



National Crime Prevention and Privacy Compact
COMPACT COUNCIL MEETING
SAN DIEGO, CALIFORNIA
NOVEMBER 19-20, 2008

DRAFT MINUTES

Ms. Donna M. Uzzell, Chairman, National Crime Prevention and Privacy Compact Council (Council), called the Council meeting to order at 9:00 a.m. on November 19, 2008, in the Aventine Ballroom of the Hyatt Regency La Jolla Hotel, San Diego, California.

Mr. Gary S. Barron, FBI's Compact Officer, conducted roll call of the Council members. The following Council members, or their proxies, were in attendance.

State Compact Officers:

- Ms. Wendy L. Brinkley, North Carolina State Bureau of Investigation
- Mr. Paul C. Heppner, Georgia Bureau of Investigation
- Mr. Jeffrey R. Kellett, New Hampshire State Police
- Mrs. Julie A. LeTourneau Lackner, Minnesota Department of Public Safety
- Captain Timothy P. McGrail, Missouri State Highway Patrol
- Ms. Liane Moriyama, Hawaii Criminal Justice Data Center
- Ms. Dawn Peck, Idaho State Police
- Mr. David G. Sim, Kansas Bureau of Investigation
- Ms. Donna M. Uzzell, Florida Department of Law Enforcement

State/Local Noncriminal Justice Agency Representative:

- Mr. Robert M. Finlayson III, Georgia Department of Human Resources -
Participated via teleconference on 11/19/2009

State/Local Criminal Justice Agency Representative:

- Captain Thomas W. Turner, Virginia State Police

Federal Noncriminal Justice Agency Representative:

- Mr. William Marosy, Office of Personnel Management
Proxy for Ms. Kathy Dillaman

Federal Criminal Justice Agency Representative:

- Mr. Steve Cooper, Department of Homeland Security
Proxy for Mr. Jonathan Frenkel

Advisory Policy Board Representative:

- Mr. William Casey, Boston Police Department - *Not in Attendance*

Federal Bureau of Investigation:

- Mr. Thomas E. Bush, III, FBI CJIS Division

Other meeting attendees introduced themselves and the agency they represented.

(Attachment 1)

Chairman Uzzell welcomed the newest Council member Wendy Brinkley, North Carolina, and also announced the re-election of Julie LeTourneau-Lackner, Liane Moriyama, and David Sim, as Compact Officers on the council. Kathy Dillaman, Federal Noncriminal Justice Agency Representative, Bill Casey, Advisory Policy Board Representative and Tom Bush representing the FBI. Ms. Uzzell also recognized new State Compact Officers: Sergeant John Fortunato, New Jersey, and Captain Andrew Jordan, South Carolina. Chairman Uzzell also recognized the following newly appointed Standards Committee members: Ms. Cathy Kester, California, and Mr. Brad Bates, Kentucky. Captain Timothy P. McGrail was appointed as the new Sanctions Committee Vice Chair at its meeting the night before the Council meeting. Additionally, there are three states, Kentucky, Michigan, and Washington, that are pending legislation or have requested information regarding the Compact. Puerto Rico is now a Memorandum of Understanding (MOU) signatory, bringing that total to 12. All 50 states and Washington, D.C. are now Interstate Identification Index (III) participants.

Chairman Uzzell stated that approval was granted from the Director of the FBI regarding two Council initiatives:

- Modification to the CJIS Security Policy to include a state requirement to audit noncriminal justice agencies.
- Change in the NFF State Qualification Requirement III (A), which currently contains a 10-minute response time to criminal history record requests to a mean response time of 15 seconds.

Finally, Chairman Uzzell concluded by stating that for future meetings, if anyone has a

topic they want addressed by the Council, to submit a Topic Paper Request Form and return it to FBI Compact Officer Gary Barron. A copy of the form can be found on the Council's website.

Next, the Council approved the minutes from the May 2008 meeting.

Compact Council Action: Mr. David G. Sim moved to approve the May 2008 minutes. Seconded by Ms. Julie A. LeTourneau Lackner. The motion carried.

Agenda topics were discussed.

Topic #1 FBI's Criminal Justice Information Services Division Update

Mr. Thomas E. Bush, III, FBI CJIS Division, provided an update on the CJIS Division. Mr. Bush provided operational updates on CJIS services, update on CJIS initiatives, and discussed the Division's strategic vision. More specifically, Mr. Bush provided updates on the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center, the National Instant Criminal Background Check System, Law Enforcement Online, the National Dental Image Repository, Uniform Crime Reporting, Next Generation Identification and the Law Enforcement National Data Exchange programs. He also provided information on Biometric Center of Excellence, which is a focal point to foster collaboration, improve information sharing and advance the adoption of optimal biometric and identity management solutions across the law enforcement and national security communities; interoperability between the IAFIS, and Secure Architecture for International File Exchange, where the FBI is in the process of drafting the Concept of Operations to enhance data exchange between the FBI and the United Kingdom's Metropolitan Police Services.

(Attachment 2)

Compact Council Action: This topic was accepted as information only.

Topic #2 The National Fingerprint File Program Update

Ms. Joyce R. Wilkerson, FBI CJIS staff, provided a status of the fifteen non-NFF Compact states' progressions toward NFF implementation. Ms. Wilkerson reported that a total of twenty states are anticipating NFF participation by the end of calendar year 2009.

Ms. Wilkerson provided the Non-NFF Compact States Matrix Summary to the Council members and State Compact Officers, per the Council Committees' request, that the FBI to survey the non-NFF Compact states twice a year for a status on NFF

participation. Ms. Wilkerson reported that Ohio is scheduled for NFF participation the first quarter of 2009; Connecticut late 2008/early 2009; Maryland is now scheduled for March 2009 due to AFIS upgrades; Iowa, Hawaii, Maine, Arkansas, Minnesota, Missouri and South Carolina expect participation in 2010; Nevada and Arizona in 2011. West Virginia had not determined a participation date and no response was received from Alaska. Wyoming and Tennessee were the most recent NFF participants. New Hampshire has requested an on-site visit in June 2009.

(Attachment 3)

Compact Council Action: This topic was accepted as information only.

Topic #3 **The Standards Committee Report on the Proposed Modifications to the State National Fingerprint File (NFF) Qualification Requirements Relating to Potential Image Updates to the FBI's Criminal Master File (CMF)**

Ms. Joyce R. Wilkerson, FBI CJIS staff, discussed the proposed modifications to current state NFF Qualification Requirements that all Fingerprint Image Submission (FIS) transactions would be submitted to the FBI. The Council members and State Compact Officers were provided the NFF On-site Assessment State FIS Implementation Status handout. The Compact Council Standards Committee was asked at its Fall 2008 meeting to discuss a means to enforce the NFF Qualification Requirements II (H) and (I) and that the Sanctions Committee and Council closely monitor the compliance. The CJIS Division provided the following options for consideration: 1.) Require each NFF state to maintain a system of logs of all improved or permanently changed fingerprint image updates to the state's AFIS and all FIS transactions that are submitted to the FBI as a result of those image updates. This log would provide the CAU a means to ensure that each state's AFIS image update resulted in a FIS transaction to the FBI. 2.) Revise the current State NFF Qualification Requirements II (H) and (I) as such:

II (H) "A NFF state shall submit **all** criminal fingerprint impressions to the FBI for second and/or subsequent criterion offenses if these fingerprint impressions show new amputations or new permanent scars ."; and II (I), "NFF states shall submit **all** ten-finger fingerprint impressions to the FBI as they become available when second and/or subsequent offenses yield improved image quality fingerprint impressions."

Ms. Wilkerson noted that in the current IAFIS auditing methodology, NFF states are asked if they are using the FIS TOT and this information is noted in the assessment. However, they do not compare the number of times the state AFIS updates its images

verses the times the FIS TOT is submitted to the FBI. The importance of updating the criminal fingerprint images in the FBI's Criminal Master File (CMF) and the use of the FIS Type of Transaction (TOT) by NFF states was re-emphasized. Currently 7 NFF states submit the FIS TOT.

(Attachment 4)

Compact Council Action: Mr. Paul C. Heppner moved that NFF states identify the methodology by which the FIS transactions are being submitted. Seconded by Ms. Dawn A. Peck. The motion carried.

Topic #4 The Standards Committee Report on the Proposed Criminal Justice Information Services (CJIS) Division Modifications to the Security and Management Control Outsourcing Standard (Outsourcing Standard)

Ms. Barbara S. Wiles, FBI CJIS staff, reported 12 recommended changes to the Outsourcing Standard based on audits conducted by the CJIS Audit Unit (CAU) of seven Authorized Recipients that outsourced the performance of noncriminal justice administrative functions (other than "Channeling") to three Contractors. Ms. Wiles provided a current version (**Attachment 5**) of the Outsourcing Standard to Council Members and State Compact Officers. The 12 recommended changes are as follows:

RECOMMENDED CHANGE #1

Section 2.05

The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that *an compliance review audit* was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the terms of the contract. **Such 90-day compliance review audit and certification is not applicable to an Authorized Recipient contracting with an FBI-approved Channeler solely for the purpose of electronically transmitting noncriminal justice fingerprints to the FBI and receiving the results of the fingerprint checks for prompt transmittal to the Authorized Recipient. Instead, the 90-day compliance reviews audits of FBI-approved Channelers shall be performed by the FBI.**

Section 3.06

The Contractor shall make its facilities available for announced and unannounced

security inspections audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council. Such facilities are also subject to triennial audits by the state and the FBI on behalf of the Compact Council. An audit may also be conducted on a more frequent basis.

Compact Council Action: Mr. Paul C. Heppner moved to accept Sections 2.05 and 3.06 as indicated above.

Seconded by Captain Thomas W. Turner. The motion carried

RECOMMENDED CHANGE #2

Section 2.03

The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; maintain up-to-date updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur; and ensure that Contractor personnel comply with this Outsourcing Standard.

(Attachment 5)

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended changes to Section 2.03.

Seconded by Captain Thomas W. Turner. The motion carried.

RECOMMENDED CHANGE #3

Section 2.03a

The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access. The Authorized Recipient shall update records of Contractor personnel who have access to CHRI within 24 hours when

changes to that access occur, and if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.

Section 6.04

The Contractor shall maintain updated records of personnel who have access to CHRI within 24 hours when changes to that access occur, and if a criminal history record check is required, the Contractor shall maintain a list of personnel who successfully completed the criminal history record check.

Section 10.01b5

Maintain updated records of IT contractor personnel who have limited access to CHRI and update those records within 24 hours when changes to that access occur;

Compact Council Action: Mr. Paul C. Heppner moved to table recommended change #3 pending additional work on the language and revisit the second day of the meeting. Seconded by Captain Thomas W. Turner. The motion carried.

Compact Council Action: Mr. Paul C. Heppner moved to accept the revised recommended changes to Sections 2.03, 6.04 and 10.01b.5. Seconded by Captain Timothy P. McGrail. The motion carried.

RECOMMENDED CHANGE #4

Footnote 4

If a national criminal history record check of government personnel having access to CHRI is mandated or authorized by a state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended change to Footnote 4 from Section 2.03a. Seconded by Ms. Julie A. LeTourneau Lackner. The motion carried.

RECOMMENDED CHANGE #5

Section 2.03c

The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy. The FBI, rather than the Authorized Recipient, shall notify Channelers of changes or updates to the Outsourcing Standard and/or CJIS Security Policy.

Section 7.01

The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy as they are made known to the Contractor by the Authorized Recipient.

Compact Council Action: Mr. William Marosy moved to accept the recommended changes to Sections 2.03c and 7.01.

Seconded by Ms. Wendy L. Brinkley. The motion carried.

RECOMMENDED CHANGE #6

Section 3.03

The Contractor shall develop and document a Security Program to comply with the current Outsourcing Standard and any revised or successor Outsourcing Standard. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard, the associated Security Training Program, and the reporting guidelines for documenting and communicating security violations and corrective actions to the Authorized Recipient. The Security Program shall be subject to the written approval of the Authorized Recipient.

Section 3.05

Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with

access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program.

Immediate training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that ~~the~~ annual refresher training was completed for those Contractor personnel with access to CHRI. ~~The Security Training Program shall be subject to review by and the written approval of the Authorized Recipient.~~

Compact Council Action: Ms. Dawn A. Peck moved to table Sections 3.03 and 3.05 until day two of the meeting, pending additional work on the language.

Seconded by Mr. William Marosy. The motion carried.

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended changes to Sections 3.03 and 3.05, as provided on day two of the meeting.

Seconded by Captain Thomas W. Turner. The motion carried.

RECOMMENDED CHANGE #7

Section 3.05

Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. ~~Immediate t~~Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall certify to the Authorized Recipient that the annual refresher training was completed for those Contractor personnel with access to CHRI. The Security Training Program shall be subject to the approval of the Authorized Recipient.

**** See Recommended Change #6 for additional changes to Section 3.05**

Section 8.01b

Pending investigation, the Contractor shall, *immediately upon detection or awareness*, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

Section 8.01c

The Contractor shall *immediately (within four hours)* notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

Section 8.01d

The Authorized Recipient shall *immediately (within four hours)* notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

Section 8.03b

If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be *immediately* deleted or returned *in accordance with the provisions and time frame* as specified by the Authorized Recipient.

***Compact Council Action:* Mr. Paul C. Heppner moved to accept the recommended changes to Sections 3.05, 8.01b, 8.01c, 8.01d, 8.03b. Seconded by Captain Thomas W. Turner. The motion carried.**

RECOMMENDED CHANGE #8

Section 3.08

The Contractor shall maintain CHRI only for the period of time necessary to fulfill *their* contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI. **CHRI disseminated by a Channeler to an Authorized Recipient via an authorized Web site shall remain on such Web site only for the time necessary to meet the Authorized Recipient's requirements but in no event shall that time exceed 30 calendar days. CHRI successfully received by the Authorized Recipient, regardless of mode of transmission, shall be destroyed by the Channeler immediately after confirmation of successful receipt by the Authorized Recipient. The manner of, and time frame for, CHRI dissemination by a Channeler to an Authorized Recipient shall be specified in the contract or agreement.**

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended changes to Section 3.08.

Seconded by Mr. William Marosy. The motion carried.

RECOMMENDED CHANGE #9

Section 5.09

The Contractor's system shall be supported by a *well-written documented* contingency plan *as defined in the CJIS Security Policy and approved by the FBI.*

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended changes to Section 5.09.

Seconded by Captain Thomas W. Turner. The motion carried.

RECOMMENDED CHANGE #10

Section 6.03

The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm *in writing* that each employee *understands has certified in writing that he/she understands* the Outsourcing Standard requirements and laws that apply to his/her responsibilities. *The Contractor shall maintain the employee certifications in a file that is subject to review*

during audits. Employees shall make such certification prior to performing work under the contract.

Compact Council Action: Mr. Paul C. Heppner moved to table discussion of the recommended change #10 until day two of the meeting, pending additional work on the language.

Seconded by Captain Thomas W. Turner. The motion carried.

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended changes to Section 6.03.

Seconded by Captain Timothy P. McGrail. The motion carried.

RECOMMENDED CHANGE #11

Section 7.02

The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

- a. CHRI shall be stored in a physically secure location.
- b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.
- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended change to Section 7.02.

Seconded by Captain Thomas W. Turner. The motion carried.

RECOMMENDED CHANGE #12

Section 7.03

To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient must be identified by an Originating Agency Identifier (ORI) or a state assigned identifier, and each Contractor or sub-Contractor must be uniquely

identified each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

Compact Council Action: Mr. Paul C. Heppner moved to accept the recommended changes to Section 7.03.

Seconded by Captain Thomas W. Turner. The motion carried.

Topic #5 Report from the National Infrastructure Advisory Council (NIAC)

Chairman Uzzell introduced Topic 5, the NIAC report and provided the Council and State Compact Officers a copy of the report (**Attachment 6**). The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of the critical infrastructure sectors and their information systems. The NIAC is comprised of a maximum of thirty members appointed by the President from private industry, academia, and state and local government. Ms. Barbara Wichser, Dominion Energy and NIAC study group member, provided to the Council the purpose for conducting background checks at Dominion. Dominion is considered a company that demonstrates best practices when it comes to background investigations. Ms. Wichser provided a presentation outlining Dominion's employee screening process and Dominion's concerns over the need for a national fingerprint-based background check.

(Attachment 7)

Next, Ms. Nancy Wong, Department of Homeland Security (DHS), provided the Critical Infrastructure Key Resources (CIKR) Sector partnership overview. Ms. Wong reported that CIKR are those whose disruption or destruction could cause catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Critical infrastructure protection is a shared responsibility of the federal, state, local and tribal governments, and the owners and operators of the nation's CIKR. Homeland Security Presidential Directive identified 17 CIKR sectors (e.g. energy, transportation, communication, chemical, etc.). The National Infrastructure Plan identifies security partners, their rules, and responsibilities; outlines leadership, coordination, and partnering mechanisms and outlines a strategy for information sharing.

(Attachment 8)

Compact Council Action: This topic was accepted as information only.

Topic #6 **Update on the Joint Advisory Policy Board (APB)/National Crime Prevention and Privacy Compact Council (Council) Site Security Task Force (Task Force) Meeting**

Mr. James Gray, FBI CJIS staff, provided an update on the Joint APB/Council Site Security Task Force (Task Force) meeting. He advised at the May 13, 2008, Task Force meeting held in Orlando, Florida, the FBI's CJIS Division presented a white paper which provided the FBI staff's research and analysis regarding the recommendations and motions from the previous Task Force meeting. After discussing the white paper, the Task Force decided against expanding the "Federal Facility Site Security" and "Criminal Justice Agency Site Security" policies. The Task Force addressed the issues of contractor personnel and visitors to critical infrastructure facilities separately. The Standards and Policy and Planning Committees' recommendations were:

Contractor Personnel

Authorize the use of noncriminal justice purpose code X under the Council's Fingerprint Submission Requirements Rule for contractor personnel with local, state, or federal governments when an authorizing statute is in place and a specific proposal is approved by the Council.

Visitors to Critical Infrastructure Facilities

1. The FBI, in conjunction with CJIS Systems Officers, should take specific action to educate criminal justice agencies on their existing authority to conduct NCIC hot file checks on visitors to critical infrastructure facilities and that no additional authority is needed to allow such checks.
2. The Department of Homeland Security, in conjunction with the FBI, should educate critical infrastructure protection owners and operators on their ability to enter into partnerships with criminal justice agencies to explore critical infrastructure site security using NCIC hot file information.
3. Requesters for access to CHRI should be educated on the difference between NCIC checks and III checks and should be directed to first work with local criminal justice agencies to conduct NCIC hot file checks which are currently broadly authorized.
4. Recommend that, after exhausting the alternative mechanisms mentioned in this paper for information sharing and after understanding the differences between the NCIC hot file and III information, an agency seeking access to CHRI should provide a specific

proposal to the FBI to be forwarded to the Task Force that includes the following details:

- the specific need for the CHRI being requested;
- why alternative mechanisms do not adequately address the security risks it is seeking to mitigate;
- the method CHRI would be obtained and vetted;
- the method the criminal history record check results would be screened and applied;
- the methodology to determine which individuals would be screened; and
- any other information the agency deems relevant to assist the Task Force in making future recommendations.

***Compact Council Action:* Ms. Dawn A. Peck moved to accept the recommendations made by the Standards and Policy and Planning Committees and the Identification Services Subcommittee. Seconded by Mr. Paul C. Heppner. The motion was carried.**

Topic #7 Access to Department of Homeland Security (DHS) Information by Federal, State, and Local Criminal Justice, Intelligence, and Authorized Noncriminal Justice Agencies: Update on the Progress to Date With Interoperability

Ms. Cynthia D. Estep, FBI CJIS staff, presented an update on the Interoperability project between the FBI's IAFIS System and DHS's Fingerprint Identification (IDENT) System.

Ms. Estep reported on the interim Data Sharing Model (iDSM). She advised that the FBI has transitioned from iDSM to a shared services type query. This transition dates back to October 2008 and all iDSM pilot agencies, except DOD, have made the switch. The iDSM pilot agencies have now gained access to over 90 million records within the IDENT system.

Ms. Estep advised the FBI modified the system to allow the master fingerprint image to be retrieved based on the FBI number provided in an NFF state's Criminal Print Identification (CPI) message and to conduct a full search of the IDENT repository when a CPI messages is received.

Additionally, Mr. James Buckley, DHS, Immigration and Customs Enforcement (ICE) provided an update on the ICE Secure Communities Initiative which will increase

state and local partnerships to ensure time-sensitive screening of all foreign-born detainees and identification of criminal aliens. ICE will leverage the Interoperability solution to integrate local booking data so that ICE can determine eligibility for removal and quickly prioritize each case to initiate the appropriate level of response.

(Attachment 9)

Compact Council Action: This topic was accepted as information only.

Topic #8 Report on DHS's Citizenship and Immigration Services Agency Systemic Alien Verification for Entitlements (SAVE) Program E-Verify

Ms. Phyllis Bell, DHS, presented this topic. She provided an overview of the SAVE and E-Verify programs. The Verification Division of the U.S. Citizenship and Immigration Services (USCIS) operates the Verification Information System (VIS). VIS is a composite information system incorporating data from various DHS databases. It is the underlying information technology that provides immigration status verification for (1) benefits determinations through the SAVE program for government benefits and (2) verification of employment authorization for newly hired employees through the E-Verify program (formerly known as the Basic Pilot/Employment Eligibility Verification Program).

The SAVE Program is an inter-governmental information sharing initiative designed to aid benefit-granting agency workers in determining a non-citizen applicant's immigration status, and thereby ensure that only entitled non-citizen applicants receive federal, state, or local public benefits and licenses. It is an information service for benefit-issuing agencies, institutions, licensing bureaus, and other entities.

E-Verify is an Internet based system operated by the DHS in partnership with the Social Security Administration that allows participating employers to electronically verify the employment eligibility of their newly-hired employees. This program is free and voluntary and is the best means available for determining employment eligibility of new hires and the validity of social security numbers.

(Attachment 10)

Compact Council Action: This topic was accepted as information only.

Topic #9 Policy and Planning Committee Report

Mr. David G. Sim provided the Council an update on the Strategic Plan and the Standards to Invoke Noncriminal Justice Record Checks in the Matter of Emergencies and Disasters.

Mr. Sim discussed several factors in relation to Standards to Invoke Noncriminal Justice Record Checks in the Matter of Emergencies and Disasters. He referenced the report published by The National Consortium for Justice Information and Statistics (SEARCH) in 2007 titled *National Focus Group on Emergency Housing and Criminal Record Checks, the Hurricane Katrina Experience*. This report concluded it is appropriate for law and policy makers to anticipate future instances of massive relocation and to prepare to conduct criminal history record checks to assist in relocation. In May 2008, the Council suggested that the Standards Committee examine the model used in conducting background checks for hurricane Katrina and make suggestions for improvement of that model, develop a different model or recommend that model as the standard process for future emergencies. Mr. Sim reported that at the Fall 2008 Policy and Planning Committee meeting the committee addressed a series of questions that were presented by the CJIS staff. A straw man proposal is to be presented at the Spring 2009 Policy and Planning Committee Meeting.

Next, Mr. Sim reviewed the Policy and Planning Committee's four recommended changes to the Strategic Plan. The recommended changes he discussed were:

1. Goal 2, Objective 2.1 - Add the words "and security" to the Objective and Strategies 2.1.1 through 2.1.4 to account for the concept of security as a complement to privacy and deleted the words "and best practices" because it overlapped Objective 4.5. This change focuses Objective 2.1 on developing policy and Objective 4.5 on publishing guidance. Also add Strategy 2.1.5 to recognize the Global Justice Information Sharing Initiative.
2. Goal 2, Objective 2.2 - Add the words "and security" to the Objective to account for the concept of security as a complement to privacy.
3. Goal 2 - Add Objective 2.3 to account for strategies regarding safety and security of outsourced noncriminal justice administrative functions. Also added three Strategies to attain the Objective.
4. Goal 4 - Add wording to Objective 4.5 to share "best practices" in the

noncriminal justice user community and four Strategies to meet the Objective.

5. Goal 4 - Added Objective 4.6 to strengthen the Compact Council infrastructure and three Strategies to meet the Objective.

(Attachment 11)

Compact Council Action: Mr. David G. Sim moved that the Council accept the Strategic Plan as presented.

Seconded by Captain Thomas W. Turner. The motion was carried.

Topic #10 The Standards and Policy and Planning Committees' Reports on the Best Practices Guide to Identify Evacuees and Emergency Credentialing Issues

Ms. Paula A. Barron presented this report and referenced the report published by SEARCH in 2007 titled *National Focus Group on Emergency Housing and Criminal Record Checks, the Hurricane Katrina Experience* and summarized the recommendations provided by this report for the Standards and Policy and Planning Committees. The report noted that many evacuees lacked identification documents and stressed the importance of establishing the identities of evacuees, even if those identities could not be immediately confirmed. Additionally, the committees moved to request the SEARCH focus group develop a best practices publication for identity matters and credentialing during times of natural disasters or emergencies. The Committees felt that the SEARCH convening a focus group would provide broader scope regarding the development of best practices.

Compact Council Action: Mr. Paul C. Heppner moved to submit a letter to SEARCH requesting their focus group develop a best practices guide for identity matters and credentialing during times of natural disasters and emergencies

Seconded by Captain Thomas W. Turner. The motion carried.

Topic #11 Overview of Extensible Mark-up Language (XML) Format Rapsheets

This topic was presented by Mr. Patrice Yuh, FBI CJIS staff. Mr. Yuh provided a high level overview of the two XML representations: Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM). XML is the Web's

standard structure for information sharing and it is the plain text that allows the interoperable exchange of information. Mr. Yuh explained that NIEM provides the data dictionary and the structure for the sharing of information between agencies and systems. Information Exchange Package Documentation (IEPD) is the concept of the NIEM project. It defines the specifications and provides additional documentation to enhance comprehensibility of the exchanges. Nlets is developing a NIEM-based version of the XML Rap Sheet Specification. Nlets will support both the GJXDM-and NIEM-based versions of the XML Rap Sheet Specification. XML is a web standard structure for information sharing Mr. Yuh anticipates NCIC NEIM testing to begin in the spring 2009. The program has a projected release date of 2010.

(Attachment 12)

Compact Council Action: This topic was accepted as information only.

Topic #12 Transportation Security Administration Update

Mr. Nathan Tsoi, Transportation Security Administration (TSA), provided an update on the TSA Hazmat Assessment Program. There are 221 TSA Assessment Program sites operational within 38 states, including the District of Columbia. TSA averages about 25,000 drivers who apply for security threat assessments monthly. The states have the option to contract with TSA's agent, Integrated Biometric Technologies (IBT), or to submit fingerprint information to the FBI directly. To date, TSA has completed approximately one million security threat assessments and 9,000 individuals have been disqualified from holding a hazardous material (HAZMAT) endorsement. TSA's contract with IBT will end on January 31, 2009. The HAZMAT Assessment Program has a sister program, the Transportation Workers Identification Credential (TWIC) Program. A joint rule within TSA allows drivers who have completed the threat assessment for the HAZMAT endorsement to obtain a reduced fee if they enroll in the TWIC Program. Currently, TSA is exploring different options regarding the fee and the actual technological equipment behind transferring and obtaining the results from the TWIC threat assessments for the HAZMAT endorsement. A looming topic is obtaining the state rap sheet information. Several conference calls have been conducted by a technical working group established to discuss standards that would enable TSA to receive the state rap sheet information. The Florida Department of Law Enforcement (FDLE) was contacted to discuss FDLE's process in which Florida connects with the TSA fingerprint servers to obtain information from the Florida Repository and the FBI. The FDLE utilizes the CJIS Wide Area Network to provide its records to TSA electronically. All non-ident fingerprints at the FDLE are forwarded to the FBI for

processing. Several states are interested in providing the state records to TSA utilizing the same process that FDLE has in place. Mr. Wilbur Rehman, TSA contractor, provided an update that TSA will explore adjustments in its system to allow state rap sheets for those states that are conducting TSA-related background checks, following FDLE's process. Mr. Tsoi reported the states might need to use XML-based transmission and that this avenue is being investigated by the working group.

Ms. Maurine Fanguy, TSA's TWIC Program Director, provided background on the TWIC program. The Maritime Transportation Security Act requires that TSA conduct the program jointly with the U.S. Coast Guard. The TSA conducts similar background checks for TWIC as they conduct for HAZMAT. The TWIC has aligned its regulations so that the criminal disqualifiers are identical. There are currently 150 TWIC enrollment centers. The TWIC Program conducts the initial enrollment process by conducting a background check. A determination is made based on adjudication standards and a card is produced for the individual. One contractor will conduct these checks for the entire country. Ms. Fanguy provided an update on the enrollment and successes within the program.

(Attachment 13)

Compact Council Action: This topic was accepted as information only.

Topic #13 State Applicant Models

Two State Identification Bureau (SIB) representatives provided overviews of their states' applicant processing programs.

Mr. Brad Truitt, Tennessee Bureau of Investigation (TBI), presented an overview of Tennessee's Applicant Processing Service (TAPS) and the use of a contractor to capture fingerprints via live scan devices throughout the state. Public Law 92-544 fingerprints are submitted electronically to the States Automated Fingerprint Identification System (AFIS) from the contractor's central server, and state and national criminal history record check results are disseminated via a secure web site for retrieval by an Authorized Recipient. TAPS was implemented in October 2007 to provide an electronic means for fingerprint-based submissions for public and private agencies.

(Attachment 14)

Major Scott Snyder, Pennsylvania State Police (PSP), discussed Pennsylvania's applicant fingerprint processing, consolidated criminal history record responses, and the

Pennsylvania Access to Criminal History (PATCH) system. Noncriminal justice agencies authorized to access criminal history record information can submit either through a standard fingerprint based check, mail application or online submission through the PATCH system. (**Attachment 15**).

Compact Council Action: This topic was accepted as information only.

Topic #14 Advisory Policy Board Update

Mr. Paul C. Heppner presented the APB Update. He briefed the Council on the following APB initiatives: Revisions to the Security Addendum; Use of Video Teleconferencing for CJIS Advisory Meetings; Adding the Name Check Caveat when Applicable to Reject Messages L0116, 117 and 118; XML Format Messages IAFIS; Type 14 Flat Fingerprints; NFF Qualification Requirements; Standardized Reason Fingerprinted; and Automatic NCIC Check Based on Ten Print Searches.

(**Attachment 16**)

Compact Council Action: This topic was accepted as information only.

Topic #15 Sanctions Committee Report

Ms. Julie A. LeTourneau Lackner, Sanctions Committee Chairman, addressed the Council with the Sanctions Committee Report.

Ms. Lackner reported that the Sanctions Committee met on Tuesday, November 18, 2008 to discuss five topics. The first was a summary of the responses to the Sanctions Committee recommendations at the fall 2007 meeting and the spring 2008 meetings. The Sanctions Committee reviewed responses to the Sanctions letters that were sent out following the review of the audit findings at the fall 2007 meeting. The Sanctions Committee reviewed the responses to the letters and determined that no follow-up was required.

The second topic was a summary of recently-conducted NFF audits. The Sanctions Committee reviewed audit findings from one NFF state for the appropriate sanctions based on the Council's Sanctions Rule, Title 28, Code of Federal Regulations, Part 905 (Sanctions Rule). From March 2008 through September 2008, two NFF audit reports were finalized for the New Jersey and North Carolina repositories. The states

reviewed had no serious violations requiring action, however the committee requested a letter be sent identifying the non-serious violations based on the criteria set forth in the Sanctions Rule and any corrective actions taken.

The third topic was a Summary of Recently Conducted IAFIS Audits with NCIC III Summaries. The Sanctions Committee reviewed the audit findings from nine states/territories for appropriate sanctions based on the Sanctions Rule. None of the states reviewed had any serious violations requiring action, however the committee requested a letter be sent identifying the non-serious violations based on the criteria set forth in the Sanctions Rule and corrective actions taken.

The fourth topic discussed was Summary of the Recently Conducted Outsourcing of Noncriminal Justice Administrative Functions (Outsourcing) Audit. Two representatives of the Bank of America addressed the committee. The committee moved to include language in the letters that will be sent to the Bank of America acknowledging the proactive approach taken as well as the detailed correction action plan and documentation provided by Bank of America related to the audit findings.

The fifth topic discussed was the application of the Security and Management Control Outsourcing Standard (Standard) to third parties (Governmental or Private) with Incidental Access to Criminal History Record Information (CHRI). The Standards Committee provided its motion on this topic in the Council's discussion of Topic #16.

Compact Council Action: Ms. Julie A. LeTourneau Lackner moved that the Council accept the Sanctions Committee report. Seconded by Captain Timothy P. McGrail. The motion was carried.

Topic #16 The Standards Committee Report on the Application of the Security and Management Control Outsourcing Standard (Standard) to Third Parties (Governmental or Private) with Incidental Access to Criminal History Record Information (CHRI)

Mr. Timothy Neal, FBI Staff, discussed the proposed amendments to the Outsourcing Standard. During its May 2008 meeting, the Council endorsed a proposal that amended the Standard and outlined the requirements for when an Authorized Recipient outsources CHRI to IT contractor personnel, in which the access to CHRI is in a limited/supervised environment. While the scenarios in this staff paper do not relate to IT contractor personnel having electronic access to CHRI on behalf of the Authorized Recipient, they do relate to third parties having incidental access or access to a secure

storage facility where CHRI is maintained.

The Council was requested to consider if the *CJIS Security Policy* (Sections 4.6, 8.2.1, 8.3.2, and 8.6) adequately addresses the security of the destruction of CHRI by a third party when the destruction is witnessed by the Authorized Recipient. In addition, the Council was also requested to consider if the Standard should be revised to include an exemption section for governmental archives personnel (not just IT personnel) with incidental access to CHRI or access to a secure storage facility where CHRI is maintained. Section 9.05 of the Standard provides that the “Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.” If the Council decides the Standard should be modified, the Council was requested to consider the following option:

Add a new section to 10.0 identifying:

- 10.02a.** An Authorized Recipient that contracts with a governmental archives facility (Government Contractor) is exempt from Sections 1.0 through 9.0 of this Outsourcing Standard when:
1. Access to CHRI by the Government Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Government Contractor’s facility; (B) retrieval of the CHRI by Government Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Government Contractor personnel when not observed by the Authorized Recipient;
 2. Access to CHRI is incidental, but necessary, to the duties being performed by the Government Contractor;
 3. The Government Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
 4. The Government Contractor’s personnel are subject to the same criminal history record checks as the Authorized Recipient’s personnel;
 5. The criminal history record checks of the Government Contractor personnel are completed prior to work on the contract or agreement;
 6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to

- perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Government Contractor stores the CHRI in a physically secure location.
- b. To utilize this exemption, the Authorized Recipient shall, at a minimum and prior to providing CHRI to the Government Contractor, comply with the following requirements as an alternate method of providing adequate security, integrity, and confidentiality of CHRI:
1. Obtain written permission from the appropriate Compact Officer/Chief Administrator;
 2. Take positive actions to ensure that the Government Contractor cannot access any CHRI other than that necessary to accomplish the contracted work;
 3. Execute a contract with the Government Contractor which specifies the work to be performed to include any storage (archiving), method of retrieval, and/or method of destruction which results in the Government Contractor's personnel having limited access to CHRI. A Management Control Agreement is also acceptable;
 4. Incorporate the CJIS Security Policy, by reference, in the contract;
 5. Ensure the Government Contractor's facility where the CHRI is stored is a "physically secure" location;
 6. Maintain updated records of Government Contractor's personnel who have limited access to CHRI or access to the physically secure location where the CHRI is being stored and update those records within 24 hours when changes to that access occur;
 7. Perform an appropriate criminal history record check of each of the Government Contractor's personnel, prior to their work on the contract, with limited access to CHRI or access to the physically secure location where CHRI is stored; and
 8. Require each of the Government contractor's personnel with limited access to CHRI or access to the physically secure location where the CHRI is stored to sign a Nondisclosure Statement providing that CHRI may be disclosed only to the Authorized Recipient's personnel and that the CHRI shall not be further disclosed.

The Council was requested to review information given in the presentation and to endorse that the *CJIS Security Policy* adequately addresses the security of the destruction of CHRI by a third party when the destruction is witnessed by the Authorized Recipient.

They were also requested to endorse a new Section 10.0 identifying new exemptions as presented.

Compact Council Action: Mr. Paul C. Heppner moved to endorse that the Standards Committee motion on Issue 1: CJIS Security Policy adequately addresses the security of the destruction of CHRI by a third party, when the destruction is witnessed by the Authorized Recipient and Issue 2: add new Section 10.0 identifying new exemption as outlined in the paper. [Insure the language in the new section 10.02 is consistent with the revised language as approved by the Council in the (Topic 4) revisions to the Standard.]
Seconded by Ms. Julie A. LeTourneau Lackner. The motion was carried.

(Attachment 17)

Topic #17 The CJIS Security Policy as it Applies to Noncriminal Justice Agencies

Mr. George A. White, FBI Staff, provided an overview of the draft re-written CJIS Security Policy as it relates to noncriminal justice agencies. Mr. White discussed the impetus for change, impact to the noncriminal justice agencies and the time line for the re-write.

The Security Policy Working Group has been established to discuss the re-write. Eighteen people made up this working group which is comprised of Security and Access Subcommittee members, APB members, and Council members. Mr. White pointed out that agency applicability is one of the major reasons for the policy re-write. Another reason is because the user community is expanding and changing, and along with a changing business model, the current policy is difficult to implement as well as to audit.

The implementation of the re-written security policy will impact the noncriminal justice community in the following manners: applicability is clear, adaptable to individual agency business models, stronger security controls, new implementations lean forward as well as more in-depth audits.

Until full implementation of the security policy, the FBI CJIS Division will be advising agencies to follow the future policy guidelines with the help and guidance of the FBI, although the audit staff will not be creating its new auditing guidelines until the new security policy is fully implemented. The anticipated publication date of the new policy is set for August 2009.

(Attachment 18)

Compact Council Action: This topic was accepted as information only.

Topic #18 The Policy and Planning Committee Report on the National Criminal History Record Information Audit Guide for Noncriminal Justice Agency Audits (NCJA Audit Guide)

Mr. Timothy Neal, FBI Staff, reported that the Committee approved the *NJCA Audit Guide* with the following changes:

- Include *Authorized Users and Uses* to be updated as new federal legislation is enacted;
- Provide sampling methodology;
- Provide time frames to the generic audit methodology;
- Provide audit requirements pertaining to outsourcing;
- Provide to each SIB and publish on the Web site; and
- Utilize versioning for the audit guidelines and change management.

The Policy and Planning Committee further requested that the *NCJA Audit Guide* be forwarded to the Council for review and approval. The Council was then requested to review the information presented to them and also was requested to provide guidance on how the *NJCA Audit Guide* should be distributed to the SIB and State Repositories. Mr. Neal requested the Council review the listing of legislative resources, and informational documents to determine if these documents would be appropriate for the on-line asset library.

(Attachment 19)

Compact Council Action: Mr. David G. Sim moved to approve the Audit Guide as presented to the Council and make the guide available on the Council's Web site and in a publication form.

Seconded by Ms. Dawn A. Peck. The motion was carried.

Topic #19 The National Consortium for Justice Information and Statistics (SEARCH) and the National Crime Prevention and Privacy Compact Council (Council) Initiative to Update the User Fee Survey

Mr. Owen Greenspan, SEARCH, presented the Council with the Initiative to Update the User Fee Survey. The Council requested that SEARCH partner with the Council to

conduct an updated User Fee Survey. SEARCH was advised that the Bureau of Justice Statistics (BJS) would have to provide a justification to the Office of Management and Budget (OMB) to administer the survey and that OMB would have to review and analyze the labor and time involved, and approve/disapprove SEARCH to conduct the survey. Recently, SEARCH entered into a grant with BJS to continue updating the repository survey that has been conducted for eight years. SEARCH is anticipating releasing an updated survey on December 31, 2008. SEARCH requested that the Policy and Planning Committee provide input for inclusion in the future survey. The Policy and Planning Committee recommended that SEARCH provide clarification on the state and federal fee in the survey questions, and further recommended the survey be continued on a biannual basis.

In addition, Mr. Greenspan reported that during the September 2008 Policy and Planning Committee meeting, SEARCH shared its findings of the 2006 Repository Operations Survey, which does include fee questions.

(Attachment 20)

***Compact Council Action:* This topic was accepted as information only.**

Topic #20 Update From the Global Privacy and Information Quality Working Group

Mr. Owen Greenspan, SEARCH, provided an overview on the recent initiatives of the Global Privacy and Information Quality Working Group. Mr. Greenspan reported that recent events, such as terrorist threats and catastrophic natural disasters, have revealed a critical need for increasing information sharing capacities across disciplines, jurisdictions, agencies, and geographic areas. The rapid proliferation and evolution of new technologies and increased data sharing requires increased responsibility for information quality and for the protection of individual privacy and civil rights.

The U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) has developed standards, policies, guides, and handbooks and is a clearinghouse for information on information exchange protocols as well as the Global Advisory Committee. This committee reports directly to the Attorney General.

The Global Privacy and Information Quality Working Group (GPIQWG) assists government agencies, institutions, and other justice entities in ensuring that personally identifiable information is appropriately collected, used, and disseminated within

integrated justice information systems.

The GPIQWG created a guide to conducting privacy impact assessments for state, local and tribal information sharing initiatives. Information was distributed at the meeting to assist agencies in developing their own privacy guidelines. Mr. Greenspan shared a website that is a great resource for those who want to look at privacy standards and protocols or to obtain additional information about Global. The Web site, <www.it.ojp.gov>, enables justice agencies to obtain timely and useful information on computer system integration processes, initiatives, and technology developments.

(Attachment 21)

***Compact Council Action:* This topic was accepted as information only.**

Topic #21 Legislative Update

Mr. Danny R. Moye, FBI staff, provided an overview of pending and recently-enacted federal legislation introduced in the 110th Congress that may impact the FBI CJIS Division and the non criminal justice community. **(Attachment 21)**

Mr. Moye reported that The Criminal History Background Checks Pilot Extension Act of 2008, extends the PROTECT Act pilot until January 2010.

The Secure and Fair Enforcement For Mortgage Licensing Act was passed in July 2008. This act provides uniform licensing and reporting requirements for state licensed loan originators. It provides a comprehensive national licensing and supervisory database. States are expected to enact state statutes. In those states where statutes are not in place, the Department of Housing and Urban Development is to ensure the licensing requirements are met.

***Compact Council Action:* This topic was accepted as information only.**

Topic #22 Update on the Adam Walsh Child Protection and Safety Act of 2006 Implementation

Ms. Barbara S. Wiles, FBI staff, provided an update on state implementation Sections 151 and 153 of the Adam Walsh Child Protection and Safety Act of 2006 and the FBI's effort to provide guidance to states on implementing the access to CHRI for NCJ record

checks made available under this authority. The FBI guidance included a letter to all CJIS Systems Officers and state bureau representatives dated October 31, 2006. Ms. Wiles reported that in addition to the National Center for Missing and Exploited Children (NCMEC), six states have been approved for access under Section 151.

Section 153, also known as the Schools Safely Acquiring Faculty Excellence Act of 2006 (SAFE) Act, which provides that the Attorney General shall, upon request from a state's chief executive officer, conduct fingerprint-based criminal history record checks for: child welfare agencies on prospective foster or adoptive parents; and public or private elementary or secondary schools or local or state educational agencies on current and prospective employees or individuals in positions that would work with or around children in the school or agency. In addition to Washington, DC, eight states have been approved to submit fingerprints pursuant to Section 153. Twelve states and one tribal nation have made informal inquiries regarding the Act.

Ms. Wiles also reported that in March 2008, the CJIS Division began assigning ORIs to qualifying private schools under the Act. CJIS plans to include in a future CJIS Information Letter a notation about this change in policy. The Adam Walsh Act does not permit a national fingerprint-based background check of employees of private colleges. The schools authorized fingerprint-based access to CHRI under the Act are limited to public or private elementary or secondary schools. However, if a student teacher who is attending a private college is assigned to a qualifying public or private elementary/secondary school, a national fingerprint-based background check may be conducted on the student teacher pursuant to Section 153 by the public/private elementary/secondary school.

On July 2, 2008, the office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART) Office published the national guidelines for sex offender registration and notification in the Federal Register. Ms. Wiles provided the online address as <<http://www.ojp.usdoj/smart/guideline.htm>> The SMART office can also be reached via e-mail <getsmart@usdoj.gov> or telephone 202-514-4689.

(Attachment 22)

***Compact Council Action:* This topic was accepted as information only.**

Topic #23 Update on CJIS Division Departmental Order (DO) 556-73 Fingerprint Processing

Mr. Danny R. Moye provided an update on the recent efforts to modify the DO fingerprint processing procedures and request form.

Mr. Moye provided information from the new point of contact for the DO fingerprint processing procedures and request form. Mr. Eric Gormsen, DOJ, requested Mr. Moye request clarification on whether the requirement for the attorney letterhead or the power of attorney to be included within the Departmental Order request for those individuals who are requesting that his/her criminal history records be disseminated to a third party is too onerous. Mr. Gormsen suggested that the individual certify his/her record as an alternative means. As a result, both the Standards and Policy and Planning Committees opined that the certification on the part of the individual is not going to be satisfactory policy and that the requirement of the attorney letterhead or power of attorney letterhead was not too onerous. DOJ efforts on this issue are on hold until the next administration takes office in January 2009.

The Policy and Planning Committee also discussed drafting a rule in which the Council would take a firm stand to address the issue of state identification bureaus' encouraging the use of the Departmental Order process for backgrounding purposes.

Mr. Moye also announced that the FBI's use of III purpose code R in DO record requests to NFF states was implemented on September 7, 2008.

Compact Council Action: This topic was accepted as information only.

Topic #24 Proposal to Eliminate the Requirement That States Submit Expungement Documentation (documentation) to the FBI's CJIS Division as a Prerequisite to Expunging State-Maintained Criminal History Records (CHRs) from the Interstate Identification Index (III)

Topic #24 was not discussed. Staff paper was provided for information purposes only.

Compact Council Action: Staff paper was provided for information purposes only.

Topic #25 Next Generation Identification (NGI) Program Update

Ms. Rachael E. Tucker, FBI staff, presented a high level summary of the planned incremental implementation of the NGI capabilities, which included a series of Biometric Search Analysis studies, an incremental timeline and summary of the development

schedule.

Ms. Tucker first reported on the NGI stakeholder canvassing efforts and the incorporation into NGI's system requirement and specifications. She identified NGI's six core services as: identification, verification, information, investigation, notification and data management.

Ms. Tucker also discussed the new III Message Key for the submission of, and response to, disposition information electronically transmitted to the FBI's Fingerprint Identification Records System (FIRS). This capability has been implemented as an NGI QUICKWIN and on June 10, 2008, the Arizona Department of Public Safety (DPS) began electronically submitting dispositions via the III Message Key.

(Attachment 23)

***Compact Council Action:* This topic was accepted as information only.**

Topic #26 Integrated Automated Fingerprint Identification System (IAFIS) Status Report

Topic #26 was not discussed. Staff paper was provided for information purposes only.

***Compact Council Action:* Staff paper was provided for information purposes only.**

The meeting adjourned.