CJIS ADVISORY POLICY BOARD
SPRING 2010 WORKING GROUP MEETINGS
INFORMATIONAL TOPIC

STAFF PAPER

INFORMATIONAL TOPIC

Access to Department of Homeland Security Information by Federal, State, and Local Criminal Justice, Intelligence, and Authorized Non-Criminal Justice Agencies: Update on the Progress to Date with Interoperability.

PURPOSE

Provide stakeholders with information regarding the implementation of biometric-based interoperability between the IAFIS and IDENT.

POINTS OF CONTACT

[redacted] Federal Bureau of Investigation/Criminal Justice Information Services Division (FBI/CJIS)/Interoperability Initiatives Unit, [redacted]

[redacted], DHS/United States - Visitor and Immigrant Status Indicator Technology (US-VISIT) Program/Project Management Branch - IDENT, [redacted]

b2
b6
b7C

[redacted] DHS/Immigration and Customs Enforcement (ICE)/Secure Communities [redacted]

BACKGROUND

The Department of Justice/Federal Bureau of Investigation (DOJ/FBI) and the Department of Homeland Security/United States – Visitor and Immigrant Status Indicator Technology (DHS/US-VISIT) both operate fingerprint-based identification systems. These systems were developed concurrently by DOJ in the 1990's and were not designed to be interoperable. The FBI manages the Integrated Automated Fingerprint Identification System (IAFIS) which was deployed in 1999 and DHS operates the Automated Biometric Identification System (IDENT) which was deployed in 1994.

The lack of interoperability between the two systems created gaps for immigration and law enforcement officials when relying on a single system check. The information contained in either system was not directly retrievable by users of the

other system. Various legislative acts have required the FBI and DHS to ensure that the biometric systems are interoperable to share information.

The DHS, DOJ, and Department of State (DOS) recognized the need to efficiently share biometric and related biographic information to support the missions of those agencies dependent upon their services. The agencies worked together to satisfy Congressional mandates and developed an approach for sharing information. A phased approach to Interoperability was developed which included interim and long-term capabilities. In July 2008, the Interoperability Memorandum of Understanding (MOU) was signed by the DOJ/FBI, DHS/US-VISIT, and DOS.

The interim Data Sharing Model (iDSM), deployed on September 03, 2006, was the prototype that provided the initial step for bi-directional information sharing. The iDSM provided increased data-sharing capabilities until additional Interoperability enhancements were implemented. With the iDSM, the FBI and DHS exchanged read-only copies of fingerprint images of limited data subsets from the IAFIS and IDENT. The IAFIS subsets include known or suspected terrorists (KSTs), as well as all subjects with wanted notices associated with an FBI record. The subsets of data from IDENT include DHS expedited removal records and the DOS category one visa refusals (statutorily inadmissible) records. Authorized users of each system are able to access the others records to determine if an encountered subject is located within the shared records.

Full Search of IDENT Repository

The DOJ/FBI and DHS began transitioning from the iDSM to the operational use of Shared Services functionality in October 2008. However, the FBI CJIS Division continues to exchange KSTs and the Wants and Warrants data with DHS/US-VISIT through the iDSM to enable DHS to place these in the IDENT Watchlist. The transition to Shared Services provides previous iDSM users the ability to access the full IDENT Repository with a single query. The transition of all iDSM participants, with the exception of DoD, was completed on November 17, 2008. Until DHS, and DoD determine how they will operate, DoD queries will continue to be searched against the iDSM dataset.

The transition of the iDSM participants to Shared Services marked a significant milestone allowing, for the first time, participating Interoperability stakeholders to have biometric-based access to the full IDENT repository. The necessary methodology and mechanisms were implemented to support a search request of both IDENT and the IAFIS through a single interface. This process, known as Shared Services, enables a participating agency, either an authorized IAFIS or

IDENT user, to access certain biometric and biographic information retained in the other system through a single query.
When a fingerprint submission is forwarded to the FBI CJIS Division from these participating agencies, a concurrent search of the IAFIS and IDENT is executed. A Shared Services search results in separate responses from the IAFIS and IDENT. The IAFIS response continues to be returned separately following current business processes and response times based on type of transaction. These submissions are also searched against the two print and 10-print records within IDENT which responds with either a match or no-match IDENT Data Response (IDR). The IAFIS generates an Immigration Alien Query (IAQ) message to the DHS Immigrationa and Customs Enforcement (ICE) Law Enforcement Support Center (LESC), based on the information returned within the match IDR. The LESC responds to IAFIS with an Immigration Alien Response (IAR) and the IAFIS returns a combined IDR/IAR to the State Identification Bureau (SIB). Upon receipt of a no-match IDR, the IAFIS forwards the IDR to the SIB.

In addition to the IAFIS response, Interoperability participants now receive a second response via the CJIS Wide Area Network (WAN). The second response is either the match IDR/IAR or the no match IDR. Not all states are currently programmed to receive a second response. A match IDR/IAR could include up to five photographs which may pose another impact to the state. Additionally, routing issues to the local law enforcement agencies have also been encountered with the second response. However, a state is still able to participate in the ICE Secure Communities initiative while routing issues are being resolved. Fingerprint submissions from Interoperability participants will be forwarded to IDENT and queries sent to the LESC with the IAR being forwarded to the local ICE Detention Removal Office (DRO).

All requests for a search of IDENT will be limited to criminal submissions by state, local, and federal law enforcement, as well as for authorized noncriminal justice purpose checks, in accordance with the Interoperability MOU. Noncriminal justice purpose checks will be considered on a case-by-case basis in accordance with the MOU for an authorized user with an authorized use. Both IDENT and the IAFIS have control mechanisms in place to ensure users are authorized to request and receive the IDR.

Currently, 110 jurisdictions representing 15 states and two federal agencies are participating in shared services. As of January 6, 2010, there have been 2,883,975 submissions sent to the DHS's IDENT, resulting in 331,379 matches to IDENT data.

Full Search of the Criminal Master File (CMF) Repository

In December 2007, utilizing Shared Services, IDENT began submitting 10-prints gathered by DHS CBP at ports of entry to the FBI CJIS Division for a full search of the CMF. All positive identifications are returned to IDENT within 72 hours (the majority of searches and results are returned within 15 minutes). Since the individuals have already been admitted into the United States (U.S.), the positive identification records are promoted to the IDENT Watchlist. Upon subsequent entry into the United States, the individuals are identified at CBP primary inspection as an IDENT Watchlist "hit" and are referred to CBP secondary inspection for further determination of admissibility. The DHS ICE began reviewing the criminal histories of those positively identified in November 2009, and it was reported in December that of those that have been reviewed 90% have been demoted from the IDENT Watchlist.

The DHS response request for CMF searches of 10-prints submitted from CBP primary is now 10 seconds. The FBI CJIS Division is evaluating the request within Next Generation Identification (NGI), and is currently evaluating the feasibility of providing a rapid response with the IAFIS. If feasibly possible, the DHS will need to make technical changes that are necessary to receive the response back at primary inspection.

As of 12/31/2009, IAFIS processed 28, 818, 314 submissions from CBP primary which resulted in the positive identification of 319,944 individuals who have criminal history information that may impact their admissibility to the U.S. Additionally, IAFIS processed 43, 394, 717 submissions from IDENT (including those from DOS) which resulted in 426,666 positive identifications.

Secure Communities Update

The DHS/ICE Secure Communities initiative is improving community safety by transforming the way the federal government cooperates with state and local law enforcement agencies to identify, detain, and remove all criminal aliens held in custody. The Secure Communities strategy is changing immigration enforcement by using technology to share information between law enforcement agencies and by applying risk-based methodologies to focus resources on assisting all local communities with removing high-risk criminal aliens. In conjunction with the Interoperability effort, additional state and local law enforcement agencies are gaining biometric-based access to the full IDENT repository through the DHS/ICE Secure Communities initiative. IDENT /IAFIS Interoperability is assisting ICE and local law enforcement officers by positively identifying criminal aliens in prisons and jails. The initial focus has been to identify and remove aliens who

have been convicted of or are currently charged with a Level 1 crime. Level 1 crimes include, but are not limited to the following: homicide, kidnapping, sexual assault, and aggravated assault. The long term goal will focus on identifying and removing all criminal aliens held in federal, state and local jails and prisons.

Cumulative Secure Communities Statistics

10/27/2008 through 12/25/2010

Number of Fingerprint Submissions Received Through Interoperability	Number of Matches (Hits) in IDENT	IARs Generated by LESC (Level 1 Crimes)	Number of Detainers Issued (Level 1 Crimes)
1,159,205*	**137,525***	**12,881**	**5,610**

* Does not include OPM, FBI Mobile data or data from 287 (g) sites.

Success Stories:

GWINNETT COUNTY, GA – On December 4, 2009, the Gwinnett County Sheriffs Office arrested a native of the Bahamas for violating terms of probation, which he received for felony residential burglary conviction. Upon initial booking into Gwinnett County Jail, he claimed to be a United States citizen and provided false biographic information; thus he did not come to the attention of ICE agents. However, and IDENT/IAFIS Interoperability hit prompted records checks that revealed a criminal history that spans ten years and two states. His convictions include felony battery on law enforcement, felony cocaine possession, felony habitually driving without a license, battery, and family violence. He has used at least 15 aliases during 25 previous encounters with law enforcement, The subject is currently incarcerated at the Gwinnett County Jail, and will be released into ICE custody upon completion of his current sentence.

LOS ANGELES, CA – On November 18, 2009, the Huntington Park Police Department (HPPD) arrested a Mexican male subject for using improper lighting equipment on a bicycle. Upon book-in at the HPPD, his fingerprints were automatically submitted through IDENT/IAFIS Interoperability. Records checks indicated he is a previously deported aggravated felon who was convicted of second degree murder in 1990. After serving nine years in prison, he was removed from the U.S. He has used multiple aliases during previous arrests for weapon possession, drug possession, and parole violation. He is also believed to be an active member of the Florencia 13 street gang. The subject is currently in custody awaiting his criminal trial for Title 8 U.S.C. § 1326 (re-entry of removed alien) prosecution.

FBI Mobile

The Quick Capture Platform (QCP) initiative allows FBI Special Agents to capture biometric samples in remote field settings for submission to both IAFIS and other biometric databases that will accept the data. The initial user of the QCP was the CJIS Division's Hostage Rescue Team (HRT) which operates in both domestic and foreign theaters, often in conjunction with U.S. military assets. The HRT operationally deployed the QCP in Iraq in April 2007, searching the IAFIS and the DOD Automated Biometric Identification System (ABIS).

The capture and analysis of biometrics from suspects encountered during these missions has proven to be a vital tool in determining associations and past criminal, law enforcement with US agencies. With the deployment of Shared Services in October 2008, FBI Agents using QCP devices became an obvious candidate for its use. Consequently, with an Interoperability Initiative known as FBI Mobile, the FBI began forwarding QCP searches from the HRT in Iraq over to the DHS IDENT system in March 2009, through Shared Services.

For Phase I, the same IDENT Data Response (IDR) that is currently being provided to state and local law enforcement agencies was provided for FBI Mobile through the same technical infrastructure, with the exception that no IAQs were to be sent to the ICE LESC on biometric matches. This was due to the fact that the initial subjects of FBI Mobile were out of the country in Iraq.

FBI Mobile Phase II is focusing on providing the full IDENT response. Furthermore, in December 2009, the DHS approved additional FBI Mobile searches of IDENT from QCP devices located domestically and used by FBI Agent Task Forces of various FBI Field Offices throughout the country (i.e., Crimes Against Children Units or CACUs). This change in the FBI Mobile population, to include subjects of interest who were domestically located, necessitated discussions with the DHS ICE and approval was obtained to incorporate the capability of IAQs for an immigration status for the domestic, FBI Mobile searches. Finally, the most recent current FBI Mobile efforts have involved establishing a way for the ICE LESC to distinguish the FBI Mobile searches as criminal investigative searches from the criminal bookings of state and local law enforcement.

DHS Transition from 2 to 10 Print

In September 2009, DHS achieved a major milestone toward interoperability by deploying 10-print scanners to the CBP primary processing lanes that provide the capability to capture 97% of in-scope travelers with full deployment. The 10-Print process allows for enhanced border security. The DHS 10-Print process benefits state and local law enforcement by identifying aliens with active wants/warrants

with improved accuracy and permits DHS to better screen individuals with criminal histories seeking admission to the United States.

Identification for Firearms Sales/Sexual Offender Registry Data

Prior to the delivery of a 10 second search of the entire CMF through NGI, CJIS has identified two distinct data sets (Sexual Offender Registry [SOR] and Identification for Firearms Sales [IFFS] flagged records with a disqualifier) that can be shared using the existing Shared Services functionality. Retention of this data will remain consistent with the Interoperability MOU. The MOU states "the fingerprint images will not be retained outside of the separate repositories so established, unless the data repository that the holding Party manages (IAFIS and IDENT, respectively) reflects an independent encounter with the subject." Once a 10 second search of the entire CMF is available, this preemptive searching of IFFS and SOR records will cease.

Each of these data sets will require separate processing for legacy and day-forward records. Through an established Working Group, the day-forward record processing has been identified and documented jointly through workflow diagrams and use cases. The legacy processes are still being considered. An IFFS/SOR working document has been created to work through process and technical agreement. The official technical agreement will be captured in an update to the jointly held Interface Control Agreement.

Data Protection Strategies

The Interoperability IPT continues to work toward implementation of the nine data protection strategies previously endorsed by the APB. The Interoperability IPT has agreed to continue their implementation as follows:

Data Protection Strategy	Shared Data	Shared Services	Status
Strategy 1: Communication	Fully brief composite model to all Interoperability Stakeholders (OMB, Congress, Homeland Security Council, DHS Stakeholders, FBI Advisory Policy Board, National Crime Prevention and Privacy Compact, etc.)		Ongoing
Strategy 2: Inventory of Shared Data	Prior to deployment, DHS/US-VISIT and DOJ/FBI will compare the data residing in each system and ensure each system reflects data that is accurate, current, timely, and relevant.	DHS/US-VISIT and DOJ/FBI will work together to begin identifying and linking "common" records	In June 2008, an APB Informational Topic Paper discussed an implementation change to Data Protection Strategy #2. As opposed to a technically challenging "initial sync" of both systems, the agencies intend to incrementally establish record

			links as transactions are directed to the alternate agency.
Strategy 3: Mission-Related Data	Data will be retained within each respective system consistent with the agency's mission.		Strategy will be achieved with implementation of the shared data and shared services methodologies.
Strategy 4: Data Management	Strict data management policies will be developed to govern the removal and demotion of records to ensure each system contains accurate, complete, timely, and relevant data.	By nature of this model, each agency will be assured of receiving the most current and accurate data	The IS Subcommittee's Recommendations for Clarification on Record Linking were presented to the Spring 2009 APB. The APB passed a motion to accept Option #1 with amended verbiage stating a state can opt out of receiving response. Additionally the approved motion included a friendly amendment to continue the use of the TCN/FBI number conversion. As of September 2009: - removal of all "non-linked" records within IDENT - Database delete: completed - Matcher delete: completed 1 year ahead of schedule - Software changes to handle future demote/delete messages: * Change Request was approved within US-VISIT * Under review to schedule for deployment * Implemented process to deleted unlinked wants/warrants on a weekly basis until the CR is deployed
Strategy 5: Data to be Shared	Information to be shared will consist of data necessary to accomplish the mission in a timely and efficient manner (e.g., fingerprint images and limited biographic data). Data will be shared in a consistent manner with existing business practices.		Ongoing – data remains consistent with iDSM data. Additionally, CJIS has identified two distinct data sets (IFFS and SOR) and is working to provide the data sets utilizing the existing Shared Services functionality.
Strategy 6: FBI Number	A unique identifier will be exchanged in the shared data model to point back to the owning agency's record. This unique identifier will provide for immediate access to remaining information for authorized purposes. The	FBI Number will be a manner consistent with existing business services.	The current use and process of the FBI Number will remain, as well as the use of the TCN/FNU conversion.

	unique identifier will support current business practices.		
Strategy 7: Audit	Rigorous audit and run controls will be established and implemented.		Presented approach during Spring 2008 round of APB. Agreed to expand log reviews as appropriate; real-time audits supported within constraints; exploration of new audit tools.
Strategy 8: Prevention of Third-Party Sharing	Develop a Memorandum of Understanding (MOU) to prevent third party sharing of IAFIS and DHS data outside of the original purpose.		Strategy addressed in Interoperability MOU and Appendices – final signature received August 1, 2008.
Strategy 9: Hit Notification	Administrative messages will be issued to the wanting agency and the inquiring agency when subjects of wants and warrants are encountered by DHS.	Current business practices will continue.	DHS and FBI working to resolve multiple hit notifications in activity log.

Next Steps

This paper outlines the recent progress achieved by the Interoperability IPT toward enhancing the exisiting biometric-based Interoperability between the IAFIS and IDENT. The FBI CJIS Division will continue to work towards bringing on additional criminal justice and non-criminal justice users through the Interoperability User Evaluation and Deployment Strategy, as well as continuing to work with DHS/ICE to deploy additional sites through the Secure Communities initiative. In addition, the FBI and DHS is preparing a final report on the IDR Evaluation. Finally, the functionality for Next Generation Identification (NGI) is being developed and will be delivered incrementally. The FBI is working to determine the impacts to Interoperability participants when the transition to NGI occurs.