr. Kenneth Bischoff
Action: Motion passed

IS Issue #16
Integrated Justice Information Systems (IJIS) Update
(This was not on the original agenda.)

Mr. Sudhindra Umarji, Trusted Federal Systems, Inc. presented this issue. The purpose of this issue was to discuss the current work of IJIS and where CJIS initiatives fall within it. IJIS's hope is to provide a channel of communication between industry and government. One of these areas deals in standards. Currently latent interoperability has been the focus. The encodings between work station and AFIS is proprietary to that brand, and not extendable to other systems. IJIS is looking for guidance on how to raise issues to industry. IJIS questioned if the issue with latent interoperability something the IS Subcommittee would want IJIS to take to industry? Interoperability is more than just passing a standards conformance test. IJIS is proposing having joint industry government sessions; a teleconference in May, a work shop June, and an IJIS industry brief in July. IJIS intends to make this an ongoing dialog, but wants to make sure the right topics are discussed. IJIS is looking for guidance to which topics to focus their efforts.

Discussion: Mr. Loudermilk stated that latent interoperability is a big deal, and the Subcommittee of Forensic Science is about to issue a report on it, and it will likely become a big deal to this committee. Mr. German added that even if the problem were solved technically, the states don't have the resources to look at all of the new hits that would be generated. The Biometrics Identity Management Agency has software to consolidate and sort these results by score. Mr. Lesko stated that it is still needed for industry to adopt national standards. Currently the user community is not articulate enough to ask for it or powerful enough to demand it from their vendor without a huge price increase. Mr. Loudermilk noted that we can incorporate this into the Bureau of Justice Assistance Grant wording. Mr. Edgell stated that adherence to standards is a big issue for all the disciplines. From experience we know agencies have been sold minutia based mobile devices that are not interoperable with the NGI services, and the vendor new that when it was sold. The NGI Program Office will provide resources to support this, but we don't want to drive this. This problem is collectively ours. Mr. Lesko stated that sounds like there's value in this summit, the issues need to be defined that we want to deal with before we have a meeting.

Motion: Mr. Ed German moved to request IJIS focus on the mobile ID and latent interoperability issues before the BCC.
Second: Mr. Kenneth Bischoff
Action: Motion passed

IS Issue #17
Rapid Deoxyribonucleic Acid (R-DNA) Task Force Update
(This was not on the original agenda.)

Mr. Thomas Callaghan, FBI Laboratory Division, presented this issue. The purpose of this issue was to brief the Subcommittee on the work of the R-DNA Task Force. After a synopsis of previous meetings and progress, Mr. Callaghan presented the work done during the R-DNA Task Force meeting #5, at the Louisiana State Police (LSP) Headquarters in Baton Rouge, Louisiana. LSP has integrated DNA collection and search into their process and has operated this way for eight years. LSP was invited to join the R-DNA Task Force. Development is underway of a DVD/Video of the LSP system to demonstrate and share lessons learned and best practices. Mr. Callaghan further discussed progress made with the concept of "John Doe DNA Warrants" and a distinction about the use of these warrants as mitigation to toll statute of limitation laws. The next R-DNA Task for meeting is set for August, 2012. To be discussed are CODIS requirements, CODIS policy and issue list, and continued work on John Doe DNA Warrants.

Discussion: Mr. Loudermilk stated an efficacy study for DNA was desirable, but a valid methodology for the evaluation had yet to be identified. Mr. German asked if CJIS and NIST could develop a certification for DNA collection equipment, like they currently do for various biometric capacities. Mr. Callaghan advised that this was already in progress and they expected to have two completed within the next three months and a third in six months. Additionally, this work is growing due to diminishing rights to privacy for convicted felons. Twenty-seven states currently allow collections from arrestees. The privacy work is already completed; they are just changing the mechanisms through which the information is captured within CODIS.