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

INFORMATION ONLY AGENDA as of 5/09/12

Informational Topic A*
Legislative Update

Informational Topic B
Integrated Automated Fingerprint Identification System (IAFIS) Enhancements Status

Informational Topic C
National Crime Prevention and Privacy Compact Council Update

Informational Topic D
Notification of Revised Fee Schedule

Informational Topic E
IAFIS Status Report

Informational Topic F
Biometric Information Sharing Update

Informational Topic G
CJIS Division Intelligence Group Overview

Informational Topic H
Federal Agency Participation in Automated Biometric Identification System (IDENT) /IAFIS Interoperability

Informational Topic I
Biometric Interoperability Update

Informational Topic J
State Participation in IDENT/IAFIS Interoperability

Informational Topic K
National Crime Information Center (NCIC) Status Report

Informational Topic L
Law Enforcement National Data Exchange (N-DEx) Enhancements Status

Informational Topic M
Strategy to Promote N-DEx Usage by Fusion Centers

Informational Topic N
CJIS Division NCIC Enhancements Status

Informational Topic O
NCIC 2000 Header Requirement

Informational Topic P
Warrant Task Force Status Report

Informational Topic Q
NCIC Fiscal Year 2011 Audit Results Summary

Informational Topic R
National Center for Missing and Endangered Children (NCMEC) Notification of Missing Juveniles in the NCIC Disability Category

Informational Topic S
Implementation of the Next Generation Identification (NGI) Enhanced Repository

Informational Topic T
Information Security Officer Update

Informational Topic U
NGI Program Implementation and Transition Update

Informational Topic V
The National Instant Criminal Background Check System (NICS) Section's Expansion of the NICS Index to Include Information Pertaining to Persons Disqualified from Possessing or Receiving a Firearm or a Firearm-Related Permit Based on State Law

Informational Topic W
NICS Update

Informational Topic X
Summary of Results from the CJIS APB Meeting, December 2011

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

Informational Topic Z
Secondary Access to III Criminal History Records by Maine Bail Commissioners

* Updated for the APB Meeting

CJIS ADVISORY POLICY BOARD
SPRING 2011 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC A

Legislative Update

PURPOSE

To provide an overview of legislation introduced in the 112th Congress, which may impact the CJIS Division and the user community.

AUTHOR

Ms. Melody Ferrell

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>.

ENACTED LEGISLATION

FAA MODERNIZATION AND REFORM ACT OF 2012
[Public Law (Pub. L.) 112-95]

On February 14, 2012, the President signed Pub. L. 112-95, formerly HR 658, the Federal Aviation Administration (FAA) Modernization and Reform Act of 2012. Section 802 of the law authorizes the FAA to establish a process to conduct state and FBI fingerprint-based criminal history background checks of airmen in compliance with the National Crime Prevention and Privacy Compact Act of 1998 (Title 42, United States Code (U.S.C.), Section 14616). The FAA may not use the authority to conduct criminal investigations and may collect reimbursement for processing the fingerprint-based checks, including the FBI fee.

JUMPSTART OUR BUSINESS STARTUPS ACT (Pub. L. 112-106)

On April 5, 2012, the President signed Pub. L. 112-106, formerly HR 3606, the Jumpstart Our Business Startups Act. Section 302 of the bill is entitled the "Capital Raising Online While Deterring Fraud and Unethical Nondisclosure Act of 2012" or the "CROWDFUND Act" and amends 15 U.S.C. § 77a et. seq. by adding Section 4a. This section requires the Securities and Exchange Commission to take measure to reduce the risk of fraud by requiring the Commission to promulgate a rule that includes obtaining a background and securities enforcement regulatory history check on each officer, director, and person holding more than 20 percent equity of each issuer whose securities are offered by such person. The rule shall establish disqualification provisions which includes that an issuer, broker, or funding portal has not been convicted of any felony or misdemeanor in connection with the purchase or sale of any security or a false filing with the Commission. The bill does not specifically indicate if this will include an FBI fingerprint check.

PROPOSED LEGISLATION
112th CONGRESS
2nd Session

Note: **Categories are:** Background Checks, NICS/Brady Act, Immigration, National Crime Information Center, Sex Offender Registry, Uniform Crime Report, and Miscellaneous.
All bills are "In Committee" unless otherwise indicated.
Bold indicates updates.

BACKGROUND CHECKS:

Bill Name:	Safety for Our Schoolchildren Act of 2011
Designation:	S 124
Sponsor:	David Vitter (R-LA) 01/25/11
Cosponsor:	0-D, 0-R (as of 04/02/12)

Section 2 of the bill amends 20 U.S.C. § 7101 et. seq. by adding a new section which requires that state or local educational agencies that receive federal funds obtain an FBI background check, as defined under 42 U.S.C. § 1304, on school employees prior to employment. As required under 42 U.S.C. § 1304, the background check would be a fingerprint-based check and requires a state and FBI check. The agency must also report to a local law enforcement agency if an individual that has applied for employment is a sexual predator. School employees include employees in a public school, administrators, teachers, substitute teachers, custodians, cafeteria workers, and school bus drivers and also includes contractor employees that have exposure to students.

Bill Name: Passport Identity Verification Act
Designation: S 744
Sponsor: Ben Cardin (D-MD) 04/06/11
Cosponsor: 2-D, 0-R (as of 04/02/12)

Previously introduced in the 111th Congress as S. 3666, Section 3 of the bill provides that data sharing activities, engaged in by Department of State (DOS) personnel, relating to granting, refusal, revocation, or adjudication of a passport, will be considered law enforcement activities that involve the administration of criminal justice, as defined in 28 CFR § 20.3. The DOS personnel may access information in relevant databases maintained by any federal, state, tribal, territory, local government department or agency, or private organization which contains: (1) criminal history information; (2) driver's license or motor vehicle information, including photographs; (3) marriage, birth, or death information; (4) naturalization or immigration information; or (5) other information that may be used to verify the identity of the passport applicant, detect fraud, or revoke a passport. The DOS will promulgate regulations concerning this access. Section 4 requires the DOS, Department of Homeland Security (DHS), Attorney General (AG), and the U.S. Postmaster General to conduct an analysis to determine if passport renewal applicants should provide biometric information, including photographs, for the purpose of verifying the identity and detecting passport fraud.

Bill Name: Foster Care Mentoring Act of 2011
Designation: S 420
Sponsor: Mary Landrieu (D-LA) 02/28/11
Cosponsor: 3-D, 0-R (as of 04/02/12)

Previously introduced in the 111th Congress as S 986, Section 3 of the bill amends 42 U.S.C. § 629, et. seq. by adding Section 440. This Section authorizes the Secretary of the Department of Health and Human Services (DHHS) to conduct criminal background checks of mentors to children in foster care. The bill does not specify how the background checks are to be conducted.

Bill Name: Foster Care Mentoring Act of 2011
Designation: HR 2012
Sponsor: Karen Bass (D-CA) 05/26/11
Cosponsor: 11-D, 0-R (as of 04/02/12)

House version of S 420.

Bill Name: Child Protection Improvements Act of 2011
Designation: HR 1360
Sponsor: Adam Schiff (D-CA) 04/04/11
Cosponsor: 5-D, 1-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 1469, this bill requires the AG to establish a criminal history review program to conduct national criminal history background checks for child-serving organizations. The AG or the background check designee shall handle inquiries from covered entities concerning national background checks; provide participating entities with access to the national checks on covered individuals; negotiate agreements with each state authorized agency; receive both paper and electronic fingerprint submissions and convert paper cards to an electronic format; negotiate agreements with each authorized state agency; collect both a state and FBI fee; coordinate with the FBI and state authorized agencies to ensure background checks are completed within the designated time period; and electronically transmit national background check requests to the FBI and/or state agency within two business days. The FBI and/or state authorized agency shall provide criminal history record information (CHRI) to the AG or criminal history review designee within two business days after receipt of the request. The AG or criminal history review designee would be required to establish procedures to receive CHRI from the FBI and state authorized agencies; transmit the CHRI to the covered individual, along with a detailed notification of the individual's rights; make determinations whether the CHRI bears upon the individual's suitability to provide care to children, and convey information to the participating entity. The fee charged may not exceed the actual cost to the AG or background check designee and the criminal history review designee, and cannot be more than $25 for volunteers. The fee may also be waived by the AG upon showing of substantial hardship. Additionally, the state fee may not exceed $25. Any fingerprints or CHRI obtained under this Act must be destroyed unless the individual signs a release permitting the retention for up to five years. However, this does not apply to the retention of fingerprints by the FBI, upon consent of the individual or in accordance with state or federal procedures, for the purpose of subsequent verification or hit notification. Within one year, the AG is also required to prepare a report to Congress concerning this program.

Bill Name: Child Protection Improvements Act of 2011
Designation: S 645
Sponsor: Charles Schumer (D-NY) 03/17/11
Cosponsor: 4-D, 4-R (as of 04/02/12)

Bill is almost identical to HR 1360.

Bill Name: Child Care Protection Act of 2011
Designation: S 581
Sponsor: Richard Burr (R-NC) 03/15/11
Cosponsor: 4-D, 4-R (as of 04/02/12)

Previously introduced in the 111th Congress as S 2903, this bill amends 42 U.S.C. § 9858 et. seq. by requiring states receiving funds under this section to have procedures requiring criminal background checks for child care staff members and prospective child care staff members. The criminal background check includes an FBI fingerprint check and a search of the state criminal repositories, state-based child abuse and neglect registries, the National Crime Information Center (NCIC), and the National Sex Offender Registry (NSOR). The child care provider will submit the requests to the appropriate state agency and must be submitted at least once during a five-year period. The results of the background check shall be provided to the child care provider. The state may charge a fee for conducting the criminal background check, but it may not exceed the actual cost to the state.

Bill Name: Child Care Protection Act of 2011
Designation: HR 1726
Sponsor: C.A. Dutch Ruppersberger (D-MD) 05/04/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

House version of S 581.

Bill Name: Child Care Criminal Background Check Act of 2011
Designation: HR 1711
Sponsor: Andre Carson (D-IN) 05/04/11
Cosponsor: 3-D, 0-R (as of 04/02/12)

This bill amends 42 U.S.C. § 9858 et. seq. and the purpose of the bill is to assist states in improving the quality of child care services by providing a national criminal background check of child care providers that are licensed by the state or receive funds under the Child Care and Development Block Grant Act of 1990. However, the bill only requires states receiving funds to obtain a State criminal background check of child care services' employees, applicants, and family child care providers.

Bill Name: CARE for Kids Act of 2012
Designation: HR 3829
Sponsor: Gwen Moore (D-WI) 01/25/12
Cosponsor: 6-D, 0-R (as of 04/02/12)

This bill amends 42 U.S.C. § 9858 et. seq. by providing for a state and national background check for an individual who is a child care staff member, family child care provider, or an adult who resides in a family child care provider's home, that receives funds under the Child Care and Development Block Grant Act of 1990. It also requires a search of the NSOR, NCIC, and state abuse and neglect registries. The bill provides that not more than one request for a state and national background check may be conducted in a 5-year period. The state will provide a copy to the child care provider or, upon request, to the individual subject to the criminal background check. The state may collect a fee from the child care provider or family care provider, but it may not exceed the actual costs to the state, and the fee for all background checks may not exceed $36. Money is also authorized to be appropriated to offset the administrative costs of conducting the state and national background check.

Bill Name:	Domestic Minor Sex Trafficking Deterrence & Victims Support Act of 2011
Designation:	S 596
Sponsor:	Ron Wyden (D-OR) 03/16/11
Cosponsor:	8-D, 4-R (as of 04/02/12)

Section 5 of the bill amends the Social Security Act (42 U.S.C. § 671(a)), by requiring that states have procedures to require state child welfare agencies to promptly report information of missing or abducted children to the law enforcement authorities for entry into the NCIC. Section 3701(c) of the Crime Control Act of 1990 is also amended by requiring the AG to prepare a statistical summary of the total number of reports and entries made to the NCIC.

Bill Name:	Strengthening the Child Welfare Response to Human Trafficking Act of 2011
Designation:	HR 2730
Sponsor:	Karen Bass (D-CA) 08/01/11
Cosponsor:	4-D, 1-R (as of 04/02/12)

Section 2 has provisions similar to Section 5 of S 596.

Bill Name:	Secure Chemical Facilities Act
Designation:	S 709
Sponsor:	Frank Lautenberg (D-NJ) 03/31/11
Cosponsor:	1-D, 0-R (as of 04/02/12)

This bill amends the Homeland Security Act of 2002 by requiring the DHS Secretary to issue regulations to conduct security background checks of unescorted visitors and permanent, part-time, temporary, and contract chemical facility personnel

having access to restricted areas or critical assets. The security background check, including a check of relevant databases to verify and validate identity, criminal history databases, and the consolidated terrorist watch list, would be conducted at no cost to the individual. The regulations would determine how the background checks will be conducted.

Bill Name:	National Association of Registered Agents and Brokers Reform Act of 2011
Designation:	HR 1112
Sponsor:	Randy Neugebauer (R-TX) 03/16/11
Cosponsor:	26-D, 34-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 2554, Section 2 of the bill amends 15 U.S.C. § 6751 et seq. by requiring the National Association of Registered Agents and Brokers (Association), when requested by an insurance producer, to submit identification information obtained from a state-licensed insurance producer to the FBI for a criminal history record check. The FBI would return the CHRI to the Association, a nonprofit corporation.

Bill Name:	Internet Gambling Regulation, Consumer Protection, and Enforcement Act
Designation:	HR 1174
Sponsor:	John Campbell (R-CA) 03/17/11
Cosponsor:	24-D, 5-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 2267, this bill requires persons, including corporations, partnerships, or other business entities, who apply for Internet gambling licenses, and individuals under their control, to have a background check conducted. The Secretary of the Treasury will establish the procedures for conducting the background checks.

Bill Name:	Internet Gambling Prohibition, Poker Consumer Protection, and Strengthening [Unlawful Internet Gambling Enforcement Act] UIGEA Act of 2011
Designation:	HR 2366
Sponsor:	Joe L. Barton (R-TX) 06/24/11
Cosponsor:	19-D, 8-R (as of 04/02/12)

Section 104 of the bill requires each qualified state agency to conduct background checks and investigations of Internet poker licensees and all significant vendors, as well as any other person the state agency determines has a significant influence on the licensee applicant.

Bill Name:	Electronic Life Safety & Security Systems Federal Background Check Act of 2011
Designation:	HR 1331
Sponsor:	Blaine Luetkemeyer (R-MO) 04/01/11
Cosponsor:	5-D, 11-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 1939, Section 3 of the bill requires the AG to establish, within 180 days of enactment, a method to permit employers in the electronic life safety and security systems industry to access CHRI acquired under 28 U.S.C. § 534 and issue identification (ID) cards, valid for one year, to the employees in this industry. The Electronic Security Association would be designated as the channeling organization for such checks. The AG is authorized to set reasonable fees for conducting these background checks; however, the bill does not specify that the check will be fingerprint-based.

Bill Name:	Electronic Life Safety & Security Systems Federal Background Check Act of 2011
Designation:	S 1319
Sponsor:	Charles Schumer (D-NY) 06/30/11
Cosponsor:	0-D, 0-R (as of 04/02/12)

This bill is the Senate version of HR 1331. Section 4 of the bill requires the AG to establish, within 180 days of enactment, a method to permit employers in the electronic life safety and security systems industry to request a state and federal fingerprint-based background check. The bill allows employers to discover if employees have been convicted of a felony or an offense involving dishonesty or a false statement, or the use of force during the prior 10 year period. Employers may obtain a state and federal background check by submitting fingerprints to the AG through the relevant state criminal history record repository, or if the state declines to allow access, in a manner determined by the AG.

Bill Name:	Public Lands Service Corps Act of 2011
Designation:	S 896
Sponsor:	Jeff Bingaman (D-NM) 05/05/11
Cosponsor:	4-D, 1-R (as of 04/02/12)
Status:	**Reported in the Senate, as amended, 1/13/12**

Section 4(j) of the bill mandates that the requirements, of Section 189D(b) of the National and Community Service Act of 1990 (42 U.S.C. 12645g(b)), apply to each individual 18 years or older seeking to become a Corps participant; to receive funds under the Act; or to supervise or have regular contact with Corps participants. A Corps

participant is an individual, a resource assistant or consulting intern, enrolled in the Public Land Service Corps or the Indian Youth Service Corps. Unless exempt for good cause, Section 4(j) requires a criminal history check, which includes submission of fingerprints to the FBI for a national criminal history background check.

Bill Name:	WMD Prevention and Preparedness Act of 2011
Designation:	HR 2356
Sponsor:	Bill Pascrell (D-NJ) 06/24/11
Cosponsor:	4-D, 6-R (as of 04/02/12)

Section 406 of the bill amends 42 U.S.C. § 262a(e) by requiring the AG to coordinate with the Secretaries of Homeland Security, Defense, and State to determine if they have information relevant to the identification of an individual that is restricted from possessing, using, or transferring agents or toxins, or is reasonably suspected by a federal law enforcement or intelligence agency of certain crimes, involvement in particular organizations, or of being a foreign agent.

Bill Name:	Families Beyond Bars Act of 2011
Designation:	HR 2464
Sponsor:	Bobby L. Rush (D-IL) 07/08/11
Cosponsor:	13-D, 0-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 5747, this bill authorizes the AG to award grants to qualified organizations to carry out child-parent visitation programs of children with an incarcerated parent. The qualified program facilitators of these programs would be required to undergo a criminal background check; however, the bill does not specify how these checks will be conducted.

Bill Name:	Safeguarding America's Pharmaceuticals Act of 2011
Designation:	HR 3026
Sponsor:	Jim Matheson (D-UT) 09/22/11
Cosponsor:	0-D, 1-R (as of 04/02/12)

Section 8 of the bill requires mandatory background checks and fingerprinting of wholesale drug distributors facility managers and designated representatives. The bill does not specify how these will be conducted.

Bill Name:	National Parents Corps Act of 2011
Designation:	HR 3055
Sponsor:	John Lewis (D-GA) 09/23/11
Cosponsor:	1-D, 0-R (as of 04/02/12)

This bill was previously introduced in the 111th Congress as HR 3075. Section 5 of the bill requires that Parent Leaders employed to carry out the National Parents Corps Program have a fingerprint-based state and national criminal background check, a check of the child abuse and neglect registries, and a check of available sex offender registries.

Bill Name:	Stop Child Abuse in Residential Programs for Teens Act of 2011
Designation:	S 1667
Sponsor:	Tom Harkin (D-IA) 10/6/11
Cosponsor:	0-D, 0-R (as of 04/02/12)

Section 3 of the bill requires the DHHS to conduct a state check, a search of the NSOR, and an FBI fingerprint check, within 180 days of enactment, of staff members and volunteers having unsupervised contact with children and youth in covered programs. A covered program includes both public or private programs that provide a residential environment such as a wilderness or outdoor experience, boot camp, therapeutic board school, or behavioral modification programs.

Bill Name:	Stop Child Abuse in Residential Programs for Teens Act of 2011
Designation:	HR 3126
Sponsor:	George Miller (D-CA) 10/6/11
Cosponsor:	17-D, 0-R (as of 04/02/12)

Section 3 of the bill is identical to S 1667.

Bill Name:	Transportation Security Administration Authorization Act of 2011
Designation:	HR 3011
Sponsor:	Mike Roger (R-AL) 9/22/11
Cosponsor:	0-D, 5-R (as of 04/02/12)

Section 304 of the bill amends 6 U.S.C. 101 et. seq. by adding Section 2103 which prohibits a state or political subdivision from requiring a separate security threat assessment of an individual who possesses a valid hazardous materials transportation security credential, unless the state demonstrates a compelling need for a separate threat assessment.

Bill Name:	**Modernizing of Documentation & Elimination of Redundant Identification (MODERN) & Security Credentials Act**
Designation:	**HR 1690**
Sponsor:	**Mike Roger (R-AL) 05/03/11**
Cosponsor:	**0-D, 3-R (as of 04/02/12)**

Section 2 of the bill requires the DHS Secretary to, by rulemaking, consolidate and harmonize DHS' security threat assessment process for transportation workers in order to reduce redundant background checks. Section 5 of the bill amends the Homeland Security Act by adding Section 2103. This section prohibits a commercial motor vehicle operator licensed in Mexico or Canada from transporting security-sensitive materials in the U.S., unless a federal security background check had been conducted that is similar to those required for U.S. operators. Section 2104 is similar to Section 304 of HR 3011.

Bill Name:	Guardian Accountability and Senior Protection Act
Designation:	S 1744
Sponsor:	Amy Klobuchar (D-MN) 10/20/11
Cosponsor:	1-D, 0-R (as of 04/02/12)

Section 202 of the bill requires the AG to establish a pilot program to conduct background checks on prospective guardians and conservators. The appointing state court shall request the state and national background checks in accordance with procedures established by the participating state. The AG shall enter into agreements with not more than 5 states. The highest state court must have procedures where the prospective guardian or conservator may appeal the accuracy of the information in the background check, and must agree to obtain non-Federal contributions, toward the cost of carrying out the pilot program, in an amount equal to not less than $1 for each $4 of federal funds. A state that currently has a background check program in place will be eligible to participate.

Bill Name:	Democratizing Access to Capital Act of 2011
Designation:	S 1791
Sponsor:	Scott P. Brown (R-MA) 11/02/11
Cosponsor:	0-D, 2-R (as of 04/02/12)

Section 7 of the bill amends 15 U.S.C. § 780c(a)(4) by adding Section (G) which requires a background check on the issuer's principals.

Bill Name:	Capital Raising Online While Deterring Fraud and Unethical NonDisclosure (CROWDFUND) Act of 2011
Designation:	S 1970
Sponsor:	Jeffrey A. Merkley (D-OR) 12/8/11
Cosponsor:	3-D, 0-R (as of 04/02/12)

Section 2 of the bill amends 15 U.S.C. § 77a et. seq. by requiring the Securities and Exchange Commission to take measures to reduce fraud by obtaining criminal

background checks and a securities enforcement regulatory history check on each officer, director, and person holding more than 20 percent of the shares of the issuer.

Bill Name: District of Columbia Employee Suitability Act of 2011
Designation: HR 3285
Sponsor: Darrell Issa (R-CA) 10/31/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

This bill requires criminal background checks of individuals for appointment to excepted service in D.C. Such background checks will be conducted according to the Criminal Background Checks for the Protection of Children Act of 2004 and the corresponding regulations.

Bill Name: Medicare and Medicaid FAST Act
Designation: HR 3399
Sponsor: Peter Roskam (R-IL) 11/10/2011
Cosponsor: 14-D, 4-R (as of 04/02/12)

Section 302 of the bill requires a criminal background check of providers of services and suppliers who the DHHS Secretary determines present a high risk of waste, fraud, and abuse. The background screening will not duplicate any screening required under 42 U.S.C. 1395cc(j)(2), provider screening. The bill does not indicate how the background check will be conducted.

Bill Name: No official title given
Designation: HR 3404
Sponsor: Richard Hastings (R-WA) 11/14/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

Section 3 of the bill establishes a Director of Energy Safety within the Department of the Interior Ocean Energy Safety Service. The Director shall require that an individual hired as an inspection officer have an employment investigation that includes a criminal history record check.

Bill Name: Act for the 99%
Designation: HR 3638
Sponsor: Raul M. Grijalva (D-AZ) 12/13/11
Cosponsor: 21-D, 0-R (as of 04/02/12)

Section 1050 of the bill prohibits distribution of funds for school improvements, authorized under the bill, if a local educational agency does not have a policy that requires a criminal background check on all employees of the agency. The bill does not indicate how the background check will be conducted.

Bill Name:	21st Century Green High-Performing Public School Facilities Act
Designation:	HR 3490
Sponsor:	Ben Chandler (D-KY) 11/18/11
Cosponsor:	4-D, 0-R (as of 04/02/12)

Section 212 of the bill is identical to Section 1050 of HR 3638.

Bill Name:	Jeremy Bell Act of 2011
Designation:	HR 3766
Sponsor:	Michael G. Fitzpatrick (R-PA) 12/23/11
Cosponsor:	0-D, 4-R (as 04/02/12)

Section 3 amends the Elementary and Secondary Education act of 1965 by requiring that private or public elementary schools, local education agencies, and/or a state educational agency that receives funds have in effect policies that require every employee to undergo a fingerprint-based check of both state and national databases.

Bill Name:	**Private Security Officer Screening Improvement Act**
Designation:	**HR 4112**
Sponsor:	**Tom Marino (R-PA) 02/29/12**
Cosponsor:	**0-D, 0-R (as of 04/02/12)**

This bill amends Section 6402 of the Intelligence Reform Prevention Act of 2004 (codified at 28 U.S.C. 534 note) by permitting authorized employers of private security officers to submit fingerprints to a screening entity if the state of employment is a nonparticipating state. The screening entity will then submit the fingerprints to the AG for these individuals. A screening entity is defined as a private business, nonprofit organization, or individual authorized by the AG to submit, receive, and screen CHRI for purposes of a CHRI search pursuant to the Act. The AG shall provide the CHRI to the SIB or the screening entity, as applicable. If a state has no state standards, the SIB or the screening entity will use the criteria established under Section 6402. If a state has state standards the SIB or the screening entity will use the state standards.

Bill Name:	**Allowing Social Security to Electronically Screen for Suitability (ASSESS) Act**
Designation:	**S 2026**
Sponsor:	**Robert P. Casey, Jr. (D-PA) 12/16/11**
Cosponsor:	**0-D, 0-R (as of 04/02/12)**

Section 2 of the bill requires the AG and the FBI Director to provide the Commissioner of Social Security with access to CHRI contained in the NCIC-III, Wanted Person File, and any other files maintained by the NCIC that may be mutually agreed upon by the AG and the Commissioner. Access to this information will be provided by means of an extract of the files and for placement in the appropriate databases by the Commissioner. To obtain the full content of the CHRI, the Commissioner must submit fingerprints of the person, along with the appropriate fingerprint processing fee. The Commissioner will promulgate regulations within 12 months concerning the procedures for the taking of fingerprints and the use of the information.

Bill Name: **Home Care Consumer Bill of Rights Act**
Designation: **S 1750**
Sponsor: **Al Franken (D-MN) 10/20/11**
Cosponsor: **3-D, 0-R (as of 04/02/12)**

Section 301 of the bill amends 42 U.S.C. 3012(b) by requiring the DHHS to identify quality assurance standards for home and community-based long-term care programs and service providers. The standards include a background check of service providers, but the bill does not indicate how it will be conducted.

NICS/BRADY ACT:

Bill Name: Denying Firearms and Explosives to Dangerous Terrorists Act of 2011
Designation: S 34
Sponsor: Frank Lautenberg (D-NJ) 01/25/11
Cosponsor: 9-D, 0-R (as of 04/02/12)

This bill amends 18 U.S.C. § 922 by adding §§ 922A and 922B which authorize the AG to deny the transfer of a firearm or the issuance of firearms or explosives licenses or permits to known or suspected terrorists. The AG may also deny or revoke a Federal Firearm License (FFL) if the applicant is known or suspected of terrorism. Further, the AG may withhold the information, upon which the denial or revocation is based, from the licensee or applicant if such disclosure would compromise national security.

Bill Name: Denying Firearms and Explosives to Dangerous Terrorists Act of 2011
Designation: HR 1506
Sponsor: Peter T. King (R-NY) 04/13/11
Cosponsor: 35-D, 2-R (as of 04/02/12)

House version of S 34.

Bill Name: Gun Show Background Check Act of 2011
Designation: S 35
Sponsor: Frank Lautenberg (D-NJ) 01/25/11
Cosponsor: 13-D, 0-R (as of 04/02/12)

Previously introduced in the 111th Session as S 843, Section 2 of this bill amends Chapter 44 of Title 18 U.S.C. by adding Section 932. It would require gun show promoters to register and pay a fee to the AG and verify the identity of each participating vendor by valid photo ID. The bill requires all gun show firearm transfers to be accomplished through a licensed federal firearms dealer, including transfers between two unlicensed persons. Further, the bill requires all gun show transfers to be preceded by a National Instant Criminal Background Check (NICS). The bill also grants the AG the authority, without a warrant or reasonable cause, to enter a promoter's place of business or gun show during business hours to examine records and lists of the inventories of licensees conducting business at the gun show.

Bill Name: Gun Show Loophole Closing Act of 2011
Designation: HR 591
Sponsor: Carolyn McCarthy 02/09/11
Cosponsor: 13-D, 0-R (as of 04/02/12)

House version similar to S 35.

Bill Name: Firearms Interstate Commerce Reform Act
Designation: HR 58
Sponsor: Steve Scalise (R-LA) 01/05/11
Cosponsor: 23-D, 147-R (as of 04/02/12)

Title 18, U.S.C. § 922 states that authorized licensed importers, manufacturers, dealers, or collectors may not transfer firearms to any person who does not reside in the state in which the licensee's place of business is located with the exception of the sale or delivery of any rifle or shotgun. This bill extends this exception to apply to all firearms and out-of-state temporary locations of the business. Title 18, U.S.C. § 923 is also amended by removing the restriction that licensees must conduct business in the state specified on the license, authorizing these licensees to conduct business in temporary location in other states. Finally, the bill amends 18 U.S.C. § 921(b) to define an Armed Forces member's residence as the state of legal residence, permanent duty station, or the state where the member resides while commuting to the permanent duty station.

Bill Name: **Firearms Interstate Commerce Reform Act**
Designation: **S 1691**
Sponsor: **Mark Begich (D-AK) 10/12/11**
Cosponsor: **0-D, 1-R (as of 04/02/12)**

Senate version of HR 58.

Bill Name: Child Gun Safety and Gun Access Prevention Act of 2011
Designation: HR 227
Sponsor: Sheila Jackson Lee (D-TX) 01/07/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

Section 2 of the bill amends 18 U.S.C. 922(x) by prohibiting the transfer of handguns, semiautomatic weapons, or large capacity ammunition feeding devices to individuals less than 21 years of age.

Bill Name: Fire Sale Loophole Closing Act
Designation: HR 263
Sponsor: Gary Ackerman (D-NY) 01/12/11
Cosponsor: 31-D, 0-R (as of 04/02/12)

This bill amends 18 U.S.C. § 922 by making it unlawful, for an individual about whom the AG has made a determination to revoke a license to import, manufacture, or deal in firearms, to transfer the business inventory into the personal collection of an employee of that individual. Further, the revoked licensee may not transfer the business inventory to anyone else.

Bill Name: Large Capacity Ammunition Feeding Device Act
Designation: HR 308
Sponsor: Carolyn McCarthy (D-NY) 01/18/11
Cosponsor: 112-D, 0-R (as of 04/02/12)

This bill amends 18 U.S.C. § 922 by making it unlawful to transfer or possess a large capacity ammunition feeding device, but does not apply to devices lawfully possessed prior to enactment.

Bill Name: Large Capacity Ammunition Feeding Device Act
Designation: S 32
Sponsor: Frank Lautenberg (D-NJ) 01/25/11
Cosponsor: 10-D, 0-R (as of 04/02/12)

Senate version of HR 308.

Bill Name: Freedom to Serve Without Fear Act of 2011
Designation: HR 367
Sponsor: Laura Richardson (D-CA) 01/20/11
Cosponsor: 1-D, 0-R (as of 04/02/12)

This bill amends 18 U.S.C. § 922 by making it unlawful for a person to carry a firearm within 250 feet of an entrance to a building or structure where a Member of Congress is performing official duties or engaged in campaign activities. Such violations would carry a penalty of a fine and/or imprisonment of up to ten years. The restriction would not apply to on-duty or off-duty law enforcement officers.

Bill Name: Fix Gun Checks Act of 2011
Designation: S 436
Sponsor: Charles Schumer (D-NY) 03/02/11
Cosponsor: 4-D, 0-R (as of 04/02/12)

Section 102 of the bill requires that federal agencies certify that all records pertaining to 18 U.S.C. § 922(g) and (n) have been provided to the AG. Section 104 of the bill amends 18 U.S.C. § 921 by adding the definition of an unlawful user of controlled substance. Title II of the bill extends the Brady Law to cover all sales and transfers of firearms, including unlicensed transfers, which must be conducted through a licensed dealer or a law enforcement agency. A licensed dealer conducting the background check must comply with the same requirements as for all other sales and transfers. State or local law enforcement agencies conducting the transfers must conduct a background check through the NICS and comply with the same requirements as licensed dealers. A licensed dealer or law enforcement agency may collect a fee, not to exceed $15, for each firearm transfer processed.

Bill Name: Fix Gun Checks Act of 2011
Designation: HR 1781
Sponsor: Carolyn McCarthy (D-NY) 05/05/11
Cosponsor: 86-D, 0-R (as of 04/02/12)

House version of S 436.

Bill Name: Keep Kids Safe Act of 2011
Designation: HR 505
Sponsor: Jerrold Nadler (D-NY) 01/26/11
Cosponsor: 16-D, 0-R (as of 04/02/12)

This bill amends 18 U.S.C. § 922 by adding an additional NICS prohibitor, to include persons convicted of misdemeanor sex offenses against minors, for possession, sale, and disposition of firearms.

Bill Name: Bureau of Alcohol, Tobacco, Firearms, & Explosives Act of 2011
Designation: HR 1093
Sponsor: Steve King (R-IA) 03/15/11
Cosponsor: 23-D, 146-R (as of 04/02/12)

Section 202 of the bill amends 18 U.S.C. § 922(o) by requiring that every three years, the AG determine whether a person possessing a machine gun is prohibited by federal or state law from possessing or receiving a firearm based on information provided by the NICS and a fingerprint-based CHRI check.

Bill Name: Preventing Gun Violence Act
Designation: HR 1552
Sponsor: Steve Israel (D-NY) 04/14/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

This bill amends 18 U.S.C. § 922(g) by prohibiting the possession of a firearm by a person who has been adjudicated to have committed a violent juvenile act.

Bill Name: Trafficking Reduction and Criminal Enforcement (TRACE) Act
Designation: HR 1642
Sponsor: Mike Quigley (D-IL) 08/02/11
Cosponsor: 5-D, 0-R (as of 04/02/12)

Section 3 of the bill amends Section 511 of the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2010, by deleting provisions which prohibit the use of funds for any system that does not require the destruction of identifying information within 24 hours after the NICS determines and advises an FFL licensee that a person's possession or receipt of a firearm would not violate federal or state law.

Bill Name: Second Amendment Protection Act of 2011
Designation: HR 2615
Sponsor: Ron Paul (R-TX) 07/21/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

Section 2 of the bill repeals Public Law 103-159, the Brady Handgun Violence Prevention Act of 1993, which established the NICS.

Bill Name: Gun Trafficking Prevention Act of 2012
Designation: S 1973
Sponsor: Kirsten E. Gillibrand (D-NY) 12/08/11
Cosponsor: 4-D, 0-R (as of 04/02/12)

Section 7 of the bill amends 18 U.S.C. § 923 by requiring the AG to identify licensed firearms dealers who have a heightened risk of diverting firearms for criminal use. The AG may impose special conditions on such dealers, including a requirement that a firearm sale or transfer may not be completed until the NICS has informed the dealer that it may proceed.

Bill Name: **National Right-to-Carry Reciprocity Act of 2011**
Designation: **HR 822**
Sponsor: **Cliff Stearns (R-FL) 02/18/11**
Cosponsor: **35-D, 211-R (as of 04/02/12)**
Status: **Passed the House 11/16/11**

This bill amends 18 U.S.C. § 926 by adding Section 926D which authorizes a person who has a valid concealed firearm license or permit to possess or carry a concealed handgun in any other state that permits its residents to obtain a license or permit to carry a concealed firearm.

Bill Name: **Respecting States' Rights and Concealed Carry Reciprocity Act of 2012**
Designation: **S 2213**
Sponsor: **John Thune (R-SD) 03/20/12**
Cosponsor: **0-D, 34-R (as of 04/02/12)**

Senate version of HR 822.

SEX OFFENDER REGISTRY:

Bill Name: Holley Lynn James Act
Designation: HR 1517
Sponsor: Bruce Braley (D-IQ) 04/13/11
Cosponsor: 6-D, 2-R (as of 04/02/12)

Section 2 of the bill amends Chapter 3 of Title 10, U.S.C., by adding a new Section 130e. Among other things, this section requires the Department of Defense's Deputy Inspector General for Policy and Oversight to determine the feasibility of establishing a database to be known as the "Military Sexual Predator Database." The database under consideration could report and register sex offenders in the Armed Forces and coordinate information with the NSOR.

Bill Name: Sexual Assault Training Oversight and Prevention (STOP) Act
Designation: HR 3435
Sponsor: Jackie Speier (D-CA) 11/16/2011
Cosponsor: 119-D, 1-R (as of 04/02/12)

Section 6 of the bill establishes a Military Sexual Registry (MSR) database for reporting and maintenance of information regarding sexual assaults involving Armed Forces members. This would include information about the nature of the assault, victim, offender, and outcome of the legal proceedings. The Secretary of Defense is required to consult with the AG to ensure the MSR facilitates the reporting of relevant information of those individuals for inclusion in the NSOR. The MSR will include the name, alias, Social Security Number, address, license plate number, criminal history, DNA sample, current photograph, and any other information required by the Secretary.

Bill Name: International Megan's Law of 2009
Designation: HR 3253
Sponsor: Chris Smith (R-NJ) 10/24/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

This bill was previously introduced in the 111th Congress as HR 1623. Under this bill, individuals required to register under the Sex Offender Registration and Notification Act must report international travel to the DHS no later than 30 days prior to departure or arrival in the U.S. Individuals failing to report travel would be fined or imprisoned. The U.S. diplomat or consular mission in each foreign country would also be required to establish and maintain a countrywide nonpublic sex offender registry for sex offenders temporarily or permanently living in that country. Federal, state, local, tribal, and territorial law enforcement will have access for official purposes to all information in the sex offender registry maintained by the U.S. diplomat. The information would be transmitted to the NSOR.

IMMIGRATION:

Bill Name: Illegal Immigration Enforcement and Social Security Protection Act of 2011
Designation: HR 98
Sponsor: David Dreier (R-CA) 01/05/11
Cosponsor: 1-D, 12-R (as of 04/02/12)

Section 9 of the bill requires the Secretary of the DHS and the AG to integrate their fingerprint databases within two years of enactment.

Bill Name: CLEAR Act of 2011
Designation: HR 100
Sponsor: Marsha Blackburn (R-TN) 01/05/11
Cosponsor: 1-D, 64-R (as of 04/02/12)

Section 4 of the bill is identical to Section 904 of HR 1196.

Bill Name: LEAVE Act
Designation: HR 1196
Sponsor: Gary G. Miller (R-CA) 03/17/11
Cosponsor: 0-D, 7-R (as of 04/02/12)

Section 904 of the bill requires that, within 180 days of enactment, the DHS provide to the NCIC information on aliens (1) against whom final orders of removal have been issued; (2) who have entered into voluntary departure agreements; (3) who have overstayed their authorized period; and (4) whose visas have been revoked. Title 28, U.S.C. § 534(a) would also be amended to add "(4) acquire, collect, classify, and preserve records of violations of immigration laws of the United States, regardless of whether any such alien has received notice of the violation or whether sufficient identifying information is available with respect to any such alien and even if any such alien has already been removed from the United States; . . . ."

Bill Name: Keeping the Pledge on Immigration Act of 2011
Designation: HR 1274
Sponsor: Ed Royce (R-CA) 03/30/11
Cosponsor: 0-D, 14-R (as of 04/02/12)

Section 204 of the bill is similar to HR 100 and HR 1196. In addition, this bill also requires the Secretaries of State and Homeland Security, the Administrator of the Social Security Administration, the Commissioner of the Internal Revenue Service, the AG, and other federal agencies responsible for law enforcement to exchange records in accordance with 28 U.S.C. § 534. These records include visa applications and photographs, fingerprints, or other information obtained pursuant to the automated entry and exit control system.

Bill Name: Comprehensive Immigration Reform Act of 2011
Designation: S 1258
Sponsor: Robert Menendez (D-NJ) 06/22/11
Cosponsor: 10-D, 0-R (as of 04/02/12)

Section 111 of the bill requires that before the Secretary grants lawful prospective immigrant status to an alien, a background check be conducted utilizing biometric,

biographic, and other data to determine the existence of criminal, national security, or other factors that would render the alien ineligible for status. Section 112 requires a renewed background check before an alien with a lawful prospective immigrant status is adjusted to permanent resident status. Similar background checks are required under Section 143 and 145 for long-term residents who entered the U.S. as children and prior to removal of the conditional basis of a permanent resident status.

Bill Name:	Development, Relief, and Education for Alien Minors Act (DREAM) Act of 2011
Designation:	S 952
Sponsor:	Richard J. Durbin (D-IL) 05/11/11
Cosponsor:	32-D, 0-R (as of 04/02/12)

Section 3 of the bill authorizes the Secretary to cancel removal of, and adjust the status of, an alien who is inadmissable or deportable from the U.S. or is in temporary protected status if certain conditions are met. The Secretary may not grant permanent resident status on a conditional basis unless the alien submits biometric and biographic data, according to procedures to be established by the Secretary. The Secretary may also provide alternative procedures for applicants who are unable to provide this data because of a physical impairment. The biometric and biographic data will be used to conduct security and law enforcement background checks. Section 5 authorizes that the conditional basis permanent resident status may be removed if certain conditions are met, including submission of biometric and biographic data for a security and law enforcement background check. The Secretary will publish regulations within 180 days of implementing these sections.

Bill Name:	Development, Relief, and Education for Alien Minors Act (DREAM) Act of 2011
Designation:	HR 1842
Sponsor:	Howard L. Berman (D-CA) 05/11/11
Cosponsor:	78-D, 1-R (as of 04/02/12)

House version similar to S 952.

Bill Name:	The Adjusted Residency for Military Service (ARMS) Act
Designation:	HR 3823
Sponsor:	David Riversa (R-FL) 01/24/12
Cosponsor:	1-D, 0-R (as of 04/02/12)

Section 2 and 6 contain similar provisions to S 952 and HR 1842.

Bill Name:	Legal Agricultural Workforce Act
Designation:	HR 2895
Sponsor:	Daniel E. Lungren (R-CA) 09/12/11
Cosponsor:	0-D, 0-R (as of 04/02/12)

This bill requires a criminal background check of nonimmigrant agricultural workers prior to issuance of a visa. The bill does not specify how the background checks will be conducted.

NATIONAL CRIME INFORMATION CENTER:

Bill Name:	National Blue Alert Act of 2011
Designation:	HR 365
Sponsor:	Michael Grimm (R-NY) 01/20/11
Cosponsor:	25-D, 29-R (as of 04/02/12)

Section 4 of the bill requires the AG to assign an officer of the DOJ to act as the national coordinator of the Blue Alert communications network. The Coordinator is responsible for establishing voluntary guidelines for state's and local government's submission of information, relating to law enforcement officers who are seriously injured or killed in the line of duty, to the NCIC and the relevant state criminal information repository.

Bill Name:	National Blue Alert Act of 2011
Designation:	S 657
Sponsor:	Ben Cardin (D-MD) 03/28/11
Cosponsor:	8-D, 3-R (as of 04/02/12)
Status:	Reported in the Senate, as amended, 9/8/11

This bill is similar to HR 365.

Bill Name:	Help Find the Missing Act or Billy's Law
Designation:	HR 1300
Sponsor:	Chris Murphy (D-CT) 03/31/11
Cosponsor:	6-D, 2-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 3695, this bill authorizes the AG to maintain a public database, known as the National Missing and Unidentified Persons System (NamUs), which would contain missing persons records and unidentified remains cases. Section 3 of the bill requires the AG to provide information on missing and unidentified human remains, currently in the NCIC, to the NamUs database. Within one year, the AG, in consultation with the FBI, shall promulgate rules specifying the information to be shared, including Advisory Policy Board recommendations approved by the Director. The AG shall also provide grants to law enforcement agencies to facilitate the reporting of this information to the NCIC and NamUs databases.

Bill Name: Billy's Law
Designation: S 702
Sponsor: Joseph I. Lieberman (CT) 03/31/11
Cosponsor: 2-D, 0-R (as of 04/02/12)

Senate version of HR 1300.

UNIFORM CRIME REPORT:

Bill Name: Fighting Gangs and Empowering Youth Act of 2011
Designation: S 867
Sponsor: Robert Menendez (D-NJ) 05/03/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

Section 321 of the bill amends 28 U.S.C. § 534 by creating a separate Uniform Crime Report (UCR) category for juvenile offenses. For each fiscal year that a state or local government fails to comply, it shall not be eligible to receive those funds that may be allocated to the state or local government under the Act. Note that the reporting requirements may be waived if the action would be prohibited by the applicable state Constitution. The bill also requires the AG to develop a national strategy to coordinate, consolidate, and standardize all investigations by federal law enforcement agencies of crimes, reported in the UCR. The AG will also submit a report to Congress regarding this strategy.

Bill Name: Fighting Gangs and Empowering Youth Act of 2011
Designation: S 977
Sponsor: Robert Menendez (D-NJ) 05/12/11
Cosponsor: 1-D, 0-R (as of 04/02/12)

Section 321 of the bill is identical to S 867, with the exception of the report deadline.

Bill Name: Fighting Gangs and Empowering Youth Act of 2011
Designation: HR 1820
Sponsor: Frank Pallone, Jr. (D-NJ) 05/10/11
Cosponsor: 0-D, 0-R (as of 04/02/12)

House version similar to S 867 and S 977.

Bill Name: Violence Against Women Reauthorization Act of 2011
Designation: S 1925
Sponsor: Patrick J. Leahy (D-VT) 11/30/11
Cosponsor: 57-D, 8-R (as of 04/02/12)
Status: **Reported in the Senate, as amended, 03/12/12**

Section 808 of the bill requires the DHS Secretary to conduct a background check of the NCIC's Protection Order database on each petitioner for a visa. Any appropriate information obtained through this check shall be provided to the Secretary of State and shared with the beneficiary of the petition. The DHS Secretary will also create a cover sheet to accompany the information that is required to be provided to the visa applicant. This cover sheet will report whether the petitioner disclosed a protection order, restraining order, or criminal history information on the visa petition. Further, the applicant will be advised of criminal background, protection order, and other data reported in the multiple visa tracking databases.

Bill Name:	Illegal Alien Crime Reporting Act of 2011
Designation:	HR 3168
Sponsor:	Walter B Jones (R-NC) 10/12/11
Cosponsor:	0-D, 9-R (as of 04/02/12)

This bill requires that each state or federal agency or department that receives funds from DHS must compile statistics of persons arrested, charged or convicted of a crime, or incarcerated, including the immigration status and country of origin. The state must report these statistics monthly to the FBI.

Bill Name:	Hate Crimes Against the Homeless Statistics Act of 2011
Designation:	HR 3528
Sponsor:	Eddie Bernice Johnson (D-TX) 11/30/11
Cosponsor:	16-D, 1-R (as of 04/02/12)

Previously introduced in the 111th Congress as HR 3419, this bill amends the Hate Crime Statistics Act (28 U.S.C. § 534 note) by requiring the AG to collect data on crimes against the homeless.

Bill Name:	Human Trafficking Reporting Act
Designation:	HR 2982
Sponsor:	John Carter (R-TX) 09/21/11
Cosponsor:	34-D, 31-R (as of 04/02/12)

The bill amends 42 U.S.C. § 3755. Section 2 requires that data concerning "several forms of trafficking in persons," as defined in the Trafficking Victims Protection Act of 2000, be reported to the FBI. This data will be included in the Part 1 Violent Crimes Section of the UCR, which state and local governments receiving Byrne Justice Assistance grants are required to report to the FBI.

MISCELLANEOUS:

Bill Name: Second Chance for Ex-Offenders Act of 2011
Designation: HR 2065
Sponsor: Charles B. Rangel (D-NY) 06/01/11
Cosponsor: 9-D, 0-R (as of 04/02/12)

This bill amends Chapter 229 of Title 18 U.S.C. by adding a new Subchapter D. Subsection 3631 provides that an individual who has been convicted of a nonviolent offense, and fulfills certain requirements, may file a petition to expunge the record of the conviction. A nonviolent offense is defined as a misdemeanor or felony against the U.S. that does not include the use of a weapon or violence. Subsection 3635 authorizes the DOJ to maintain a nonpublic manual or computerized index of expunged records containing only the name and alphanumeric identifiers of the petitioner for expungement, and the agency, office, or department maintaining the expunged offense. This nonpublic index will not specify the expunged offense. The expunged records shall be made available to any prosecutor, law enforcement agency, or court which has responsibility for criminally investigating, prosecuting, or adjudicating the individual; state or local agencies that issue a license to possess a gun; or prospective city, state, or federal employers or agencies involved in investigating applicants for the position of police or peace officer, or prosecuting individuals under criminal or civil statutes.

Bill Name: Fresh Start Act of 2011
Designation: HR 2449
Sponsor: Steve Cohen (D-TN) 07/07/11
Cosponsor: 9-D, 0-R (as of 04/02/12)

This bill is similar to HR 2065.

The full text of any bill may be obtained by accessing http://thomas.loc.gov/.
The Legislative Update may also be accessed by going to the **Access Integrity Unit LEO Website:**

1. LEOSIGS
2. Unrestricted SIGS
3. CJIS
4. General Information
5. Access Integrity Unit Information
6. Legislative Update

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

STAFF PAPER

INFORMATIONAL TOPIC B

Integrated Automated Fingerprint Identification System (IAFIS) Enhancements Status

PURPOSE

To provide information and updates regarding the FBI's Criminal Justice Information Services (CJIS) Division's IAFIS enhancements.

AUTHOR

Travis L. Olson, (304) 625-2978

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 APB meeting, the APB approved the CJIS System Enhancement Strategy Group's (SESG's) proposal regarding the development of a process to manage the pending 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 the APB 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 APB members an opportunity at each meeting to reassign priorities and use the current list of enhancements for perspective with 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 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, Advisory Process 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.

The table below contains a list of IAFIS enhancements including pending and completed enhancements since the last round of APB meetings. The pending enhancements are in the order of priority level assigned by the APB.

The members are requested to:

1. Review the attached table regarding the IAFIS enhancements.

2. If a member believes that a priority level needs to be changed or an enhancement should be removed from the list, please provide input to be forwarded to the APB.

ENHANCEMENT		PRIORITY LEVEL	APPROVED BY APB	STATUS	TENTATIVE IMPLEMENTATION DATE
25	Allow for multiple Citizenship codes in IAFIS and amend the EFTS accordingly.	3H	12/04	Requirements complete.	Will be implemented as part of NGI Increment 4
26	Include Name and DOB fields and include the words "as submitted in the original transaction" to the SRE, ERRT and rap sheet responses.	3H	12/04	Requirements currently being developed.	Post NGI
27	Allow for single cycle sealing via fingerprint submissions	3M	12/05	Post NGI Post NGI	Phase II-Single Cycle Sealing - Post NGI Phase III-Sealing via Fingerprint Submissions - Post NGI
28	DNA flag for III DNA indicator	3M	12/05	Requirements complete.	Post NGI
29	Notate name or descriptive information from non-retain fingerprint submissions on FBI identification records	None assigned.	12/05	Requirements currently being developed.	Post NGI
30	Automation of manual name checks	3M+	12/05	Requirements complete.	Post NGI
34	Establishment of IAFIS Test Environment	3M	12/06	Post NGI	Post NGI
35	Establishment of the III Delete Record Cycle (DRC) and Modify Record Cycle (MRC) file maintenance messages	3M	12/06	Post NGI	Post NGI

ENHANCEMENT		PRIORITY LEVEL	APPROVED BY APB	STATUS	TENTATIVE IMPLEMENTATION DATE
36	Fraudulent Identity Caveat - Modify IAFIS response to indicate when there has been an exact match of the name, DOB, and SOC, but fingerprints do not match	3M	12/06	Requirements completed.	Post NGI
37	Utilize state records when states can respond for criminal justice purposes	3M	06/06	Requirements currently being developed.	Will be implemented as part of NGI Increment 4
40	IAFIS ULF Cascade Capabilities to Support Automated Searches for Retain and Non-retain Criminal and Civil Tenprint Transactions	None Assigned	06/07	Requirements completed.	Will be implemented as part of NGI Increment 3
41	Modification to IAFIS to support a new record retention schedule	3M	12/07	Requirements completed.	Will be implemented as part of NGI Increment 4
42	Modification to III to release deceased CHRI	3M	12/07	Post NGI	Post NGI
44	XML format in fingerprint transactions	None assigned	6/08	N/A	Will be implemented as part of NGI Increment 3/4
45	Online notification of criminal history record automation	3M	6/08	Requirements completed.	Post NGI
46	Automation of notifications for Want Notices that fail III edits	3M	12/07	N/A	Will be implemented as part of NGI Increment 4
47	Consolidation Notification to Arresting Agency	3M	12/08	Post NGI	Post NGI

	ENHANCEMENT	PRIORITY LEVEL	APPROVED BY APB	STATUS	TENTATIVE IMPLEMENTATION DATE
49	Foreign and Unknown Place of Birth Notifications to U.S. Immigration and Customs Enforcement (ICE) Law Enforcement Support (LESC)	3M	12/08	Requirements completed.	Will be implemented as part of NGI Increment 4
50	Expanded III Response to Point-of-Contact (POC) and Partial POC states	None assigned.	12/08	Post NGI	Post NGI
51	Eliminate the Requirement That States Submit Expungement Documentation to the FBI's CJIS Division as a Prerequisite to Expunging State-Maintained Criminal History Records (CHRs) from the III	3M	12/08	N/A	Will be implemented as part of NGI Increment 4
52	Return the Attention Field in III QH Responses	3M	06/2009	Post NGI	Post NGI
53	Department of Homeland Security (DHS)/Automated Biometric Identification System (IDENT) Fingerprint Identification Number (FIN) to be added to the Integrated Automated Fingerprint Identification System (IAFIS) Miscellaneous Number (MNU) field.		12/09	N/A	Will be implemented as part of NGI Increment 4 NGI will include a linking number, may be a different number and separate field than this enhancement proposes

Note - All implementation dates are dependant on the personnel resources allowed to implement the change(s). Depending on the negotiation of the NGI contract, the APB IAFIS enhancements may be implemented during the regular IAFIS Operation and Maintenance or they may be deferred to NGI.

The following table lists approved pending NCIC enhancements that will impact the IAFIS. These enhancements have been discussed by the appropriate subcommittee and working groups, then subsequently approved by the APB and the Director of the FBI. These enhancements are included on the NCIC Enhancement Status staff paper that is provided to the NCIC Subcommittee. The status of these enhancement are being provided in this staff paper for informational purposes only.

ENHANCEMENT		PRIORITY LEVEL	APPROVED BY APB	STATUS	TENTATIVE IMPLEMENTATION DATE
N-57A	Operational and Policy Changes For the Supervised Release File - create notice on CHRI when record contains FBI number	4M	06/02	Post NGI	Post NGI
N-93	Expand the Automatic NCIC Check Based on a Tenprint Submission (Hot Check) to 1 - include additional files and 2 - search Master Name from ident record if different from submitted name	2M	12/05	1-Complete - All Identified NCIC Person Files are now searched 2-Post NGI	2-Post NGI
N-99	Create Missing Person Notice on CHRI when NCIC record includes an FBI Number	N/A	06/06	Post NGI	Post NGI
N-125	Create Immigration Violator Notice on CHRI when NCIC record contains an FBI Number	3H	06/07	Post NGI	Post NGI

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

STAFF PAPER

INFORMATIONAL TOPIC C

National Crime Prevention and Privacy Compact (Compact) Council (Council) Update

PURPOSE

To summarize the recent activities and initiatives of the Council.

AUTHOR

Ms. Anissa C. Drabish

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>.

DISCUSSION

The Council held its fall meeting on December 8-9, 2011, in Albuquerque, New Mexico. The following is an update on the number of party states, Memorandum of Understanding (MOU) signatory states, and National Fingerprint File (NFF) Program participants, as well as some of the initiatives the Council is currently addressing.

Compact Signatories - Twenty-nine states and the federal government have enacted the Compact. The following are the Compact states in the order that they enacted the legislation: Montana, Georgia, Nevada, Florida, Colorado, Iowa, Connecticut, South Carolina, Arkansas, Kansas, Oklahoma, Maine, Alaska, New Jersey, Minnesota, Arizona, Tennessee, North Carolina, New Hampshire, Missouri, Ohio, Maryland, Wyoming, Idaho, Oregon, West Virginia, Hawaii, Michigan, and Vermont.

National Fingerprint File (NFF) Update - On October 9, 2011, Minnesota became the fifteenth state to participate in the NFF program. Current participants include: Colorado, Florida, Georgia, Hawaii, Idaho, Kansas, Maryland, Minnesota, Montana, New Jersey, North Carolina, Oklahoma, Oregon, Tennessee, and Wyoming. It is anticipated that Ohio and Missouri will become NFF participants in early 2012. Additionally, West Virginia and Vermont have both approximated participation in mid 2012. In 2011, NFF on-site assessments were conducted at the Arizona Department of Public Safety, the Iowa Division of Criminal Investigation Bureau of Identification, and the Michigan State Police.

MOU Signatories – Currently, 11 nonparty states/territories have signed the Council's MOU as a voluntary recognition of the Council's authority to promulgate rules, procedures, and standards for the noncriminal justice use of the Interstate Identification Index (III) system. The 11 MOU signatories are Illinois, Kentucky, Mississippi, North Dakota, Nebraska, New Mexico, South Dakota, American Samoa, Guam, Virginia, and Puerto Rico.

Elections - The following Council members were re-elected to serve a two-year term as the Chair and Vice Chair of the Council:

Chair: Liane M. Moriyama, Hawaii Criminal Justice Data Center
Vice Chair: Jeffrey R. Kellett, New Hampshire Department of Safety

Compact Ratification and NFF Program Brochures - The Council has been focusing efforts on outreach, increasing Compact ratification, and ultimately NFF participation. With that, the Planning and Outreach Committee of the Council wanted a high-level informational pamphlet that could be utilized to market Compact ratification and NFF participation to Chief Administrators, legislators, Attorney Generals, and the like. Since some states have not ratified the Compact, which is a step toward NFF participation, it was determined that rather than a single informational pamphlet, each topic deserved its own marketing material to accommodate differing audiences. At the December 2011 Council meeting, Council approved the Compact ratification and the NFF participation brochures for distribution. In a continuing effort to be environmentally-friendly, the brochures will be available on the Compact Council's website.

Report on NFF Implementation Plans - At the November 2010 Council meeting, Council approved a motion that each non-NFF Compact state will create its own NFF implementation plan. Examples of items to be included in an NFF implementation plan are: host an NFF on-site, identify ways to obtain funding for required system changes, and methods to include NFF changes when upgrading or replacing systems. The

Standards and Policy Committee will be reviewing and assessing the plans at the Spring 2012 Committee meeting.

Changes to the Outsourcing Standard - As background, the Management Control and Outsourcing Standard (Outsourcing Standard) for Channelers and Non-Channelers requires adequate security and privacy of criminal history record information (CHRI) that has been provided to a Contractor that is performing administrative functions for an Authorized Recipient. Both the Outsourcing Standard for Channelers and the Outsourcing Standard for Non-Channelers require that audits be conducted by Authorized Recipients, the states, and the FBI at various intervals. Section 2.05 of each Standard stipulates that the audit timeline begins with a 90-day audit of the Contractor by the Authorized Recipient (for non-channelers) or the FBI (for Channelers).

Section 2.05 includes a reference to "the terms of the contract" as a trigger for the 90-day audit requirement. The purpose of the 90-day audit requirement is for the Authorized Recipient to establish an initial baseline assessment of a Contractor's compliance in an effort to identify and correct shortfalls prior to entering into the longer-term triennial audit cycle. As written, the 90-day audit requirement could be interpreted as being triggered by any change in the terms of a contract between the Authorized Recipient and the Contractor. By associating the trigger with the approval to outsource rather than the terms of the contract, 90-day baseline assessments would only occur when there is increased risk for potential compliance issues due to the contractor performing a new function(s) or a new contractor performing the function(s).

As such, the Council approved a motion to associate the audit trigger directly to the approved outsourcing request rather than to the terms of the contract. The revision will be incorporated into both of the Outsourcing Standards. The specific changes to Section 2.05, as well as footnote 2, include striking the phrase, "terms of the contract," and replacing it with the phrase, "approved outsourcing agreement."

SEARCH Update - The National Consortium for Justice Information and Statistics (SEARCH) provided an overview of the results of the 2010 Survey of the State Criminal History Information Systems. The survey provides a snapshot of continuing growth, ongoing improvements, and practices associated with the initiation and updating of state held criminal history records. Additionally, SEARCH provided results from the Survey of State Policies Requiring Electronic Capture of Fingerprints. This survey identified issues or difficulties that arose following implementation of an all electronic fingerprint submission policy. Finally, SEARCH presented an update on the Repository Records and Reporting Quality Assurance Program.

Update on the Implementation of the Centers for Medicare and Medicaid Services' (CMS) National Background Check Program - As background, Section 6201 of the Patient Protection and Affordable Care Act (PPACA), Public Law 111-148, requires the Secretary of the United States Department of Health and Human Services to establish a program for long-term care facilities and providers to conduct nationwide background checks on prospective direct patient access employees. States and territories must apply to become a program participant and obtain federal matching grant funding.

At the December 2011 Council meeting, the CMS announced that over $38.6 million dollars in grants have been awarded to 16 states and the District of Columbia. A fifth solicitation was issued in November 2011. States and territories were encouraged to apply by the February 28, 2012, deadline.

As part of the grant program, the CMS hosts periodic training conferences for grantee states and also invites applicant states and states that are interested in applying for the grant. The 3rd National Conference is tentatively scheduled for May 8-10, 2012, in Salt Lake City, Utah.

Rap Back Focus Group Update - As background, the Rap Back Task Force (Task Force) was created by the Council in 2009 to assist in the identification of user requirements for the Rap Back Service. With the completion of the Rap Back service design, the Council requested the reengagement of the Task Force. In order to concentrate on operational and policy impacts related to the Rap Back implementation, the Task Force was reconstituted into a 13 member Focus Group.

The Focus Group held its first meeting via conference call in June 2011. The Focus Group then met in Clarksburg, West Virginia, on November 8-9, 2011. The agenda included an overview of the States' rap back programs, discussion on current rap back service features and rap back requirements, a review of the draft Rap Back Executive Concept of Operations, discussion on validation and pre-notification services as they relate to privacy, and an overview of the conceptual services. The meeting provided a forum for the Focus Group, Next Generation Identification Program Office staff, and various Criminal Justice Information Services (CJIS) Division staff to discuss current and emerging issues relating to the development of a national rap back solution.

Frequently Asked Questions of State Agencies – At the September 2010 Standards and Policy Committee meeting, the Committee discussed the challenges faced when instructing agencies on the proper access and use of the Interstate Identification Index (III) system for noncriminal justice purposes and responding to their inquiries. As a result, states are looking for innovative ways to share information.

At the May 2011 Council meeting, the Standards and Policy Committee's Report from its March 2011 meeting provided the Council with discussion points and potential solutions for enhancing standardization and consistency of implementing rules and procedures relating to noncriminal justice access to and use of CHRI. The Council discussed the information and, as an alternative, requested that the FBI's CJIS Division staff compile a list of frequently asked questions from agencies which would be discussed at the September 2011 Committee meeting.

During the September 2011 Committee meeting, the Committee reviewed the list of frequently asked questions and identified a LEO SIG as an appropriate forum to host the information. The Committee recommended, and the Council endorsed, creating a LEO SIG to post frequently asked questions that have been vetted by the Committee and will include a caveat which states that the information is not an official opinion of the FBI. The first round of vetting will occur at the Spring 2012 Committee meeting.

White House National Security Staff Update - As background, the White House National Security Staff (NSS) hosted a meeting in April 2011, of the Information Sharing and Access (ISA) Interagency Policy Committee (sub-IPC) regarding expanded access to the National Crime Information Center and the III. Since then, subsequent meetings have been held by the NSS concerning requests by other federal agencies for expanded access to FBI-maintained systems, specifically the III, and solutions for obtaining this access. One of the recommendations provided to the NSS was that topic papers would be presented to both the FBI CJIS Advisory Policy Board (APB) and the Council regarding their requests.

On September 20, 2011, the Council's Executive Committee, along with representation from the APB, met in Pittsburgh, Pennsylvania with the federal agency representatives that are requesting expanded access. The agencies, which included the Department of Homeland Security, the U.S. Citizenship and Immigration Services, the U.S. Customs and Border Protection, the Transportation Security Administration, the Office of Personnel Management, the Department of State, and the Federal Aviation Administration, each presented case scenarios in which the expanded access would have been useful. The Executive Committee considered the information and determined that the Council was committed to working with the agencies to provide appropriate access where it was legally permissible. The federal agencies were asked to formalize the request and present the information at the Spring 2012 APB and Council meetings.

National Background Check System Task Force Update - As the volume of legislative initiatives requiring a national fingerprint-based background check increases, valuable

criminal history information found at the state level may not be provided. In response, the Council established the National Background Check System Task Force (NBCS Task Force) which is responsible for identifying core issues and defining a recommended scope of action for a national solution.

The NBCS Task Force, chaired by Terry Gibbons from the Georgia Bureau of Investigation, held its inaugural meeting on September 20, 2011. The NBCS Task Force determined that the most comprehensive criminal history record for noncriminal justice purposes would be achieved through Compact ratification and NFF participation. With that, the NBCS Task Force is exploring options to increase NFF participation. Options include alternative methodologies for NFF participation and a potential reimbursement arrangement for NFF participating states. The goal is to present these options in a topic paper from the NBCS Task Force to the Standards and Policy Committee for consideration at the Spring 2012 Committee meeting.

Future Compact Council Meetings - The next Standards and Policy Committee meeting is scheduled for March 21, 2012, and the Planning and Outreach Committee meeting is scheduled for March 22, 2012. Both Committee meetings will be held in Clarksburg, West Virginia. The next Council meeting is tentatively scheduled for May 16-17, 2012, and the location is yet to be determined. Please be reminded that all Council meetings are open to the public, with prior meeting notices published in the Federal Register. Representatives from state and federal agencies are invited to attend Council meetings to become more familiar with the issues addressed by the Council.

For additional information on upcoming Council meetings or any Council initiative, please contact Compact Council Chairman Liane Moriyama at (808) 587-3110 or electronically at <lmoriyam@hcjdc.hawaii.gov> or the FBI Compact Officer Gary S. Barron at (304) 625-2803 or electronically at <gary.barron@leo.gov>.

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

STAFF PAPER

INFORMATIONAL TOPIC D

Notification of Revised Fee Schedule

PURPOSE

To provide details regarding the Criminal Justice Information Services (CJIS) fee schedule change effective March 19, 2012.

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>.

DISCUSSION

The details regarding the fee schedule change are provided via the CJIS Information Letter, issued January 3, 2012. A copy of the document is provided as an attachment.

CJIS Information Letter **January 3, 2012**

Notification of Revised Fee Schedule for Fingerprint-based Criminal History Record Information Checks

In July 2011, the Criminal Justice Information Services (CJIS) Division announced the anticipation of an adjustment to the current fee schedule. This adjustment was publicized on December 20, 2011, via a **N**otice in the *Federal Register*. The revised rates will become effective March 19, 2012. The purpose of this letter is to provide details of the fee change.

WHY THE CJIS DIVISION IS REVISING THE USER FEES

The user fee structure for fingerprint-based and name-based Criminal History Record Information (CHRI) checks was last adjusted in 2007. Pursuant to Title 28, *Code of Federal Regulations,* Part 20.31, the Director of the FBI shall review the amount of the fee periodically. The FBI conducted an analysis to determine the cost associated with providing fingerprint-based and name-based CHRI checks based on the criteria in the Office of Management and Budget Circular A-25, User Charges. To help accomplish this analysis, the FBI contracted with an independent consulting firm. The results of this analysis are the basis for the revised user fees.

CHANGES TO THE FEE SCHEDULE

For all users, the only change will be a reduction in the fingerprint-based CHRI rates. **N**ame-based CHRI rates remain unchanged.

WHAT DOES NOT CHANGE

The categories of fee classes (different types of transactions), both fingerprint-based and name-based CHRI checks, remain unchanged. The current business practice for those federal, state, and nongovernmental entities that submit fingerprint-based CHRI checks and function as *de facto* centralized billing service providers (CBSPs) remains unaffected. The CJIS Division will continue the practice of allowing approved CBSPs to retain a portion of the user fees as reimbursement for this centralized billing service. (The reimbursement amount will remain at $2.) For these purposes, federal agencies should remit the CBSP amount shown on the following fee schedule.

PROCEDURAL GUIDELINES FOR BILLING

Please note that the FBI bills based upon transaction completion as opposed to transaction receipt. The FBI will make every attempt to process all received transactions prior to the fee change on March 19, 2012.

CURRENT AND REVISED USER FEES

The current and revised user fee rates are:

Fingerprint-based CHRI Checks				
Service	**Current Fee**	**Current Amount Remitted to FBI by Central Billing Service Providers (CBSP)*** **	**Revised Fee (effective March 19, 2012)**	**Revised Amount (effective March 19, 2012) Remitted to FBI by CBSPs*** **
Electronic	$19.25	$17.25	$16.50	$14.50
Electronic In / Manual Out*	$26	$24	$23.25	$21.25
Manual	$30.25	$28.25	$27.50	$25.50
Volunteer**	$15.25	$13.25	$15	$13
Name-based CHRI Checks (available only to federal agencies with specific statutory authority)				
Service	**Current Fee**	**Current Amount Remitted to FBI by CBSPs*** **	**Revised Fee (effective March 19, 2012)**	**Revised Amount (effective March 19, 2012) Remitted to FBI by CBSPs*** **
Manual	$6	$6	$6	$6
Electronic	$2.25	$2.25	$2.25	$2.25

*Available only when authorized. Only non-federal users have requested this service to date; federal and non-federal users may request authorization under revised schedule.

**Fingerprint submissions for volunteer positions must be authorized under the National Child Protection Act, as amended by the Volunteers for Children Act, Title 42, *United States Code*, Section 5119a(e).

***CBSPs remit full fee. The amount the FBI allows billed agencies to retain to offset their handling costs apply only to fingerprint-based CHRI checks.

Fingerprint contributors with specific questions regarding their fees should contact the centralized billing service provider to which they submit fingerprints. A contact list follows. For general questions or comments regarding this notification, please contact the Fee Programs Unit at <feeprogramsunit@leo.gov> or at (304) 625-2360.

STATE CONTACTS

Alabama Bureau of Investigation
Department of Public Safety
Post Office Box 1511
Montgomery, AL 13102-1511
(334) 242-4322

Criminal Records and Identification Bureau
Department of Public Safety
5700 East Tudor Road
Anchorage, AK 99507-1225
(907) 269-5511

Criminal History Records Section
Arizona Department of Public Safety
Post Office Box 6638
Phoenix, AZ 85005-6638
(602) 223-2000

State Identification Bureau
Arkansas State Police
One State Police Plaza Drive
Little Rock, AR 72209
(501) 618-8000

Bureau of Criminal Identification and Information
California Department of Justice
Room G-118
4949 Broadway
Sacramento, CA 95820-1528
(916) 227-3854

Colorado Bureau of Investigation
Suite 3000
690 Kipling Street
Denver, CO 80215-8001
(303) 239-4442

Criminal Justice Information Systems Section
Connecticut Bureau of Identification
Department of Public Safety
1111 Country Club Road
Middletown, CT 06457
(860) 685-8441

Delaware State Bureau of Identification
Post Office Box 430
Dover, DE 19903-0430
(302) 739-5961

Metropolitan Police Department
Room 168
300 Indiana Avenue, NW
Washington, DC 20001-2188
(202) 406-5773

Criminal Justice Information Services
Florida Department of Law Enforcement
Post Office Box 1489
Tallahassee, FL 32302-1489
(960) 410-7000

Georgia Crime Information Center
Georgia Bureau of Investigation
Post Office Box 370748
Decatur, GA 30037-0748
(404) 244-2600

Marshal Division
Judicial Center
120 West O'Brien Drive
Agana, GU 96910
(671) 475-3106

Hawaii Criminal Justice Data Center
Department of the Attorney General
Kekuanao'a Building
465 South King Street
Honolulu, HI 96813-2911
(808) 587-3100

Bureau of Criminal Identification
Idaho State Police
Post Office Box 700
Meridian, ID 83680-0700
(208) 884-7000

Bureau of Identification
Illinois State Police
260 North Chicago Street
Joliet, IL 60432-4072
(815) 740-2742

Indiana State Police
Room N340
Indiana Government Center North
100 North Senate Avenue
Indianapolis, IN 46204
(317) 232-8250

Iowa Division of Criminal Investigation
First Floor
Wallace State Office Building
215 East Seventh Street
Des Moines, IA 50319
(515) 281-7006

Kansas Bureau of Investigation
1620 Southwest Tyler Street
Topeka, KS 66612
(785) 296-8200

Criminal Identification and Records Branch
Kentucky State Police
1250 Louisville Road
Frankfort, KY 40601-1907
(502) 227-2221

Bureau of Criminal Identification and Information
Louisiana State Police
Department of Public Safety
Post Office Box 66614, Mail Slip A-6
Baton Rouge, LA 70896-6614
(225) 925-6095

Maine State Bureau of Identification
Maine State Police
42 State House Station
Augusta, ME 04333-0042
(207) 624-7200

Maryland Department of Public Safety and Correctional Services
Post Office Box 5743
Pikesville, MD 21282-2708
(410) 764-4501

State Identification Section
Massachusetts State Police
59 Horse Pond Road
Sudbury, MA 01776
(508) 358-3170

Criminal Justice Information Center
Michigan State Police
7150 Harris Drive
Lansing, MI 48913
(517) 322-5531

Criminal Justice Information System
Minnesota Department of Public Safety-BCA
1430 Maryland Avenue East
St. Paul, MN 55106
(651) 793-7000

Criminal Information Center
Mississippi Department of Public Safety
Post Office Box 958
Jackson, MS 39205-0958
(601) 933-2600

Criminal Records and Identification Division
Missouri State Highway Patrol
Post Office Box 9500
Jefferson City, MO 65102-9500
(573) 526-6153

Criminal Justice Information Services Bureau
Information Technology Services Division
Montana Department of Justice
Post Office Box 201406
Helena, MT 59620-1406
(406) 444-2026

Criminal Identification Division
Nebraska State Patrol
State House Station
Post Office Box 94907
Lincoln, NE 68509-4907
(402) 471-4545

Division of Records/Technology
Nevada Department of Public Safety
808 West Nye Lane
Carson City, NV 89703
(775) 684-6222

Division of State Police
New Hampshire Department of Safety
33 Hazen Drive
Concord, NH 03305
(603) 271-2575

State Bureau of Identification
New Jersey State Police
Post Office Box 7068
West Trenton, NJ 08628-0068
(609) 882-2000

Law Enforcement Records Bureau
Department of Public Safety
Post Office Box 1628
Santa Fe, NM 87504-1628
(505) 827-9181

Office of Criminal Justice Operations
New York State Division of Criminal Justice Services
4 Tower Place
Albany, NY 12203-3702
(800) 262-3257

North Carolina State Bureau of Investigation
Post Office Box 29500
Raleigh, NC 27626-0500
(919) 716-6411

Bureau of Criminal Investigation
North Dakota Office of the Attorney General
Post Office Box 1054
Bismarck, ND 58502-1054
(701) 328-2210

Ohio Bureau of Criminal Identification and Investigation
Post Office Box 365
London, OH 43140-0365
(740) 845-2000

Criminal Identification Section
Information Services Division
Oklahoma State Bureau of Investigation
6600 North Harvey
Oklahoma City, OK 73116-7912
(405) 848-6724

Identification Services Section
Oregon State Police
3772 Portland Road NE
Salem, OR 97301
(503) 378-3070

Bureau of Records and Identification
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110
(717) 783-5599

Technical Service Bureau
Police of Puerto Rico
G.P.O. Box 70166
San Juan, PR 00936
(787) 729-2121

Bureau of Criminal Identification
Department of Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400

Criminal Justice Records Section
South Carolina Law Enforcement Division
Post Office Box 21398
Columbia, SC 29221-4012
(803) 896-1446

South Dakota Division of Criminal Investigation
Suite 5
Mickelson Criminal Justice Center
1302 East Highway 14
Pierre, SD 57501
(605) 773-3331

Records and Identification Section
Tennessee Bureau of Investigations
901 RS Gass Boulevard
Nashville, TN 37216-2639
(615) 744-4008

Administration Division
Texas Department of Public Safety
Post Office Box 4143
Crime Records Building G
Austin, TX 78765-4143
(512) 424-2077

Utah Bureau of Criminal Identification
Post Office Box 148280
Salt Lake City, UT 84114-8280
(801) 965-4445

Vermont Criminal Information Center
Vermont Department of Public Safety
103 South Main Street
Waterbury, VT 05671-2101
(802) 244-8727

Criminal Justice Information Services
Virginia State Police
Post Office Box 27472
Richmond, VA 23261-7472
(804) 674-4605

Criminal Justice Records Improvement
Law Enforcement Planning Commission
8172 Subbase
St. Thomas, VI 00802-5803
(340) 774-6400

Criminal Records Division
Washington State Patrol
Post Office Box 42619
Olympia, WA 98504-2619
(360) 705-5100

Criminal Records Section
West Virginia State Police
725 Jefferson Road
South Charleston, WV 25309-1698
(304) 746-2100

Crime Information Bureau
Wisconsin Department of Justice
Post Office Box 2718
Madison, WI 53701-2718
(608) 266-7314

Criminal Justice Information Section
Division of Criminal Investigation
Rogers Building
316 West 22nd Street
Cheyenne, WY 82002
(307) 777-7181

FEDERAL CONTACTS

U.S. Bureau of Customs and Border Protection
7375 Boston Boulevard
Springfield, VA 22153
(703) 354-1000

Law Enforcement Support Center
U.S. Immigration and Customs Enforcement
188 Harvest Lane
Williston, VT 05495
(802) 872-6000

Air Force Office of Special Investigations Headquarters
Suite AA-323
1535 Command Drive
Andrews Air Force Base, MD 20762-7000
(240) 857-5911

U.S. Secret Service
950 H Street, NW
Washington, DC 20223-0001
(202) 406-8000

Federal Investigative Services Division
U.S. Office of Personnel Management
Post Office Box 618
Boyers, PA 16020-0618
(724) 794-2005

Coast Guard Investigative Service
U.S. Coast Guard
4200 Wilson Boulevard
Arlington, VA 22203
(202) 493-6600

Department of State
1801 North Lynn Street
Washington, DC 20522-2008
(202) 647-4000

Crime Records Division
U.S. Army Crime Records Center
6010 Sixth Street
Fort Belvoir, VA 22060
(703) 806-0422

Naval Criminal Investigative Service
Washington Navy Yard Code 0115C
716 Sicard Street, SE
Washington Navy Yard, DC 20388-5380
(202) 433-3853

U.S. Postal Inspection Service
Security Investigations Service Center
4th Floor
225 North Humphreys Blvd.
Memphis, TN 38161-001
(901) 747-7757

U.S. Department of Justice
600 E Street, NW
Washington, DC 20530
(202) 514-2000

As of April 15, 2012, the FBI will no longer process hard copy fingerprint cards for civil or criminal submissions

In July 1999, the FBI implemented the Integrated Automated Fingerprint Identification System (IAFIS) to electronically process civil and criminal fingerprint submissions, thus speeding up processing and response times. In the past 2 years, the FBI has encouraged all agencies to modify any remaining manual processes and implement full electronic capabilities for current and resubmitted fingerprint transactions. As a result, the FBI has received fewer hard copy fingerprint cards for processing.

Beginning on Sunday, April 15, 2012, the FBI will no longer accept hard copy fingerprint cards or hard copy biometrics such as palmprints. The FBI realizes that some agencies will need an alternate method to submit hard copy fingerprints after that date. Agencies that need an alternate method can:

- Update current processing at the local and/or state agencies.
- Submit fingerprints through a channeling agency that has access to the IAFIS.
- Submit criminal fingerprints through a federal agency via the Joint Automated Booking System.
- Submit civil fingerprints through a federal agency via the Civil Applicant System.

For more information, please contact the CJIS Division's Customer Service Group (CSG) by telephone at (304) 625-5590.

The National Child Protection Act/Volunteers for Children Act

In *CJIS Information Letters* 99-3 (dated December 1, 1999) and 01-2 (dated January 26, 2001), the CJIS Division provided information regarding the IAFIS and fingerprint submissions for the National Child Protection Act/Volunteers for Children Act (NCPA/VCA). As a follow up, the CJIS Division would like to reiterate the procedures for processing NCPA/VCA submissions via the IAFIS.

When an agency submits a civil fingerprint for processing via the IAFIS, the agency must use the Type of Search (TSR) of V for volunteer positions directly related to the care of children, the elderly, or individuals with disabilities. If an agency submits an incorrect TSR or User Fee Billing code, an incorrect fee may be applied to the user fee bill.

If an agency submits a civil fingerprint with a TSR of V, the agency must specify either the NCPA/VCA or a state statute in the Reason Fingerprinted (RFP) Field. The RFP Field is a mandatory, alphanumeric field provided to indicate the purpose of a civil fingerprint submission is related to criminal justice employment or noncriminal justice licensing and employment pursuant to a state statute approved by the FBI or authorized by federal legislation or executive order.

To receive the billing rate for volunteer positions, agencies must include the word "volunteer" and the state or federal statutory authority in the RFP Field. Examples include: "NCPA/VCA—volunteer" or "National Child Protection Act/Volunteers for Children Act—volunteer." Please note that volunteer firefighters do **not** qualify for the volunteer billing rate (emphasis added).

For additional information regarding the NCPA/VCA, agencies should contact the CJIS Division's CSG by telephone at (304) 625-5590.

Tools available to help participants with the Interstate Identification Index and National Fingerprint File

The CJIS Division provides operational and technical assistance to participants of the Interstate Identification Index (III) and the National Fingerprint File (NFF) Program by:

- Researching and analyzing proposed changes to the III/NFF system and making recommendations to the CJIS Division's executive management, the CJIS Advisory Policy Board, and the National Crime Prevention and Privacy Compact Council.

- Providing technical and operational assistance to local, state, and federal agencies on the use and operation of the III/NFF system.

- Providing technical and operational assistance to states that are working toward or upgrading their III and NFF participation.

- Performing record updates and modifications to criminal history records as requested by state and federal criminal justice agencies.

Recently, the CJIS Division added two new tools to assist users in obtaining information regarding the III and NFF Programs.

First, agencies that need III or NFF assistance may submit inquiries to the newly established e-mail at <iii.nff.assistance@listserv.leo.gov> or call the III/NFF assistance line at (304) 625-3652. Analysts are available from 6:30 a.m. to 5:30 p.m. Eastern time to answer questions and provide assistance.

Second, agencies can visit the unrestricted Special Interest Group for the III and NFF Programs on the Law Enforcement Online (LEO) at <https://www.leo.gov/http://leowcs.leopriv.gov/lesig/cjis/programs/iii/>.

CJIS Information Letters available on the Law Enforcement Online

CJIS Information Letters are available via the Internet on the LEO at <https://www.leo.gov/http://leowcs.leopriv.gov/lesig/cjis/general_information/newsletters/information_letter/> or by clicking on:

- SIGs
- Unrestricted
- CJIS
- General Information
- CJIS Informational Letters

Users with questions concerning access to the LEO should contact the LEO Help Desk by telephone at (888) 334-4536.

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

STAFF PAPER

INFORMATIONAL TOPIC E

Integrated Automated Fingerprint Identification System (IAFIS) Status Report

PURPOSE

The purpose of this paper is to report the operational status of the IAFIS and to provide related information.

POINT OF CONTACT

Charles E. Ware, 304-625-5455, charles.ware@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

Report completed: Wednesday, December 21, 2011

This report covers the following IAFIS related topics:

- Tenprint Fingerprint Identification Services
- Change in IAFIS performance reporting for FY 2012
- Latent Fingerprint Services
- Palmprint and Iris Projects
- Border Security
- BSS Unit Spotlight
  - Process Improvement Team (PIT)
  - Latent Investigative Services Team (LIST)
- Internet Resources Available Regarding Submissions to the IAFIS

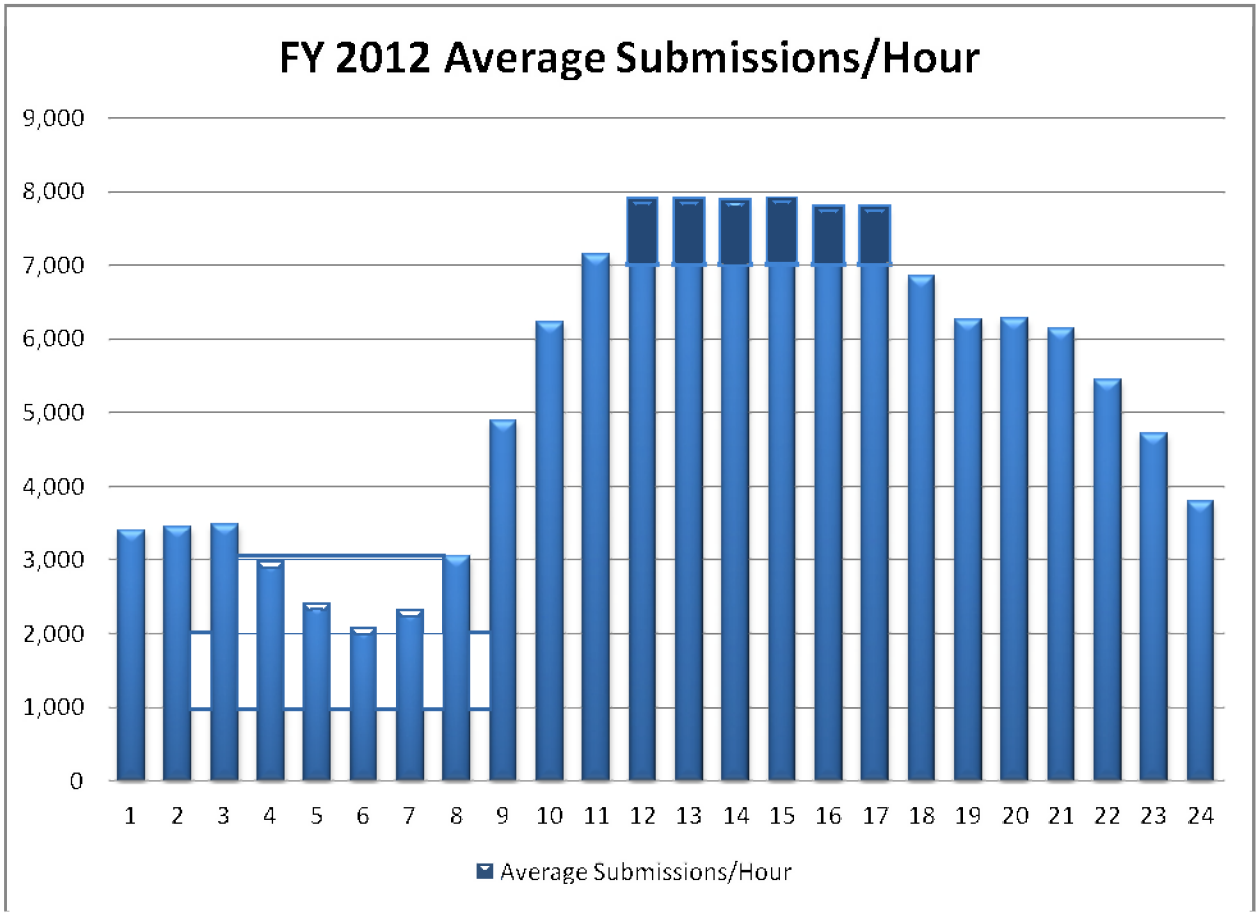
All data contained in this report is provided by the STAR Group and is based on information made available to the STAR Group through December 20, 2011.

TENPRINT FINGERPRINT IDENTIFICATION SERVICES

IAFIS Records	Date	Total Fingerprint Submissions
Receipts	April 30, 2010	*300,113
Closeouts	April 30, 2010	*297,816

**These submission records occurred during the 2010 US Census Project*

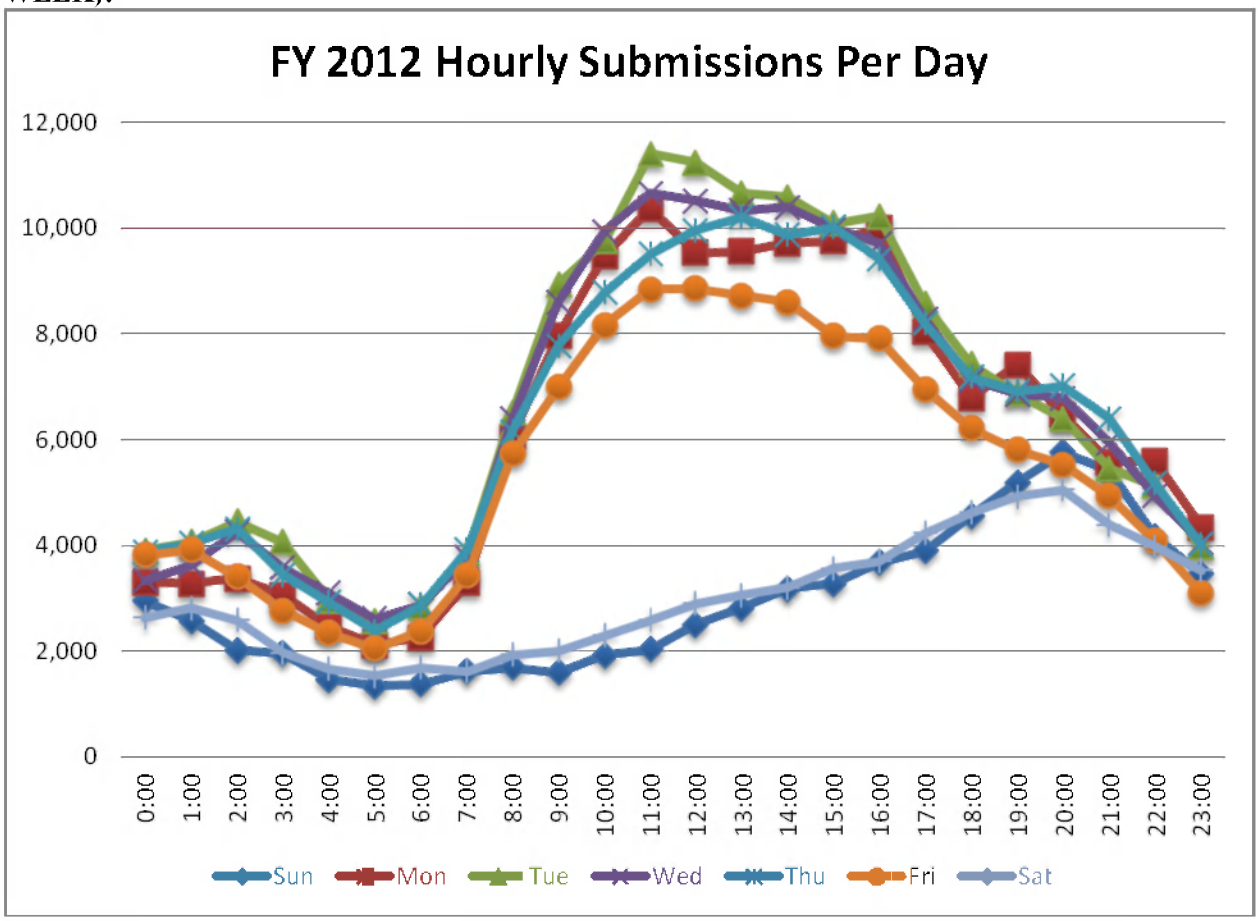
AVERAGE SUBMISSIONS PER HOUR (TOTAL FY 2012 SUBMISSIONS):



TOTAL RECEIPTS & PERCENTAGE CHANGE OVER PREVIOUS YEAR (PAST 5 YEARS):

	2008	2009	2010	2011	2012
Total Receipts	35,510,752	52,681,275	61,255,074	50,785,515	7,871,628
% Change	36.26%	48.35%	16.27%	-17.09%	-5.33%

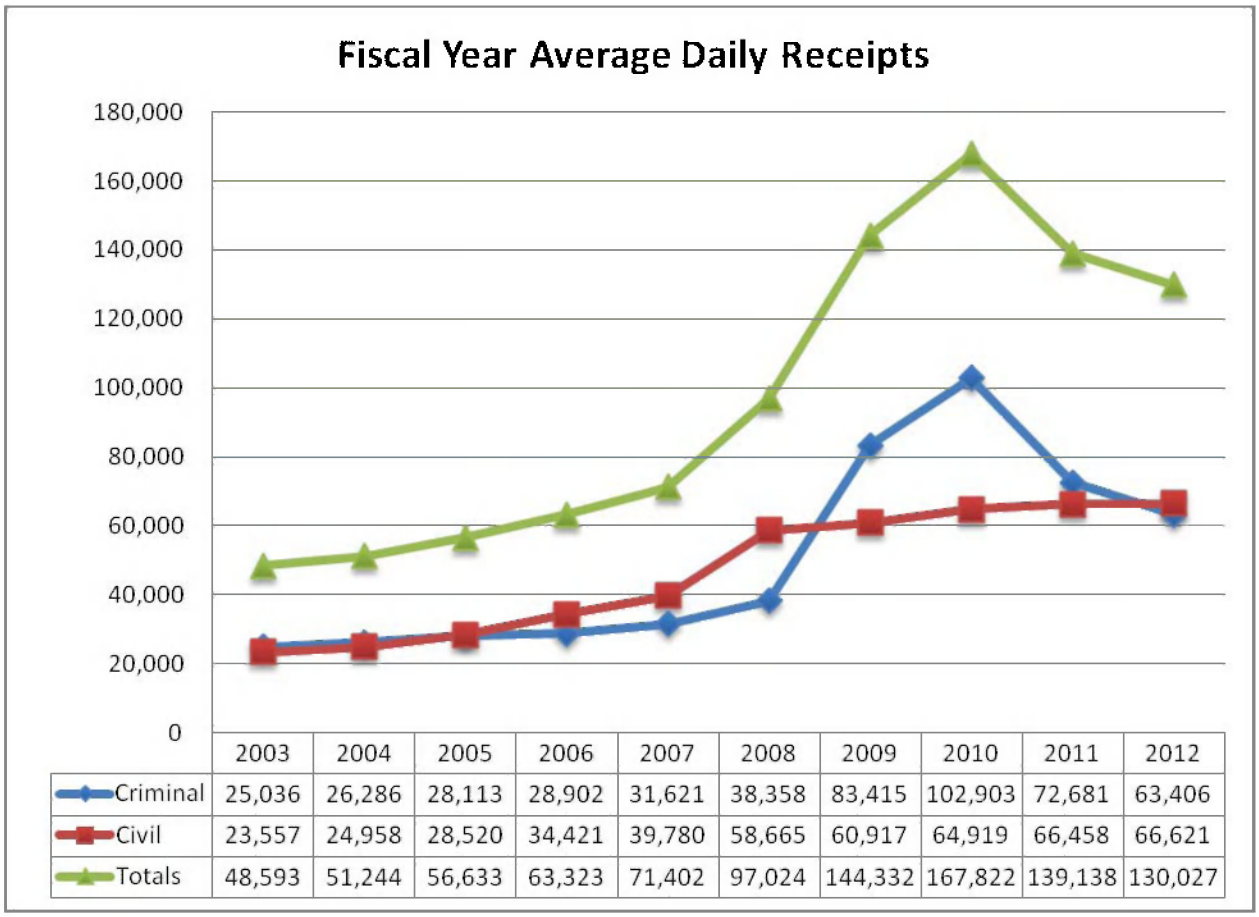
AVERAGE SUBMISSIONS PER HOUR (FY 2012 SUBMISSIONS BY DAY OF THE WEEK):



FY 2012 PERCENTAGE OF TOTAL SUBMISSIONS BY WORK SHIFT (SUNDAY-SATURDAY):

	MIDNIGHT SHIFT	DAY SHIFT	EVENING SHIFT
SUNDAY	21.73%	27.02%	***51.26%***
MONDAY	15.47%	***48.34%***	36.19%
TUESDAY	17.73%	***48.90%***	33.37%
WEDNESDAY	17.23%	***48.71%***	34.06%
THURSDAY	18.00%	***46.81%***	35.19%
FRIDAY	18.21%	***48.19%***	33.60%
SATURDAY	22.79%	29.74%	***47.47%***
7 Day Average	**17.23%**	***48.71%***	**34.06%**

AVERAGE DAILY RECEIPTS (PAST 10 YEARS):

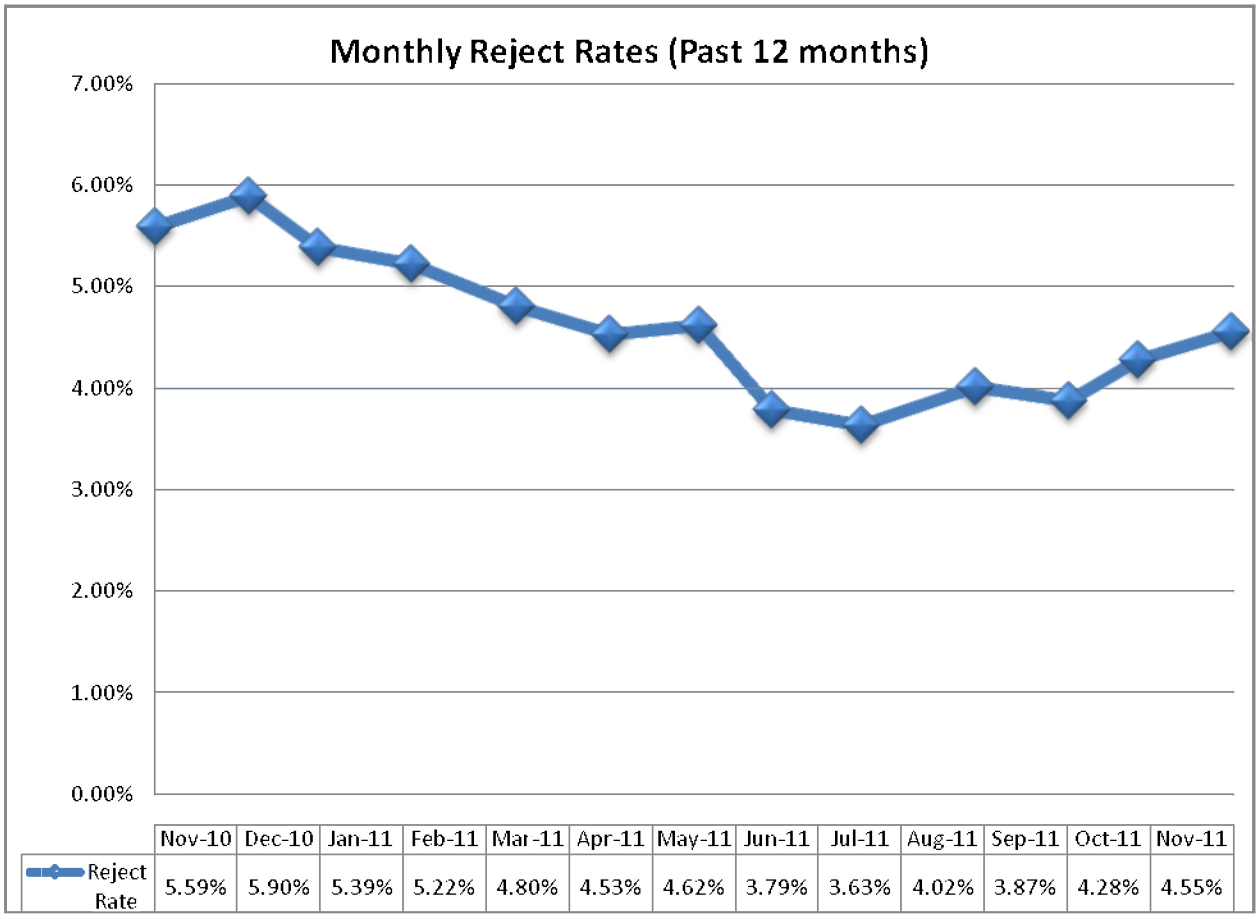


	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Criminal	25,036	26,286	28,113	28,902	31,621	38,358	83,415	102,903	72,681	63,406
Civil	23,557	24,958	28,520	34,421	39,780	58,665	60,917	64,919	66,458	66,621
Totals	48,593	51,244	56,633	63,323	71,402	97,024	144,332	167,822	139,138	130,027

AVERAGE SUBMISSION BY DAY OF THE WEEK (PAST 5 YEARS):

Fiscal Year	SUN	MON	TUE	WED	THU	FRI	SAT	DAILY AVERAGE
2008	44,115	99,194	122,526	***124,317***	123,784	114,069	50,615	**97,024**
2009	88,230	153,049	170,317	***175,570***	172,821	158,345	91,393	**144,332**
2010	106,749	183,141	***201,251***	196,951	195,502	180,008	106,448	**167,822**
2011	74,714	153,453	***165,451***	161,010	152,652	141,317	81,871	**139,138**
2012	69,019	154,249	***165,610***	160,161	159,364	136,951	70,370	**130,027**

MONTHLY REJECT RATE COMPARISON (PAST 12 MONTHS):



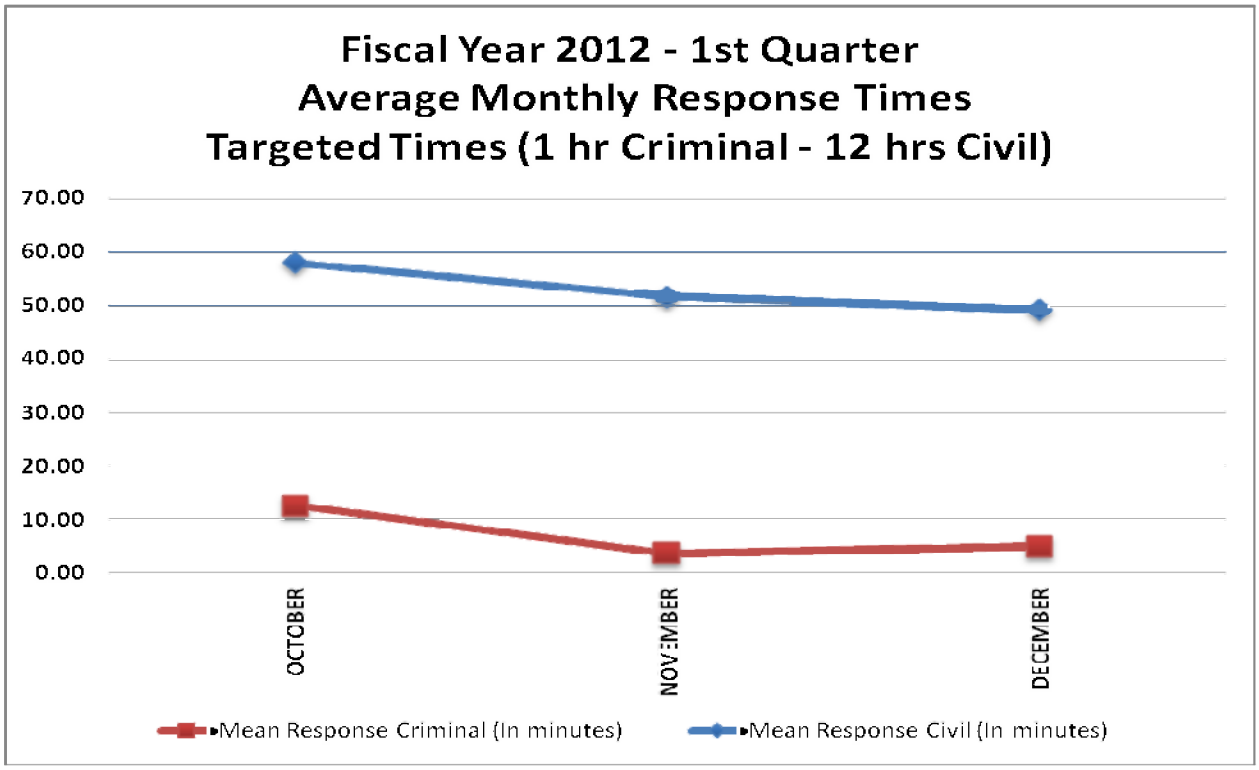
	Nov-10	Dec-10	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11
Reject Rate	5.59%	5.90%	5.39%	5.22%	4.80%	4.53%	4.62%	3.79%	3.63%	4.02%	3.87%	4.28%	4.55%

TOP REJECT REASONS (FY 2012):

Reject Code	Reject Type	Percentage of total rejects
L0008	Characteristics quality too low	**69.65%**
L0118	ITN Image Quality/Sequence Error	**10.89%**
E0004	EFTS record parse error	**4.96%**
L0117	Fingerprint Pattern Area Error	**3.37%**
L0032	Duplicate DOA & DOS	**3.01%**
L0116	General Logic Error	**1.83%**
L0013	Fingerprint pattern Quality Error	**1.60%**

CHANGE IN IAFIS PERFORMANCE REPORTING FOR FY 2012:

In 2008, the BSS Statistical Trending, Analysis, and Reporting (STAR) Group was established as the POC for workload statistics of the IAFIS. Over several months, the STAR Group determined that actual mean response times (hours; minutes; seconds) were a better performance metric than the previously utilized percentage completed. In communication with the Director's Office, the group learned changes could not be implemented until FY 2012 but continued to monitor the response times. BSS management made the decision to request the response times be reduced by half in FY 2012 to 1 hour for electronic criminal and 12 hours for electronic civil submissions. This change was approved on December 1, 2011.



CRIMINAL AND CIVIL RECEIPT COMPARISON (FY 2012 VS. FY 2011):

FY 2012	% of Total Work	% Received Electronically	Average Response Time	Identification Rate
Criminal	48.8%	98.3%	7 mins 43 secs	32.2%
Civil	51.2%	97.2%	1 hr 4 min 25 sec	10.9%
FY 2011	**% of Total Work**	**% Received Electronically**	**Average Response Time**	**Identification Rate**
Criminal	52.2%	96.0%	9 mins 56 secs	30.0%
Civil	47.8%	97.2%	1 hr 4 mins 32 secs	10.4%

LATENT FINGERPRINT SERVICES

The IAFIS supports latent fingerprint search requests from the FBI Laboratory Division and accepts remote location searches from 49 states and the District of Columbia.

TOTAL PROCESSED & RESPONSE TIMES: (Through December 20, 2011)

Type of Transaction	FY 2012 Total Processed	Hours	Minutes	Seconds
LFFS	60,036		59	12
LFIS	6,138	1	51	53

Type of Transaction	FY 2011 Total Processed	Hours	Minutes	Seconds
LFFS	203,715		41	12
LFIS	14,058		52	20

TOTAL PROCESSED: (Through December 20, 2011)

Type of Transaction	FY 2012 Total Processed	FY2011 Total Processed
IRQ	6,092	178,117
ULAC	326	2,268
ULD	28,381	3,636
ULM	1,646	14,311

REMOTE LATENT PRINTS:

Date of count	Total Processed
January 1, 2006 thru November 30, 2011	948,697

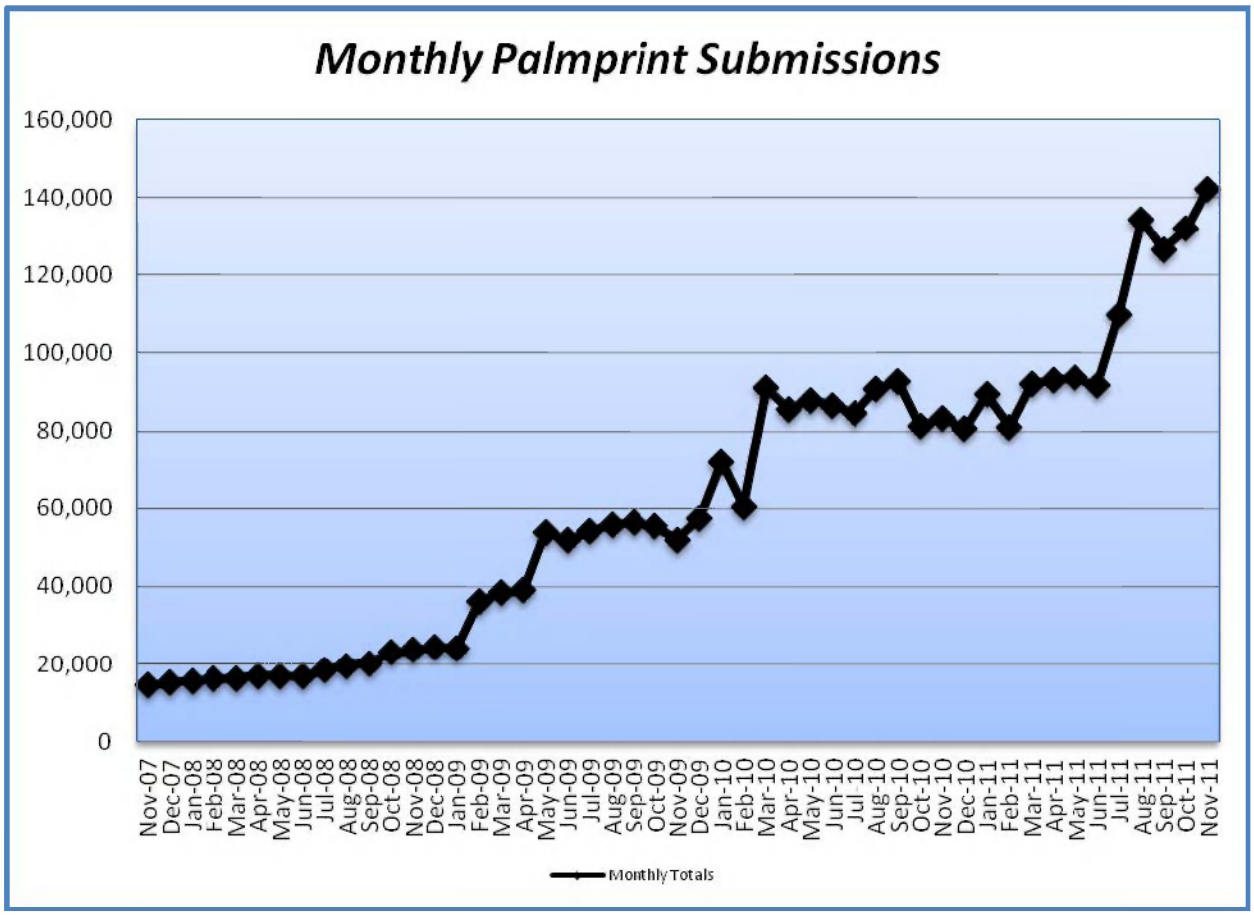
PHOTO COUNTS:

Date of count	Number of Photos	Number of Records with Photos
December 1, 2011	12,735,514	7,041,924

PALMPRINT AND IRIS PROJECTS

On April 7, 2009, IAFIS was enhanced to accept palmprints and iris images for storage purposes when submitted with criminal and civil tenprint submissions. Photographs may be submitted with civil tenprint submissions.

MONTHLY PALMPRINT SUBMISSIONS (NOVEMBER 2007 – NOVEMBER 2011):



Although the primary biometric modality used by the CJIS Division for identification purposes is fingerprints, the collection of additional biometrics will become valuable identification and investigative tools for the criminal justice community. With advancements in biometric technologies, the CJIS Division will continue to evaluate and improve services in order to remain responsive to customer needs by enhancing existing and implementing new biometric capabilities.

TOP PALM PRINT CONTRIBUTORS (FY 2012):

TOP PALM PRINT CONTRIBUTORS		
Texas	Florida	Michigan
FBI	Missouri	Washington

BORDER SECURITY

The full scope of this category is not yet defined, but for the purpose of this paper, refers to those fingerprint submissions received and processed through the IAFIS which are comprised of non-citizens entering into the United States.

The Department of Homeland Security's (DHS) Customs and Border Protection (CBP) submits 10-prints from non-U.S. Citizens collected during the primary inspection process at ports of entry to the FBI CJIS Division for full search of the CMF. These CBP transactions come to the IAFIS via the Automated Biometric Identification System known as IDENT that is maintained by the United States Visitor and Immigration Status Indicator Technology (USVISIT) Program.

The Department of State (DOS) submits fingerprints for all visa applicants and was the first large scale deployment of Identification Flats (Type 14 or slap prints) to the IAFIS. Type 14 submissions currently comprise **50.0%** of the daily total receipts.

The two major Types of Transactions (TOT's) that make up the Border Security submissions:

1. **CPNU (Fingerprint Card Processing Non-Urgent)** submissions are criminal TOT's with a 72 hour processing time. CPNU submissions reached a peak of nearly **98,000** per day in January 2010.

2. **NFUE (Non-Federal User Fee Expedite)** submissions are civil TOT's with a 15 minute processing time.

BORDER SECURITY SUBMISSIONS:

Border Security Submissions	FY 2012	Daily Average	FY 2011	Daily Average	Daily Limit
CPNU	* 2,164,115	34,943	* 15,094,028	***41,354***	98,000
NFUE	639,277	***11,027***	3,668,082	10,050	15,000

**CPNU submission totals include a small percentage of submissions from agencies not associated with Border Patrol.*

CPNU AVERAGE SUBMISSIONS (PAST 12 MONTHS):

December 10	January 11	February 11	March 11	April 11	May 11
42,460	33,325	35,067	36,415	43,296	38,270
June 11	**July 11**	**August 11**	**September 11**	**October 11**	**November 11**
39,672	***47,309***	45,153	42,979	38,622	32,228

BSS UNIT SPOTLIGHT

PROCESS IMPROVEMENT TEAM (PIT):

The Criminal Justice Information Services Division, Biometric Services Section's PIT utilizes a variety of Lean/Six Sigma tools within business processes to assist in identifying and eliminating waste. The goal is to improve the workflow, reduce inventory, and aid in the design of more efficient, effective, streamlined and standardized processes to realize significant time, cost, and resource savings.

David Sturm – Supervisor 304-625-5936 david.sturm@leo.gov

Contact via internet: LEAN@leo.gov

Leave a message: 304-625-5326 (LEAN)

LATENT INVESTIGATIVE SERVICES PROGRAM OFFICE (LISPO):

The LISPO provides IAFIS Latent Business Line support to all local, state, federal, tribal, and international law enforcement agencies, as well as FBI Field Offices, Legal Attaches, and the FBI Laboratory Division. The LISPO serves as the liaison between the IAFIS and the latent community by upholding the accuracy, integrity, and timeliness of latent services; educating and transitioning the latent user community to new latent services and technologies as developed and implemented by the FBI; and serving as facilitator for the interoperable sharing of high-profile and/or time-sensitive latent prints amongst authorized law enforcement and national security partners.

Michelle Meder - Supervisor 304-625-2614 michelle.meder@ic.fbi.gov

Gary L. Williams – Supervisor 304-625-2849 gary.williams@ic.fbi.gov

BSS UNIT CONTACT INFORMATION:

Customer Service Group (CSG)

Gary Stroupe - Supervisor 304-625-4627 gary.stroupe@leo.gov

Customer Service Group 304-625-5590

Training and Records Testimony Team (TRTT)

Contact via internet: fingerprint_training@leo.gov

Leave a message: 304-625-5279

Fax Number: 304-625-2337

INTERNET RESOURCES AVAILABLE REGARDING SUBMISSIONS TO THE IAFIS

- **FBI Web Page –** www.fbi.gov
  - Fingerprints

    Criminal Background Checks

    Fingerprint Identification Overview

    Taking Legible Fingerprints

    Ordering Fingerprint Cards & Training Aids

    Submitting Arrest Dispositions

    Checks on Bank Employees

    Name Checks for Fingerprint Submissions (pdf)

    Fingerprint & Criminal History Record Training

- **Law Enforcement Online –** www.leo.gov

  LEO is a 7 days a week, 24 hours a day online (real-time), controlled-access communications and information sharing data repository.

  - (SIGs/Public) General Information
    - CJIS Informational Letters
    - Customer Service Directory
    - Directions to the CJIS Site in Clarksburg, West Virginia
    - Online Fingerprint Card Order Form
  - (SIGs/Public) Biometrics Services Section — Information
    - BSS Training and Records Testimony Information
    - Fingerprint Card Inquiries
    - Frequently Asked Questions
- **Biometric Center of Excellence (BCOE) –** www.biometriccoe.gov

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

STAFF PAPER

INFORMATIONAL TOPIC F

Biometric Information Sharing Update

PURPOSE

To provide an update on biometric information sharing initiatives.

POINT OF CONTACT

SSA D.A. (Andy) Loftin, 304-625-4554

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 CJIS Division's Global Initiatives Unit (GIU) has previously briefed APB Subcommittees and Working Groups on the following biometric information sharing initiatives:

- Foreign Biometric Exchange
- Preventing and Combating Serious Crime Agreements
- The Biometric Information Sharing Policy and Biometric Information Sharing Working Group

UPDATE:

Foreign Biometric Exchange (FBE): Based on previous briefings to and recommendations from the APB as well as pre-existing information sharing authorities of the FBI, the GIU's Foreign Biometric Exchange (FBE) program obtains and delivers biometric samples and related information from foreign law enforcement sources to the CJIS Division for data ingest, review, analysis, and

comparison with IAFIS. These samples are typically comprised of potential terrorist subjects, transnational criminals, or persons of national security interest. Retention of foreign biometric data in IAFIS depends on the particular agreement with the foreign agency. The GIU also assists with improving FBE capabilities by providing training and analysis to the foreign agency. Furthermore, the GIU receives and processes *ad hoc* international biometric inquiries as well as facilitates such inquiries of a foreign country's AFIS for the FBI. These *ad hoc* requests are brokered through the FBI's Legal Attaches (LEGATs) based on their authorities to share information with foreign law enforcement partners.

Through the FBE program, the CJIS Division has sharing relationships with 77 countries, in the form of both informal (*ad hoc,* verbal) agreements and formal agreements (Memoranda of Agreement, Memoranda of Understanding, or Letters of Cooperation). Collections by GIU from foreign partners range from a few records to thousands of records. To date, GIU has collected over 990,000 records from foreign partners, with over 600,000 from Afghanistan collection missions alone.

Preventing and Combating Serious Crime (PCSC): The PCSC agreements represent a White House and Congressionally-mandated joint effort between the Department of Justice, the Department of Homeland Security, and the Department of State to enter into bilateral information sharing agreements with the 36 Visa Waiver Program (VWP) countries in order to make the VWP more secure. These agreements are being implemented by the FBI at the direction of the Attorney General and will allow each party to have access to each other's fingerprint databases on a hit/no hit basis. Requests for additional information will be coordinated on a case-by-case basis, and provided through established channels (e.g., the appropriate LEGAT). All requests made under PCSC are strictly limited to Criminal Justice purposes.

Currently 20 of the 36 VWP countries have entered into PCSC agreements with the U.S.; however, none are currently sharing via the agreements. These countries include Australia, Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Portugal, Slovakia, South Korea, and Spain. Additionally one non-VWP country, Croatia, has signed a PCSC agreement.

Although Germany is not yet sharing via their PCSC agreement, the CJIS Division established PCSC connectivity with Germany's BKA in early December 2011. PCSC related sharing can commence once Germany addresses remaining internal details. Meanwhile, Spain, Estonia, Czech Republic, and Slovakia have expressed a willingness to begin sharing information under PCSC through interim measures

until the automated connections can be established. The FBI and DHS plan to travel to these countries in early 2012 to initiate the interim PCSC sharing solution.

Biometric Information Sharing Policy and the Biometric Information Sharing Working Group (BISWG): A working group has been established to approve and track the sharing of biometric extracts. The Biometric Information Sharing Policy and its Charter remain in draft form and are currently undergoing revision. However, all foreign biometric extract requests are being reviewed and approved through this process. To date, only FBI owned records have been shared via foreign extracts.

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

STAFF PAPER

INFORMATIONAL TOPIC G

CJIS Division Intelligence Group Overview

PURPOSE

To provide an informational update on the CDIG.

AUTHOR

Julie Kay Bumgardner

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 CJIS Division has an established tradition of providing outstanding informational services to federal, state, local, and tribal law enforcement users through its timely and accurate responses to specific requests. In order to improve customer service, the CJIS Division continues to develop expanded connectivity with the Department of Defense (DoD), the Department of Homeland Security (DHS), and our law enforcement partners, while simultaneously reducing the systems' query response times.

After September 11, 2001, the CJIS Division leadership determined that the data contained within CJIS systems would be of significant value to the intelligence or law enforcement communities. However, that data was not being extracted, analyzed, and utilized to its full potential. The CJIS Division had utilized its resources to assist with high priority investigations and other unique situations by providing additional research and analysis of the data contained in its systems based on specialized queries such as National Crime Information Center (NCIC) off-line searches. However, prior to 9/11, the CJIS Division had not collated the information housed in its databases for trends, patterns, and connections based on existing law enforcement or national security priorities.

In order to respond to the increased demand for threat assessment information and intelligence, the CJIS Division established the CJIS Division Intelligence Group (CDIG). The CDIG mission is to promote public safety and prevent terrorism by providing tactical and strategic intelligence to FBI Headquarters and field offices, the Law Enforcement and Intelligence Communities, and the DHS by leveraging the information contained in the CJIS Division's databases. This allows the CJIS Division to meet current and emerging national security and criminal threats, while continuing to serve its law enforcement customers.

DISCUSSION AND ANALYSIS

Historically, the CJIS Division's interaction with customers has been based on query-responses to end user requests for specific information. While this has been an adequate business practice in most instances, situations do arise in which an immediate response is not optimal. In these cases, additional review or extensive research and analysis are required to provide a qualitative intelligence response. The CDIG accomplishes this by integrating experts from various fields to conduct specialized searches, follow-up analysis, and comprehensive reporting on the subjects of interest. The CDIG personnel pro-actively conduct queries to extract, analyze, and leverage relevant information from the CJIS databases. These results are scrutinized, analyzed, and validated through various systems and applications to ensure that associations and linkages are identified in order to develop a complete picture of the subject(s) of interest. The final product is then compiled into a manageable, user-friendly product and disseminated to the customer.

CDIG is comprised of two groups:

Bioterrorism Security Risk Assessment Group (BRAG)

Pursuant to the Public Health and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) the FBI is responsible for conducting a Security Risk Assessment (SRA) on individuals who are identified by the US Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) and the Department of Health and Human Services' Centers for Disease Control and Prevention (CDC) as requiring access to select biological agents and toxins (BSAT). The CJIS Division's Bioterrorism Risk Assessment Group (BRAG) conducts the Bioterrorism SRAs based upon names and other identifying information submitted by individuals with access requirements. The SRA is done by accessing electronic databases and other sources of information available on the individuals and by consulting with appropriate officials of the HHS and the USDA to ascertain whether certain individuals should be denied access to or granted limited access to specified agents.

BRAG remains engaged in a number of projects to enhance service to its customers.

On July 2, 2010, the President of the United States signed Executive Order 13546, entitled, "Optimizing the Security of Biological Select Agents and Toxins in the United States." The E.O. established the Federal Experts Security Advisory Panel (FESAP) to provide recommendations concerning biosecurity measures of the Select Agent Program with the goal of enhancing security measures while minimizing the adverse impact on the legitimate use of BSAT. BRAG staff participates continuously in the FESAP process, lending expertise in the FESAP's efforts to shape policies within the biosecurity and biosafety communities. They have provided guidance to the Foreign National Vetting Subcommittee of the FESAP, most recently regarding escorting policies for Tier One laboratories and guidance to registered entities on assessing personnel suitability and reliability.

BRAG staff and their Unit Chief are looked to by the White House National Security Staff; the Department of Justice National Security Division and the Office of Legal Policy, for guidance on policy issues. In December, 2011, BRAG provided consultation concerning the management of access to Sensitive But Unclassified information generated from NIH-funded research on the H5N1 Virus.

BRAG consults closely with The FBI's Weapons of Mass Destruction Directorate, Criminal Investigative and Counterterrorism Divisions, as well as the Foreign Terrorist Tracking Task Force on biosecurity and national security issues discovered within their statutory authority.

BRAG, in partnership with the WMDD, who chaired the Personnel Reliability Program subcommittee, and the FBI White House liaison detailee aggressively advocated measures of improvement to the SRA component of the Select Agent Program. In November 2010, following a comprehensive collaboration effort between federal departments and agencies with scientific, public health, security, intelligence and policy expertise, the FESAP provided recommendations to Select Agent Program managers. A particularly critical recommendation proposed by the FESAP was that the BRAG be provided the authority and resources to access the mental health component of the NICS Index to more reliably determine whether an individual is ineligible to have access to BSAT for mental health reasons based on the statutory prohibitors. BRAG continues to pursue efforts to gain access to the mental health component. At the December, 2011 Advisory Policy Board meeting, BRAG successfully submitted a motion that BRAG be permitted to access the NICS Index in support of the SRA process. As a part of the motion, BRAG noted that access to the NICS data would be automatically suppressed unless the states affirmatively indicate their data may be used in support of the BRAG.

BRAG continues to pursue acquiring access to additional US Government data bases to enhance the vetting of all candidates. During the last year, BRAG has not only increased the search capabilities of FBI information, but has added additional searches of DHS and DOD databases. Also, BRAG increased the frequency of SRA rechecks from every five years to every three years.

Operationally, the BRAG has processed 3,777 applicants from January thru November 2011, resulting in 26 notifications that the individual was within a restricted category. Since the CJIS Division began processing SRA in 2003, 41,861 applications have been received and processed, resulting in 275 notifications that the individual was within a restricted category.

Analysis Group

The Analysis Group provides investigative and intelligence analysis support to federal, state, local, and tribal law enforcement agencies; the DoD; and the DHS. The Analysis Group researches CJIS Division internal database resources and available open source databases to provide focused tactical analysis support to both criminal and counterterrorism investigations. The Analysis Group pro-actively queries, extracts, and analyzes information from CJIS Division databases, in order to provide intelligence products to customers based on established requirements and specific user requests.

Since its inception, the Analysis Group has delivered a unique array of products and services in support of intelligence community and law enforcement priorities. Upon request, the Analysis Group is capable of furnishing customers with conventional criminal justice information, or more extensive, in-depth reviews of specific information based on queries of CJIS systems. The CDIG has established a customer service hotline and an email portal in order to more effectively assist law enforcement with these requests.

The Analysis Group continues to work to expand the use of CJIS information to support both law enforcement and intelligence operations. The following are projects of note for the Analysis Group.

> FBI Field Office Support: In an effort to proactively provide intelligence to the field, the Analysis Group extracts Interstate Identification Index (III) US criminal history information from the Integrated Automated Fingerprint Identification System (IAFIS). CDIG analyzes that data for patterns or anomalies and in turn provides Field Offices with investigative information on subjects of interest within its area of responsibility. CDIG also provides investigative support and analysis to field agents during ongoing investigations. This includes checking

CJIS systems, other federal and state databases as well as open source resources to generate additional leads, compile dossiers, and identify subjects of interest. CDIG also possesses a unique set of analytical tools and skills that are utilized to manipulate large data sets and identify social networks and associations based on links revealed in evaluating the data. CDIG has been instrumental in locating and identifying key subjects that otherwise would have gone undetected.

NICS Denial Information: The Analysis Group developed a program to leverage and disseminate denial information from the National Instant Criminal Background Check System (NICS)[1]. This project was conceptualized to see if NICS denial information would be of value to the law enforcement or intelligence communities. Working in conjunction with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Analysis Group analyzes the denial data for trends/patterns where legally prohibited individuals have attempted to purchase firearms. These denial results are then fused with existing investigative data and/or intelligence to develop new investigative leads. CDIG AG generates and disseminates approximately 150 NICS information notes to FBI Field Offices, Joint Terrorism Task Forces, and the ATF annually.

US DoD: The Analysis Group works closely with entities of the DoD, including the Biometric Fusion Center, the National Ground Intelligence Center, and various US commands globally, to provide support to active theaters of war. This support includes efforts to capture biometric records of all foreign fighters who may pose a threat to the United States. The Analysis Group works with the DoD to ensure that the detainees' biometrics are captured and maintained within IAFIS. CDIG also provides additional information to assist DoD in compiling biographics, biometrics, and intelligence for their watchlisting purposes.

CONCLUSION

With the growth and development of the CDIG, the CJIS Division continues to look forward to functioning in a leadership role within the law enforcement and intelligence communities with respect to information sharing. The CDIG's distinctive role as a channel between conventionally separate communities facilitates the exchange of threat information and general actionable intelligence for customers. The CJIS Division believes the exchange of information will foster further cooperation among the intelligence community and law enforcement in the future.

---

[1] The National Instant Criminal Background Check System (NICS) is a computerized name-based background check system designed to provide Federal Firearms Licensees (FFL) with a response within 30 seconds on most background check inquiries. The background check determines eligibility for firearms and explosives by providing the timely determination of a person's eligibility to possess firearms or explosives in accordance with federal law. If it is determined that prohibitive criteria exists, the FFL is advised to deny the transaction.

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

STAFF PAPER

INFORMATIONAL TOPIC H

Federal Agency Participation in Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability

PURPOSE

To inform the FBI Criminal Justice Information Services (CJIS) Division Advisory Process members of a change in processing that may impact federal agencies. There are several federal agencies using State Identification Bureaus (SIBs) to submit transactions to the IAFIS. Due to a change in the activation process for the U.S. Immigration and Customs Enforcement's (ICE's) Secure Communities program, federal agencies using the SIB to submit transactions to IAFIS will begin receiving the benefit of searching the Department of Homeland Security (DHS) IDENT. This topic paper will discuss the business operations and technical changes that may need to occur to realize the full benefit of IDENT/IAFIS Interoperability.

POINT OF CONTACT

Robert D. Holman, FBI/CJIS Division, Interoperability Initiatives Unit, (304) 625-2173

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 Department of Justice (DOJ), DHS, and Department of State (DOS) recognized the need to efficiently share biometric and related biographic information to support the missions of each agency. The agencies worked together to satisfy congressional mandates and developed an approach for sharing information between the DHS' IDENT and the FBI's IAFIS.

A phased approach to IDENT/IAFIS Interoperability was developed, including short-term and long-term capabilities. The short-term solution, or the interim Data Sharing Model (iDSM), was deployed on September 3, 2006, to selected agencies. As of November 17, 2008, pilot sites, with the exception of the Department of Defense, were successfully transitioned to allow for a search of the full IDENT repository through a single query. The ICE Secure Communities Program leverages the technical capability available through IDENT/IAFIS Interoperability and as of October 8, 2011, jurisdictions in 43 states and one U.S. territory are participating in IDENT/IAFIS Interoperability.

DISCUSSION

In July 2011, the FBI CJIS Division received a request from DHS ICE to modify the process for deployment of state and local law enforcement agencies in ICE Secure Communities. ICE suggested that the CJIS Division eliminate the Originating Agency Identifier (ORI) validation by the SIBs. The CJIS Division sought guidance from FBI Headquarters and the Department of Justice (DOJ) with regard to the ICE request. The DOJ determined that federal law requires the FBI to share fingerprint data in the IAFIS with the DHS, as that data is relevant to admissibility or deportability determinations made by DHS.

On November 8, 2011, the IIU began statewide deployment. For states being deployed under this new process, all Criminal Answer Required (CAR) transactions received from the SIB are being sent to the IDENT. As a result, federal agencies that submit CAR transactions to IAFIS through the SIB are also searching the DHS IDENT. In Fiscal Year 2011 there were 347 federal ORIs that submitted 11,891 CAR transactions through various SIBs.

Once the submission is received at the CJIS Division, a search of the IAFIS and IDENT will occur. There is no change to the IAFIS processing. Upon a match in IDENT, an Immigration Alien Query (IAQ) will be sent to the ICE Law Enforcement Support Center (LESC) asking for the immigration status. The CJIS Division combines the IDENT response and the Immigration Alien Response from the LESC and returns one response from DHS to the state. Even if the state is unable to receive or pass the response to the federal agency, ICE will receive the immigration status and may contact the federal agency for follow-up. When there is no match against IDENT but the submission indicates a foreign or unknown place of birth, an IAQ is generated to the LESC for ICE follow-up. The no match response is the only response received by the SIB.

SIBs participating in IDENT/IAFIS Interoperability had to make technical changes if they chose to receive the unsolicited DHS response. Federal agencies submitting to the IAFIS through the SIB are dependent upon the SIB making these technical changes in order to

receive the IDENT response. To date, the following states have made the technical changes to receive the IDENT response: California, Colorado, Delaware, Florida, Michigan, North Carolina, Texas, Virginia, Utah, and Wyoming. The CJIS Division's technical responsibility ends when the DHS match or no match response is returned to the state (when the state has the capability to receive it). If the federal agency that submits through the SIB wishes to receive the DHS response, it must communicate that desire to the SIB.

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

STAFF PAPER

INFORMATIONAL TOPIC I

Biometric Interoperability Update

PURPOSE

Provide IAFIS users with information regarding the implementation of biometric-based interoperability between the FBI Criminal Justice Information Services (CJIS) Division and other federal and international agencies, including the Department of Homeland Security (DHS) and Department of Defense (DoD).

POINTS OF CONTACT

Robert D. Holman, FBI/CJIS Division/ Interoperability Initiatives Unit, (304) 625-2173

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 CJIS Division's initial focus to achieve biometric interoperability has been between the Integrated Automated Fingerprint Identification System (IAFIS) and the DHS/United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program's Automated Biometric Identification System (IDENT). Recognizing the need to efficiently share biometric and related biographic information, the DHS, FBI, and Department of State (DOS) worked together to satisfy congressional mandates by developing a phased approach for sharing information and services.

The phased approach to Interoperability between the FBI's IAFIS and the DHS' IDENT included interim and long-term capabilities. The interim Data Sharing Model (iDSM), deployed in September 2006, provided the initial step for bidirectional information sharing. The iDSM offered increased data-sharing capabilities as additional

Interoperability enhancements were implemented. From October 2008 through December 2008, most CJIS Division stakeholders participating in iDSM transitioned to Shared Services. The Shared Services functionality enables an authorized IAFIS user access to certain biometric and biographic information retained in the other system through a single query. The transition from the iDSM to Shared Services marked a significant milestone by providing, for the first time, participating IDENT/IAFIS Interoperability users with biometric-based access to the full IDENT repository. In the future, the Shared Services functionality will continue to be extended to additional CJIS Division stakeholders until Next Generation Identification (NGI) Increment 4 delivers the enhanced interoperability functionality to all CJIS stakeholders submitting criminal transactions. Currently DHS is undergoing a thorough Policy review of accepting all criminal transactions from the CJIS Division to search IDENT.

STATE /LOCAL LAW ENFORCEMENT USING INTEROPERABILITY WITH IAFIS

The DHS Immigration and Customs Enforcement's (ICE) comprehensive strategy to improve and modernize the identification and removal of convicted criminal aliens from the United States is leveraging IDENT/IAFIS Interoperability to quickly and accurately identify aliens who have been charged with a crime and booked into law enforcement custody. State and local law enforcement within 43 states and one U.S. territory are participating.

In July 2011, the CJIS Division received a request from DHS ICE to modify the current process for deployment of state and local law enforcement agencies in IDENT/IAFIS Interoperability. Additionally, the CJIS Division received letters from state and local agencies requesting that the FBI not forward their submissions to IDENT. Consequently, the CJIS Division sought guidance from FBI Headquarters and the Department of Justice (DOJ). The DOJ determined that federal law requires the FBI to share fingerprint data in the IAFIS database with DHS as that data is relevant to admissibility or deportability determinations made by DHS. As a result of this decision, statewide deployment began on November 8, 2011, and is to be completed incrementally.

DHS ICE also made the request that the CJIS Division remove the seven-day filter. This filter was put in place to prevent state and local law enforcement transactions with dates of arrest older than seven days from being sent to the DHS ICE Law Enforcement Support Center. This filter was removed on November 8, 2011.

FEDERAL AGENCIES USING INTEROPERABILITY WITH IAFIS

In addition to DHS, the CJIS Division is expanding its focus for biometric interoperability by working towards improved information sharing with other federal and international

agencies. The long-term vision of biometric interoperability is to make IAFIS/NGI fully interoperable with additional biometric systems. These continued interoperability efforts ensure that local, state, tribal, federal, and international agencies have access to relevant and up-to-date information.

Department of Defense (DoD)

In December 2005, the DoD's Automated Biometric Identification System (ABIS) and the FBI's IAFIS became interoperable. The biometric data held in ABIS is primarily from foreign collections and only select submissions to the IAFIS are searched against this data.

In April 2007, the DoD was added to the agencies participating in IDENT/IAFIS Interoperability as an iDSM participant. As other iDSM participants transitioned to the Shared Services functionality, the DoD continued searching the portion of the iDSM containing DHS-provided data (expedited removal records and DOS category one visa refusals). During the IDENT/IAFIS Interoperability Executive Steering Committee meeting on March 18, 2009, DoD's participation was elevated from "ESC participant" status to that of an executive voting member.

As a result of an analysis, the DoD requested the discontinuance of its participation in the iDSM; accordingly, that participation was discontinued on January 20, 2011. The FBI, DHS, and DoD have agreed that until the DoD and DHS establish direct connectivity between the ABIS and IDENT, the IAFIS can be used as an interim strategy to support bidirectional information sharing between those systems.

Based on current agreements between the DoD and DHS, the Special Operations Command (SOCOM) is approved to search IDENT. These transactions will come through IAFIS to IDENT until a direct connection is established between the ABIS and IDENT. The projected implementation date for SOCOM to begin submitting transactions for a search of IDENT is 2012.

DOS Consular Affairs

At the direction of the Homeland Security Council in October 2006, the FBI and DOS initiated a tenprint pilot program that leveraged IDENT/IAFIS Interoperability to determine the benefit of conducting biometric checks for visa issuance against the IAFIS Criminal Master File. The pilot required that 100 percent of visa applicants at limited, high-priority consulate sites be fingerprinted and checked against the IAFIS. The pilot program resulted in biometric criminal history record information check results being expeditiously provided to appropriate Consular Officers. In 2007, the decision was made to conduct fingerprint-based checks of IAFIS of all persons applying for United States visas worldwide. In January 2008, the DOS transitioned to submitting approximately

30,000 fingerprint check requests per day via IDENT to IAFIS, with 15,000 high priority transactions per day to be completed within 15 minutes.

United States Office of Personnel Management (OPM)
The OPM began participating in iDSM in December 2006. In November 2008, the OPM submissions for background checks for national security purposes and positions of public trust were transitioned to the Shared Services functionality.

DHS Customs and Border Protection (CBP)
In December 2007, utilizing IDENT/IAFIS Interoperability, IDENT began submitting tenprints collected by DHS CBP primary processing lanes to the CJIS Division for a full search of the CMF. The tenprint process allows for enhanced border security by identifying aliens with criminal histories seeking admission to the United States via air and sea ports of entry.

In an effort to meet the CBP operational requirement for a rapid search and response against the full CMF during primary inspection process, the CJIS Division implemented technical changes in IAFIS in May 2010. The CJIS Division worked with DHS to transition CBP primary searches from Criminal Fingerprint Non-Urgent (CPNU) submissions to Ten Print Rap Sheet (TPRS) submissions. DHS implemented the necessary system modifications and on December 13, 2010, the Rapid Response pilot was deployed at the Detroit airport. Additionally, the Dallas airport was deployed on April 4, 2011; the Houston airport on April 6, 2011; and the Atlanta airport on May 18-19, 2011.

DHS is working to deploy additional rapid response functionality to the four original ports. The new functionality combines the IDENT and IAFIS search results into one response rather than two responses. Nationwide deployment of all rapid response functionality is expected to begin in January 2012, and will be completed incrementally.

FBI Using Mobile Capabilities
The Quick Capture Platform (QCP) allows FBI personnel to capture biometric samples in remote field settings for submission to IAFIS and other biometric databases. The FBI's Hostage Rescue Team (HRT) was the initial QCP user, operating within the United States and in foreign theaters, often in conjunction with United States military assets. The HRT operationally deployed the QCP in Iraq in April 2007, searching IAFIS and the DoD's ABIS.

In March 2009, DHS authorization of the FBI mobile initiative allowed the collections made on the QCP to utilize the IDENT/IAFIS Interoperability to search IDENT. In December 2009, approval was given by US-VISIT to expand the population of FBI Mobile searches of IDENT to include QCP devices located domestically and used by FBI agent task forces in various FBI Field Offices.

Initially, FBI mobile submissions received the limited IDENT Response. In September 2010, FBI QCP users began receiving the full identification response from IDENT which includes additional immigration identity information.

CJIS Division Bioterrorism Risk Assessment Group (BRAG)

The CJIS Division BRAG began searching the DoD's ABIS on September 20, 2010, and DHS's IDENT on October 27, 2010. Access to ABIS and IDENT enhances BRAG's ability to obtain additional information which could impact the determination as to an individual's suitability to possess, use, or transport biological select agents or toxins.

DOS Office of Personnel Security and Suitability (OPSS)

The DOS OPSS was deployed on September 27, 2010. The DOS OPSS' search of IDENT enhances its ability to conduct more thorough personnel security investigations for the DOS. On October 26, 2011, the DOS OPSS began receiving the full identification response from IDENT.

Additionally, the DOS OPSS has requested these transactions to search ABIS. The CJIS Division, DOS OPSS, and DoD are working together to address all business, policy, and technical issues associated with this initiative.

ICE Biometric Identification Transnational Migration Alert Program (BITMAP)

The BITMAP is an ICE - Homeland Security Investigations (HSI) led initiative, in collaboration with the DoD Biometric Identify Management Agency (BIMA), DHS US-VISIT, and CJIS Division to biometrically search and enroll suspect individuals abroad for intelligence and screening purposes. BITMAP is in partnership with various DoD components within Southern Command (SOUTHCOM), SOCOM, and Special Operations Command South (SOCSOUTH) to capture biometric identification data from foreign nationals encountered outside the continental United States through formal and informal agreements developed by ICE-HSI Attaché offices. ICE-HSI has a footprint of 65 offices in 45 countries.

BITMAP will primarily focus on special interest aliens transiting through the Horn of Africa, South and Central America, and Mexico. Currently, 13 countries are participating in the BITMAP effort. Other categories of collections include gangs, persons of interest, and vetting enrollments. BITMAP transactions began searching and receiving responses in April 2011. These biometric collections are submitted through ABIS to IAFIS and then to IDENT. Leveraging IDENT/IAFIS Interoperability, the CJIS Division will continue to forward the submissions to IDENT for search and enrollment until DoD and DHS have established a direct connection or ICE can submit directly to IDENT.

United States Coast Guard (USCG)

In September 2010, the CJIS Division and the USCG tested off-shore connectivity to IAFIS from a maritime location ten miles off the coast of Boston, Massachusetts. Since

then, discussions to utilize DoD mobile technology to capture the biometrics from crew members of Liquefied Natural Gas (LNG) vessels have occurred in an effort to enhance the existing process of the USCG providing maritime security and national defense. The USCG has requested to utilize Interoperability functionality between ABIS, IDENT, and IAFIS. Representatives from the USCG, the CJIS Division, DoD BIMA and DHS US-VISIT worked together to address all business, policy, and technical issues associated with this request. In April 2011, ABIS began forwarding USCG transactions for LNG Vessel Checks to IAFIS for a search. Leveraging IDENT/IAFIS Interoperability, the IAFIS forwards the submissions to IDENT. The CJIS Division will continue to forward the submissions to IDENT for search and enrollment until DoD and DHS have established a direct connection or USCG can submit directly to IDENT.

CJIS Division Special Identities Unit

The CJIS Division Special Identities Unit (SIU) represents the operational arm of the Global Operations Section. In order to accomplish this mission, the SIU requires the ability to query the IDENT database on a case-by-case basis to fully support the FBI's domestic and foreign customers. The SIU was approved for search of IDENT in December 2010, and deployed in June 2011. On October 26, 2011, the SIU began receiving the full identification response from IDENT.

INTERNATIONAL AGENCIES USING INTEROPERABILITY WITH IAFIS

Preventing and Combating Serious Crime Information Sharing (PCSC)

In 2008, the United States began signing PCSC agreements with countries who participate in the Visa Waiver Program. In relation to the PCSC agreements, the United States government is represented by the DOJ, DOS, CJIS Division and DHS US-VISIT. The agreements formalize the sharing of biometric and limited biographic data for the purposes of preventing and combating serious crime.

The Federal Republic of Germany (FRG) officially ratified the PCSC agreement in February 2011, and is scheduled to be the first fully automated PCSC partner to participate in this information sharing initiative. The CJIS Division and DHS US-VISIT have coordinated communication with the FRG to exchange fingerprint data for the purpose of enhancing cooperation in preventing and combating serious crime. The IAFIS will act as a pathway for fingerprint search requests from the FRG to DHS' IDENT and from IDENT to the FRG. This effort will leverage existing IDENT/IAFIS Interoperability capabilities in order to fulfill the agreement between the FRG and the United States. Fingerprint queries will be processed according to documented policies and procedures between and among the three parties. The parties are working to establish the capabilities needed for implementation of this functionality.

International Criminal Police Organization (INTERPOL)

The CJIS Division has been working with the United States National Central Bureau (USNCB) of the INTERPOL and DHS US-VISIT on an effort to make INTERPOL records accessible to DHS stakeholders via FBI's IAFIS. In order to implement this joint initiative, USNCB was required to make technical upgrades to its system. The first phase of this project is anticipated to be deployed in 2012. This phase will provide the initial capability for automated sharing to IDENT through IAFIS.

INTELLIGENCE COMMUNITY USING INTEROPERABILITY WITH IAFIS

Terrorist Screening Center (TSC)

The TSC is responsible for maintaining a biometrically enabled watchlist of Known or Appropriately Suspected Terrorist (KST) records. The TSC is also required to distribute this watchlist to various screening agencies, including the CJIS Division. In an effort to meet the demands for improved information sharing as outlined in the National Security Presidential Directive-59/Homeland Security Presidential Directive-24, the CJIS Division is coordinating the automated exchange of KST watchlist biometric and biographic information between the CJIS Division and TSC. The policy and business processes associated with this effort are currently in development.

National Counterterrorism Center (NCTC)

The CJIS Division, DHS, and DoD continues to work with the NCTC on an effort to synchronize the KST watchlist using interoperability with IAFIS to IDENT and IAFIS to ABIS. This synchronization is the first time that the three major unclassified biometric systems (ABIS, IAFIS, and IDENT) are fully synchronized. The synching of these systems provides access to additional KST data and assists in identifying these individuals through biometric searches.

IDENT/IAFIS INTEROPERABILITY ENHANCEMENTS

New IDENT/IAFIS Interoperability Participants

In an effort to bring on new users to IDENT/IAFIS Interoperability, the CJIS Division and DHS developed the IDENT/IAFIS Interoperability User Deployment and Evaluation Strategy Plan. This plan describes the strategy and processes to identify, evaluate, select, and prioritize new IDENT/IAFIS Interoperability users with regard to the IDENT/IAFIS Interoperability Memorandum of Understanding (MOU). Although, the document has not been finalized, a joint working group has facilitated the addition of users such as DOS OPSS, as well as the CJIS Division BRAG and SIU to IDENT/IAFIS Interoperability.

The CJIS Division has requested that DHS recognize all FBI-approved criminal justice users as authorized users of IDENT/IAFIS Interoperability. A motion carried at the 2011 spring APB meeting to endorse "the concept of criminal justice access to IDENT in support of all lawful contacts and encounters in the criminal justice continuum." Meetings are ongoing to work through the policy and privacy concerns associated with this request.

The new user application from the Florida Department of Law Enforcement (FDLE) Region IV Domestic Security Task Force has been approved by DHS. The CJIS Division and DHS are working with FDLE to deploy a pilot program for Region IV.

The CJIS Division has received several new user/new use applications for IDENT/IAFIS Interoperability access. These include the CJIS Division SIU for contract linguist submissions, the DoD Naval Criminal Investigative Service, and the Nuclear Regulatory Commission. Currently, these applications are under review by DHS US-VISIT.

Record Linking

During the spring of 2009, the CJIS Division and DHS US-VISIT prepared an action topic paper regarding "Clarification on Record Linking." The paper detailed the record linking concept for IDENT/IAFIS Interoperability. The establishment of record links in NGI and IDENT will enable the retrieval of information using link identifiers as opposed to having to re-perform biometric comparisons.

In June 2009, the CJIS APB passed a motion to accept the first option with amended verbiage: For record linking/maintenance purposes, a search/record update will be sent to IDENT for all criminal submissions regardless of the CJIS Division users request for an IDENT search; however, the state can opt out of receiving the response. The approved motion also included an amendment to continue the use of the Transaction Control Number/FBI Number conversion.

The joint agency Record Linking Working Group is tentatively scheduled to reconvene in February 2012, and will meet as necessary to discuss record linking requirements in greater detail, in accordance with current NGI requirements and the previous decisions of the APB.

Identification for Firearms Sales/Sexual Offender Registry Data

The CJIS Division identified two distinct data sets (Identification for Firearms Sales [IFFS] flagged records with federal firearm disqualifiers and Sexual Offender Registry [SOR]) data that will be shared using the existing Shared Services functionality. Retention of this data is to remain consistent with the IDENT/IAFIS Interoperability

MOU, whereby DHS will only link an IFFS or SOR record when it matches against an independent DHS or DOS encounter.

On April 18, 2011, the IFFS/SOR effort was deployed. Through this effort new IFFS/SOR records are proactively shared with DHS using the Shared Services framework. The legacy load (predating April 18, 2011) will be shared with US-VISIT utilizing Shared Services at a future date.

The IIU is conducting an analysis to confirm that data retention is consistent with the IDENT/IAFIS Interoperability MOU.

Latent Interoperability

Currently, state and local law enforcement agencies have the ability to search latent prints against the IAFIS. However, state and local law enforcement latent print searches of IDENT are limited to a case-by-case basis because, at this time, the automated functionality does not exist for these agencies to submit latent searches to IDENT. The CJIS Division, DHS US-VISIT, and the Texas Department of Public Safety (TX-DPS) are collaborating to pilot a latent print interoperability project. The projected implementation date is scheduled for April 2012.

The CJIS Division is also coordinating with the DOD in efforts to provide the option of searching the DoD's ABIS for the Latent Interoperability Pilot with the TX-DPS. Further discussions and the development of policy documents have been initiated and are required prior to the scheduled implementation.

In an effort to expand the availability of latent services beyond established user communities, DHS US-VISIT is developing latent capabilities to allow automated latent searches of IDENT. The CJIS Division is also determining the feasibility to make changes to IAFIS to allow early implementation of this NGI functionality in support of latent interoperability.

NEXT STEPS

This paper outlines the recent progress achieved with biometric-based interoperability between the CJIS Division, DHS, and other federal and international agencies. The CJIS Division and DHS will continue to accept additional applications for authorized criminal justice and noncriminal justice users through the IDENT/IAFIS Interoperability User Evaluation and Deployment Strategy, as well as continue to work with DHS ICE to provide interoperability benefits to additional state and local law enforcement participants. The CJIS Division will continue to work with DoD to manage and document current and emerging DoD/DOJ/DHS biometric interoperability in support of agency and national goals. Finally, NGI functionality enhancements are being developed and delivered incrementally. The CJIS Division is working to address the probable impacts to biometric interoperability participants as the transition to NGI occurs.

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

STAFF PAPER

INFORMATIONAL TOPIC J

State Participation in Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability

PURPOSE

Provide stakeholders with information regarding the enhancements and changes made by the FBI Criminal Justice Information Services (CJIS) Division in order to enable all states to participate in IDENT/IAFIS Interoperability and to receive the Department of Homeland Security (DHS) response.

POINTS OF CONTACT

Robert D. Holman, FBI/CJIS Division/Interoperability Initiatives Unit, (304) 625-2173

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 DHS, FBI and Department of State (DOS) recognized the need to efficiently share biometric and related biographic information to support the missions of each agency. The agencies worked together to satisfy congressional mandates and developed an approach for sharing criminal history and immigration identity information.

The FBI CJIS Division deployed the Shared Services functionality on October 27, 2008. The Shared Services functionality enables an authorized IAFIS user access to certain biometric and biographic information retained in the DHS IDENT through a single query.

Shared Services marked a significant milestone by providing, for the first time, participating state and local users with biometric-based access to the full IDENT repository.

STATE AND LOCAL LAW ENFORCEMENT USING INTEROPERABILITY WITH IAFIS

State and local law enforcement within 43 states and the territory of Puerto Rico are currently participating in IDENT/IAFIS Interoperability. In addition to the District of Columbia, the states listed below are not yet participating:

- Alaska
- Maine
- Minnesota
- New Hampshire
- New Jersey
- North Dakota
- Vermont

As of December 31, 2011, the total number of state and local searches of IDENT was 12,250,566. These searches resulted in 995,430 (8.12 percent) matches to IDENT data.

IDENT/IAFIS INTEROPERABILITY ENHANCEMENTS

Shared Services Functionality

As mentioned above, the CJIS Division implemented technical changes in 2008 to enable state and local submissions access to DHS IDENT. The process works as follows:

- CJIS receives state or local criminal answer required (CAR) submission via the state identification bureau (SIB).
- CJIS forwards the state and local submission to DHS IDENT.
- CJIS receives the response from DHS IDENT.
    - If there is no biometric match in IDENT, CJIS forwards the IDENT response to the SIB as an additional Submission Results Electronic (SRE), if the SIB is technically capable of receiving the IDENT response.
    - If there is a biometric match in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the Immigration and Customs Enforcement (ICE) Law Enforcement Support Center (LESC).
        - CJIS receives an Immigration Alien Response (IAR) in response to the IAQ.
            - The LESC also forwards the IAR to the appropriate ICE Field Office. The ICE Field Office takes action based on this investigative lead and places a detainer as needed.
        - CJIS combines the IDENT response with the IAR and forwards to the SIB as an additional SRE, if the SIB is technically capable of receiving the response.
    - If there is no biometric match in IDENT and the submission indicates a foreign or unknown place of birth, CJIS forwards the IDENT response to

the SIB as an additional SRE, if the SIB is technically capable of receiving the IDENT response.

- CJIS also generates an IAQ to the ICE LESC.
  - The LESC does not return an IAR to CJIS.

In order to receive the DHS IDENT response, several states have upgraded their systems. However, there are many states that are still unable to receive these responses and may need to consider system changes.

States Receiving the DHS (IDENT and IAR) Response

- California
- Colorado
- Delaware
- Florida
- Michigan
- North Carolina
- Texas
- Virginia
- Utah
- Wyoming

Idaho, Arizona, and Georgia are currently working on upgrading their systems to receive the DHS response.

Changes and Anticipated Changes in the IDENT Response

- **Addition of DHS Fingerprint Identification Number (FIN):** The IDENT response originally provided the fields of Name, Date of Birth, Place of Birth, Gender, Encounter Identifier, and photographs, if available. On June 6, 2010, the FIN was added to the IDENT Response.
- **Title Change:** The IDENT response that state and local law enforcement agencies receive was originally titled IDENT Data Response. The DHS US-VISIT later decided to refer to it as the IDENT Response.
- **Addition of Officer Safety Alerts:** The CJIS Division requested that US-VISIT add another field to the IDENT Response to provide "Officer Safety Alerts" contained in the IDENT. US-VISIT agreed to the request and is planning to add the alerts in the near future.

IDENT Response: Benefits to law enforcement

- IDENT Response may be used as an investigative tool by
  - District Attorney
  - Magistrates/Judges

    - Law enforcement officers during investigations
- IDENT response contains identity information that was provided during DHS encounters, and may assist in determining use of aliases

Shared Services Functionality for National Fingerprint File (NFF) States

The NFF states send fingerprints to the CJIS Division only at the time of the initial arrest. Second or subsequent criminal bookings in the NFF states result in a Criminal Print Ident (CPI) file maintenance message to the CJIS Division. NFF states are required to send the CPI message within 24 hours after the state system receives the fingerprint submission from the local agency. Approximately two-thirds of criminal submissions from the NFF states consist of CPI messages. The CJIS Division currently supports IDENT searches triggered by the CPI messages which are generated by the NFF states. As implemented, the criminal master file image associated with each CPI message from a participating agency is retrieved and forwarded to IDENT for search and response. CPI messages initially included:

- State Arresting Agency Identifier – ORI
- State Identification Number (SID) of record for which an NFF state identified a subsequent criminal ten print
- FBI Number (FNU) of the identified record

The CJIS Division added an additional field to the CPI message to enable participating NFF states to properly route the DHS responses. Along with the three fields mentioned above, the CPI message now includes:

- Transaction Control Number (optional)

Shared Services Process for NFF States

The process for an initial arrest in an NFF state is the same as the CAR process described above. The process for the CPI message entails the process listed below:

- CJIS receives CPI notifications via the National Crime Information Center/Interstate Identification Index.
- CJIS uses the FNU included in the CPI message to retrieve fingerprint images from the master record.
- CJIS forwards the fingerprint images to the IDENT repository in a manner similar to the CAR process.

The initial CAR transaction from NFF states will receive the DHS response as an additional SRE via the same channel as the current IAFIS SRE. It is important to note that NFF states will also receive the DHS response as an SRE to the CPI messages. Ordinarily, CPI messages submitted by NFF states would not result in an SRE from the CJIS Division via the CJIS Wide Area Network (WAN). NFF states wanting to receive the additional SRE will have to take this into consideration in configuring the state system for receiving an additional response for the initial arrest.

The CPI messages do not contain biographical data. NFF states do not provide the biographic information for the second or subsequent arrest to the CJIS Division. The DHS IDENT will not process a fingerprint submission unless the required fields listed below are populated.

CJIS populates the CPI-based submission with default values:

- Name: CPI,CPI
- Date of Birth: 000000
- Gender: XX

The CJIS Division does not retrieve biographic information from the master record because the biographic data included in the master record may not be the same as the information that is provided at the time of the arrest, which generated the CPI.

The National Crime Prevention and Privacy Compact (Compact) Council has addressed the possibility of providing Fingerprint Image Submission (FIS) transactions to IAFIS for all subsequent criterion arrests from NFF participants. Factors to be considered include available data elements, reprogramming, widespread use of the FIS, ability of the IAFIS to support the workload, and Compact direction. Potentially, FIS messages may be considered in the future to trigger searches of IDENT, as an alternative to or an enhancement of the current CPI trigger.

Recent Changes

- **Foreign Born No Match:** The foreign born no match pilot was deployed on July 25, 2011. This effort automatically spawns a biographic IAQ to the LESC when there is no match in IDENT but the CAR submission indicates a foreign or unknown place of birth. This pilot is effective only for those CAR submissions originating from the agencies participating in IDENT/IAFIS Interoperability.

- **Seven Day Filter:** Shared Services functionality was originally deployed with a filter in place to prevent CAR submissions with date of arrest of seven days or older from searching IDENT. The filter was removed on November 8, 2011. Currently, CAR submissions from participating state and local agencies are forwarded to IDENT regardless of the date of arrest.

- **Statewide Deployment:** In July 2011, the CJIS Division received a request from DHS Immigration and Customs Enforcement (ICE) to modify the process for deployment of state and local law enforcement agencies in IDENT/IAFIS Interoperability. ICE suggested that the CJIS Division eliminate the ORI validation by the SIBs. The CJIS Division sought guidance from FBI

Headquarters and the Department of Justice (DOJ) with regard to the ICE request. The DOJ determined that federal law requires the FBI to share fingerprint data in the IAFIS with the DHS as that data is relevant to admissibility or deportability determinations made by DHS. Under the new statewide deployment process, all CAR transactions received from the SIB are being sent to the IDENT. As of December 31, 2011, the following states have been deployed statewide:

- Missouri on 11/08/2011
- Oklahoma on 11/15/2011
- Mississippi on 11/22/2011
- Idaho on 11/29/2011
- Georgia on 12/06/2011
- Indiana on 12/13/2011
- Utah on 12/20/2011
- Kansas on 12/28/2011

- **Agencies with Direct Connectivity to IAFIS:** There are some state and local agencies that have direct connectivity to the IAFIS. The CJIS Division is ensuring that the CAR submissions originating from those agencies are also being forwarded to the IDENT. The list of ORIs with direct connectivity to the IAFIS will be monitored and updated as appropriate.

NEXT STEPS

This paper outlines the various changes and enhancements made by the CJIS Division from October 2008, to present date with regard to IDENT/IAFIS Interoperability for state and local law enforcement agencies. The CJIS Division will continue to deploy additional state and local agencies to utilize IDENT/IAFIS Interoperability. It would be beneficial for the states to upgrade their systems in order to take advantage of the enhanced interoperability features which will be offered by the Next Generation Identification (NGI) Increment 4. The NGI Increment 4 is scheduled to be delivered in 2014. State and local agencies will have the potential option to search multiple systems and to receive responses from those systems if the state systems are upgraded. These additional searches and responses can become valuable resources by offering supplementary investigative tools to the law enforcement agencies. State agencies that have questions or would like to discuss system changes that may be necessary for receiving the additional responses may contact Joseph L. Bohnert at 304-625-4211.

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

STAFF PAPER

INFORMATIONAL TOPIC K

NCIC Status Report

PURPOSE

The purpose of this paper is to provide a status report on the National Crime Information Center (NCIC).

AUTHOR

Krista L. Koch

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>.

UPDATE

REGULARLY SCHEDULED MAINTENANCE

The regularly scheduled maintenance for the NCIC usually occurs the first Sunday of each month restricting service from 4am to 6am.

ADVISORY POLICY BOARD (APB) ENHANCEMENT

The APB Enhancement slated for the NCIC Software Enhancement Build 12 that will tentatively be implemented on **Sunday, August 5, 2012** consists of the following:

- 172 NICS Denied Transaction File
- 175 Allow input of Foreign Sex Offenders into NCIC
- 179 Modify the EXL to allow agencies to indicate extradition information was unavailable.
- 180 Allow States to Opt-Out of sharing Article and Vehicle data with public website (TRACE)

- 184 Include Caveat in Acknowledgements for Gun entries agencies to perform Trace Request through ATF
- 188 & 189 Modify entry requirements of Wanted Person file to allow all address fields to be optional fields
- 190 Modify Missing Person File entry criteria and create unknown values for height and weight fields
- 192 & 193 Modify Benefit and Effectiveness Data to include Vehicle and Wanted Person Benefits Survey files and include additional NOT LOST field code

CJIS will tentatively install the enhancements for the August 5. 2012 Build into the NCIC First Level Integration Test System (FLI) environment on May 24, 2012.

STATISTICS

- The average number of NCIC transactions per day is at the 8.6 million mark.
- On Friday, July 29, 2011 NCIC had a record day where the number of transactions hit 9,768,568.
- The transaction Response Time average is .03 seconds.
- System Availability is running at approximately 99.7% each month with scheduled maintenance entailing the remaining .3%.

SYSTEM UPGRADES

- Upgraded the NCIC Central Processing Unit from IBM 2094 z9 to IBM 2817 z196 in September 2011
- NCIC Operating System upgrading to z/OS 1.12 is targeted for February 2012
- Upgrading the NCIC Database (DB2) to version 10 is targeted for March 2012

FURTHER INFORMATION

Testing

The CJIS maintains two test environments for NCIC Users to conduct testing of the NCIC systems. The first test system, Operational Test, can be accessed by using the appropriate header which starts with a 'T'. Test records are currently accepted in two formats, TL01 for NCIC Legacy formatted transactions and TN01 for NCIC 2000 formatted transactions. This test system should be accessed for User training purposes only.

The second system, First Level Integration (FLI), utilizes a different IP address than the operational environment and can be accessed using the standard

header data, 1N01 or 1L01, or the Operational Test header, TN01 or TL01. Test transactions do trigger notifications. This test system should be accessed for any type of testing whether User training or for software development purposes. The testing environments are operational 24/7, excluding infrequent maintenance activity.

Questions concerning the test environments and their usage may be directed to the NCIC team within the Global Operations Section of CJIS at (304) 625-2731. Technical issues with the NCIC test environments may be directed to the CJIS Help Desk at (304) 625-4357.

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

STAFF PAPER

INFORMATIONAL TOPIC L

N-DEx Enhancements Status

PURPOSE

To provide information and updates regarding the FBI's Criminal Justice Information Services (CJIS) Division's N-DEx enhancements.

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

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 CJIS system 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 the Working Group 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 Working Group 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 will be added to the ongoing list of enhancements. Therefore, this list will

continuously evolve as new topics are added, completed ones are deleted, and priorities change. As new topics are discussed, Working Group members are requested to assign priority levels from the list below, along with a rating of high, medium, or low within each level.

At the 2011 Spring Subcommittee Meetings, the Information Sharing Subcommittee (INSH) requested the N-DEx Program Office provide a list of priorities for enhancements to be made to the system in the remaining one year of the Raytheon contract.

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.

- The Working Group members are requested to review the attached table regarding the N-DEx enhancements.
- If a member believes that a priority level needs to be changed or an enhancement should be removed from the list, he/she should provide input to the Working Groups.

	ENHANCEMENT	PRIORITY LEVEL	STATUS	TENTATIVE IMPLEMENTATION DATE
1	**Agency Configurable Data Sharing Tools** Configure additional data sharing and access controls as necessary to extend the user base.	2H	Requirements Completed	01/2012
	Sharing controls are provided to the record owning agency to allow the agency the ability to set sharing rules in accordance with applicable laws, statutes, ordinances, and policies. The implementation of data sharing rules in Increment 3 was focused on the data element triggers (e.g. age of person, type of offense) and not user (agency/ORI) type (e.g. the type of agency such as law enforcement, probation/parole, within state, out-of-state, etc.). Currently, an agency cannot implement a policy where they can share with only certain types of agencies (e.g. Law Enforcement users, but not Probation/Parole). To meet existing agency needs for sharing data, this capability must exist. The concept of this enhancement is to allow an agency to select sharing rules based on an agency/ORI type and either include or exclude the agency users from viewing their data. For example, an agency may set a sharing rule which allows only users designated as Law Enforcement (based on the ORI) to view their data and not users whose ORI belongs to another agency category such as Prosecuting Attorney.			
1a	**ORI Validation** Validate only authorized users have access to N-DEx.	2H	Requirements Completed	TBD
	N-DEx will perform an ORI validation check with each search request to ensure users from authorized criminal justice agencies are accessing N-DEx.			
2	**Ingest Improvement** Improve Ingest Performance.	3H	Requirements Completed	03/2012
	Currently, N-DEx has a requirement to ingest up to 1 million records a day. This requirement was identified originally when N-DEx was first being developed. Recently, it was determined that many aggregation systems could be providing N-DEx with a significant amount of updated records. In addition to the planned growth of N-DEx, these additional updated records will require N-DEx's ingest rate requirement to be modified. The N-DEx program is still analyzing the information associated with this issue, but anticipates the need for N-DEx to support ingest rates above 5 million records a day.			

3	**Commercially available Off-The-Shelf (COTS)** Improve and/or replace COTS products/solutions to augment system performance.	3H	Requirements Completed	10/2011
	N-DEx will perform a study to review COTS software products in the N-DEx Increment 3 baseline configuration. The study will assess performance and scalability. For products where it appears feasible to make significant improvements in performance or scalability, alternate products will be evaluated and recommendations made for upgrading the N-DEx COTS configuration.			
4	**Search Enhancement** A variety of enhancements have been identified related to the search engine within N-DEx. This task will involve prioritizing, designing, implementing, and testing new solutions and enhancements to the current N-DEx system.	3H	Requirements Completed	03/2012
	N-DEx will provide improvements to existing search capabilities to include: data enrichment, data standardization, search synonym expansion, improved name searching, concept searching, search weighting, user search aids (misspelling, find similar, did you mean, etc.), user interface improvements, and results presentation.			
5	**LEXS-SR Added Functionality** Return Specific Entities in LEXS-SR Search.	3H	Requirements Completed	03/2012
	N-DEx returns two types of search results; documents and person entities, through the user interface. Through the user interface, documents are returned in response to every search request. Person entities are returned, in addition to document results, when the user has provided enough identifying information to return a known person from the N-DEx entity resolution engine. N-DEx currently provides only document results through the LEXS SR interface (machine to machine message-like interface). This task involves the development of enhancements to include person entity search results to support entity resolutions through the LEXS SR interface.			
6	**COTS Lifecycle Costs** Improve and/or replace COTS products/solutions to reduce Life Cycle Costs for the N-DEx system for O&M.	3H	Requirements Completed	03/2012

	N-DEx will perform a study to review COTS software products in the N-DEx Increment 3 baseline configuration. The study will assess lifecycle cost. For products where it appears feasible to make significant improvements in lifecycle costs, alternate products will be evaluated and recommendations made for upgrading the N-DEx COTS configuration. It is anticipated significant long-term cost savings can be realized.			
7	**Search / Subscribe Using Batch** Provide the ability to search and subscribe to lists of entities using Batch query/load processes.	3M	Requirements Completed	03/2012
	Batch query is the ability to supply one or more lists of searchable terms (e.g. names, identifiers, locations) which will be used to search and deliver a manageable view of results. This capability will enable a user to search or subscribe to multiple queries and manage the view of the results for in-depth review and analysis.			
8	**Geospatial and Link Visualization Improvements** Improve the geospatial and link visualization capabilities of N-DEx to augment capabilities and improve the user experience.	3M	Requirements Completed	03/2012
	The N-DEx system contains massive amounts of data about people, crimes, locations and property. In order to not overwhelm users with the plethora of information displayed in the search results, users are provided with various options to view search results in a way that is meaningful to a user. There are two parts to the visualization capability within N-DEx; Link and Geospatial (Geo). Link visualization handles the displaying of association and relationships between entities via a link/node relationship while geo-visualization displays entities by locations. Within visualization users have the ability to drill down or filter out information which is not of importance to their search. This task involves enhancing the user interface and capabilities offered in the current N-DEx system. The major difference in this release will be graphic user interface improvements which will make the visualization functionality a seamless companion to the search capability, and will improve the switching between Link and Geo visualization. Information, such as the main suspects and other aspects of these subjects will be better exposed. Also, the usability of these visualization capabilities will be enhanced by the improvements within the zoom and panning functionality.			

9	**Improve Discover Capability** Improve the capability to discover non-obvious relationships.	3M	Requirements Completed	03/2012
	The current link visualization capability does not provide any automation in the analysis of the network of entities (nodes) and their relationships (edges). Rather, the user is required to assemble and explore the network in a "piecemeal" fashion to discover useful information. By residing the entire network in a high performance graph database, network theoretic analysis's can be performed to help the user discover a wide variety of useful and non-obvious information. New visualization software will also be required that can rapidly render large graphs using sophisticated layout algorithms and provide advanced navigation features such as graph nesting/folding, user defined sub graph or graph region exclusion, edge hiding, and zooming.			
10	**LEXS-SR Additional Functionality** Support LEXS 4.0 Compliant SN functions.	3M	RCBD	TBD
	This task involves implementing LEXS 4.0 within N-DEx. The LEXS 4.0 specification supports subscription and notification capabilities for remote systems via LEXS transactions. Currently, LEXS 4.0 is being reviewed and has not officially been released. Once finalized, implementation of the N-DEx LEXS 4.0 compliant SN functionality will be initiated.			

11	**Audit Report Enhancements**	3M	Requirements Completed	01/2012
	This task involves user friendly enhancements in generating and displaying audit reports. The four reports focused on were Search Summary Report, Total Summary Report, Agency Member Report and Agency Activity Report.			
12	**Addition of External Data Source; DHS**,	3M	Requirements Completed	01/2012
	This task involves adding the Department of Homeland Security (DHS) external datasource to the user interface. Users will be able to query DHS as an external entity within N-DEx. With DHS, only people and locations targeted searches can be conducted using N-DEx.			
13	**Addition of External Data Source; USNCB - Washington (INTERPOL)**	3M	Requirements Completed	03/2012
	This task involves adding the ability to collaborate with United States' National Central Bureau (USNCB) - Washington for international exchange, via INTERPOL, of police and humanitarian information with law enforcement authorities of various INTERPOL member countries.			
14	**NIBRS Minor Fixes**	3M	Requirements Completed	01/2012
	This task involves fixes to the NIBRS extract and NIBRS XML translation.			

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.oip.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]

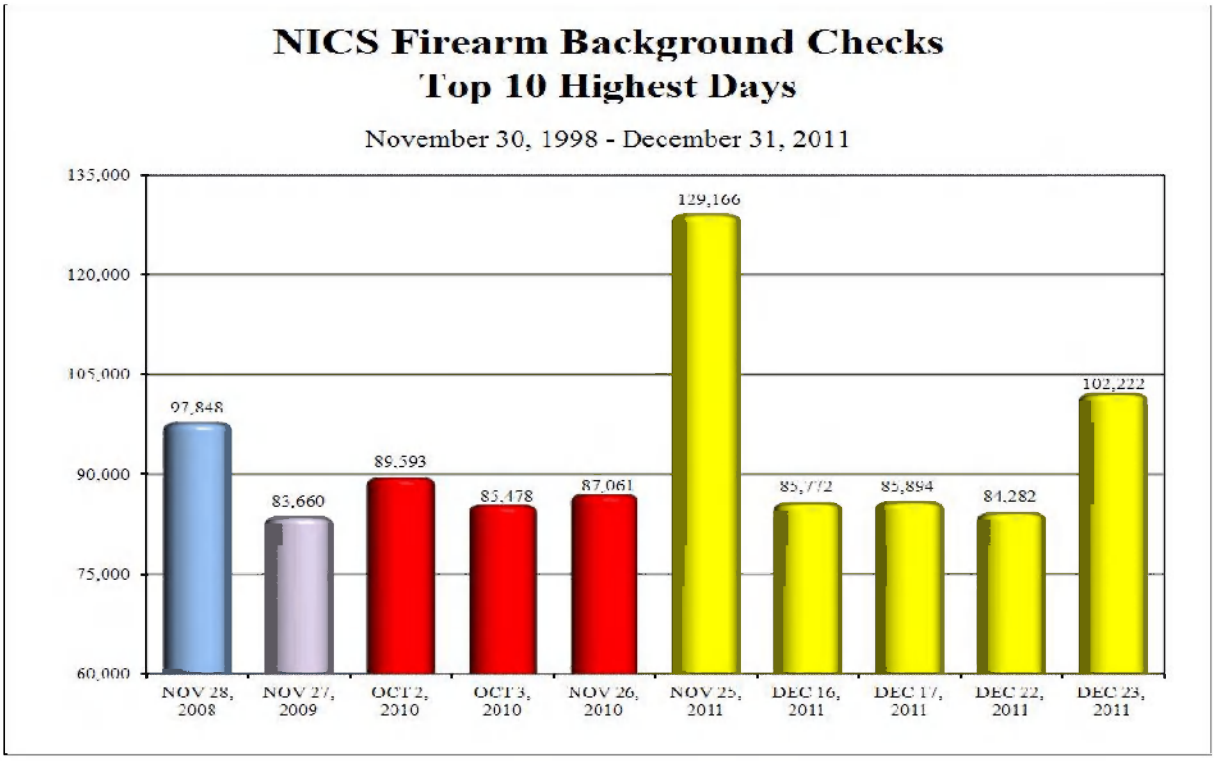
[1] The states that have designated a specific agency within the state to process NICS background checks for the states' FFLs (reference State Participation information on page 6).

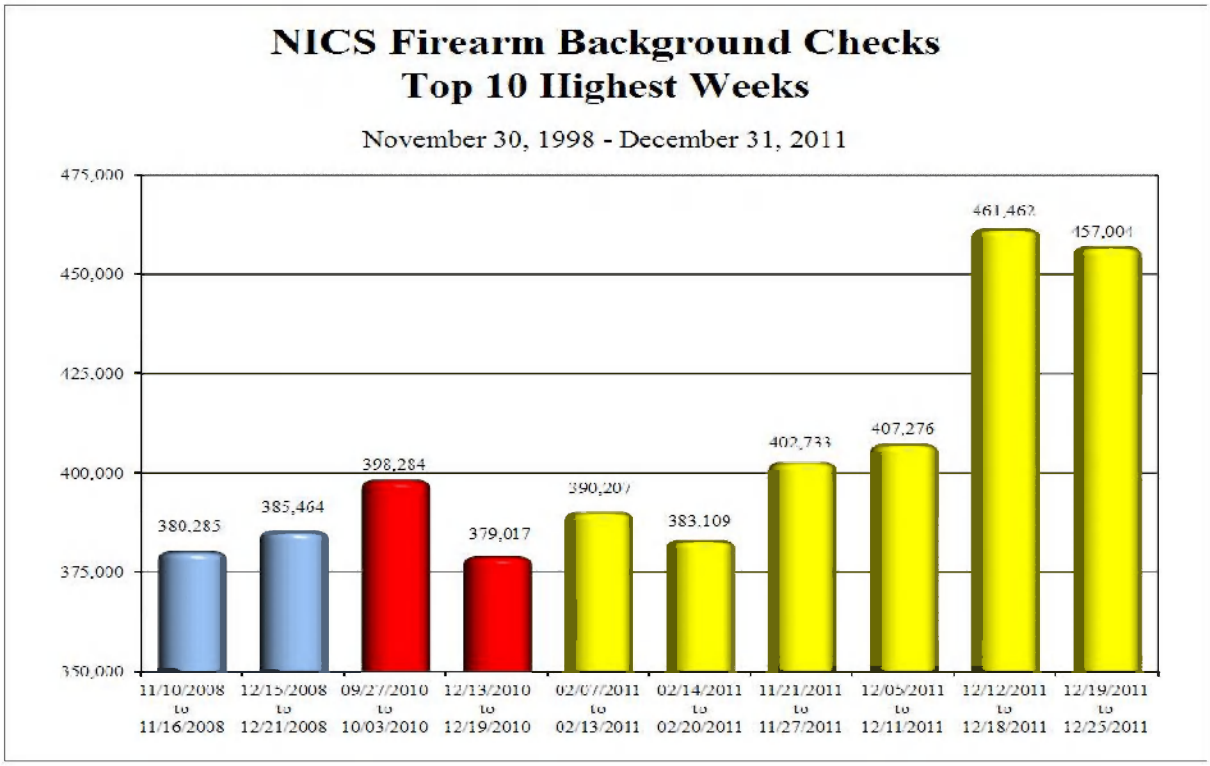
	2010*	2011*	PTD[2]
State Background Checks	8,372,222	9,579,326	73,726,947
Contracted Call Centers	5,530,099	5,872,456	62,938,227
NICS Section	36,839	42,376	1,571,425
NICS E-Check	470,456	960,793	2,645,800
Total Federal Background Checks	6,037,394	6,875,625	67,155,452
Total NICS Background Checks	14,409,616	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 Hlighest 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.