CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC M

Strategy to Promote N-DEx Usage by Fusion Centers

PURPOSE

To provide current strategy to leverage the fusion centers and institutionalize the use of the N-DEx system within Fusion Centers.

AUTHOR

Ronald C. Knight, (304) 625-2500, ronald.knight@leo.gov

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

On December 2-3, 2009 Advisory Policy Board (APB) meeting, the board passed, *"that CJIS APB leadership should be proactive in working with the development of the fusion center information sharing process by providing leadership and direction"*. As described by the N-DEx Program Office, Unit Chief, Supervisory Special Agent Jeffrey Lindsey's motto, "... to put the right information in the right hands", the N-DEx Program Office is currently implementing a strategy to leverage fusion centers and institutionalize the use of the N-DEx system within fusion centers across the country. Fusion centers provide an essential role in investigating criminal and terrorist activities nationwide. This paper outlines the actions taken by the N-DEx Program Office to increase N-DEx awareness and usage among the fusion center community.

N-DEx is a free resource available to criminal justice agencies to assist in investigating criminal and terrorist activities. Since fusion centers are defined as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the

center with the goal of maximizing their abilities to detect, prevent, investigate, and respond to criminal and terrorist activities[1], N-DEx, naturally provides fusion centers another tool to use. The N-DEx program office pro-actively developed a strategy to further the awareness and usage of the system for fusion centers across the country.

Prior to beginning N-DEx outreach, the N-DEx Program Office obtains all respective CJIS Systems Officer (CSO) approvals. Communication in working towards the N-DEx strategy is essential among the Program Office, CSOs and Fusion Center Executives.

Conduct Outreach Initiatives:

- Provide Materials and Training on Using N-DEx.
- Assist potential and approved applicants in obtaining N-DEx access.
- Establish connections to the N-DEx system either via individually or via regional systems.
- Attend conferences and regional meetings that involve fusion centers.

Prior to accessing N-DEx, all fusion center applicants must request system access by "Securing N-DEx SIG Membership." By securing membership, fusion center applicants will access the Law Enforcement Online and select the N-DEx SIG. Users will provide necessary documentation to their respective CSO via the SIG request. CSOs will review and approve or deny N-DEx access electronically. Upon CSO approval, fusion center applicants will be able to query N-DEx.

In conclusion, by increasing N-DEx awareness and usage among fusion centers, they will be able to access a national repository of criminal justice information that will greatly enhance their regional/state information sharing systems that will aid in providing accurate and timely support to their respective states.

---

[1] *The National Crime Intelligence Sharing Plan* is available at www.it.ojp.gov.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC N

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

PURPOSE

To provide information and updates regarding the CJIS NCIC enhancements.

POINT OF CONTACT

Cynthia Johnston, (304) 625-3061

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

At the June 2000 CJIS Advisory Policy Board (APB) meeting, the APB approved the CJIS System Enhancement Strategy Group's (SESG) proposal regarding the development of a process to manage pending and new NCIC enhancements. The approved proposal included prioritizing the current list of approved enhancements. The APB also approved the SESG's prioritization levels and descriptions for each level to assist members in determining what priority should be assigned to each new enhancement as it is recommended.

One of the main concepts in the strategy for managing the enhancements is to give members an opportunity at each meeting to reassign priorities and use the current list of enhancements to provide perspective relative to new priority assignments. Another concept is to track the development of the enhancements and evaluate the validity of current enhancements. As new issues are processed and approved by the APB, they are added to the ongoing list of enhancements. Therefore this list continuously evolves as new topics are added, completed ones are deleted, and as priorities change.

As new topics are discussed, members are requested to assign priority levels from the list below, along with a rating of high, medium, or low within each level.

SYSTEM ENHANCEMENT PRIORITIZATION LEVELS

Priority Description

0 Typically used for all new unassigned work requests. Tabled topics.

1 Critical project. System recovery, Production failure.

2 Essential Project. No effective work around, Legislative mandates, Data integrity problems

3 Important project. System enhancement/efficiencies, Cost saving, Adequate work around, No data integrity problems.

4 Desirable/operational enhancement.

5 Implement as resources permit.

Attachment #1 is a list of NCIC enhancements including new and pending enhancements since the last round of Advisory Process Meetings. The NCIC Build schedule constantly evolves due to programming requirements, manpower, and overall impact on the NCIC database baseline. Note, when a Technical and Operational Update is published supporting an NCIC Build, the one year notification occurs followed by a reminder letter in six months. During the fall 2002 APB meeting, a motion was passed to limit the minimum notification to three months for enhancements not affecting state programming.

Members are requested to:

Review the attached table regarding the NCIC enhancements and Build schedule.

If a member believes that a priority level needs to be changed or an enhancement should be removed from the list, provide input to the NCIC Subcommittee.

NCIC ENHANCEMENTS

BUILD SCHEDULE KEY

NCIC BUILD #13 (BROWN) - Scheduled for 8/5/2012; TOU published on 9/26/2011

POLICY CHANGE ENHANCEMENTS (ORANGE)

ENHANCEMENTS NOT ASSOCIATED WITH A BUILD (BLUE)

TABLED/AWAITING ADDITIONAL INFORMATION (BLACK)

As of: 12/27/2011

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
172	Create NICS Denied Person File (Brown)	2H	06/10	Yes	TBD	TBD
172a	Create Interim NICS Denied Person File - To include six months of data and new message key for inquiry. (Brown)	2H	06/10	Yes	2011	NCIC Build #13 (08/2012)
175	Allow inclusion of foreign sex offender records in the NSOR (Brown)	3M	06/10	Yes	2011	NCIC Build #13 (08/2012)
179	Create EXL codes 6/F; modify EXL codes 5/E; and create caveats for these EXL codes (Brown)	3H	06/10	Yes	2011	NCIC Build #13 (08/2012)
180	Create OPT Field for Article and Vehicle File records to indicate whether records will be shared with the public; field must support capturing date to move from out to in; and create default and remediation values by CSA (Brown)	4M	06/10	Yes	2011	NCIC Build #13 (08/2012)
184	Create caveat in recovered gun enter and modify acknowledgments advising agencies to perform a Trace request through ATF. (Brown)	3M	12/10	Yes	2011	NCIC Build #13 (08/2012)

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
188	Change entry requirement for all address data set fields to optional in Wanted Person File. (Brown)	3M	12/10	Yes	2011	NCIC Build #13 (08/2012)
190	Policy and operational change to allow all agencies to enter records into NCIC Missing Person File when HAI/EYE and/or HGT/WGT are not available. (Brown)	3H	12/10	Yes	2011	NCIC Build #13 (08/2012)
193	Create new RPP (Reason for Property Record Removal) code "NOT LOST" for Benefits and Effectiveness data. (Brown)	4L	12/10	Yes	2011	NCIC Build #13 (08/2012)

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
161a	Linked agencies will only be responsible for validating association. (Policy only.) (Orange)		6/11	Yes	TBD	TBD Pending Enh. 161 APB motion: Image File records will continue to be validated as part of the base NCIC record.(No change to existing policy.) Once 161 is implemented, Record owner is responsible for validating content and association with the record. (Policy change only.)
173	Allow VICAP to maintain records indefinitely for unidentified deceased remains based on NCIC Unidentified Person File record (Orange)	3M	06/10	No	2011	2012

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
174	Change validation process to require full validation at 60-90 days then only require court contact to verify validity each year thereafter. (Effects - Wanted, Missing, Unidentified, IVF, Gang, KST, POF, FFF, USSS Protective, SRF, and Id Theft) (policy only) (Orange)	NA	06/10	Yes	2011	COMPLETED TOU 11-3
181	Define completeness for NCIC records (policy only) (Orange)	NA	06/10	No	2011	COMPLETED TOU 11-3
183	Allow the NVS to compare private LPR data against the NCIC data they currently receive. (policy only) (Orange)	NA	12/10	No	2012	TBD
189	Designate all address fields in the Wanted Person File address data set as non-critical for audit purposes. (policy only) (Orange)	NA	12/10	Yes	2011	NCIC Build #13 (08/2012) *w/Enh #188*
191	Modify NCIC policy to allow INTERPOL USNCB to enter Missing Person File records when no evidence suggests they have entered the U.S. (Orange)	3H	12/10	Yes	2011	NCIC Build #13 (08/2012) *w/Enh #190*

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
199	Designate ADO (Wanted Person File) and ETN/PIE (Wanted, Missing, Protection Order Files, NSOR) fields as non-critical for audit purposes. Designate PWI data set as: critical fields (assess for completeness) for audit - PIN, PAK, PIX, PIR, PIB, PSM, and PSS and non-critical fields - PHG, PWG, PEY, PHA, PSK, and PMI. (Policy change only.) (Orange)	NA	6/11	Yes	2011	COMPLETED TOU 11-3
202a	Proof of service information and date fields should be designated as non-critical for audit. (Policy only.) (Orange)	NA	12/11	Yes	TBD	TBD *With Enh. 202.*
182	Provide extracts of stolen vehicle records to Aduana Mexico for port entry LPR databases. (Blue)	3H	12/10	No	TBD	TBD
185	Provide vehicle mirror-image extract to VINLock for one-year pilot for purpose of alerting finance industries of stolen vehicles. (Blue)	Pilot	12/10	No	2012	TBD
186	Provide real-time NCIC vehicle data to Nlets for LPR purposes. (Blue)	3M	12/10	No	2012	TBD

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
187	Provide real-time NCIC vehicle to Nlets for LoJack inquiries. (Blue)	3M	12/10	No	2012	TBD
194	Expand INTERPOL query access to include all files. (Blue)	3H	12/10	No	TBD	TBD
196	Evaluate and pursue options to address the need for status verification of trusted individuals for agencies that have authorized access to CJIS systems. (Blue)	NA	6/11	No	TBD	TBD
201	Convert Trace pilot to permanent project and ongoing receiver of CJIS data. Trace provide annual quantitative and qualitative report to include summary of success and areas of concern. NOTE: Other companies that come forward must follow same process as Trace. (Blue)	NA	6/11	No	2011	2012
11	Create the ability to transfer a fingerprint image from IAFIS to NCIC at the request of the originating agency (Black)	NA	6/95	Yes	Tabled Currently under study	Tabled

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	**PRIORITY LEVEL**	**APPROVED BY APB**	**USER IMPACT**	**TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE**	**IMPLEMENTATION DATE**
33	Create an Economic Crime Index (ECI) in NCIC. (Black)	NA	6/98	Yes	Tabled by the 12/2000 APB	Tabled
57A	Operational and Policy Change for the Supervised Release File - create notice on CHRI when record contains FBI number. (Black)	4M	6/02	Yes	TBD	TBD impacts IAFIS
93	Expand the Automatic NCIC Check Based on a Ten-Print Submission (Hot Check) Phase 2 - include NCIC hits on rapsheet and search Master Name from ident record if different from submitted name (Black)	2M	12/05	No	TBD IAFIS impact Further details need developed thru APB.	
98	Provide Nlets Access to NCIC to Conduct Vehicle File Inquiries on LOJACK Reported Stolen Vehicle (Black)	NA	06/06	No	NA	NA replaced by Enh #187
99	Create Missing Person Notice on CHRI when NCIC record includes an FBI Number (Black)	NA	06/06	TBD	TBD	TBD impacts IAFIS

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	**PRIORITY LEVEL**	**APPROVED BY APB**	**USER IMPACT**	**TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE**	**IMPLEMENTATION DATE**
101	Create the ability to search by address (wanted person and sex offender records) (Black)	3H	12/06	Yes	TBD	TBD currently under IT evaluation
119	Create an Unsolicited Message Advising of Discrepancies between Sex Offender File Record and the FBI Criminal History Record (Black)	NA	12/06	Yes	TBD	TBD impacts IAFIS
125	Create Immigration Violator Notice on CHRI when NCIC record contains an FBI Number (Black)	3H	06/07	No	TBD	TBD impacts IAFIS
161	Create ability to link an image record to multiple records and transfer ownership of image. (Black)	4M	06/09	Yes	TBD	TBD
162	Remove ECR Field from KST records (Black)	3M	06/09	No	2011	2012
169	Expand images to the NCIC Gun File (identifying and generic images) (Black)	4M	12/09	Yes	TBD	TBD

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	**PRIORITY LEVEL**	**APPROVED BY APB**	**USER IMPACT**	**TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE**	**IMPLEMENTATION DATE**
176	Incorporate the SSA's Death Master File into NCIC and generate a caveat for inquiries, entries, and modifications containing SOC that is associated with a deceased individual (Black)	4M	06/10	Yes	TBD	TBD - need to work with SSA to get data
177	Provide a mirror-image of the Vehicle File to NMVTIS to be accessible by the public (Black)	4M	06/10	No	TBD	TBD - Enh #180 must be implemented first
178	Allow NICB to use their mirror-image of the NCIC Vehicle File to be search via VINCheck (publicly accessible) (Black)	4M	06/10	No	TBD	TBD - Enh #180 must be implemented first
192	Add all additional fields from NCIC Vehicle and Wanted Person File Benefits Survey to current NCIC Benefits and Effectiveness data fields. (Black)	4L	12/10	Yes	TBD	TBD
195	Add LKI and LKA Fields to Protection Order, Gang, KST and Supervised Release Files (Black)	4L	6/11	Yes	TBD	TBD

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	USER IMPACT	TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE	IMPLEMENTATION DATE
197	CJIS conduct data quality review of Wanted Person File records and evaluate the cross-match program to review the potential matches for juvenile records in the Unidentified Person File with estimated age of 21 and below. Bring back to 2012 Working Groups. (Black)	NA	6/11	TBD	2011	TBD (Resolving issue identified with cross match algorithm.)
198	Modify the entry requirement in the Wanted Person File for the Extradition Limitation (EXL) Field from optional to mandatory, without a default. (Black)	3H	6/11	Yes	TBD	TBD
200	Add all Image File data fields to validation format. (Black)	NA	6/11	Yes	TBD	TBD
201	Provide U.S. law enforcement with access to the Canadian Firearms Interest Police (FIP) Database. Create a new MKE to access the FIP Database and create a task force to include CJIS, CPIC, APB, and Nlets. (Black)	NA	12/11	Yes	TBD	TBD
202	Include proof of service information and date fields in the Protection Order File. (Black)	3H	12/11	Yes	TBD	TBD

PENDING NCIC ENHANCEMENTS						
	ENHANCEMENT	**PRIORITY LEVEL**	**APPROVED BY APB**	**USER IMPACT**	**TIME LINE WHEN FBI WILL BE ABLE TO WORK ON TENTATIVE**	**IMPLEMENTATION DATE**
203	Develop concept to create an NCIC notification to the NSOR ORI when a registered sex offender attempts to enter or depart the United States. (Black)	4H	12/11	Yes	TBD	TBD
204	Modify the Protection Order File PCO Code 07 translation. (Black)	4H	12/11	No	TBD	TBD
205	Display the VLN Field to the CSA for local agencies that fall under their purview in a record response. (Black)	4M	12/11	No	TBD	TBD

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC O

National Crime Information Center (NCIC) 2000 Header Requirement

PURPOSE

To provide an update of the status of state, federal, and territorial agency compliance with the 1N01 Header requirement.

POINT OF CONTACT

Kimberly K. Lough, (304) 625-3855

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

In June 2002, the APB voted to affirm the NCIC 2000 full operating capability (FOC) deadline of July 12, 2002. The FOC deadline applied to the following areas:

- Upgrading Communications Protocol from Binary Synchronous Communications to Transmission Control Protocol/Internet Protocol or Systems Network Architecture.
- Implementing the 1N01 Header on all applicable NCIC transactions.
- Programming for new and expanded fields.

In addition, in June 2008, the APB recommended the establishment of an additional objective for NCIC 2000 Readiness:

- Migrate all NCIC transactions to NCIC 2000 (1N01 header) format by July 1, 2012.

The original condition of implementing the 1N01 header format on all applicable NCIC transactions was a requirement on the CJIS Systems Agencies (CSAs) to ensure that their system supported NCIC 2000 formatted transactions.

On October 15, 2008, the CJIS Division sent a letter from the APB Chairman to the CSAs advising them of the new objective and compliance date. At that time, 40 CSAs were using NCIC Legacy (1L01 header) formatted transactions. A count of each CSAs 1L01 header formatted transactions for the prior month, by ORI and message key, was provided with the letter.

The CJIS Division continues to monitor and provide a listing of 1L01 header formatted transactions via e-mail to all CSAs that continue to submit 1L01 header formatted transactions to NCIC. As of November 1, 2011, 11 CSAs continued to use the 1L01 header format. The majority of the CSAs still submitting 1L01 header formatted transactions to NCIC have minimal submission in the 1L01 header format; however, 4 of the 11 CSAs continue to forward a large volume of 1L01 header formatted transactions to NCIC each month. Of the remaining 7 CSAs, 3 of them have a low volume of submissions but are transmitted from numerous agencies. The following CSAs submitted 1L01 header formatted transactions to NCIC during November 2011.

California	Hawaii	Mississippi
Nebraska	New Mexico	Oklahoma
West Virginia	Royal Canadian Mounted Police	Bureau of Immigration and Customs Enforcement
United States National Central Bureau	U.S. Secret Service	

If a CSA cannot meet the compliance date of July 1, 2012, they will be able to request an extension through a process similar to the FOC compliance. In January 2012, the CJIS Division disseminated letters to all CSAs advising them of the process to request extensions to the header format requirement. CSAs requesting extensions should explain the CSA's reasons for failing to meet the aforementioned requirement. They are also expected to identify steps taken at the CSA level to ensure progress toward compliance. CSAs requesting extensions are also required to state when they will be able to support the NCIC 2000 header for all NCIC transactions.

FBI staff will continue to monitor these agencies' progress. Once compliance is met, the NCIC Subcommittee will be updated on the progress toward completing this objective during scheduled meetings and the compliant CSAs will be removed from future lists provided to the Subcommittee.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC P

Warrant Task Force Status Report

PURPOSE

To present the Warrant Task Force's issues and recommendations.

POINT OF CONTACT

Kimberly K. Lough, (304) 625-3855

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

During the spring 2005 Working Group and Subcommittee meetings, many topics involving warrant related issues were discussed. Proposals included: allow multiple warrants for the same individual in the National Crime Information Center (NCIC) Wanted Person File, the expansion of the NCIC Wanted Person File to include non-serious misdemeanor warrants and its impact on the Integrated Automated Fingerprint Identification System (IAFIS), and the automatic NCIC search based on a ten-print submission to the Integrated Automated Fingerprint Identification System.

The warrant related topics were multifaceted and complex resulting in detailed discussion. Furthermore, it was recommended that the topics be reviewed in depth by a task force. As a result, the Warrant Task Force was re-established to review the issues and provide recommendations back through the CJIS Advisory Process. The Warrant Task Force was formed to look at issues germane to automated warrant systems, the timely entry of NCIC Wanted Person File records, and other warrant-related topics. The mission and work flow of the Warrant Task Force was reiterated to the members. In general, topics for discussion are forwarded to the task force by the NCIC Subcommittee

then sent to the Advisory Policy Board. Ideas developed from the task force are routed as new topics through the entire Advisory Process.

The following individuals comprise the membership of the Warrant Task Force: Mr. Michael McDonald, Director, Information Technology, Delaware State Police serves as the Warrant Task Force Chairman; Mr. James Lawrence "Larry" Coffee, Criminal Justice Information Services, Florida Department of Law Enforcement; Mr. Michael Corwin, Captain, Kansas City Police Department, Missouri; Mr. Paul Embley, National Center for State Courts, Virginia; Mr. Alan Gershel, Associate Professor, Thomas M. Cooley Law School, Michigan; Ms. Mary Kay MacNichol, New Hampshire State Police; Mr. Walt Neverman, Director, Crime Information Bureau, Wisconsin Department of Justice; Mr. Lawrence A. Stelma, Sheriff of Kent County, Michigan; and Ms. Kathy Witt, Sheriff of Fayette County, Kentucky.

DISCUSSION AND ANALYSIS

The most recent meeting of the Warrant Task Force was held on December 5, 2011, in Albuquerque, New Mexico. The following issues were discussed:

1. Legislation Update (S 3120 & S 306)
2. Outreach by Warrant Task Force to Criminal Justice Organizations
3. Court Cases involving Warrants
4. Multiple Warrants in NCIC
5. Improperly Placed Locates
6. Automated Warrant Management Systems
7. 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
- Expanded the Hot Check to include all person files
- Self assessment tool provided every 6 months
- Added additional timely entry "exception" to include investigatory discretion
- Amended the completeness policy for audit assessments
- Amended the validation policy
- Flag misdemeanors in IAFIS – post NGI
- Included additional codes for extradition at the time of entry
- Changed all address fields to optional for entry and defined them as non-critical for completeness for audit assessments
- Required the Extradition Limitation Field be a mandatory field
- Addressed critical field determinations for Persons With Information dataset

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 02/08/2011. 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 03/16/2010, read twice and referred to the Committee on the Judiciary. At this time, no further action has been taken. Warrant Task Force Chairman McDonald sent a letter to Senator Durbin in November 2010, to encourage continued efforts to pass the FIND Act. In addition, Mr. McDonald requested a status on the bill and offered assistance in support of the furtherance of the Act. At this time, no response has been received. As a result of discussions during the December meeting, the chairman will again follow-up with Senator Durbin's office to obtain the status. In addition, the CJIS Division staff will contact the United States Marshals Service to gauge their interest and knowledge of the FIND Act. Findings will be reported during the June 2012 Warrant Task Force meeting.

Currently, the Warrant Task Force Chairman is also a member of the Disposition Task Force and attends meetings as both groups are similarly charged with analyzing the participation of agencies entering warrants into NCIC and updating dispositions. Both groups are working to identify technical, policy, and operational solutions to increase both disposition reporting and warrant entry at the national level. Having similar areas of concern, the Warrant Task Force and Disposition Task Force plan to work together in identifying solutions.

In addition, the Warrant Task Force further discussed the creation 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. The intent is to publish sound practices related to warrant entry and maintenance issues in an effort to aid in improving state and local warrant systems as well as NCIC.

The Warrant Task Force meeting resulted with the following recommended topics for the spring 2012 Advisory Policy Board process:

- To solicit interest in creating an additional NCIC File for warrants not meeting entry criteria requirements (e.g., local ordinances and violations).
- Recommend allowing multiple wanted person entries in the NCIC Wanted Person File under the same ORI.
- To modify the locate process allowing the entering agency the capability to locate their own records.

In addition, the FBI CJIS Division will follow-up on community outreach and training on extradition, locate procedures, and NCIC warrant policies. The CJIS Division will also work with the CJIS Systems Agencies of Delaware and New Hampshire to pilot a state warrant file synchronization project to determine the amount and type of state warrants

currently not in the NCIC. After the synchronization, the CJIS Division will perform a statistical analysis of the results to make suggested recommendations on what performance metrics can be used to measure system use and trends.

The following recommended topics will be discussed during the June 2012 Warrant Task Force meeting:

- John Doe Warrants for DNA
- Warrant Automation
- Pending legislation

Members are asked to review the Warrant Task Force Status report and provide feedback as deemed necessary. As applicable, concept papers regarding individual recommendations will be forwarded back through the Advisory Process for review.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPIC

STAFF PAPER

INFORMATIONAL TOPIC Q

National Crime Information Center (NCIC) Fiscal Year 2011 Audit Results Summary

PURPOSE

To inform Advisory Process members of the most common recommendations to CJIS Systems Agencies (CSAs) resulting from NCIC audits during fiscal year 2011.

AUTHOR

Linda S. Click, (304) 625-2278

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND AND DISCUSSION

This paper summarizes the recommendations from 18 NCIC audits of state and federal CSAs, which included 207 local agency reviews, from October 1, 2010, to September 30, 2011. It should be noted that for each deficiency found during agency audits, the CAU auditors informed agency personnel of the deficiencies, provided the assessed policy and source reference(s), explained how to comply with policies, and discussed corrective measures to achieve policy compliance. It should also be noted that local agencies may have been noncompliant with policies that were not deemed to be widespread issues within the jurisdiction of the CSA being audited, therefore was not made a recommendation to the CSA. This information is being provided through the Advisory Policy Board Process so action can be taken to address areas with widespread deficiencies, as appropriate.

Eleven (11) CSAs had a recommendation to ensure that the Interstate Identification Index (III) is used only for authorized purposes in accordance with the policy that states:

> The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applications. (*CJIS Security Policy*, Version 5.0, February 2011, 4.2.2.1 Proper Use of CHRI)

Ten (10) CSAs had a recommendation to ensure that records are entered in a timely manner in accordance with the NCIC policies that state:

> Federal Fugitive Records -- Entry is made immediately (i.e., within 24 hours) upon receipt of information by the inputting agency/office, after the decision to arrest or authorize arrest has been made. (*NCIC 2000 Operating Manual*, Introduction, Section 3.2, 2, 2)

> [Missing Person File --] A record for a missing person who is under the age of 21 should be entered into NCIC using one of the appropriate categories (Disability, Endangered, Involuntary, Juvenile, or Catastrophe Victim) within 2 hours of receipt of the minimum data required to enter an NCIC record. A missing person report filed with an agency is sufficient documentation for entering a juvenile in the NCIC Missing Person File. (*NCIC 2000 Operating Manual*, Missing Person File, Section 1.3)

Five (5) CSAs had a recommendation to ensure that purpose codes are used appropriately for III transactions in accordance with the III policy that states:

> The Privacy Act of 1974 requires that the FBI's CJIS Division maintain an audit trail of the purpose of each disclosure of a criminal history record and the recipient of that record. Therefore, all III QH and QR transactions must include the purpose for which the criminal history record information is to be used. The purposes for which authorized agencies may use III and the appropriate codes for use are:
>
> Purpose Code A - Administrative - File Maintenance - Purpose Code A is used by authorized participating state agencies to retrieve records for internal review. Purpose Code A responses cannot be disseminated for any other purpose. A QR for Purpose Code A allows a state to review CHRI, want, and sex offender registry notifications that are in the III for that state.

Purpose Code C - Criminal Justice - Purpose Code C is used for official duties in connection with the administration of criminal justice.

Purpose Code D - Domestic Violence and Stalking - Purpose Code D is used when the III transaction is for use by officials of civil or criminal courts in domestic violence or stalking cases. Civil courts may be issued Originating Agency Identifiers (ORIs) containing a D in the ninth position, at the discretion of the appropriate state CJIS Systems Officer (CSO) and the FBI's CJIS Division. ORIs ending in D are limited to QH and QR transactions for Purpose Code D.

Purpose Code F - Weapons-Related Background Checks - Purpose Code F is used by criminal justice agencies for the purposes of (a) issuing firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; (b) returning firearms to their lawful owners; and (c) enforcing federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned.

Purpose Code H - Housing - Purpose Code H is used when the III inquiry is made under the authority of the Housing Opportunity Extension Act of 1996. The use of this purpose code is limited to QH transactions. The FBI's CJIS Division may assign Public Housing Agencies ORIs containing the letter Q in the ninth position for use by authorized agencies.

Purpose Code J - Criminal Justice Employment - Purpose Code J is used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control. Such screening may include the use of III on friends, relatives, and associates of the employee or applicant, unless restricted or prohibited by state statute, state common law, or local ordinance. Criminal Justice Employment (Purpose Code J) has been separated from other Criminal Justice Purposes (Purpose Code C) due to the varying requirements of some state agencies participating in the III.

Purpose Code X - Exigent Procedures - Purpose Code X is used when a QH is made during an emergency situation when the health and safety of a specified group may be endangered. Following a QH, a QR may be used to review the individual's record. All requests for background checks for exigent purposes must be accompanied by fingerprints. When the SIB [State Identification Bureau] does not make a positive identification, the delayed submission of fingerprints to the FBI must occur within the time frame agreed to by the National Crime Prevention and Privacy Compact Council. Purpose Code X must be used by agencies authorized under an approved statute to receive criminal history record information preceding the delayed submission of fingerprints or by law enforcement agencies servicing the record needs of such agencies. Purpose Code X must be pre-approved before it can be used. The FBI may assign a T in the

ninth position of the ORI for use by authorized noncriminal justice agencies. Contact your CSA to determine if your agency has authority to use Purpose Code X. (*NCIC 2000 Operating Manual*, III, Section 2.1)

Five (5) CSAs had a recommendation to ensure records are entered with all available information in accordance with the NCIC policies that state:

> Complete records include all critical information that was available on the person or property at the time of entry. Critical information is defined as data fields that will: (1) increase the likelihood of a positive hit on a subject or property and aid in the identification of a subject or property; or (2) assist in compliance with applicable laws and requirements. Validation should include a review of whether additional information which is missing from the original entry that could be added has become available for inclusion to the record. (*NCIC 2000 Operating Manual*, Introduction, Section 3.2, 3)
>
> When additional numeric identifiers and personal descriptors regarding the subject of the record are found in other databases or documentation, the entering agency must make an informed decision as to whether or not the subject is the same as the one in the NCIC record. In the absence of biometric identifiers, the determination should be based on multiple factors such as known criminal activity, date of birth, scars, marks, tattoos, photographs, Social Security number, operator's license number, passport, military identification, last known address, and aliases. Particular attention should be paid to discrepancies in height, age, etc. When uncertain, do not include the additional information in the NCIC record and maintain documentation in the case file. (*NCIC 2000 Operating Manual*, Wanted Person File, Section 2.5, 11; Missing Person File, Section 2.5, 7; and Protection Order File, Section 2.4, 6)

Five (5) CSAs had a recommendation to ensure that local agencies conduct second-party checks of records entered into the NCIC in accordance with the NCIC policy that states:

> The accuracy of NCIC records is an integral part of the NCIC System. The accuracy of a record must be double-checked by a second party.
>
> The verification of a record should include assuring all available cross-checks, e.g., VIN/LIC, were made and that the data in the NCIC record match the data in the investigative report. (*NCIC 2000 Operating Manual*, Introduction, Section 3.2, 1)

Four (4) CSAs had a recommendation to ensure that Extradition Limitation Field (EXL) codes are used appropriately in accordance with the NCIC policies that state:

> At the time of entry, if there is a limitation concerning extradition of the wanted person, such information should be entered using the appropriate code in the Extradition Limitation Field with any specific limitations placed in the MIS Field

of the record (NCIC 2000). For NCIC Legacy-formatted messages, the entering agency may place extradition limitation information in the MIS Field. More information can be found in the Personal Descriptors chapter of the *NCIC 2000 Code Manual* (December 2000). (*NCIC 2000 Operating Manual*, Wanted Person File, Section 1.1, 5, 3)

Agencies entering warrants that do not meet the NCIC definition of extradition (e.g., intrastate only) must code the EXL Field as 4 (NO EXTRADITION) for felony warrants and D (MISDEMEANOR – NO EXTRADITION) for misdemeanor warrants. Additional details regarding intrastate limitations may be placed in the MIS Field. (*NCIC 2000 Operating Manual*, Wanted Person File, Section 1.1, 5, 1)

Three (3) CSAs had a recommendation to ensure that local agencies validate their records in accordance with the NCIC policy that states:

Validation obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, nonterminal agency, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the entry in the file. (*NCIC 2000 Operating Manual,* Introduction, Section 3.4, 1)

Three (3) CSAs had a recommendation to ensure that secondary dissemination of III requests is logged or properly logged in accordance with the policy that states:

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period. (*CJIS Security Policy,* Version 5.0, February 2011, 5.4.7 Logging NCIC and III Transactions)

Three (3) CSAs had a recommendation to ensure all terminal agencies are triennially audited in accordance with the policy that states:

Each CSA shall: 1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations, and policies. (*CJIS Security Policy*, Version 5.0, February 2011, 5.11.2 Audits by the CSA)

Two (2) CSAs had a recommendation to ensure that NCIC records contain accurate information in accordance with the NCIC policy that states:

> NCIC 2000 records must be kept accurate and up-to-date. Agencies that enter records in the NCIC 2000 System are responsible for their accuracy, timeliness, and completeness. (*NCIC 2000 Operating Manual*, Introduction, Section 1.3, 1)

Two (2) CSAs had a recommendation to ensure that NCIC inquiries are conducted in a timely manner in accordance with the NCIC policy that states:

> Timely inquiry requires that the transaction is initiated before an officer begins writing an arrest or citation document of any kind; inquiries are stored when NCIC 2000 is not available and submitted at once when the System returns, regardless of whether the subject is still in custody; inquiry is made prior to release of a person who has been incarcerated; and inquiry is made upon those who appear at a custodial facility to visit inmates. (*NCIC 2000 Operating Manual*, Introduction, Section 3.2, 2, Additional explanations of "timely," 3)

Two (2) CSAs had a recommendation to ensure that local agencies which enter records into NCIC are available 24 hours a day to perform hit confirmations in accordance with the NCIC policy that states:

> Every agency that enters records destined for NCIC 2000 must assure that hit confirmation is available for all records, except III records, 24 hours a day either at that agency or through a written agreement with another agency at its location. (*NCIC 2000 Operating Manual*, Introduction, Section 5.4, 3)

Two (2) CSAs had a recommendation to ensure that training records of terminal operators are maintained in accordance with the NCIC policy that states, CSAs must:

> Maintain records of all training, testing, and proficiency affirmation. (*NCIC 2000 Operating Manual*, Introduction, Section 3.1, 3, 3)

Two (2) CSAs had a recommendation to program for EXL Field Codes A-E and/or ensure that local agencies properly use the EXL Field codes when entering nonserious misdemeanor warrants in the Wanted Person File in accordance with the NCIC policy that states:

> Records for nonserious misdemeanor warrants must include the Extradition Limitation (EXL) Field [A-E]. (*NCIC 2000 Operating Manual*, Wanted Person File, Section 1.1, 2)

Two (2) CSAs had a recommendation to ensure that response times for III inquiries comply with NCIC standards in accordance with the NCIC policy that states:

> Average message response time for a III inquiry from the CSA to NCIC 2000 and back to the CSA should not exceed 5 seconds. [standard 1]

Average message response time from a CSA to an agency interfaced with the CSA should not exceed 15 seconds after transmission of the inquiry, with 5 of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 1 above. [standard 2]

Average message response time for an end-user terminal interfaced with a local/regional system which is interfaced with a CSA should not exceed 25 seconds after the transmission of the inquiry, with 15 of the 25 seconds allocated to the transmission to, processing by, and return of the response from the CSA and NCIC 2000 as described in standards 1 and 2 above.

Average response time from any local regional system or terminal interfaced directly with the NCIC 2000 computer (i.e., NCIC 2000 lines which terminate at an agency that is not a CSA) to an end-user terminal interfaced with the local/regional system shall not exceed 15 seconds, with 5 of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 1 above.

An additional 10 second allowance can be made for additional network interfaces. These interfaces will include servers to local area or wide area networks, intranets, and wireless communication systems (commercial and private). For example, mobile units connected to a wireless communications system and then connected to a metropolitan server which is interfaced with the CSA and then connected to NCIC will be allowed a 32 second total response time from the initial inquiry.

Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as during the installation of a new computer, should be excluded from the one-month compilation. (*NCIC 2000 Operating Manual*, Introduction, Section 5.3)

One (1) CSA had a recommendation to ensure that hit confirmation documentation is maintained in accordance with the NCIC policy that states:

When an operational inquiry on an individual or property yields a valid positive response (hit), the terminal-produced printout showing the inquiry message transmitted and the record(s) on file in NCIC 2000 should be retained for use in documenting probable cause for the detention of the missing person, arrest of the wanted person, or seizure of the property. The printout may also prove valuable in a civil suit alleging a false arrest, a false imprisonment, a civil rights violation, or an illegal seizure of property. If two-part paper is used, either the original or the legible copy is admissible in federal court. Whether a state court will accept the legible copy or whether only the original will suffice depends on the state's rules of evidence.

> When an NCIC 2000 inquiry yields a hit, the terminal employee making the inquiry should note on the terminal-produced printout precisely how, when, and to whom the information was given, initial and date this notation, and forward the printout to the inquiring officer or agency for retention in the case file. This procedure establishes the chain of evidence for the communication should the arresting officer need to substantiate actions in a judicial proceeding.
>
> The printout should be retained for as long as there remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. The printout should be retained until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated. (*NCIC 2000 Operating Manual*, Introduction, Section 3.8, 1-3)

One (1) CSA had a recommendation to ensure invalid records are removed in a timely manner in accordance with the NCIC policy that states:

> Every agency is responsible for the removal of an NCIC 2000 record as soon as it is aware that the record is no longer valid. (*NCIC 2000 Operating Manual*, Introduction, Section 5.4, 4)

One (1) CSA had a recommendation to ensure hit confirmation procedures are followed in accordance with the NCIC policies that state:

> Any agency which receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any official actions based upon the hit NCIC record: 1) arresting the wanted person, 2) detaining the missing person, 3) seizing the stolen property, 4) charging the subject with violating a protection order, 5) denying the subject the purchase of a firearm, or 6) denying the subject access to explosives as regulated under the Safe Explosives Act. Additionally, an agency detaining an individual on local charges where the individual appears identical to the subject of the wanted person record *and is within the geographical area of extradition* must confirm the hit. (*NCIC 2000 Operating Manual*, Introduction, Section 3.5, 1)
>
> Confirming a hit means to contact the agency that entered the record to:
>
> 1. Ensure that the person or property inquired upon is identical to the person or property identified in the record;
> 2. Ensure that the warrant, missing person report, protection order, or theft report is still outstanding; and
> 3. Obtain a decision regarding: 1) the extradition of a wanted person when applicable, 2) information regarding the return of the missing person to the appropriate authorities, 3) information regarding the return of stolen property to its rightful owner, or 4) information regarding the terms,

conditions, and service of a protection order. (*NCIC 2000 Operating Manual*, Introduction, Section 3.5, 1, 1-3)

One (1) CSA had a recommendation to ensure terminal operators are biennially retested in accordance with the NCIC policy that states, CSAs must:

> Biennially, provide functional retesting and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with FBI CJIS policy. (*NCIC 2000 Operating Manual,* Introduction, Section 3.1, 3, 2)

One (1) CSA had a recommendation to ensure each Protection Order File record is supported by a protection order in accordance with the NCIC policy that states:

> Each record in the POF **must** be supported by a protection order (electronic or hard copy). (*NCIC 2000 Operating Manual*, Protection Order File, Section 1.2)

One (1) CSA had a recommendation to ensure the "Other" category in the Missing Person File is programmatically available and used appropriately in accordance with the NCIC policy that states:

> A missing person record may be entered using one of the following categories:
>
> 1. Disability (MKE/EMD): a person of any age who is missing and under proven physical/mental disability or is senile, thereby subjecting him/herself or others to personal and immediate danger.
>
> 2. Endangered (MKE/EME): a person of any age who is missing under circumstances indicating that his/her physical safety may be in danger.
>
> 3. Involuntary (MKE/EMI): a person of any age who is missing under circumstances indicating that the disappearance may not have been voluntary, i.e., abduction or kidnapping.
>
> 4. Juvenile (MKE/EMJ): a person who is missing and not declared emancipated as defined by the laws of his/her state of residence and does not meet any of the criteria set forth in 1, 2, 3, or 5.
>
> 5. Catastrophe Victim (MKE/EMV): a person of any age who is missing after a catastrophe.
>
> 6. Other (MKE/EMO): a person not meeting the criteria for entry in any other category who is missing and 1) for whom there is a reasonable concern for his/her safety or 2) a person who is under age 21 and declared emancipated by the laws of his/her state of residence (NCIC 2000 format only). (*NCIC 2000 Operating Manual*, Missing Person File, Section 1.1, 1)

One (1) CSA had a recommendation to ensure caution indicators are used, if applicable, when entering Protection Order File records in accordance with the NCIC policies that state:

> A caution indicator should be added to the message key EPO or ETO when it is known that an individual is armed and dangerous, is a drug addict, or whatever is appropriate to the particular circumstances of the individual. (*NCIC 2000 Operating Manual*, Protection Order File, Section 1.3)
>
> If a caution indicator is used in the message key, the reason for the caution must be entered as the first item in the MIS Field (NCIC format only.) (*NCIC 2000 Operating Manual*, Protection Order File, Section 2.5, 6, 1)
>
> When a POF record is entered with a caution indicator, the MKE ends with C, and the CMC Field must contain a valid caution and medical code. (*NCIC 2000 Operating Manual*, Protection Order File, Section 2.6, 1)

One (1) CSA had a recommendation to ensure that local agencies appropriately use the clear and cancel transactions to remove Protection Order File records in accordance with the NCIC policies that state:

> Cancellation of a record is restricted to the agency that entered the record. A cancellation message will immediately retire the POF record. These records are not available in the inactive database. POF records that have been expunged or are determined to be inaccurate should be canceled. Active, expired, and cleared records can be canceled. (*NCIC 2000 Operating Manual*, Protection Order File, Section 4.1)
>
> When a court notifies the owner of the record that the protection order has been canceled, the entire corresponding POF record must be cleared. The clear transaction will change the status of the POF record from active to inactive. Clearance of a POF record is restricted to the agency that entered the record. Expired records cannot be cleared. (*NCIC 2000 Operating Manual*, Protection Order File, Section 7.1)
>
> When a Protection Order File record is cleared, any supplemental information appended to that record will be cleared automatically.
>
> When a POF record is cleared, its status will be changed to inactive. During this period of time, the record can be accessed via the QPO transaction. Inactive records cannot be modified. The record will remain on file for the remainder of the year plus 5 years at which time the record will be retired. (*NCIC 2000 Operating Manual*, Protection Order File, Section 7.5)

One (1) CSA had a recommendation to conduct the biennial Originating Agency Identifier (ORI) validation in accordance with the NCIC policy that states:

> ORIs are validated on a biennial basis. . . . Each CSA is responsible for verifying the accuracy of every ORI accessing NCIC through the respective state/federal system. The validation process includes verifying an agency's status and authority, as well as the other information listed in the ORI record, e.g., telephone number, street address, and ZIP code. (*NCIC 2000 Operating Manual*, ORI File, Section 1.7)

One (1) CSA had a recommendation to ensure validation efforts of NCIC records are maintained in accordance with the NCIC policy that states:

> In addition, documentation and validation efforts must be maintained for review during such audit. (*NCIC 2000 Operating Manual*, Introduction, Section 3.4, 4)

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC R

National Center for Missing and Endangered Children (NCMEC) Notification of Missing Juveniles in the National Crime Information Center (NCIC) Disability Category

PURPOSE

The purpose of this paper is to present a request on behalf of the NCMEC to receive notifications when records for juveniles are entered, modified, or canceled in the NCIC Missing Person File Disability Category.

POINT OF CONTACT

Cynthia Johnston, (304) 625-3061

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

The NCMEC is a nongovernmental, noncriminal justice agency created in April 1984 to aid law enforcement, as well as, the parents of missing and exploited children. Legislation enacted in 1984 and 1990 further defined the role and mission of NCMEC and mandated close liaison between NCMEC and law enforcement. NCMEC has been authorized by law at Title 42, United States Code, Section 534, to have access to NCIC information, and has been specifically designated through Title 22, Code of Federal Regulations, Section 94.6 as **the** entity to act under the direction of the U.S. Central Authority to receive all applications on behalf of the U.S. Central Authority pertinent to international child abduction remedies. There are also two agreements on file between the FBI and NCMEC with regard to access to NCIC files. The first is dated 12/18/84 and authorizes NCMEC access to missing juveniles and missing adults who were originally entered as juveniles in the Missing Person File and unidentified living and unidentified dead in the Unidentified Person File. By agreement dated 3/13/90, NCMEC was also authorized access to the Wanted Person File.

Therefore, through CJIS Advisory Policy Board (APB) approval, NCMEC was assigned a unique Originating Agency Identifier (ORI) with the letter **"W"** in the ninth position. This ORI structure allows NCMEC to query the NCIC Wanted, Missing and Unidentified Person Files. In July 2006, NCMEC was granted authority to access all NCIC files under the Adam Walsh Child Protection and Safety Act of 2006. As a result, the ORI structure ending in **"F"** was created. In September 2008, NCMEC requested access to the NCIC Vehicle File using their **"W"** ORI numbers. This request is in accordance with NCMEC's authority to access NCIC files and was approved by the CJIS APB Executive Committee on 01/14/2009. Therefore, effective 2/19/09, CJIS made modifications to include the query vehicle message keys to the authorized capabilities for ORI numbers ending in **"W"**.

The NCMEC currently receives $.8. notifications when the Missing Person Interest Field is set to 'Y' and for all Endangered and Involuntary entry, modify, cancel, locate, and clear transactions (including supplemental and dental data) when the Missing Person (MNP) Field reflects 'Child Abduction' or 'Amber Alert.' Receipt of the $.8. notifications allows NCMEC to collaborate with their analysis and determine necessary action as well as maintain synchronization with records in the NCIC files.

DISCUSSION AND ANALYSIS

Mr. Bud Gaylord, Executive Director, Case Analysis Division of NCMEC requests that the NCMEC receive notifications for missing juveniles in the NCIC Disability category. According to Mr. Gaylord, cases of missing children with disabilities present unique challenges. The NCMEC can provide specialized resources to law enforcement and families to assist with the fast and safe resolution of these cases.

As previously discussed, the NCMEC has access to the NCIC Missing Person File and currently receives notifications for select missing person record categories. Therefore, the CJIS Division believes that this request falls within the NCMEC's existing legislative and APB authorities. The new notification may be created similar to the existing $.8. notifications and will not impact state systems.

Members are asked to review the information in this paper and provide feedback as deemed necessary. As applicable, concept papers regarding individual recommendations will be forwarded separately through the Advisory Process for action.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC S

Implementation of the Next Generation Identification (NGI) Enhanced Repository

PURPOSE

To provide explanation as to the current process of establishing a "Master Name" within the Integrated Automated Fingerprint Identification System (IAFIS) when a civil identity exists prior to a criminal arrest, and how this process will change with NGI deployment of Increment 4.

POINT OF CONTACT

Brian Edgell, Implementation and Transition Unit Chief (304) 625-3551

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

The IAFIS criminal and civil records are maintained in separate repositories without a common mechanism to search and maintain. At present, the IAFIS has no electronic capability to consolidate or modify the civil fingerprint file's biographic data, civil history information, and fingerprint data. The civil submissions are neither stored nor accessible in an easily searchable manner. Therefore, multiple civil records are retained for the same individual, without the existence of one true identity or "Master Name". Today, an individual applying for multiple positions will have numerous civil records within the IAFIS, as opposed to only one criminal record for an individual with numerous arrest events.

When a criminal submission is subsequently searched against the civil repository for authorized purposes, the current process requires a manual intervention when this criminal search matches a civil record. In the scenario where a civil record is established prior to any criminal record, the first criminal record establishes the "Master Name" and the name used from the civil record is

added to the criminal record as an Also Known As (AKA). This practice is due to the current technical limitations of the IAFIS, where the criminal repository represents a person-centric architecture and the civil repository is an encounter based architecture.

DISCUSSION AND ANALYSIS

The mandate for the FBI to retain civil fingerprints has grown stronger in recent years. Similarly, an estimated 1,200 state statutes have been approved by the Attorney General, pursuant to the provisions of Public Law 92-544, to receive national criminal history record checks. Because states have chosen to collect and retain (or not retain) civil fingerprints in their state repositories, states will be able to direct the FBI to retain (or not retain) civil fingerprints in the national repository by making such a designation on each submission.

The NGI will consolidate multiple civil records for an individual into a single identity record similar to the criminal file. This initiative will entail migration to an automated identity management structure, which will maintain all information about a person in the system as a single logical record based on a unique identity. Biometric data will be used to positively establish an identity as separate from all other identities, and each identity will be linked to all related criminal and noncriminal justice data in the system by means of a unique identifying number established by the FBI.

In addition, the NGI will provide the capability to fully search the civil fingerprint files for criminal and authorized noncriminal justice purposes, and disseminate this information as authorized. Law enforcement, public safety, national security, and records administration priorities necessitate these technological changes in furtherance of the FBI's authorized missions.

The concept of a "Master Name" will change to that of an encounter name based on the type of submission and search being conducted. For new submissions, the "Master Name" will be established based on the name given during the original record creation event, independent of the type of submission, civil or criminal. The new combined repository will implement logical dissemination rules to protect against the sharing of civil information when the use is not appropriate. Even though the FBI is migrating to an automated identity management structure that will maintain all information about a person in the system as a single record based on a unique identity, the criminal and civil files will remain logically separated. This logical separation, and the clear distinction on the Identity History itself, will ensure that retained civil submissions remain untainted by criminal submissions.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC T

ISO Program Update

PURPOSE

Provide informational update for program activities

POINT OF CONTACT: George A. White, CJIS ISO, (304) 625-5849

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

This topic paper provides an annual update of the CJIS ISO Program.

DISCUSSION AND ANALYSIS

CJIS ISO Team Changes

There have been some notable personnel changes within the ISO program the past year. As you may know, Chris Nethken is no longer with the ISO Program having accepted another position at CJIS. His replacement, and the first to fill the newly created CJIS Assistant ISO role, is Jeff Campbell. Jeff comes to us via a career with the U.S. Air Force and most recently as a contractor with NOAA managing their Cyber Security Operations Center before entering duty with FBI CJIS. Please include him in your questions and correspondence to the ISO program. His email address is jeffrey.b.campbell@leo.gov. His direct phone number is 304.625.4961.

Another addition is Steve Exley. Steve, our CJIS ISO Program Analyst, joined the team in February. He served in the U.S. Army and most recently was a contractor at Ft. Belvoir, VA for the A-GNOSC/ARCYBER Command. Steve is the point person on several efforts including: cloud computing white and topic papers; a

new FAQ web site; the monthly chat training sessions; LEO SIG web site maintenance; use cases for Advanced Authentication and sub-committee topic paper. We welcome them both to the ISO Program.

CJIS Security Policy Publication and Maintenance

2011 was a landmark year with the CJIS Security Policy, Version 5.0, being approved and released. Version 5.0 marks the evolution from an architecture-centric approach to one focused primarily on protection of criminal justice information (CJI). Version 5.0 contains many changes which are captured in the CJIS Security Policy Transition and Requirements Document. The Transition document is a distillation of every "shall" statement requirement from the CJIS Security Policy Version 5.0 with the location in the policy annotated and whether the requirement is new or pre-existing. If pre-existing, the location in Version 4.5 is noted. Our intent is for the transition and requirements document to eventually become a standard requirements document that agencies can provide to vendors as the primary document for development efforts.

APB and Compact Council Support

The ISO program supported all APB and Compact Council meetings this year. Following are topic papers the ISO Program prepared and presented:

- Voice over Internet Protocol (VOIP) (and associated white paper) – Enhanced policy guidance for VoIP technologies in a CJIS environment and VoIP white paper on VoIP best practices incorporated in CSP as an appendix. (Approved)
- Vendor Background Checks – Alleviate requirement for vendor to complete background checks for each new client by allowing original check be used for ensuing customers. (Rejected)
- ISO Latitude for Administrative Changes – Provide CJIS ISO authority for one year to make administrative changes to the CSP with the approval of the SA Subcommittee. (Approved)
- Security Addendum Electronic Certification – Allows use of digital signature in lieu of handwritten signature on the security addendum. (Approved)
- Use and Dissemination of Hot File Info – Proposed modifications to CJIS Security Policy section 4.2 (Access, Use, and Dissemination of Criminal History Record Information (CHRI) and NCIC Hot File Information) to change the name of "hot files" to "non-restricted files" and to distinguish NCIC restricted files from non-restricted files. (Approved)
- Removal of Dissemination Restrictions from CSP – Allow the CJIS Security Policy, only Version 5.0, to be a public document without dissemination restrictions. (Approved)

- Risked-Based Authentication (RBA) Expiration Certification – Re-validate the 2013 expiration date for RBA. (Rejected…No RBA expiration cited in CJIS Security Policy so it is approved indefinitely)
- Encryption Standards Review – Proposed changes to the CJIS Security Policy clarifying when 128-bit encryption is required to be used and making the Advanced Encryption Standard (AES) the encryption requirement. (Rejected)
- Logging Criminal Justice Information – Proposed additional requirement for logging of CJI not already described in the CJIS Security Policy. (Rejected)
- Signatures for Visitors to Physically Secure Locations – Delete CJIS Security Policy verbiage requiring signatures for visitors to physically secure locations. (Approved)
- State of Residency Fingerprint-Based Background Checks (and associated white paper) – Determine the meaning of "state of residency check" verbiage in CJIS Security Policy section 5.12.1.1 and recommend a definition of state of residency and how state of residency checks should be conducted. (Approved)

Training and Outreach

The ISO Program has developed a 2012 training plan emphasizing outreach to the traditional and non-traditional CJIS communities. Following are highlights from the plan:

- Enhance content and add references section to ISO page on Law Enforcement Online (LEO) portal
- Conduct monthly ISO chats on LEO addressing topics of interest to the CJIS ISO community
- Seek opportunities to provide on-site training for agencies and organizations
- Online CJIS Security Policy web site featuring frequently asked questions

Three ISO chats covering CJIS Security Policy topics of authentication, media protection, and physical/personnel security were conducted in 2011 using the LEO chat feature. There were 70+ participants and feedback has been very positive. The slides and transcripts from each session are stored on the ISO LEO home page for easy reference. Also, take a look at the ISO page and let us know what you think about the updated content and the new references section. The ISO LEO SIG page has been updated to include personnel changes and contact information for the ISO Program staff. Outdated and irrelevant information was removed. New sections for the ISO Chat and ISO References were added.

The ISO program presented at, or supported, functions resulting in training for over 650 people. Following is a sample of the organizations and agencies trained in 2011:

- New Hampshire ISO team
- STARS Conference
- CPI User's Conference
- Motorola User's Conference
- North Carolina CJIN Board
- Florida Department of Law Enforcement (FDLE) CJIS Conference
- New Mexico ISO team
- South Carolina Law Enforcement Division

Law Enforcement Information Exchange (LInX)

The ISO worked extensively with the CJIS N-DEx and NCIS LInX Program Offices to integrate data from the LInX regions into the N-DEx systems. Differences between the CJIS Security Policy and LInX NW Security Policies were mitigated and ISO representatives joined a CJIS/LInX meeting in Portland, OR. Following the successful experience with LInX NW, the ISO team has continued to support efforts to bring additional LInX regions on-board.

Outlook for 2012

2012 is shaping up to be another productive year for the CJIS ISO Program. We've committed to provide briefings/training to the following organizations:

- SEARCH Committee
- CJIS Group
- Idaho ILETS User's Conference
- Idaho ISO Orientation
- Morphotrak AFIS User's Conference
- FDLE CJIS Conference
- IJIS Board
- Guam ISO Team
- Motorola User's Conference

The monthly ISO LEO Chats will continue with January's topic covering Information Exchange Agreements. Remember to check the ISO page on LEO for the chat slide presentation and transcript if you miss a session.

The CJIS ISO Symposium has been suspended for 2012. While we deeply regret this decision, we are evaluating other ways to provide the information and training you have come to expect at this event. We welcome any ideas you might have.

Please convey them to the ISO team via the iso@leo.gov email address or the Questions and Feedback page on the LEO ISO SIG site.

From a CJIS Security Policy perspective, we anticipate addressing cloud computing, virtualization, and the definition of CJI, amongst other topics. The CJIS Security Policy and Transition Document are going to be updated in March with APB approved changes from 2011. Those changes will include:

- Voice over Internet Protocol (VoIP)
- Security Addendum Electronic Certification
- Use and Dissemination of Hot File Info
- Signatures for Visitors to Physically Secure Locations
- State of Residency Fingerprint-Based Background Checks

The ISO Program is developing a web site to provide public access to the CJIS Security Policy. One of the additional features will be answers to frequently asked questions (FAQs) about the CJIS Security Policy. The CJIS community as a whole will benefit from the answers to each other's questions and users will be able to submit questions to the ISO staff via the web site. The site is scheduled to be premiered this July.

RECOMMENDATION

Informational paper only

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC U

Next Generation Identification (NGI) Program Implementation and Transition Update

PURPOSE

To provide a high-level overview of the NGI Program status and transition efforts

POINT OF CONTACT

Brian Edgell, Implementation and Transition Unit Chief, (304) 625-3551

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

Driven by advances in technology, customer requirements, and growing demand for Integrated Automated Fingerprint Identification System (IAFIS) services, the FBI has initiated the NGI program. This program will further advance the FBI's biometric identification services, providing an incremental replacement of current IAFIS technical capabilities, while introducing new functionality. NGI improvements and new capabilities will be introduced across a multi-year time frame within a phased approach. The NGI system will offer state-of-the-art biometric identification services and provide a flexible framework of core capabilities that will serve as a platform for multi modal functionality.

Increment 1 – Advanced Fingerprint Identification Technology (AFIT) – Complete – Increment 1, which replaced the Automated Fingerprint Identification System (AFIS), began transition February 25, 2011. This transition started with a five-day operational validation of all tenprint submissions processed through the AFIT, in parallel with the AFIS, as a secondary operational system. The implementation of AFIT required no technical or programming changes by system users; however, AFIT performance had an immediate impact on all customers. AFIT accuracy has been demonstrated at over 99%.

Also, this increase in automated accuracy has allowed operations to reduce the dependency on a supplemental name check, resulting in a 90% (weekly) decrease in the number of manual fingerprint reviews required by CJIS Division service providers. Leading up to this deployment, 1.274 Billion images have been re-characterized for use within AFIT, in eight weeks time. This task took the previous system well over one year to complete.

Increment 2 – Nationwide deployment of the Repository for Individuals of Special Concern (RISC) and Initial NGI Infrastructure – Complete – Increment 2 was deployed August 25, 2011, and included the deployment of the nationwide RISC Rapid Search in both Simple Mail Transport Protocol or Extensible Markup Language web service format. This comprised the initial deployment of the NGI Web Services interface.

Since the Increment 2 deployment, all previous RISC Pilot agencies (MD, TX, OH, MN, GA, FL) have transitioned to the new national service, as well as the addition of the California Department of Justice. Average daily search volumes have doubled since the deployment of the national service and new users continue to be added.

NGI RISC Totals 10/01/11 to 01/02/2012	
Total RISC Transactions thru 01/02/2012	37,548
Average Response Time for December 2011	6.59 seconds
Average Daily Submissions for December 2011	498
Response	**Percentage**
Green	92%
Yellow	.5%
Red	6.5%
Wants	74%
SOR	26%

The NGI Program Office (NGIPO) continues to work with interested states to identify the appropriate steps required to implement this new RISC service. Based on the feedback from contributors through extensive outreach activities, the NGIPO will publish a RISC

user guide in the summer of 2012 to help educate potential users of the nuances specific to the RISC service and the steps they can take to address these requirements early in their implementation planning. The deployment of the national service, also results in the retirement of the CJIS RISC Pilot Technical Specification document. The Electronic Biometric Transmission Specification (EBTS) version 9.3 should be used to guide new RISC participation. As always, agencies interested in participating, or just seeking additional information, are asked to contact the NGIPO at (304) 625-3437.

As recommended by the Advisory Policy Board, the addition of the National Crime Information Center Immigration Violator File (IVF) to the RISC data sets is currently scheduled for April 2012. This will give law enforcement utilizing the RISC service access to an additional 300,000 actionable records of convicted criminal aliens who have been deported for drug trafficking, firearms trafficking, or serious crimes and foreign born individuals who have violated some section of the Immigration and Nationality Act. Additional RISC enhancements cascading against the Unsolved Latent File (ULF) will begin with the deployment of Increment 3 in 2013, and with the deployment of Increment 4, photos, if available, can be retrieved as part of the requested RISC response.

DISCUSSION AND ANALYSIS

Increment 3 – Palms and Latents – In Progress – Increment 3 establishes the National Palm Print System (NPPS) and transitions IAFIS latent functionality to the new NGI infrastructure. Increment 3 will provide all latent capabilities currently supported by IAFIS and deploy NGI enhanced latent capabilities for searching palm prints and supplemental fingerprints and palm prints. The following briefly summarizes the contributor benefits from latent capabilities in Increment 3:

- Perform latent searches of all fingerprint, palm print, and supplemental print event records
- Cascade incoming tenprint, palm print, and supplemental fingerprint and palm print records against the ULF
- Retrieve images, and associated information for fingerprint, palm print, and supplemental print events
- Retrieve audit trails for palm prints and supplementals
- Retrieve images, audit trails, and associated information for ULF records
- Receive Unsolved Biometric Match notifications for hits against ULF records
- Support biometric decisions by allowing contributors to provide feedback on candidates provided from search results

- Enhanced ability for contributor maintenance of their ULF records
- Allow direct enrollment and deletion of palm print and supplemental biometrics

The EBTS Working Group has published the CJIS EBTS version 9.3. This version contains the specifications required to take advantage of the new and enhanced capabilities being delivered with Increment 3. The NGIPO has created a supplementary NGI Increment 3 EBTS Changes document to highlight changes specific to Increment 3 new functionality and enhancements. In addition to many changes for existing Type of Transaction (TOT)s, six new TOTs have been added:

- Biometric Audit Trail Retrieval Request (BATQ): Request to retrieve a dissemination audit trail for biometric imagery owned by requestor for a given Universal Control Number. Request can be further refined to a biometric set or image types
- Biometric Audit Trail Retrieval Response (BATR): Audit Trail response containing information of when images have been disseminated from NGI. Contains repeating set of new Audit Trail Record field containing the ORI that received the images, the date of dissemination, the TOT used and biometric image details
- Biometric Delete Request (BDEL): For Increment 3 this supports Fingerprint deletions from Special Population Cognizant and Latents from the ULF, Palmprint deletions, and Supplement Fingerprint and Palmprint deletions
- Biometric Delete Response (BDELR): Successful response to a BDEL request
- Biometric Decision Request (BDEC): Submission of an adjudication decision as a result of a Latent Investigative Search or an Unsolved Latent Match notification. Supports Latent decisions for Increment 3 and will support other biometric types of decisions in the future
- Biometric Decision Response (BDECR): Successful response to a BDEC request

Both documents are available at *http://www.fbibiospecs.org.*

Universal Latent Workstation (ULW) software users can anticipate a late summer 2012 delivery of ULW 2012. This version will support the new latent functionality being delivered in Increment 3 and is available at no cost from the CJIS Division. Failure to upgrade will result in users not being able to take advantage of the new functionality.

On October 14, 2011, the IAFIS ULF reached capacity and records from the Other Federal Organizations subdivision began to be deleted, starting with the oldest deposits.

Likewise, the Local and State subdivision will reach capacity in the near future. If the record owner wishes to keep the unsolved latent images in the ULF, a new search of IAFIS is required. Users of the ULW software will be required to obtain ULW Software, Version 6.0.9, to receive and manage the Unsolicited Unsolved Latent Delete notifications, as previous versions of the software are not compatible. Failure to obtain the software will preclude notification of deleted records. The Latent Investigative Services Program Office (LISPO) is drafting a letter to notify contributors of these important changes. Additional work is also underway in support of an Identification Services Subcommittee action item, to develop a best practices/policy document to define the ULF operations and maintenance requirements moving forward, slowing the growth of the ULF and ensuring the most relevant data is maintained within the repository.

The NGIPO continues to be very active and extremely successful establishing contact with contributing agencies, to develop an understanding of their unique requirements and readiness regarding their participation in new and enhanced palm print and latent capabilities. In anticipation of the upcoming NPPS search capability, the NGIPO continues its Biometric Acquisition (BA) project in an effort to have a well-populated gallery once the functionality is available. This project has supported the collection of more than 3.3 million palm prints to date, and will continue to grow as Increment 3 deployment draws near. This project supports users with day-forward palm print submissions as well as bulk submissions of legacy images. A Memorandum of Understanding (MOU) has been developed to support the collection of bulk submissions and is currently in the final legal review. Several states are awaiting its completion. Agencies interested in participating, or seeking additional information, are asked to contact the NGIPO at (304) 625-3437. The NGIPO will work with agencies and their corresponding CJIS Systems Officer (CSO) to evaluate their current system state and develop strategies for going forward with participation in these new and updated services.

Increment 4 – Rap Back, Facial, Photo/Scars, Marks, and Tattoo (SMT) Search Capabilities – In Progress. Design work continues as the increment progresses toward the Critical Design Review. The following briefly summarizes the contributor benefits from capabilities in Increment 4:

- National Rap Back Service will provide notification of criminal activity on previously cleared individuals
- Enhanced IAFIS Repository (EIR) provides access to subject information spanning multiple repositories
- Access to a national repository for Facial and SMT searches for investigative purposes
- Fingerprint verification services using 10 or fewer fingerprints
- More complete and accurate history records

The NGIPO moved forward with the NGI Facial Recognition Pilot (FRP) project in December 2011. The CJIS Division has executed an MOU with Michigan, Hawaii, and Maryland to participate in the pilot. This will be a collaborative effort between the FBI and piloting agencies to identify user needs and develop useful investigative tools for the law enforcement community. The FRP will provide searches of a repository consisting of subsets from the Interstate Identification Index (III) mug shots. The repository will be updated periodically receiving III photo pulls on a daily/weekly basis. It is anticipated that the repository will contain 12 million searchable frontal photos at deployment. The facial recognition search requests will be processed automatically (lights out), and results will be returned in a ranked candidate list. Initial piloting agencies will be limited to states with an existing Face/Photo searching capability. Pending the deployment of the Universal Face Workstation (UFW) software, participants without current Face/Photo search capabilities will be solicited to participate in the Facial Recognition Pilot as UFW users. Agencies interested in participating, or just seeking additional information, are asked to contact the NGIPO at (304) 625-3437.

The performance of facial matching systems is highly dependent upon the quality of images enrolled in the system. Therefore, it is important that agencies submit images that meet, at minimum, specific image quality metrics and recommendations so system users may realize the maximum potential benefit. The NGIPO continues to work with contributors and industry to enhance the image quality of the repository. The Facial Identification Scientific Working Group (FISWG) and the National Institute of Standards and Technology (NIST) have produced best practices documents for image capture and equipment. Additionally the NGIPO has moved forward with the generation of its first Face Report Card for the state of Oregon . The purpose of the Face Report Card is to provide feedback to individual agencies regarding the quality of images submitted. This feedback includes suggestions which, if followed, will improve the quality of future image submissions. As the quality of images submitted to the Federal Bureau of Investigation (FBI) improves, it is expected that agencies participating in the FBI's face matching systems will benefit from this improved gallery.

The NGIPO continues to work with the Rap Back Focus Group, a follow-up effort to the Rap Back Task Force, on operational impacts related to federal Rap Back implementation. The group met at the CJIS Division on November 8th and 9th to discuss privacy mitigation strategies and outstanding policy and technical issues. Although no formal recommendations were approved, the group's feedback resulted in the identification of several areas requiring further research:

- Parameters surrounding the sharing of notification data for both criminal justice and non-criminal justice purposes

- Definition of event notification triggers for both criminal justice and non-criminal justice purposes
- Clarification of data elements returned in notification transactions to ensure linkage can be established at the state between the Rap Back subscriber and the affected agency
- Further refinement of validation and pre-notification requirements

The focus group is also providing guidance on the development of a Rap Back Business Concept of Operations document (CONOPS). The CONOPS offers information to system implementers on the core, maintenance, privacy, and conceptual services available for the NGI Rap Back capability. The first draft version of the document was released at the beginning of 2012.

As announced at the December 2011 Advisory Policy Board and Compact Council meetings, the NGIPO is developing a pilot program to assess various Rap Back operational concepts. The initial participants under consideration include the Office of Personnel Management, the United States Citizenship and Immigration Services, the Transportation Security Administration, and the Customs and Border Protection. Authority to retain the civil fingerprints submitted by these federal entities is currently granted under the Fingerprint Identification Records System (FIRS) System of Records Notice (SORN). Possible state participation during the pilot is contingent upon appropriate legal authority and privacy documentation, and CJIS resource availability.

The Rap Back Pilot, which will involve limited populations of designated enrollees, will provide arrest-only, manual notifications to participants; the form of notification (e.g., email, telephone) will be predicated upon the capabilities of the receiving agency. Participation in the pilot will be fee-based, though the exact costs are being analyzed by

CJIS and will be determined at a later date. The NGIPO is anticipating the operational components of the Rap Back Pilot to be in place by late Spring 2012.

Agencies interested in participating, or just seeking additional information regarding any of these new services are asked to contact the NGIPO at (304) 625-3437. The NGIPO will work with agencies and their corresponding CSO to evaluate their current system state and develop strategies for going forward with participation in these new and updated services.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC V

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

PURPOSE

The FBI Criminal Justice Information Services (CJIS) Division's National Instant Criminal Background Check System (NICS) Section is sharing 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.

AUTHOR

Diana Jo Linn-Cook

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

The Brady Handgun Violence Prevention Act of 1993 (Brady Act) required the U.S. Attorney General to establish the NICS for Federal Firearms Licensees (FFL) to contact for information to be supplied immediately on whether the transfer of a firearm is in violation of state or federal law. When an FFL initiates a NICS background check, a prospective firearm transferee's name and descriptive information is searched against the name and descriptive information of the records maintained in the following national databases: (1) the Interstate Identification Index (III); (2) the National Crime Information Center (NCIC); and (3) the NICS Index. In addition, an immigration alien query is submitted to the Department of Homeland Security's U.S. Immigration and Customs Enforcement on all persons who claim non-U.S. citizenship when completing the required Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Form 4473.

The NICS Index collects and maintains information contributed by local, state, tribal, and federal agencies. Historically, this information was specific to persons predetermined to be *federally* prohibited from receiving firearms. The availability of federally prohibiting information, validated by the contributor prior to submission into the NICS Index, allows for greater effectiveness and efficiency in background check processing for both the

NICS Section and their state partners. Additionally, the availability of federally prohibiting information during a background check via the NICS Index supports the NICS Section's mission to provide accurate and timely determinations to FFLs and their customers. This is accomplished when a valid match in the NICS Index renders an immediate denial determination. As the NICS Section and its state partners enjoyed the benefits of the NICS Index to identify federally prohibited individuals, they recognized the need for a corresponding mechanism to be established to capture and maintain record information specific to persons prohibited based on state law. In April 2012, the NICS Section and the CJIS Division's Information Technology Management Section will expand the functionality of the NICS Index to include state-prohibiting records to provide the NICS Section and state users with the ability to effectively and efficiently retain state-prohibiting information at a national level.

CONTRIBUTING STATE-PROHIBITING INFORMATION TO THE NICS INDEX

The rules that apply to the electronic submission and maintenance of state-prohibiting information in the NICS Index are the same as when submitting/maintaining federally prohibiting information to the NICS Index. Authorized agencies voluntarily submit and perform maintenance on the information the agency has submitted to the NICS Index by sending add, cancel, modify, supplement, and display messages to the NICS through the NCIC Front End via message keys (MKE). An MKE is used by the NICS to identify the action required to process the information. Only the record-entering agency can perform maintenance on records it has entered. The record-entering agency is responsible for the accuracy, completeness, and validity of the information it has placed in the NICS Index. The record-entering agency is also subject to the existing CJIS Division audit standards pertaining to all information maintained in the NICS Index.

When electronically submitting state-prohibiting information to the NICS Index, a contributor must use the newly established prohibiting category (PCA) code of "J." The NICS' recognition of the "J" PCA code will label the information as state prohibiting and require the contributor to enter the applicable corresponding State PCA (SPC). An SPC, comprising of six alphanumeric characters, has been assigned to each of the existing state firearm-prohibiting laws (including those applicable to state firearm permits) identified and charted by the NICS Section. For example, Alaska State statute 11.61.200 would be identified as AK0001, and Alaska's permit statute 18.65.705(4) would be identified as AKP001. Each SPC directly corresponds with information identifying:

- The state firearm-prohibiting (or the state firearm permit-prohibiting) law upon which the record's disqualifying status is based.
- The state(s) of prohibition (the state[s] which is/are subject to the law prompting the disqualification).
- The scope of the prohibition (handgun, long gun, permit, all firearms, or other).
- If an expiration date must be provided by the contributor.[1]

[1] Certain state prohibitions are automatically nullified after a specified period of time has elapsed.

The agencies which are authorized to submit federally prohibiting information to the NICS Index will have the capability to voluntarily submit state-prohibiting information to the NICS Index; however, the agency must implement system programming changes in order to do so. When implemented, the required system changes will provide the agency the ability to utilize the PCA code of "J" and will provide the agency with the capability to enter the required SPC in a new field established for this purpose. When submitting state-prohibiting information to the NICS Index, a contributor will be encouraged to provide specific information explaining the underlying record in the Miscellaneous Field (MIS) of the NICS Index (e.g., a specific date of arrest). Providing this information for the NICS users may allow the user to process the state-prohibiting information without the need to contact the record's owner for additional information when processing an appeal.

The NICS Interface Control Document (ICD) provides technical guidance pertaining to system programming needs required with the electronic submission and maintenance of information in the NICS Index including the above-described added functionality. The NICS ICD is available to NICS users through the Law Enforcement Online (LEO). Each known state firearm prohibition and state firearm permit prohibition, plus the corresponding SPC and applicable state statute description, has been detailed in a spreadsheet. This spreadsheet is available on LEO under the NICS State Support Team Special Interest Group and has been shared with all State Points of Contact (POC) and CJIS Systems Officers (CSO). In addition, on an ongoing basis, the NICS Section will monitor all state-prohibiting laws to ensure applicability. State partners are also encouraged to notify the NICS Section of changes to their state-prohibiting laws. This information will be shared periodically with the NICS users and will be kept up-to-date on LEO.

NICS RESPONSE DATA

When a NICS background check is conducted, all matches to information maintained in any of the databases searched are returned to the user in the NICS-combined response. If any matches are generated by the NICS to information maintained in the NICS Index, the information is made available to the user in the NICS Response Data. State-prohibiting information maintained in the NICS Index and matched by the NICS to the prospective firearm transferee is returned to the user in the NICS Response Data in the same format as federally prohibiting information is returned. State-prohibiting NICS Index responses will contain a specific state statute (SST) and SST description upon which the underlying record's state-prohibiting status was predicated. The SST and SST description is queued from the SPC provided by the record-entering agency. This information will be displayed in the MIS of the NICS Index response; therefore, no system change is needed for an agency to receive a state-prohibiting NICS Index response.

The PCA code displayed with each NICS Index hit tells the user if the information is state prohibiting (PCA code of "J") or federally prohibiting (all other available PCA codes). For federally disqualifying NICS Index records, the NICS will respond when the record is matched with the transferee’s name and descriptive information, based on algorithm. With the uniqueness of state prohibitions, the NICS will take multiple factors into consideration before a state-prohibiting NICS Index record is returned to the user. The criteria required for a state-prohibiting NICS Index response is as follows:

- A valid name and descriptive match based on algorithm.

- The state of residence (SOR) or the state of purchase (SOP) of the subject of a NICS check 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).

- The transaction's Purpose Identification Code (such as handgun, long gun, permit) corresponds to the SPC (e.g., the transaction is specific to a handgun purchase and the SPC corresponds to a state law that prohibits the transfer of a handgun).

BENEFITS OF ADDING THE STATE PROHIBITED PERSONS FILE TO THE NICS INDEX

The valid match of a state-prohibiting record maintained in the NICS Index to the name and descriptive information of a prospective firearm transferee will provide the user with:

- A prompt indicator of subject 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; and

- Reduced need for a user to replicate previously conducted research and outreach when processing subsequent background checks for the same individual.

Other benefits and efficiencies anticipated with including state-prohibiting records in the NICS Index are:

- 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 (under certain circumstances[2]) during the background check process;

[2] The NICS will only respond with a NICS Index match if the SOR or the SOP of the subject of a NICS check 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).

- 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;

- The ability to maintain information subject to some expungements[3];

- Reduced potential to misinterpret or misapply another state's laws, which helps to reduce inaccurate transaction decisions; and

- Reduced potential that a firearm will transfer in default to a prohibited person because of an "open" status, which could also reduce the number of firearm retrieval scenarios referred to the ATF.

Since the implementation of the NICS in November 1998, the NICS Section has witnessed the value of providing predetermined federal firearms-prohibiting records at a national level through the NICS Index. The NICS Section has enhanced this process by expanding the NICS Index to also collect and maintain firearm-prohibiting records derived from state law. Because of the potential challenges faced by state agencies such as funding, personnel limitations, technological and/or operational inadequacies, the NICS Section will provide guidance and training to state agencies through available means. The NICS Section is working to educate and share information pertaining to the value of making state-prohibiting information available at a national level to all NICS users as it does with federally prohibiting information in the NICS Index. The NICS Section has:

- Incorporated information pertaining to the NICS Index expansion into existing training modules and implemented training with state agencies pertaining to submitting state-prohibiting information to the NICS Index;

- Disseminated e-mails to state POCs and CSOs regarding the April 2012 expansion of the NICS Index;

- Shared information with NICS users regarding the expansion of the NICS Index and the value of providing state-prohibiting information available on a national level in teleconferences, the annual NICS User Conference, and ongoing training sessions with state agencies; and

- Provided training materials pertaining to the submission and maintenance of state-prohibiting information in the NICS Index to the states via LEO.

The value and benefits of expanding the NICS Index to include state-prohibiting information should quickly become evident to all NICS users. The NICS Section's partnership with its state and federal counterparts is paramount to the success of the NICS

[3] Some state laws allow expunged information to be used to determine firearms eligibility (and other law enforcement purposes). The NICS Index provides a place to store the otherwise unavailable (expunged) data.

and, thus, the NICS Index. It is with this spirit of cooperation the NICS Section offers guidance in assisting state users to expand in the utility of the NICS Index and enhance public safety.

For further information regarding submitting state-prohibiting information to the NICS Index, you may contact Diana Jo Linn-Cook, NICS Liaison Specialist, by telephone at (304) 625-7451 or by e-mail via <diana.linn-cook@ic.fbi.gov>.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC W

National Instant Criminal Background Check System (NICS) Update

PURPOSE

The information outlined in this paper provides a current update of the NICS.

AUTHOR

Margaret Kisner

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

The Brady Handgun Violence Prevention Act of 1993 (Brady Act) required the U.S. Attorney General to establish the NICS for Federal Firearms Licensees (FFL) to contact for information to be supplied immediately on whether the transfer of a firearm would violate state or federal law. Through a cooperative effort with the Department of Justice (DOJ); the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and state and local law enforcement agencies, the FBI developed the NICS, which was implemented on November 30, 1998.

NICS TRANSACTIONS

The following program-to-date (PTD) data outlines the NICS background check transactions processed by the FBI CJIS Division's NICS Section, in addition to data specific to the background checks processed through the NICS by the Point-of-Contact (POC) states.[1]

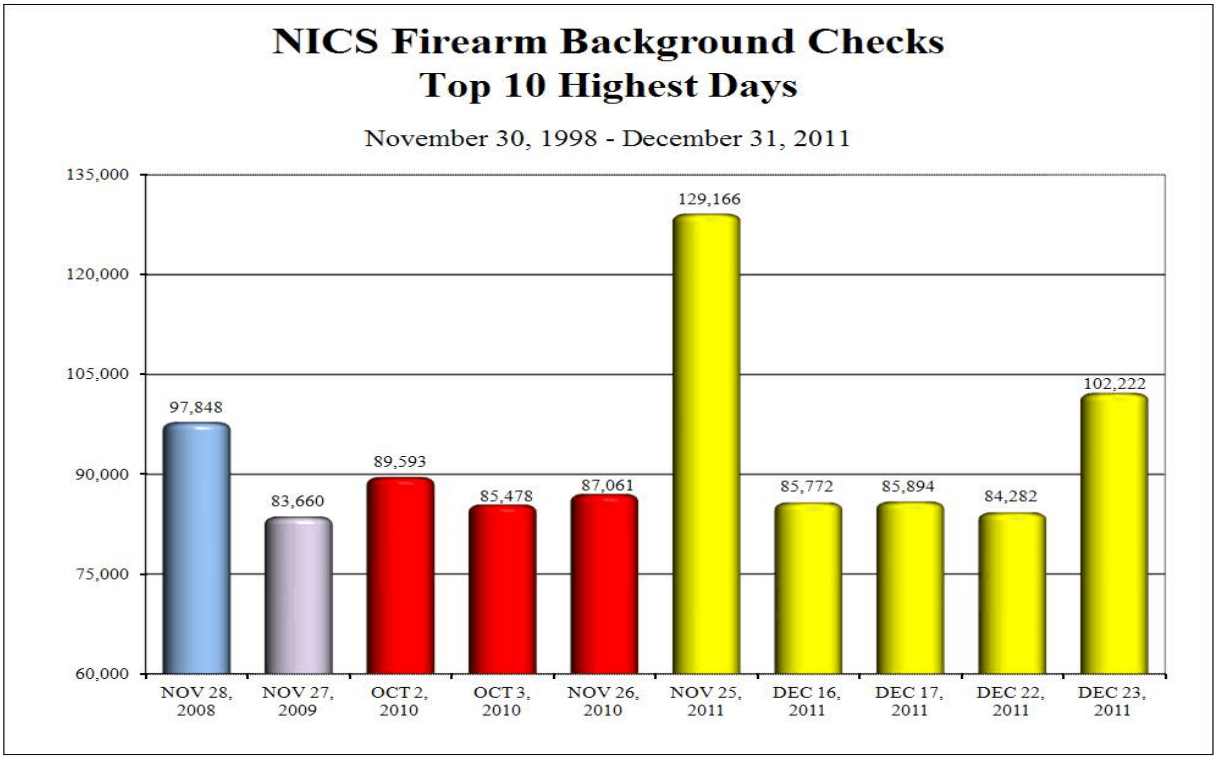
[1] The states that have designated a specific agency within the state to process NICS background checks for the states' FFLs (reference State Participation information on page 6).

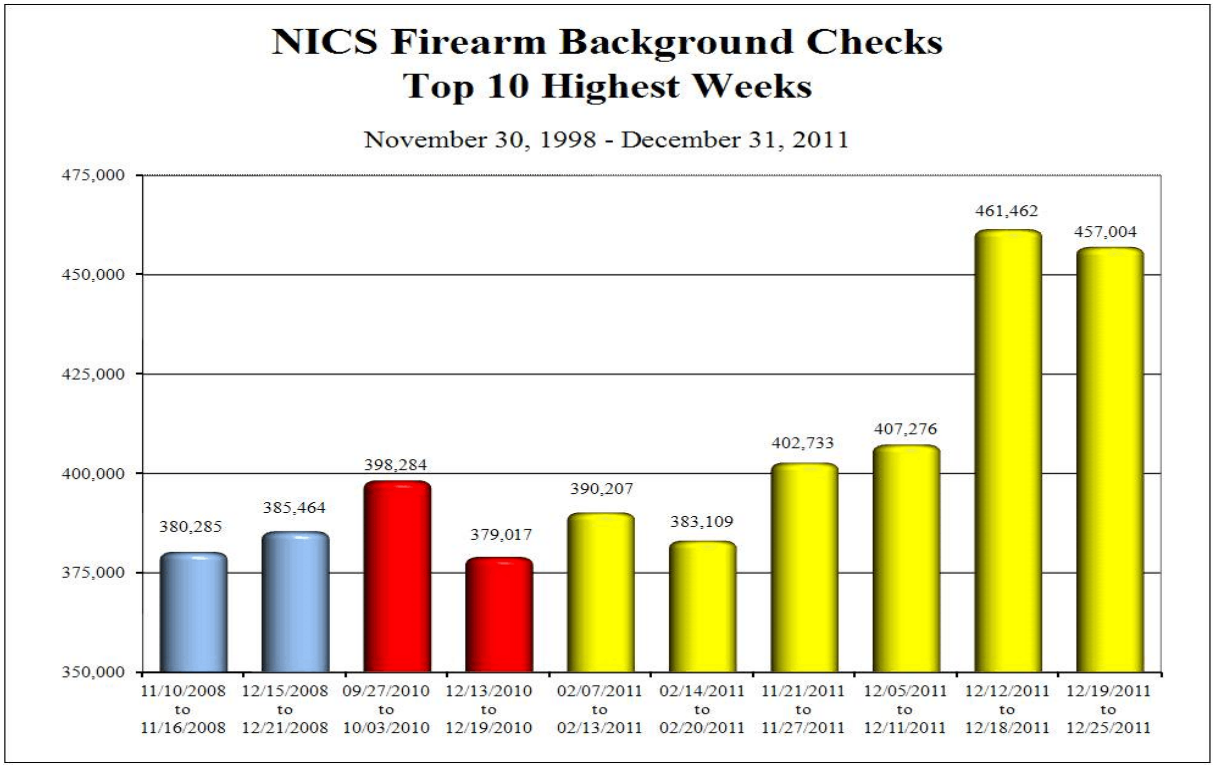
	2010*	2011*	PTD[2]
State Background Checks	8,372,222	9,579,326	73,726,947
Contracted Call Centers	5,530,099	5,872,456	62,938,227
NICS Section	36,839	42,376	1,571,425
NICS E-Check	470,456	960,793	2,645,800
Total Federal Background Checks	6,037,394	6,875,625	67,155,452
Total NICS Background Checks	14,409,616	16,454,951	140,882,399
Federal Immediate Proceeds	5,448,435	6,210,169	57,728,674
Federal Denials	72,659	78,211	899,099
Explosives Background Checks	74,464	110,938	590,917

* January 1 through December 31

As referenced in the following charts, the NICS experienced five of its ten highest transaction volume days and four of its ten highest transaction volume weeks in the first quarter of Fiscal Year (FY) 2012.

[2] Program inception through December 31, 2011.


NICS Firearm Background Checks
Top 10 Highest Days
November 30, 1998 - December 31, 2011
135,000
120,000
105,000
90,000
75,000
60,000
97,848
83,660
89,593
85,478
87,061
129,166
85,772
85,894
84,282
102,222
NOV 28, 2008
NOV 27, 2009
OCT 2, 2010
OCT 3, 2010
NOV 26, 2010
NOV 25, 2011
DEC 16, 2011
DEC 17, 2011
DEC 22, 2011
DEC 23, 2011


NICS Firearm Background Checks
Top 10 Highest Weeks
November 30, 1998 - December 31, 2011
475,000
450,000
425,000
400,000
375,000
350,000
380,285
385,464
398,284
379,017
390,207
383,109
402,733
407,276
461,462
457,004
11/10/2008 to 11/16/2008
12/15/2008 to 12/21/2008
09/27/2010 to 10/03/2010
12/13/2010 to 12/19/2010
02/07/2011 to 02/13/2011
02/14/2011 to 02/20/2011
11/21/2011 to 11/27/2011
12/05/2011 to 12/11/2011
12/12/2011 to 12/18/2011
12/19/2011 to 12/25/2011

NICS PROCESSING RECORDS

To help manage the heightened level of transaction volume that typically occurs with the onset of state hunting seasons and year-end holidays, the normal operating hours for the NICS are temporarily expanded. Accordingly, the hours of NICS availability were expanded for the period of November 1, 2011, through January 20, 2012. During this time, on November 25, 2011 (the day after the Thanksgiving holiday), the following records were achieved by the NICS:

- A combined total of 16,454,951 background checks were processed by the states and the FBI in Calendar Year 2011, making it the highest year ever for background check submissions to the NICS.

- A combined total of 129,166 NICS background checks were processed by the states and the FBI. This is a 32.01 percent increase over the number reported for the same day in 2010. To date, this is the highest day ever for total (state and federal) firearm background check submissions to the NICS.

- A total of 81,609 NICS background checks were processed by the FBI. This is a 26.69 percent increase over the number reported for the same day in 2010. To date, this is the highest day ever for background check submissions to the NICS for processing by the FBI.

- A total of 11,953 NICS E-Check transactions were processed by the FBI. To date, this is the highest day ever for background check submissions to the NICS E-Check; a 119.76 percent increase over the number reported for the previous highest volume day on February 11, 2011.

- A total of 47,557 NICS background checks were processed by the states. To date, this is the fourth highest day ever for background check submissions to the NICS for processing by the states. Excluding a batchload of firearm permit rechecks processed by one of the states in October 2011, this would have been the highest day ever for background check submissions to the NICS for processing by the states.

NICS INDEX

The NICS Index, originally created for the sole use of the NICS, collects and maintains information pertaining to persons who are federally prohibited from receiving or possessing firearms pursuant to the Brady Act. The records maintained in the NICS Index are contributed by local, state, tribal, and federal agencies. Each contributing

agency is responsible for the maintenance of their NICS Index submissions. Accordingly, all contributors of NICS Index information are required to modify, supplement, or delete their NICS Index entries in order to keep the information valid, accurate, and complete.

The information maintained in the NICS Index, as of December 31, 2011, by prohibiting category (PCA) follows:

PCA Description	Number of Records
Convicted in any court of a crime punishable by imprisonment for a term exceeding one year or any state offense classified by the state as a misdemeanor and punishable by a term of imprisonment of more than two years, whether or not imposed	612,936
Under Indictment/Information	721
Fugitive from Justice	368,567
Controlled Substance Abuse	14,930
Mental Health Information	1,364,613
Illegal/Unlawful Aliens	4,802,154
Dishonorable Discharge	10,010
Renounced U.S. Citizenship	16,004
Protection/Restraining Order	2,267
Misdemeanor Crime of Domestic Violence	83,340
Denied Person File[3] (DPF)	35,096
Total NICS Index Entries	7,310,638

STATE PARTICIPATION

As of December 31, 2011, the NICS Section processed background checks on all firearm transactions for FFLs in 29 states, 5 territories, and the District of Columbia. For 8 states, the NICS Section performs the background checks solely for long gun transactions, while

[3] On May 19, 2008, the NICS Index PCAs were realigned to more closely adhere to the specific federal prohibitor upon which the disqualifying status of the information is based. The information currently remaining in the DPF is information submitted prior to this change which has not been or can not be relocated to a more appropriate PCA by the contributor.

the state conducts its own background checks on handguns and/or handgun permits. A total of 13 states participate with the NICS in a full-POC capacity by performing all background checks for the FFLs in those states. In addition, a total of 21 states have ATF-approved alternate permits. The NICS participation map is located at <http://www.fbi.gov/hq/cjisd/nics.htm>.

VOLUNTARY APPEAL FILE (VAF)

Persons who have experienced an extended delay or, in certain instances, have been denied a firearm transfer, may request the NICS Section to maintain specific information about them for use in subsequent background checks to help determine their eligibility (at the time of the check) to receive firearms. Successful applicants whose documentation is validated and have no prohibiting records will be provided a Unique Personal Identification Number (UPIN) to provide during future NICS firearm background checks. The VAF was developed and implemented on July 20, 2004, to house the supplemental clarifying information voluntarily provided for use during the background check process.

The VAF information is maintained in an electronic file checked by the NICS during the background check process when a UPIN is supplied by the customer to the FFL. The statistics for the VAF follow:

VAF	July 20, 2004–December 31, 2011
Successfully Entered	19,783
Active UPINs	19,932
Applications in Progress	1,574
Transactions Processed with a UPIN	39,461

NUCLEAR REGULATORY COMMISSION (NRC) BACKGROUND CHECKS

The Guidelines on the Use of Firearms by Security Personnel Protecting U.S. NRC-Regulated Facilities, Radioactive Material, and Other Property and the *NRC Notice of Proposed Rulemaking (NPRM)* were published in the Federal Register on February 3, 2011. A six-month public comment period was provided. The NICS

Section submitted comments pertaining to the NRC NPRM in August 2011 and is awaiting the finalization and eventual approval of the NRC Regulations.

Representatives from the NICS Section, the FBI's Office of the General Counsel, and the CJIS Division's Biometric Services Section attended an NRC public meeting in Rockville, Maryland, on June 1, 2011. The NICS Section shared information pertaining to the processing of NRC background checks (including NRC appeal requests) anticipated to begin in Spring 2012.

DISPOSITION OF FIREARMS INITIATIVE

In December 2005, the CJIS APB approved a motion to request the DOJ to amend the current federal regulation to allow access to the NICS by law enforcement and criminal justice agencies (CJA) for the purpose of conducting NICS background checks when disposing of firearms in the possession of law enforcement. A regulation change to amend Title 28, Code of Federal Regulations, Section 25.6 (j) to allow such access has been requested and has been approved by the Office of the Deputy Attorney General for release to the Office of Management and Budget.

ACCESS TO THE DISPOSITION DOCUMENT FILE (DDF)

In an effort to promote consistency in the processing of NICS background checks, in Spring 2007, the APB approved a motion to provide the POC states and the partial-POC states with access to the DDF for purposes specific to processing NICS background checks. On January 11, 2010, this access was made available via the National Crime Information Center (NCIC). The information maintained in the DDF can be accessed by conducting a "Query NICS Record" via the NCIC. To participate, a POC or partial-POC state must modify their Graphic User Interface to allow the DDF to return information matched by name or FBI number.

During the Spring 2007 APB meetings, the NICS Section was asked to explore the feasibility of providing access to the DDF for other law enforcement purposes. The NICS Section conducted research and presented its findings to the 2009 Fall APB. The NICS Section asked the APB to allow access to the DDF by authorized local, state, tribal, and federal agencies via existing CJIS systems for other law enforcement purposes beyond processing NICS background checks (e.g., investigations, prosecutions). The motion passed the APB in December 2009 and was approved by the FBI Director in

Spring 2010. The approval also included a request to permit access to the DDF by agencies conducting civil applicant background checks (e.g., the Office of Personnel Management [OPM]). This topic was presented to the Compact Council Standards Committee and the Compact Council Policy and Planning Committee in March 2010.

The Compact Council Standards Committee recommended the APB allow access to the DDF for concealed weapons purposes and for purposes specific to the OPM. The Compact Council Policy and Planning Committee moved to endorse the plan to make the DDF available via an existing CJIS system to authorized local, state, tribal, and federal CJAs for law enforcement purposes, firearms licensing and purchase purposes, and to federal non-CJAs for Security Clearance Information Act (SCIA) purposes. These recommendations were presented to the Full Compact Council on May 13, 2010, by the NICS Section. The Full Compact Council endorsed the option for FBI to make the DDF available on an existing CJIS system to authorized local, state, tribal, and federal CJAs and to provide such agencies with the capability to search, view, add, modify, supplement, and delete information in real time for law enforcement purposes only.

The NICS Section and the CJIS Division's Information Technology Management Section (ITMS) are deciding how to implement this functionality. Because of NCIC limitations and the 2012 baseline freeze of the NICS, the project cannot move forward at the current time. The NICS Section and the ITMS will continue to work toward the appropriate placement of the DDF for the accessibility described above and a potential time frame for its deployment.

STATE INFORMATION-SHARING INITIATIVE (SISI)

The SISI provides the POC states with access to the VAF, the ATF Relief from Disabilities Documents (ATFRDD) database, and the DDF when requesting a record as part of a NICS background check. This access was deployed in January 2010. The VAF, the ATFRDD, and the DDF (via the SISI project) are accessible to a POC state via the NICS upon request. Currently, the states of Arkansas, Colorado, Wisconsin, and Florida are utilizing the services provided through the SISI.

NEW NICS PROJECT

On August 3, 2011, the New NICS Project was presented to the Procurement Review Board at FBI Headquarters and received procurement approval. On August 25, 2011, the

New NICS Project was presented to the Acquisition Review Board (ARB). The ARB determines the investment value of a project. Accordingly, the New NICS Project will continue through the Life Cycle Management process. In addition, a Request for Proposal was released to vendors for comment on October 20, 2011, and a vendor day was held at the CJIS Division on November 17, 2011.

NICS IMPROVEMENT AMENDMENTS ACT OF 2007 (NIAA)

The NIAA seeks to increase the quality and quantity of relevant records available to the NICS and to close the information gap that, at times, enables persons to obtain a firearm when they are otherwise disqualified and the disqualifying information is not available. The NIAA:

- Requires federal agencies and departments to identify and provide to the NICS the information they hold demonstrating that a person falls within one of the ten federal categories of federal firearm prohibitions; and

- Authorizes grant programs for local, state, and tribal executive and judicial agencies to establish and upgrade information automation and identification technologies which will, in turn, provide for the timely submission of final criminal history dispositions and other relevant information to the NICS.

To be eligible for NIAA grant funding, a state must:

- Provide to the U.S. Attorney General a reasonable estimate of records which are subject to the NIAA's completeness requirements; and

- Certify, to the satisfaction of the U.S. Attorney General, the state has implemented a relief from disabilities program for persons who have been adjudicated as a mental defective or involuntarily committed to a mental institution.

The NICS Section works with federal agencies to help them determine if agency-held information is relevant to the NICS and how the agency can effectively and efficiently accomplish the electronic submission of the information to the NICS. The NICS Section continues to educate the federal agencies about the NICS and the federal firearm-prohibiting criteria through outreach efforts. Because of the combined efforts of the

NICS Section and the NIAA-partnering agencies, certain federal agencies have begun submitting records electronically to the NICS.

The NICS Section also continues to work with and educate state agencies on the importance of identifying and electronically submitting information to the NICS. To this end, another in a series of planned regional meetings was conducted by the NICS Section with participation by eight states on July 27, 2011, in Nashville, Tennessee. One of the main goals of the meeting was specific to sharing information to assist the states with obtaining available grant funding through the NICS Act Record Improvement Program. In addition:

- On December 13, 2011, the NICS Section conducted a regional meeting in DuPont, Washington, with numerous state representatives.

- On January 10, 2012, the NICS Section attended a meeting of the Arizona NICS Record Improvement Project Task Force.

- On February 29, 2012, the NICS Section facilitated a regional meeting in Denver, Colorado, with representatives from various venues within participating states (e.g., officials from POC state-designated agencies, CJIS Systems Officers, National Criminal History Improvement Program representatives, and state court system officials).

Many states continue to work on changes to state legislation and on the creation of the required ATF-approved relief from (mental health) disabilities program in compliance with the requirements of the NIAA. The NICS Section continues to support and work with the states (and the federal agencies who adjudicate mental health) in this effort. In addition, several states are establishing an electronic NICS Index submission process.

NICS DENIED TRANSACTION FILE (DTF)

On a nightly basis, information pertaining to persons who have been denied by the NICS is forwarded to the ATF by the FBI. The ATF determines if investigative action should be pursued. In December 2009, the CJIS APB approved:

- The NICS Section's recommendation to provide information about persons denied by the NICS to local, state, tribal, and federal law enforcement agencies for law enforcement purposes; and

- The addition of a new NCIC file, entitled the NICS DTF, to house the NICS deny information applicable to this purpose.

The NICS DTF will be comprised of records identifying NICS-denied persons by name and date of birth, in addition to other descriptive data (if available, e.g., place of birth, gender, race) plus the person's state of purchase, state of residence, the date the transaction was denied, the NICS Transaction Number, and the date of record entry.

Due to NCIC system limitations, the NICS DTF will be deployed in August 2012 via a phased-in approach. With initial deployment, the NICS DTF will make available to NICS' users the last six months of NICS denial information. When a user conducts a NICS background check, a search of the NICS DTF will be included as part of the search. To search the NICS DTF through the NCIC, a unique inquiry message must be used. When a search of the NCIC results in a hit to a NICS DTF record, a caveat message cautioning the querying agency about the use of the information will be displayed with the hit response information.

At the current time, the CJIS Division is finalizing the requirements for the NICS DTF functionality and the Technical and Operational Update. A target date for full deployment (e.g., all NICS denied transactions) is unknown at this time.

NICS AVAILABILITY

June 8, 2011: The NICS was taken out of service at 10:29 a.m. due to an Interstate Identification Index (III) issue which impacted the NICS response time. Adjustments were made to the Tuxedo Communication Process and service to the NICS was restored at 10:44 a.m.

June 21, 2011: The NICS was taken out of service at 3:39 p.m. due to III issues which impacted the NICS response time. The necessary adjustments were made, and the NICS was restored to service at 4:01 p.m.

June 24, 2011: The NICS was taken out of service at 3:06 p.m. because of NICS Contracted Call Center system-based problems. The problem was resolved, and service to the NICS was restored at 3:42 p.m.

June 25, 2011: The NICS was taken out of service at 4:14 p.m. due to a problem similar to that of the previous day. The problem was quickly resolved, and service to the NICS was restored at 4:25 p.m.

August 25, 2011: The NICS was taken out of service at 8:00 a.m. for scheduled maintenance pertaining to the NICS servers. The NICS also experienced approximately 17 minutes of downtime due to III issues.

Despite the minor occurrences described above, the NICS availability level remained high throughout 2011.

NICS Availability–2011	
January	99.87%
February	99.50%
March	99.80%
April	100%
May	99.98%
June	99.58%
July	99.76%
August	99.69%
September	100%
October	99.96%
November	100%
December	100%

NICS OUTREACH

The Annual Shooting, Hunting, and Outdoor Trade (SHOT) Show: The NICS Section participated in the Annual SHOT Show from January 17-20, 2012, in Las Vegas, Nevada. As the largest and most comprehensive trade show for all professionals involved with shooting sports and hunting industries, the SHOT Show is the world's premier exposition of firearms, ammunition, archery, camping, and related products. The NICS Section shared with the attendees information about the NICS and the background check process, the NICS E-Check (including live demonstrations), the VAF, the recent upgrade of the

NICS Web site, the NICS Resolution Card, and an overview of the services provided by the NICS. The NICS Section also participated in a town hall meeting.

The Annual NICS User Conference: Planning is underway for the 2012 Annual NICS User Conference which is scheduled for May 1-3, 2012, at the CJIS Division in Clarksburg, West Virginia. Numerous topics of mutual interest to the states and the FBI are being determined at this time.

FBI'S MAJOR CASE CONTACT CENTER (MC3)

Currently, the NICS Section's MC3 staff is:

- Updating the MC3 Concept of Operations document to include information from the Operational Response and Investigative Online Network (ORION);

- Coordinating with the FBI Washington Field Office for MC3 backup services; and

- Researching the possibility of creating an MC3 database accessible through LEO when the ORION is not used.

A corporate policy, establishing guidelines for seeking MC3 activation approval, was submitted to the FBI's Corporate Policy Office (CPO). In turn, the CPO released a corporate policy directive entitled "Implementation of the FBI Major Case Contact Center" on their Policy Collaboration Web site on August 29, 2006, for review and comment by all affected parties. The comments received were reviewed and evaluated by the NICS Section. The NICS Section is developing a Policy Implementation Guide and separate corporate policy documents for the Continuity of Operations Plan and MC3 activations.

Recent MC3 Activations:

- On August 5, 2011, the NICS Section activated the MC3 at the request of the Oklahoma City, Oklahoma, FBI Field Office, in support of the investigation of a series of Oklahoma-based bank robberies committed by an unknown subject referred to the "fake beard robber." This individual was also suspected of robbing banks in Missouri and Kansas. The tip line received 42 calls. One of the calls received by the MC3 led to the subject's apprehension in Tulsa, Oklahoma. The tip line was deactivated on August 11, 2011.

- On August 5, 2011, the NICS Section activated the MC3 at the request of the Atlanta, Georgia, FBI Field Office, in support of efforts to apprehend three

individuals who allegedly robbed the Certus Bank in Valdosta, Georgia. The tip line received 58 calls. All three individuals were apprehended, and the tip line was deactivated on August 10, 2011.

- On August 19, 2011, the NICS Section activated the MC3 at the request of the Oklahoma City, Oklahoma, FBI Field Office, in support of efforts to locate an individual accused of rape who failed to appear for trial. The tip line received 37 calls. The individual was apprehended in Texas on August 25, 2011, and the tip line was deactivated the same day.

- On September 1, 2011, the NICS Section activated the MC3 at the request of the Atlanta, Georgia, FBI Field Office, in support of efforts to apprehend an individual suspected of robbing banks in Georgia, West Virginia, and Kentucky. The tip line received 13 calls. Beginning September 7, 2011, all subsequent calls were forwarded to the Atlanta Field Office.

- On September 8, 2011, the NICS Section activated the MC3 at the request of the Knoxville, Tennessee, FBI Field Office, in support of efforts to identify an individual (referred to as the "bad hair bandit") suspected of being involved in several bank robberies in Tennessee and Kentucky. The tip line received 14 calls. Beginning September 12, 2011, all subsequent calls were forwarded to the Atlanta Field Office.

- On September 27, 2011, the NICS Section activated the MC3 at the request of the Seattle, Washington, FBI Field Office, in support of an investigation pertaining to the murder of an Assistant U.S. Attorney which had occurred ten years earlier. The tip line received 199 calls, and all subsequent calls were forwarded to the Seattle Field Office on October 14, 2011.

- On October 19, 2011, the NICS Section activated the MC3 at the request of the Richmond, Virginia, FBI Field Office, in support of an investigation pertaining to a bank robbery which occurred in Winchester, Virginia. The tip line received 14 calls. Beginning October 20, 2011, all subsequent calls were forwarded to the Richmond Field Office.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC X

Summary of Results from the CJIS APB Meeting, December 2011

PURPOSE

To inform Advisory Process members of the actions taken by the APB topics discussed at the December 2011 meeting.

AUTHOR

Skeeter J. Murray

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on the Law Enforcement Online (LEO) or via the feedback form provided to the Training Systems and Education Unit (TSEU) at facsimile, (304) 625-5090, or email: AGMU@leo.gov.

BACKGROUND

The following are recommendations and actions taken at the December 2011 APB meeting. The topic papers addressed by the APB can be found on the CJIS Special Interest Group (SIG) on LEO.

To retrieve the topic papers, select:

*Advisory Process Information
*Advisory Policy Board

Then scroll down to "APB Topic Papers" and select "12/6-7/2011-Action Topics-Albuquerque, New Mexico."

The APB meeting minutes will be distributed and posted to the CJIS SIG in the future.

APB RECOMMENDATIONS

RECOMMENDATION #1
APB Item #5 Chairman's Report on the Information Sharing (INSH) Subcommittee
INSH Issue #4 N-DEx Policy Statements

APB Recommendation: The APB moved to endorse the following policy statement for inclusion into the N-DEx Policy and Operating Manual.

Scope of N-DEx Policy: The N-DEx Policy and Operating Manual applies to all entities accessing N-DEx. N-DEx information shall be used only for the purpose indicated by the Use Code and used consistently with the coordination required by the Advanced Permission Requirement (confirming the terms of N-DEx information use). Any subsequent use of N-DEx information inconsistent with the original Use Code or the previously conducted Advanced Permission Requirement requires re-satisfaction of the Advanced Permission Requirement.

"On behalf of" Log Retention: Each N-DEx search shall clearly identify the N-DEx user, requesting agency, and any individual the search was made "on behalf of" if known at the time the search was conducted. Identification shall take the form of a unique identifier, which shall be captured and maintained in a transaction log, with the identifier remaining unique, for a minimum of one year.

While N-DEx supports this logging requirement through the N-DEx User Interface, entities accessing N-DEx data through a trusted broker must independently maintain these logs immediately and are encouraged to automate the logging requirement.

Using the search reason field to capture "on behalf of" meets the requirement of a log.

Use Code: The FBI's CJIS Division maintains an audit trail of each disclosure and receipt of N-DEx data. Therefore, all N-DEx searches must include a Use Code identifying why the search was performed. The following Use Codes are considered acceptable when searching N-DEx:

i. Criminal Justice Use Code: Must be used when N-DEx is utilized for official duties in connection with the administration of criminal justice as the term is defined in 28 Code of Federal Regulations (CFR) § 20.3 (2011).
ii. Administrative Use Code: Must be used when N-DEx is utilized by a record-owning agency to retrieve and display N-DEx contributed records in association with performing the agency's data administration/management duty. Responses for this purpose shall not be disseminated for any other reason and are limited to the record-owning agency portion of N-DEx records.

While N-DEx supports this logging requirement through the N-DEx User Interface, entities accessing N-DEx data through a trusted broker must independently maintain these logs immediately and must automate the use code transmission prior to any additional use other than "C."

Search Reason: In addition to the Use Code requirement for each N-DEx search, all users are required to provide a search reason. While the Use Code provides some lead information, it only provides a minimal audit trail. Requiring the reason for all searches will ensure N-DEx searches are conducted for authorized uses and use codes are correctly applied. It is recommended unique information, e.g., incident number, arrest transaction number, booking number, project name, description, etc., be entered to assist the user in accounting for appropriate system use for each transaction. This information shall be captured and maintained in a transaction log for a minimum of one year.

While N-DEx supports this logging requirement through the N-DEx User Interface, entities accessing N-DEx data through a trusted broker must independently maintain these logs immediately and are encouraged to automate the logging requirement.

RECOMMENDATION #2

APB Item #5 Chairman's Report on the Information Sharing (INSH)Subcommittee
INSH Issue #5 The Use of N-DEx to support Criminal Justice Employment Background Investigations

APB Recommendation : The APB moved to endorse the recommended policy statement that addresses the privacy and legal concerns which have been previously identified by the Office of General Counsel which reads:
The N-DEx Program Office will incorporate into the N-DEx Policy and Operating Manual the policies and language regarding Notice and Consent, Redress and Audits in order for the N-DEx system to be accessed for criminal justice employment background checks.

RECOMMENDATION #3

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee
NCIC Issue #1 Proposal to Create an Opportunity to Provide U.S. Law Enforcement with Enhanced Awareness of Canadian Police Agency Information Held at Local Levels

APB Recommendation: The APB moved to create a new message key to access the Canadian Federal Identity Program (FIP) Database along with creating a task force to include CJIS, Canadian Police Information Centre, APB, and the International Justice and Public Safety Information Sharing Network (Nlets) representative to discuss the implementation of the FIP access.

RECOMMENDATION #4

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #3 Proposal for Inclusion of Proof of Service Information in the NCIC Protection Order File

APB Recommendation : The APB moved to add the Service Information (SVC) and Service Date (SVD) Fields as outlined with the following modifications (underlined):

Add two new fields in a POF record that can be populated using the enter and modify transactions to capture the service status and the service date information of the protection order. The suggested service status field name and code is "Service Information" and "SVC." The suggested service date field name and code is "Date Served" and "SVD." The SVC values would be established as: Served, Not Served, or Unknown. If the SVC Field is populated with "Served," it would be mandatory to populate the SVD Field with the eight-digit date that the officer served the notice/paperwork to the respondent.

The fields would be optional and independent of one another, therefore only states wanting to include this information in their NCIC records would have to modify their entry and modify message formats. Any states using the validation fixed formats would have to make changes to accommodate the additional fields.

RECOMMENDATION #5

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #3 Proposal for Inclusion of Proof of Service Information in the NCIC Protection Order File

APB Recommendation : The APB moved to exclude the following caveat from the record response: THE SERVICE STATUS OF THE FOLLOWING PROTECTION ORDER RECORD NIC/XXXXXXXXXX IS SERVED.

RECOMMENDATION #6

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #3 Proposal for Inclusion of Proof of Service Information in the NCIC Protection Order File

APB Recommendation: The APB moved that the fields should be designated as non-critical for the completeness review during an FBI NCIC Audit of the POF.

RECOMMENDATION #7

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #4 Request to Create an Automatic Notification Indicating International Travel by Registered Sex Offenders

APB Recommendation : The APB moved to approve concept to develop an NCIC notification to the Originating Agency Identifier of the National Sex Offender Registry record when a registered sex offender attempts to enter or depart the U.S.

RECOMMENDATION #8

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #5 Proposal to Modify the NCIC Protection Order File (POF) Protection Order Condition (PCO) Code 07

APB Recommendation : The APB moved modify the NCIC POF PCO Code 07 by adding the language "WEAPONS AS IDENTIFIED IN THE MISCELLANEOUS FIELD". Proposed language would be as follows (new language underlined):

07 THE SUBJECT IS PROHIBITED FROM POSSESSING AND/OR PURCHASING A FIREARM OR OTHER WEAPONS AS IDENTIFIED IN THE MISCELLANEOUS FIELD.

RECOMMENDATION #9

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #6 Proposal to Modify the Response for NCIC Record Inquiries to include the Name of Validator Field

APB Recommendation : The APB moved to display the VLN Field to the CJIS Systems Agency (CSA) *"for local agencies that fall under their purview"* in a record response.

RECOMMENDATION #10

APB Item #8 Chairman's Report on the National Crime Information Center (NCIC) Subcommittee

NCIC Issue #7 Establishment of Minimum Audit Standards for CJIS Systems Agency Audit Programs, to Include Timely Entry of Missing Individuals Under Age 21

APB Recommendation : The APB moved for no change. Minimum audit requirements for CSA audit programs will not be established, therefore, continuing to leave discretion with CSAs to decide the specific policy areas that their audit programs will encompass.

RECOMMENDATION #11

APB Item #9 White House National Security Staff Update to Include the Department of State (DOS) Request for Expanded Access to the NCIC Supervised Release and Identity Theft Files

APB Recommendation: The APB moved to authorize NCIC Supervised Release File, **Missing Person File**, and Identity Theft File access, for the DOS's Consular Affairs Passport Services in order to support their passport screening processes**.** (Changes shown in bold.)

RECOMMENDATION #12

APB Item #13 Chairman's Report on the Security and Access (SA) Subcommittee
SA Issue #2 Security Addendum Electronic Certification

APB Recommendation : The APB moved to accept the language change (shown in italics) in the policy as follows:

Appendix A, Terms and Definitions

Digital Signature - *A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.*

Appendix H, Security Addendum

2.01 The Contracting Government Agency (CGA) will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. *The acknowledgment may be signed either by hand or via digital signature (see glossary for definition of digital signature).*

RECOMMENDATION #13

APB Item #13 Chairman's Report on the Security and Access (SA) Subcommittee
SA Issue #3 State of Residency Fingerprint Based Background Checks

APB Recommendation : The APB moved to approve the definition and examples of acceptable documentation of "state of residency" to be added to the CJIS Security Policy in Appendix A, Terms and Definitions based on information gathered and presented by the CJIS ISO office in the Background Paper as follows:

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. Examples of acceptable documented evidence permitted to confirm an individual's state of residence are: driver's license, state or employer issued ID card, voter registration card, proof of an address (such as utility bill with one's name and address as the payee), passport, professional or business license, and/or insurance (medical/dental) card.

RECOMMENDATION #14

APB Item #13 Chairman's Report on the Security and Access (SA) Subcommittee
SA Issue #3 State of Residency Fingerprint Based Background Checks

APB Recommendation : The APB moved to accept the following additions to Paragraph 5.12.1.1 (1) and Paragraph 5.12.1.2 (1). (Additions shown in bold.)

Paragraph 5.12.1.1(1) – "to verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to Criminal Justice Information (CJI). ***However****, if the person resides in a different state than that of the assigned agency, the agency shall conduct both state (****of the agency****) and national fingerprint-based record checks and execute an Nlets Criminal History Record Information Canadian Criminal History Name Index Query (IQ)/Full Query (FQ)/CHRI Inquiry Query (AQ) using purpose code C, E, or J depending upon the circumstances. Where appropriate, the screening shall be consistent with: (i) 5 CFR 731.106; and/or (iii) agency policy, regulations, and guidance. (See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check."*

Paragraph 5.12.1.2(1) – "Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. ***However****, if the person resides in a different state than that of the assigned agency, the agency shall conduct both state (****of the agency****) and national fingerprint-based record checks and execute an Nlets CHRI IQ/FQ/AQ query using purpose code C, E, or J depending upon the circumstances.*

RECOMMENDATION #15

APB Item #13 Chairman's Report on the Security and Access (SA) Subcommittee
SA Issue #4 Signatures for Visitors to Physically Secure Locations

APB Recommendation: The APB moved to accept the language change in the policy as presented, striking "Signature of the visitor" from the required list as follows:

Paragraph 5.9.1.8 (with proposed deletion shown in strikeout)

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 s publically accessible) that includes;

1. Name and agency of the visitor
2. ~~Signature of the visitor~~
3. Form of identification
4. Date of access
5. Time of entry and departure
6. Purpose of visit
7. 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.

RECOMMENDATION #16

APB Item #15 Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee

UCR Issue #4 Quality Assurance Review (QAR) Methodology to Calculate Classification Error Rates

APB Recommendation : The APB moved to modify the UCR Quality Assurance Review (QAR) methodology to apply a formula, after the QAR, to weigh the error rates for each agency based on the volume of submissions at each agency.

RECOMMENDATION #17

APB Item #15 Chairman's Report on the Uniform Crime Reporting (UCR) Subcommittee

UCR Issue #5 Definition of Prostitution as it Relates to Human Trafficking

APB Recommendation: The APB moved to approve the UCR Program definition change to read "Prostitution – to engage in commercial sex acts for anything of value."

RECOMMENDATION #18

APB Item #15 Chairman's Report on the Uniform Crime Reporting(UCR) Subcommittee

UCR Issue #5 Definition of Prostitution as it Relates to Human Trafficking

APB Recommendation: The APB moved for no change and not to modify the National Incident-Based Reporting System (NIBRS) collection of Crimes Against Society to allow prostitutes to be reported as either victims or offenders.

RECOMMENDATION #19
APB Item #22 Chairman's Report on Identification Services (IS) Subcommittee
IS Issue #2 Biometric Interoperability Update

APB Recommendation : The APB moved to task the CJIS Division with exploring multi-modal interoperability opportunities with other federal stakeholders to include privacy and policy issues.

RECOMMENDATION #20
APB Item #16 Discussion of the Summary Reporting System (SRS) Definition of Forcible Rape

The definition of rape within the UCR SRS falls under the category of "Forcible Rape." Instances of rape that do not involve force might fall outside the purview of the current category.

APB Recommendation: The APB moved to remove the term "Forcible" from sexual offenses in the UCR Program.

RECOMMENDATION #21

This is a continuation of recommendation #20.

The current definition of rape within the UCR SRS is "the carnal knowledge of a woman forcibly and against her will" and was instituted in 1929. The APB expressed concern that the definition is too narrowly written and recommended an expansion. A change in definition will require state and local law enforcement agencies reporting in the SRS to implement changes to their records management systems. The FBI UCR Program will work with the law enforcement community to assist in addressing associated funding issues.

APB Recommendation #21: The APB moved to change the definition of rape in the UCR SRS to: "Penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another person, without the consent of the victim."

RECOMMENDATION #22

This is a continuation of recommendation #20.

A change to the current definition will result in difficulties obtaining accurate, meaningful statistics while state and local law enforcement agencies transition to the new definition. With this recommendation the APB intends to maintain greater statistical integrity while locations transition to the new definition.

APB Recommendation: The APB moved to establish in the UCR SRS a rape category which incorporates the new definition and to establish a subset category

RECOMMENDATION #23
APB Item #22 Chairman's Report on the Identification Services (IS)Subcommittee
IS Issue #3 Biometric Interoperability: Data Protection Strategy #6

APB Recommendation: The APB moved that the IS subcommittee review the current data protection strategies and make recommendations to create additional strategies, modify the current ones, or delete the ones that no longer apply.

RECOMMENDATION #24
APB Item #22 Chairman's Report on the Identification Services (IS) Subcommittee
IS Issue #5 NGI Implementation and Transition Update

APB Recommendation: The APB moved to request CJIS staff to review, analyze, and report back to the Identification Services Coordination Group (ISCG) and IS Subcommittee the level of effort and time line necessary to expand RISC searches to additional repositories to include the CMF.

RECOMMENDATION #25
APB Item #22 Chairman's Report on the Identification Services (IS) Subcommittee
IS Issue #6 Identification Services Coordination Group Update

APB Recommendation : The APB moved to endorse the recommendation by the ISCG to relax the Electronic Biometric Transmission Specification 9.2 clause which stipulates a January 2012 conformance date for Service Availability Plan 30 RISC devices to no earlier than January 2013.

RECOMMENDATION #26
APB Item #22 Chairman's Report on the Identification Services (IS) Subcommittee
IS Issue #8 Rapid Deoxyribonucleic Acid Task Force Update

APB Recommendation: The APB moved to endorse the concept of "John Doe" DNA warrants.

The APB also recommended the ISCG *collaborate with the FBI Science and Technology Branch* to explore modifications of the EBTS and the Interstate Identification Index to include the Rapid DNA Index Number (RDIS#).

RECOMMENDATION #27
APB Item #28 CJIS Division Bioterrorism Risk Assessment Group
SA Issue #8 Request for Access to the NICS Index

APB Recommendation: The APB moved that the BRAG be permitted to access the NICS Index in support of the SRA process. Access to this data will be automatically suppressed, unless the states affirmatively indicate their data may be used in support of the BRAG.

RECOMMENDATION #28
APB Item #5 Chairman's Report on the Information Sharing (INSH) Subcommittee
INSH Issue # 9 & #12 N-DEx and UCR Relationship/IJIS Update

APB Recommendation: The APB moved to request that CJIS work with the UCR subcommittee and INSH subcommittee to explore the technical and policy issues involved with the use of the N-DEx IEPD to support NIBRS submissions at the request of the state and local agencies.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPIC

STAFF PAPER

INFORMATIONAL TOPIC Y

Removal of the Term "Forcible" from Sexual Offenses in the FBI's Uniform Crime Reporting (UCR) Program

PURPOSE

Present to the Working Groups the changes that will occur to the UCR Program as a result of Fall 2011 Criminal Justice Information Services Advisory Policy Board (APB) Motion 1—to remove the term "Forcible" from the sex offenses collected in the UCR Program. This Change Affects the Summary Reporting System (SRS), National Incident-Based Reporting System (NIBRS), Hate Crime Statistics Program, and Cargo Theft.

AUTHOR

Nancy E. Carnes, (304) 625-4830

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

At the Fall 2011 APB meeting, the APB approved, and was subsequently approved by FBI Director Mueller, the new UCR SRS definition of rape. It is: Penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another person, without the consent of the victim. In response to APB Motion 1, this Information Topic paper was prepared.

Listed below are the UCR Program changes:
(If a definition is shown, the original definition is provided first and listed in bold is the revised definition with any use of the word "forcibly and against the person's will" removed.)

SRS
Any references to "forcible" and in relation to rape and sex offenses in the SRS, will be adjusted accordingly.

Age, Sex, Race, and Ethnicity of Persons Arrested, Under 18 Years of Age
Age, Sex, Race, and Ethnicity of Persons Arrested, 18 Years of Age and Over
Classification of Offenses:

Sex Offenses (Except Forcible Rape and Prostitution) (17)—in the *UCR Handbook* this offense is defined as: This classification includes offenses against chastity, common decency, morals, and the like. Sexual attacks on males are included in this classification. However, depending on the nature of the crime and the extent of the injury, the offense could be classified as an assault. This classification includes all sex offenses except forcible rape, prostitution, and commercialized vice. Agencies must include in this classification: adultery and fornication, buggery, seduction, and sodomy or crime against nature, incest, indecent exposure, indecent liberties, statutory rape (no force) and attempts to commit any of the above.

Sex Offenses (Except Rape and Prostitution) (17)—This classification includes sex offenses that involve sexual penetration and consent or involve no sexual penetration and no consent. Depending on the nature of the crime and the extent of the injury, the offense could be classified as an assault. This classification includes all sex offenses except rape (as newly defined), prostitution, and commercialized vice. Agencies must include in this classification any sex offense not included in Rape, e.g., fondling, adultery. (The addition of Statutory Rape and Incest is dependent upon decisions relevant to Action Topic.)

Supplementary Homicide Report—No change

This form allows for reporting additional information (e.g., circumstance) on each murder incident. Rape (02) and Other Sex Offense (17) are murder circumstances. Therefore, as with reporting according to the new rape definition for the above-mentioned SRS forms, the murder circumstance will change as well. Any murder circumstance meeting the rape definition should be reported as Rape. Any murder circumstance that was a sex offense not meeting the rape definition criteria should be reported as Other Sex Offense.

NIBRS

The NIBRS sex offenses of rape, sodomy, and sexual assault with an object will be converted for publication purposes to rape. This entails expanding the current conversion procedure. Previously, only NIBRS incidents in which the rape of a female by a male was reported were converted to the SRS. (The conversion process transforms NIBRS data to the SRS format.)

The NIBRS sex offense, fondling does not meet the SRS rape definition and will not be converted for inclusion in the SRS rape total. For SRS-reporting purposes, this offense will remain a Part II arrest category.

For NIBRS reporting purposes, Sex Offenses are defined as: (Removing the word forcible, the Sex Offenses will no longer be identified as forcible.)

Definition: Any sexual act directed against another person, forcibly and/or against that person's will or not forcibly or against the person's will in instances where the victim is incapable of giving consent.

Definition: Any sexual act directed against another person, without the consent of the victim, including instances where the victim is incapable of giving consent.

> Forcible Rape (Except Statutory Rape)—The carnal knowledge of a person, forcibly and/or against that person's will or not forcibly or against the person's will in instances where the victim is incapable of giving consent because of his/her temporary or permanent mental or physical incapacity (or because of his/her youth).
>
> **Rape—The carnal knowledge of a person, without the consent of the victim, including instances where the victim is incapable of giving consent because of his/her age or because of his/her temporary or permanent mental or physical incapacity.**
>
> This Note will remain:
>
> Note: If force was used or threatened, the crime should be classified as Rape regardless of the age of the victim. If no force was used or threatened and the victim was under the statutory age of consent, the crime should be classified as Statutory Rape.

Note: The crime should be classified as Rape regardless of the age of the victim if the victim did not consent or the victim was incapable of giving consent. If the

victim consented, victim was not forced or threatened, and the victim was under the statutory age of consent, the crime should be classified as Statutory Rape. (The addition of Statutory Rape and Incest is dependent upon decisions relevant to Action Topic.)

Sodomy—Oral or anal sexual intercourse with another person, forcibly and/or against that person's will or not forcibly or against the person's will in instances where the victim is incapable of giving consent because of his/her youth or because of his/her temporary or permanent mental or physical incapacity.

Sodomy—Oral or anal sexual intercourse with another person, without the consent of the victim, including instances where the victim is incapable of giving consent because of his/her age or because of his/her temporary or permanent mental or physical incapacity.

Sexual Assault With An Object—To use an object or instrument to unlawfully penetrate, however slightly, the genital or anal opening of the body of another person, forcibly and/or against that person's will or not forcibly or against the person's will in instances where the victim is incapable of giving consent because of his/her youth or because of his/her temporary or permanent mental or physical incapacity.

Sexual Assault With An Object—To use an object or instrument to unlawfully penetrate, however slightly, the genital or anal opening of the body of another person, without the consent of the victim, including instances where the victim is incapable of giving consent because of his/her age or because of his/her temporary or permanent mental or physical incapacity.

Fondling—The touching of the private body parts of another person for the purpose of sexual gratification, forcibly and/or against that person's will or not forcibly or against the person's will in instances where the victim is incapable of giving consent because of his/her youth or because of his/her temporary or permanent mental or physical incapacity.

Fondling—The touching of the private body parts of another person for the purpose of sexual gratification, without the consent of the victim, including instances where the victim is incapable of giving consent because of his/her age or because of his/her temporary or permanent mental or physical incapacity.

There is no penetration in fondling; therefore, this offense would not convert to the SRS rape definition.

NIBRS nonforcible sex offenses are currently under review and are not included in this paper.

Hate Crime Statistics Program

In the Hate Crime Statistics Program, Rape as newly defined should be reported as a hate crime if the offense occurred as the result of the offender's bias.

Cargo Theft

In addition, the collection of Cargo Theft was developed based on the NIBRS. In a multiple-offense incident, it is possible to report the NIBRS sex offenses if the first offense reported is a valid cargo theft offense (e.g., robbery, motor vehicle theft). Therefore, any references to the NIBRS sex offenses on the Cargo Theft Incident Report and in the document, *Cargo Theft Electronic Data Submission Specifications* will be adjusted accordingly.

Conclusion

The above-mentioned changes will require all applicable UCR documents to be revised.

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC Z

Secondary Access to III Criminal History Records by Maine Bail Commissioners

POINT OF CONTACT:

Allen Wayne Nash, (304) 625-2738

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

BACKGROUND

The Maine State Police is requesting that Maine bail commissioners be granted secondary access to criminal history record information (CHRI) maintained in the Interstate Identification Index (III) for the purpose of setting the conditions of bail.

In Maine, bail commissioners may set bail when court is not in session or a judge is unavailable. Any resident of the State of Maine who is not employed by the Judicial Department may apply to serve as a bail commissioner. The bail commissioners are not government employees; they are independent contractors. They are entitled to receive a fee not to exceed $60 which is generally paid by the defendants. The sheriff of the county in which the defendant is detained may create a fund for the payment in whole or in part of the fee for those defendants who do not have the financial ability to pay the fee.[1]

Bail Commissioners are included in the definition of "judicial officer" under Maine Bail Code and serve at the pleasure of the Chief Judge of the District Court.

[1] 15 M.R.S.A. §1023(5)

Maine bail commissioners are authorized to set pre-conviction bail for all criminal offenses, with some exceptions.[2] The exceptions are:

- Cases where a defendant is charged with murder.
- Cases in which an attorney for the state requests a Harnish bail proceeding. Such a hearing is held when the defendant is accused of crimes other than murder, such as rape, that previously warranted capital punishment in the state.
- Bail is not set in cases where a defendant is "confined in jail or held under arrest by virtue of any order issued by a court in which bail has not been authorized."

By statute, Maine bail commissioners, just as judges, are directed to consider several factors in setting bail. Among those factors that need to be considered are the defendant's past conduct, including any history relating to drug or alcohol abuse, the defendant's criminal history, the defendant's record concerning appearances at court proceedings, and whether at the time of the current offense or arrest, the defendant was on probation, parole, or other release pending trial, sentencing, appeal, or completion for a sentence. Pursuant to a recent amendment to the Maine Bail Code, bail commissioners must know the nature of a pending charge in order to understand the extent of their authority to set bail in certain cases, including those involving domestic violence and sexual assault.[3]

Based on the review of the available information a bail commissioner may issue an order that, pending trial, the defendant be released:

- On personal recognizance, or
- On execution of an unsecured bond, or
- On execution of a secured bond.

A bail commissioner may also attach a condition or a combination of conditions to the bail. A bail commissioner may also refuse to set bail and order the defendant to be detained.

[2] 15 M.R.S. §1023
[3] Public Law, chapter 431, §§2-3

DISCUSSION AND ANALYSIS

The III system is operated under the authority of Title 28, United States Code, §534 which permits the exchange of criminal history records shall be "…with, and for the official use of, authorized officials of the federal government, including the United States Sentencing Commission, the states, cities, and penal and other institutions." The Department of Justice and the federal courts have interpreted this language to restrict direct access to the III system to criminal justice agencies for criminal justice purposes and federal agencies authorized to receive criminal history records pursuant to federal statute or executive order[4].

Currently, Maine bail commissioners receive information contained in Maine criminal history records to set bail, but do not receive information contained in criminal history records maintained in the III system. Title 28, Code of Federal Regulations (C.F.R.) §20.33(a)(7) provides that CHRI contained in the III system may be made available:

> "To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to this agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it was provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and the authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee)."

The "administration of criminal justice" is defined in the regulations[5] as "the performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders."

Subsection 611(1) of Maine's Criminal History Record Information Act defines "administration of criminal justice" as follows:

> "Administration of criminal justice means detection, apprehension, detention, pre-trial release, post-trial release, prosecution, adjudication,

[4] Title 28, C.F.R. §20.33
[5] 28 C.F.R. §20.33(b)

> correctional supervision or rehabilitation of accused persons or criminal offenders. It includes criminal identification activities and the collection, storage and dissemination of criminal history record information.

For purposes of "the administration of criminal justice" pre-conviction bail determinations fall within the discretion of the trial judge as a "pre-trial release" function.

The fact that a Bail Commissioner is an independent contractor does not pose a bar to receiving CHRI from a state trial judge. The regulation cited above expressly permits a private contractor to receive CHRI so long as the release is subject to a specific agreement. In addition, several mechanisms exist to help ensure a bail commissioner properly uses and maintains any CHRI received under the agreement. First, bail commissioners in the State of Maine are appointed by, and serve at the pleasure of, the Chief Judge. As with most appointments, the position is not available to the general population, but only to those persons who instill the Chief Judge with confidence sufficient to faithfully discharge the duties of the office. It is known that with any appointment comes the possibility of dismissal for misconduct. Second, the agreement and security addendum should contain provisions to guide the Bail Commissioners about the proper use of CHRI. Third, if a bail commissioner misuses the record, the trial judge is (or should be) well aware that, as the primary recipient, his or her access to III will be subject to cancellation. Fourth, as a condition of appointment and continued service, bail commissioners must successfully complete a bail training program, as prescribed and scheduled by the Chief Judge. It is reasonable to conclude that such a program would include instruction on the proper use and handling of CHRI.

Accordingly, the CJIS Division believes the secondary dissemination of CHRI from a judge to a duly appointed bail commissioner in the State of Maine is a permissible use of the III system so long as appropriate safeguards exist to carefully control the disclosure.