

**MEMORANDUM OF UNDERSTANDING**  
**among the**  
**DEPARTMENT OF HOMELAND SECURITY**  
**the**  
**DEPARTMENT OF JUSTICE**  
**FEDERAL BUREAU OF INVESTIGATION**  
**CRIMINAL JUSTICE INFORMATION SERVICES DIVISION**  
**and the**  
**DEPARTMENT OF STATE**  
**BUREAU OF CONSULAR AFFAIRS**  
**for**  
**IMPROVED INFORMATION SHARING SERVICES**  
**July 1, 2008**

I. INTRODUCTION AND PURPOSE

This Memorandum of Understanding (MOU) and its appendices are entered into between and among the Department of Homeland Security (DHS), through its National Protection and Programs Directorate, United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, and through U.S. Immigration and Customs Enforcement (ICE); the Department of Justice's (DOJ) Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division; and the Department of State's (DOS) Bureau of Consular Affairs (CA), each a "Party" and collectively the "Parties," to improve information sharing among Federal agencies pursuant to statutes and Executive Orders and consistent with Congressional appropriations guidance.

Certain biometric and biographic data, respectively maintained by the Parties, will be exchanged through primarily automated processes between the FBI CJIS Division's Integrated Automated Fingerprint Identification System (IAFIS) and US-VISIT's Automated Biometric Identification System (IDENT). Hereafter, this process is referred to as "Interoperability."

II. SCOPE

The scope of this MOU is limited to the exchange of agreed-upon data among the Parties for the purposes of national security, law enforcement, immigration and border management, and intelligence, and to conduct background investigations for national security positions and certain positions of public trust.

### III. LEGAL AUTHORITIES

#### A. Legal authorities supporting, supported by, or relevant to the enhanced cooperation among the Parties established by this MOU:

- 5 U.S.C. §552a, as amended (Privacy Act of 1974).
- 5 U.S.C. §9101 (Security Clearance Improvement Act).
- The Homeland Security Act of 2002, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, and the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, *and subsequently codified at* 6 U.S.C. §§101, et. seq.
- 8 U.S.C. §1105 (Access to National Crime Information Center files).
- 8 U.S.C. §1182 (Inadmissible aliens).
- 8 U.S.C. §1185 (Travel control of citizens and aliens).
- 8 U.S.C. §1202(f) (Confidential Nature of Records).
- 8 U.S.C. §1225 (Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing).
- 8 U.S.C. §1229a (Removal proceedings).
- 8 U.S.C. §1281 (Alien crewmen).
- 8 U.S.C. §1357 (Powers of immigration officers and employees).
- 8 U.S.C. §1365a and *note* (Integrated entry and exit data system).
- 8 U.S.C. §1365b (Biometric entry and exit data system).
- 8 U.S.C. §1379 (Technology standard to confirm identity).
- 8 U.S.C. §1722 (Interoperable law enforcement and intelligence data system with name-matching capacity and training).
- 8 U.S.C. §1731 (Implementation of an integrated entry and exit data system).
- 28 U.S.C. §534 and *note* (Acquisition, preservation, and exchange of identification records and information; appointment of officials).
- 42 U.S.C. §14616 (National Crime Prevention and Privacy Compact Act).
- Pub. L. 107-173 (Enhanced Border Security and Visa Entry Reform Act of 2002).
- Pub. L. 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004).
- Ex. Ord. No. 13388: Homeland Security Information Sharing (October 25, 2005).
- Homeland Security Presidential Directive No. 6: Integration and Use of Screening Information (September 16, 2003).
- Homeland Security Presidential Directive No. 11: Comprehensive Terrorist-Related Screening Procedures (August 27, 2004).

- H.R. Conf. Rep. 109-699 (September 28, 2006) (Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007).
- H.R. Conf. Rep. 109-272 (November 7, 2005) (Appropriations for Science, the Departments of State, Justice, and Commerce, and related agencies for the Fiscal Year Ending September 30, 2006).
- H.R. Conf. Rep. 108-792 (November 20, 2004) (Appropriations for Foreign Operations, Export Financing, and Related Programs for the Fiscal Year Ending September 30, 2005).
- H.R. Conf. Rep.. 108-792 (November 20, 2004) (Consolidated Appropriations Act, 2005).
- H.R. Conf. Rep. 108-10 (February 13, 2003) (Making Further Continuing Appropriations for the Fiscal Year 2003, and for Other Purposes).
- H.R. Conf. Rep. 107-278 (November 9, 2001) (Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2002).
- H.R. Conf. Rep. 106-1005 (October 26, 2000) (Incorporating Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2001).
- H.R. Conf. Rep. 106-479 (November 18, 1999) (Consolidated Appropriations Act, 2000).
- H. Rep. 4818 (Consolidated Appropriations Act, 2005).
- S. Rep. 108-280 (June 17, 2004) (Department of Homeland Security Appropriations Bill, 2005).
- 71 Fed. Reg. 42651 (June 6, 2007) (Automated Biometric Identification System (IDENT)] System of Records Notice).
- 64 Fed. Reg. 52343 (September 28, 1999) (Fingerprint Identification Record System (FIRS) System of Records Notice).

#### IV. BACKGROUND

##### A. Interoperability

The requirement and need for interoperability between the IDENT and IAFIS systems is cited in, or can be inferred from, various laws, Executive Orders, and congressional appropriations guidance. Interoperability will enable the sharing of biometric and related biographic, criminal history, and immigration information to meet the respective agencies' missions.

In 2006, the Parties launched the first phase of Interoperability, known as the interim Data Sharing Model (iDSM). Under iDSM, biometric and limited biographic data on certain categories of individuals are exchanged, specifically: Expedited Removals and

Category One visa refusals are made available to the FBI CJIS Division by US-VISIT, and known or suspected terrorists (KSTs) and individuals who are subjects of wants and warrants are made available to US-VISIT by the FBI CJIS Division.

This MOU provides for the sharing of information in accordance with the agreed-upon technical solution for expanded IDENT/IAFIS Interoperability, which will provide access to additional data for a greater number of Authorized Users.

## B. Description of the Parties

1. Department of Homeland Security: an agency of the United States (U.S.) Government, acting through—
  - a. US-VISIT: An office within the National Protection and Programs Directorate that manages IDENT, a system that stores and processes biometric and limited biographic data on millions of individuals. US-VISIT serves as the steward for data stored in IDENT by itself and other offices, components, and agencies, including, among others, U.S. Customs and Border Protection, ICE, U.S. Citizenship and Immigration Services, and DOS.
  - b. ICE: A component that chairs the DHS Law Enforcement Shared Mission Community and which is principally responsible for supporting the DHS Information Sharing Coordination Council and the DHS Information Sharing Governance Board in the coordination and oversight of all law enforcement information-sharing initiatives within DHS. ICE is the primary criminal investigative arm of DHS and, as such, coordinates closely with the FBI CJIS Division on the exchange of investigation-related information.
2. FBI CJIS Division: An FBI Division that manages the Fingerprint Identification Records System (FIRS). The FIRS contains the criminal histories of millions of individuals, which are supported by ten rolled, digitized fingerprint images of U.S. citizens and aliens contributed by federal, state, local, and tribal law enforcement agencies. The FIRS also contains a civil fingerprint repository containing millions of sets of ten-fingerprint images.

Records within FIRS are maintained as automated records within IAFIS, which provides for the searching of the available fingerprint repository to provide positive identifications for both tenprint rolled and tenprint flat fingerprint submissions, as well as latent fingerprint searches.

3. CA: A bureau of DOS that manages the Biometric Visa Program, through which fingerprints are collected from visa applicants to be searched and stored in IDENT and searched in IAFIS. In addition to fingerprints, certain biographic information about visa applicants is stored in IDENT. DOS is an integral user of IDENT and IAFIS services due to its issuance of biometric visas.

## V. SCOPE AND METHOD OF DATA EXCHANGED

In support of Interoperability, the Parties currently, and under this MOU will continue to, allow for the exchange of data in a manner that is secure, timely, and controlled in accordance with this MOU and other agreed-upon technical and business documents maintained on the joint Configuration Item List (CIL).

This MOU provides for a separate data repository to be held by US-VISIT, at its location, which is reproduced from fingerprint images and related data on “high priority” subjects selected from IAFIS by the FBI CJIS Division. This MOU also provides for a separate data repository to be held by the FBI CJIS Division, at its location, that is reproduced from fingerprint images and related data on “high priority” subjects selected from IDENT by ICE. The FBI CJIS Division and DHS agree that 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.

Further, the FBI CJIS Division and DHS will provide to each other a service whereby each will query allowed data sets in IAFIS and IDENT, respectively, in search of subject(s) requested by the other system manager for the benefit of the other Parties and their Authorized Users. However, the queries for Authorized Users will only be processed for Authorized Uses. This service will be performed in accordance with each agency’s established dissemination/disclosure rules and/or processes.

A positive identification in IAFIS will generate a response that allows the retrieval of criminal history record information maintained within the IAFIS repository to Authorized Users for Authorized Uses. A verification of identity in IDENT will generate a response that allows the retrieval of identity information maintained within IDENT to Authorized Users for Authorized Uses.

These information sharing processes shall not impact other notification procedures utilized between and among the Parties, mission independence of the Parties, or existing customer service levels or capabilities.

This MOU does not permit a Party to store another Party’s data unless such storage is authorized herein; otherwise specifically authorized in writing by the originating Party; or required under statute, regulation, or Executive Order. The Parties do not intend that this MOU will change the *status quo ante* regarding storage by one Party of data originated by another Party. This MOU does not cover searching for matches of latent fingerprints, which will be addressed by another MOU.

## VI. RESTRICTIONS ON THE USE AND DISCLOSURE OF INFORMATION

Data provided, exchanged, retained, or otherwise governed by this MOU shall not be shared, handled, or further disseminated in a manner that would violate Federal law, regulation, or applicable System of Records Notices (SORNs).

The Parties agree to limit access to the information shared under this MOU to Authorized Users with a need to know the information to carry out national security, law enforcement, immigration and border management, or intelligence, or to conduct background investigations for national security positions and certain positions of public trust.

Each Authorized User seeking IDENT information through the FBI CJIS Division, and with whom the FBI CJIS Division shares information, must be fully disclosed upon request to US-VISIT (and, in the case of visa records, CA), along with the details of the information shared. Each Authorized User seeking IAFIS information through US-VISIT, and with whom US-VISIT shares information, must be fully disclosed upon request to the FBI CJIS Division, along with the details of the information shared. This disclosure shall be made through a record of the fact that the information was shared in the form of an electronic or manual audit log.

In addition to the aforementioned, all data will be exchanged between the Parties in accordance with the following conditions:

A. Information of Mutual Interest to Law Enforcement Agencies

Where one or more authorized users with a law enforcement mission have a mutual interest based on IDENT information shared pursuant to this MOU, the Authorized User shall coordinate directly with ICE. Further, unless there are exigent circumstances requiring immediate action, the Authorized Users will verify information and coordinate with the appropriate Party before taking law enforcement action. Any intelligence product derived from Interoperability that identifies potential violations of law will be referred in advance to ICE, and release of the intelligence product will be coordinated in advance with ICE. Additionally, the Parties will notify ICE of any potential violations, which fall under the statutory authority of ICE, identified during review or analysis.

B. Disclosures to Third Parties

Each Party determines whether its own data will be disclosed to third parties, as follows:

1. IAFIS Data: Before any information originating from the FBI's IAFIS can be disclosed to a third party, as defined in the MOU, US-VISIT shall contact the FBI CJIS Division to determine the appropriate action or response. In addition, other than disclosures authorized above, for any requests made to US-VISIT by DHS components, stakeholders, or third parties regarding IAFIS information in batch format (including replication of any portion of the IDENT database containing IAFIS originated biometric or biographic data) or analysis of IAFIS information, US-VISIT shall contact the FBI CJIS Division to determine the appropriate action or response. Should the FBI CJIS Division agree to US-VISIT's disclosure of the information, US-VISIT shall document the disclosure and provide such documentation to the FBI CJIS Division. The disclosed data may only be used for the stated purposes of the sharing and may not, under any circumstances, be disclosed to any other entity, including the general public, without the express written consent of the FBI CJIS Division.

2. IDENT Data: Before any information originating from DHS's IDENT can be disclosed to a third party, as defined in this MOU, the FBI CJIS Division shall contact US-VISIT to determine the appropriate action or response. If the information from IDENT is from a visa record, the procedures in section VI.B.3 apply. In addition, other than disclosures authorized above, for any requests made to the FBI CJIS Division by DOJ components, stakeholders, or third parties regarding IDENT information in batch format (including replication of any portion of the IAFIS database containing DHS originated biometric or biographic data) or analysis of IDENT information, the FBI CJIS Division shall contact US-VISIT, which will consult with the DHS data owner to determine the appropriate action or response. Should US-VISIT agree to the FBI CJIS Division's disclosure of the information, the FBI CJIS Division shall document the disclosure and provide such documentation to US-VISIT. The disclosed data may only be used for the stated purposes of the sharing and may not, under any circumstances, be disclosed to any other entity, including the general public, without the express written consent of US-VISIT.
  
3. Visa Data: DOS retains responsibility for determining whether disclosure of its records is for a purpose consistent with section 222(f) of the Immigration and Nationality Act (INA)(8 U.S.C. § 1202(f)). For the purposes of this MOU only, DOS, through CA, hereby provides its consent to the FBI CJIS Division to share DOS visa records with other agencies at the federal, state, local, and tribal levels for the administration or enforcement of the laws of the United States. The FBI CJIS Division will ensure that the recipient entity is advised in writing that DOS visa records are governed by Section 222 (f) of the INA; are being disclosed to the entity consistent with Section 222(f) and this MOU; may only be used for the purposes for which they are being shared; and may not under any circumstances be disclosed to any other entity, including the general public, without the express written consent of DOS. The FBI CJIS Division will also advise the recipient entity that any questions concerning the interpretation of DOS visa records must be addressed by DOS. However, should access to DOS visa refusals generate inquiries by end users about a person's legal status in the U.S., such inquiries are to be directed to DHS, which has jurisdiction over questions of legal status in the U.S. DHS disclosure of visa data in IDENT will be in accordance with the DOS-DHS MOU for Cooperation in Enhanced Border Security, dated January 11, 2005. The FBI CJIS Division will not disclose any DOS visa record to any foreign government or other international or multilateral entity, unless it has first obtained the express written consent of DOS, which will determine whether such disclosure would be consistent with Section 222 (f) of the INA.

#### C. Restriction to Authorized Users and Authorized Use

Each Party is responsible for ensuring that it provides data received under this MOU (and that it did not originate) only to Authorized Users and that the purpose for obtaining data by such users is for an Authorized Use. Each Party is further responsible for ensuring that its Authorized Users maintain, use, and retain such data in compliance with the terms and conditions of this MOU and its appendices.

## VII. MAINTENANCE AND DISPOSAL OF DATA

### A. Data Maintenance

1. Maintenance Rules: The data covered in this MOU will be maintained in accordance with the following rules—
  - a. Data provided to the FBI CJIS Division by federal, state, local, and tribal law enforcement and authorized noncriminal justice agencies shall be maintained by the FBI CJIS Division, except to the extent such data is originated with DHS or DOS, which would be subject to the following stipulation: data provided to the FBI CJIS Division by DHS or DOS will not be maintained by the FBI CJIS Division, unless authorized herein, otherwise specifically authorized in writing by DHS or DOS, or required to be maintained by the FBI CJIS Division under statute, regulation, or Executive Order.
  - b. Immigration and border management-related data provided to US-VISIT by DHS and CA will be maintained by US-VISIT.
  - c. Each originating Party will retain control and ownership or stewardship over the data that it shares, except where otherwise required by statute, regulation, or Executive Order.
  - d. DHS policy affords non-U.S. persons (i.e., neither U.S. Citizens nor Lawful Permanent Residents of the U.S.) from whom DHS has collected personally identifiable information (PII) maintained in a “mixed-use” Privacy Act system of records (i.e., one containing PII of both U.S. persons and non-U.S. persons), such as IDENT, the administrative rights of access (to their PII) and amendment (of their records) under the Privacy Act, subject to applicable exceptions and exemptions provided by the governing SORN and regulations. However, this policy does not extend or otherwise create a right of judicial review under the Privacy Act for non-U.S. Persons.
  - e. The maintenance of the data provided by the FBI CJIS Division will be guided by the CJIS Advisory Policy Board (APB).
  - f. The Parties shall individually and collectively use their best efforts (recognizing that some of the personally identifiable data is self-reported and may be incorrect) to ensure that PII is accurate, relevant, current, and complete, and that such data is shared and handled in accordance with the terms and conditions of this MOU which Parties represent are consistent, and shall be construed in accordance, with existing agency policies and SORNs for their respective systems.
  - g. Upon notice from the respective data owner the Parties shall, in a timely manner, correct any errors discovered. The most current information held in each system will be available upon subsequent record requests.



- h. In addition to the Parties' regular audit schedules, upon written request by any Party, the Parties shall conduct privacy and security audits of one another to ensure compliance with the privacy and security requirements set forth in this MOU. All Parties shall conduct such audits in accordance with their own audit policies. The results of such audits shall be exchanged with the other Parties.
- i. Each Party will utilize its own redress procedures to process requests by individuals seeking review or correction, or both, of data collected by that Party.

## B. Data Disposal

1. Disposal Rules: The data covered in this MOU shall be disposed of in accordance with the following rules—
  - a. Each Party shall retain and dispose of the data covered under this MOU in accordance with its own records control schedules, or, if applicable, general records schedules.
  - b. The disposition of the data provided by the FBI CJIS Division shall be guided by the CJIS APB.
  - c. A holding Party shall remove a subject's data from its separate data repository upon receiving a request to do so from the Party providing the data unless the holding Party had an independent encounter with the subject, or the data is relevant for enforcing or administering federal immigration, customs, or other law and corresponding regulations. If information on a subject is removed by one of the Parties, links to that information in the holding Party's system shall also be removed.

## VIII. DATA SECURITY

### A. Data Security Rules

1. Safeguards: The Parties agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the data shared under this MOU against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification, or deletion. All data shared under this MOU shall be protected in accordance with legal, regulatory, and policy requirements through administrative, technical, and physical safeguards appropriate to the sensitivity of the data. All personally identifiable and other Sensitive But Unclassified (SBU) information or Controlled Unclassified Information (CUI) that one Party shares with another Party under this MOU shall be encrypted when placed on portable media (including, but not limited to, thumb drives, compact discs, or laptops), excluding any media maintained under the physical safeguards of DOS Diplomatic Security. All data provided by the FBI CJIS Division shall be protected as guided by the CJIS APB and CJIS Security Policy. These safeguards are to be implemented in a manner consistent with safeguards required by law and executive branch policy, including any forthcoming requirements on the treatment and handling of SBU or CUI.

2. **Unclassified Data:** The data shared is SBU or CUI, and shall be marked and handled in accordance with existing or future policies and procedures on SBU or CUI.
3. **Audit:** The Parties agree to maintain a log of all data received and sent, including name or Originating Agency Identifier (ORI) of the recipient and sender, as well as date and type of transmission. Each Party may make a written request for a copy of this log at any time to ensure compliance with this provision. The log must be made available no later than two business days after the request. All Parties agree to reconcile the log on a regular basis.

## IX. PRIVACY AND PRIVACY AWARENESS

### A. Privacy and Privacy Awareness Principles

The Parties shall adhere to the following principles:

1. **Strict Confidentiality:** PII shall only be disclosed to Authorized Users with a need to know and only for uses that are consistent with the stated purposes under this MOU and otherwise compatible with the purpose for which the information was originally collected.
2. **Privacy and Security Awareness Training:** All persons who receive access to data pursuant to this MOU shall be appropriately trained regarding the proper treatment of PII to ensure the overall safeguarding of the information in accordance with existing policies of the Parties.
3. **Limiting Collection, Use, Disclosure, and Retention:** The collection, use, disclosure, and retention of PII shall be limited to that which is relevant and necessary for purposes of the Parties as set forth in this MOU.

## X. COMMUNICATIONS AND REPORTING

To further safeguard the privacy, security, confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the Parties agree to:

### A. Privacy or Security Breach Notification

Consistent with the Office of Management and Budget Memoranda 06-19 (OMB M-06-19) and 07-16 (OMB M-07-16), the Parties shall notify each other immediately by phone and email once a Party becomes aware of any potential breach in security, especially those that result in unauthorized use or disclosure of any personal information or other data shared under this MOU. For DHS, the point of contact is the US-VISIT Information System Security Manager (ISSM) at: Phone – (202) 298-5200; E-mail – [us-visitbreachnotification@dhs.gov](mailto:us-visitbreachnotification@dhs.gov), regarding any breaches that occur. For FBI, the point of contact is an FBI CJIS Division Computer Security Incident Response Capability representative at: Phone – (304) 625-2000; E-mail – [iso@leo.gov](mailto:iso@leo.gov). For DOS, the point of contact is the Computer Incident Response Team (CIRT) in the Bureau of Diplomatic Security at: Phone – (301) 985-8347; E-mail – [CIRT@state.gov](mailto:CIRT@state.gov).

## B. Disasters and Other Contingencies Notification

The Parties shall immediately notify each other by telephone or e-mail in the event a disaster or other contingency disrupts the normal operation of the connected systems.

## XI. COST

This MOU does not create an obligation or commitment of funds, nor is it a basis for the transfer of funds. This MOU is a basic statement of the understanding among the Parties of the tasks and methods for performing the tasks described in this MOU. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that the existence of this MOU in no way implies that Congress will appropriate funds for such expenditures.

## XII. GENERAL PROVISIONS AND CONSTRUCTION

### A. General Provisions

1. *Force Majeure*: No Party shall be responsible for delay or default in performing this MOU if such delay or default is caused by conditions beyond its control, including, but not limited to, Acts of God, wars, insurrections, or any other cause beyond the reasonable control of the Party whose performance is delayed or prevented.
2. *Settlement of Disputes*: Disagreements arising under or relating to this MOU are to be resolved by consultation among the Parties, including, as necessary, escalation within each organization and to the Executive Steering Committee (ESC) for Interoperability. Disagreements not resolved among the Parties shall be resolved pursuant to Executive Order No. 12146 § 1-4 (Resolution of Interagency Legal Disputes).
3. *Data Governance*: The Parties agree to maintain a joint CIL containing all jointly-held business and technical interoperability documents and to comply with the provisions of those documents as they are updated.
4. *Termination*: This MOU may be terminated by the mutual written consent of all Parties. Additionally, any Party may terminate its participation for any reason whatsoever upon ninety (90) calendar days written notice to the other Parties.
5. *Collaborative Reviews*: The Parties shall designate responsible officials to meet, at the request of any Party, to discuss and review the implementation of this MOU. Any disagreement over the implementation of this MOU shall be resolved in accordance with section XII.A.2.

### B. Construction

1. *Contra Proferentem*: This MOU was formed by all Parties, and ambiguities, vagueness, or omissions shall not be construed against any specific Party.

2. Severability: This MOU is not intended to conflict with current law or regulation or the directives of DHS, DOJ, DOS, or OMB. If any term of this MOU is inconsistent with such authority, then the term shall be invalid, but the remaining terms and conditions of this MOU shall remain in full force and effect. The failure by a Party to require performance of any provision of this MOU shall not affect that Party's right to insist upon performance at any time thereafter, nor shall a waiver of nonperformance in a single instance constitute a waiver of nonperformance thereafter.
3. No Right or Benefit Created: This MOU is not intended, nor should it be construed, to create any right or benefit, substantive or procedural, enforceable at law, equity, or otherwise, by any third party against the Parties, their parent agencies, the U.S., or the officers, employees, agents, or contractors thereof.
4. Other Agreements: This MOU and its appendices, any amendment to this MOU, or the termination of this MOU shall not affect any other agreements or understandings that are outside of the scope of this MOU. This MOU does, however, supersede the Letters of Concurrence under which the Parties had been operating, which address matters within the scope of this MOU.

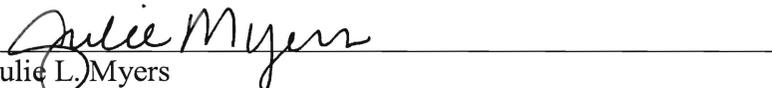
XIII. AMENDMENT

Any amendment, modification, or waiver of this MOU or its provisions shall be documented in writing and executed by the signatories or their delegates or successors.

ON BEHALF OF DEPARTMENT OF HOMELAND SECURITY

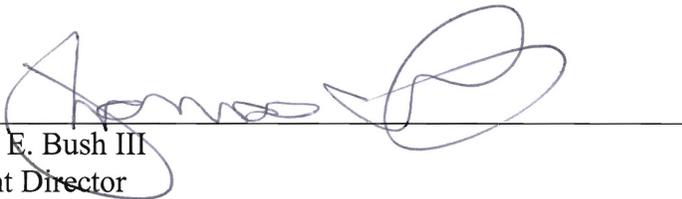
  
\_\_\_\_\_  
Robert A. Moczynski  
Director  
US-VISIT Program  
National Protection and Programs Directorate

JUL 2 2008  
Date

  
\_\_\_\_\_  
Julie L. Myers  
Assistant Secretary  
U.S. Immigrations and Customs Enforcement

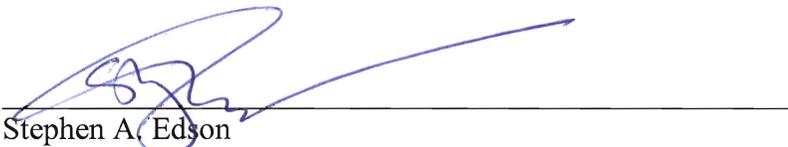
7/08/08  
Date

ON BEHALF OF THE DEPARTMENT OF JUSTICE

  
\_\_\_\_\_  
Thomas E. Bush III  
Assistant Director  
FBI CJIS Division

8/1/08  
Date

ON BEHALF OF THE DEPARTMENT OF STATE

  
\_\_\_\_\_  
Stephen A. Edson  
Deputy Assistant Secretary for Visa Services  
Bureau of Consular Affairs

7/17/08  
Date

## Appendix 1

### Definitions

**Administration of Criminal Justice:** means 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. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information. 28 C.F.R. 20.3(b).

**Authorized Users:** See Appendix 2.

**Authorized Use:** See Appendix 2.

**Breach:** means “the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.” Office of Management and Budget Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).

**CJIS Advisory Policy Board (APB):** means the Board established to obtain the criminal justice community’s advice, guidance, and concurrence on proposed enhancements to existing FBI CJIS Division information services as well as new information services being developed. The APB is responsible for reviewing appropriate policy, technical, and operational issues related to the FBI CJIS Division programs and makes recommendations to the FBI Director. The Advisory Process consists of two main components, the APB and Working Groups, which have been chartered by the Attorney General under the provisions of the Federal Advisory Committee Act.

**Configuration Item List:** means a list of jointly held artifacts/documents agreed to by the parties for the purposes of the Interoperability initiative that are subject to a joint change management process.

**Criminal History Record Information:** means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system. 28 C.F.R. 20.3(d).

**Executive Steering Committee (ESC) for Interoperability:** means a committee, consisting of DOJ, DHS, and DOS executives and members (including stakeholder representation) considered to be business owners for Interoperability, that identifies and determines high-level policy, business, and data requirements; as well as guide the design, development, and implementation of Interoperability.

**Interstate Identification Index (III):** means the cooperative Federal-State system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI. 28 C.F.R. 20.3(m).

**National Crime Prevention and Privacy Compact (Compact) Act of 1998:** established an infrastructure by which federal and state agencies may exchange criminal history records for noncriminal justice purposes according to the laws of the requesting Party. The Compact established a 15-member council comprised of representatives from federal and state criminal and noncriminal justice agencies. This council monitors the operations of the III system and promulgates rules and procedures for the effective use of the III for noncriminal justice purposes. (See 42 U.S.C. 14616)

**Noncriminal Justice Purposes:** means uses of criminal history records for purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. 42 U.S.C. 14616.

**Personally Identifiable Information (PII):** means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records (i.e., fingerprints and photographs), phone number, e-mail address, physical address, signature, passport number, and radio frequency identification (RFID) tag numbers, including any other personal information which is linked or linkable to an individual.

**Third Party:** means agencies and business organizations that are neither Parties nor Authorized Users that seek to query IDENT or IAFIS through the FBI CJIS Division or US-VISIT for an Authorized Use. For third parties seeking to become Authorized Users, refer to Appendix 2 ("Authorized Use" Section I.G.).

## Appendix 2

### Authorized Users/Authorized Uses

This appendix defines and clarifies the terms Authorized User and Authorized Use, as used in the MOU.

**Authorized User:** means the Parties (the DHS, the DOS, and the DOJ), together with federal, state, local, tribal, foreign, and international law enforcement agencies and other users of the IAFIS and IDENT repositories, provided such users make queries for Authorized Uses. Authorized Users will be subject to a Deployment Strategy Plan maintained on the joint CIL.

**Authorized Use:** means a submission by an Authorized User to query data, made available under this MOU, for the purposes of national security, law enforcement, immigration and border management, intelligence functions, and for the performance of background investigations for national security positions and certain positions of public trust. Specific Authorized Uses, including data sets searched and responses provided, are set forth below in Appendix 2 and in documentation maintained on the joint CIL.

- I. The Authorized Uses of IDENT data, as made available under this MOU, are limited to the following situations:
  - A. By federal, state, local, and tribal law enforcement agencies for law enforcement purposes with respect to a subject who is arrested and fingerprinted.
  - B. By federal, state, local, and tribal law enforcement agencies for select law enforcement purposes involving a nonarrest encounter in which fingerprints are collected.
  - C. For the following federal employment purposes, provided that the requesting agency can timely make requisite investigative data (including last known address) available to ICE:
    1. inquiries by federal agencies under 5 U.S.C. § 9101 that relate to determining eligibility for (a) national security positions or (b) access to classified information; and
    2. inquiries by federal agencies under 5 U.S.C. § 9101 that relate to determining eligibility for public trust positions.
  - D. By federal, state, local, and tribal government agencies for the purpose of determining eligibility or clearance for national security purposes, as deemed appropriate by DHS and the FBI, provided that the requesting agency use is in accordance with the governing SORNs and that the requesting agency can make requisite investigative data (including last known address) available to ICE in a timely manner. When such uses for national security purposes are deemed appropriate by DHS and the FBI, DHS will notify DOS.
  - E. By foreign and international government agencies for law enforcement (including immigration) purposes, provided the request is made via an Authorized User that is a



U.S. federal agency, and provided that DHS has reviewed and approved the conditions and agreements governing the data exchange in question.

F. Authorized Use specifically excludes:

1. use for state or local licensing or banking institution security under Public Law 92-544; and
2. use for any purpose by private third parties.

G. Nothing in this definition shall be construed to limit DHS' right, upon appropriate written determination, in its sole discretion and consistent with law, to authorize other uses or users of DHS-originated information by the FBI CJIS Division and its users of the data made available under this MOU.

H. DOS recognizes the uses described in (A), (B) and (C)(1) as Authorized Uses of visa data in accordance with section 222(f) of the INA. Otherwise, whether any query of visa data under this MOU is an Authorized Use will be resolved exclusively under section VI.B.3 (pertaining to visa data).

I. Nothing in this definition shall be construed to limit DHS users' access to IDENT information or IAFIS users' access to IAFIS information.

Data sets to be searched for each situation above will be limited to those data deemed appropriate by DHS after consultation with the relevant IDENT data owners (and subject to (H) above).

II. Authorized Use of IAFIS data, as made available under this MOU, shall be in compliance with existing user agreements, policies, and statutes governing the dissemination of criminal history record information contained within the IAFIS repository.

Additionally, the storage of any FBI file and tracking numbers by DHS, and their use subsequent to the original encounter by DHS or DOS, will adhere to the following conditions:

- A. For the administration of criminal justice, authorized IDENT users may retrieve the criminal history record information from the Interstate Identification Index (III) based upon an FBI Number stored as a biographic within the IDENT system.
- B. For noncriminal justice purposes, authorized IDENT users may receive notification of the existence of a criminal history record from the IDENT system. Notification of the existence of a record within IAFIS does not entitle the user to obtain the criminal history record from the III. To obtain the corresponding criminal history record, the authorized IDENT user must submit a fingerprint-based request through the FBI in compliance with the National Crime Prevention and Privacy Compact.

Criminal history record information contained within the IAFIS repository may be shared with foreign and international government agencies for law enforcement and immigration

purposes, provided the request is made via an Authorized User that is a U.S. federal agency, in accordance with authorized IAFIS uses (A) and (B) above, and provided DOJ has reviewed and approved the conditions and agreements governing the data exchange in question. In the event DHS obtains a DOJ review that was not drafted by the FBI's CJIS Division, DHS will provide a copy of that review to the CJIS Division point of contact prior to relying on that review for dissemination purposes.

## Appendix 3

### List of Acronyms

APB:	Advisory Policy Board
CA:	Bureau of Consular Affairs
CIL:	Configuration Item List
CJIS:	Criminal Justice Information Services
CUI:	Controlled Unclassified Information
DHS:	Department of Homeland Security
DOD:	Department of Defense
DOJ:	Department of Justice
DOS:	Department of State
ESC:	Executive Steering Committee for Interoperability
FBI:	Federal Bureau of Investigation
FIRS:	Fingerprint Identification Records System
IAFIS:	Integrated Automated Fingerprint Identification System
ICE:	U.S. Immigration and Customs Enforcement
IDENT:	Automated Biometric Identification System
iDSM:	Interim Data Sharing Model
III:	Interstate Identification Index
INA:	Immigration and Nationality Act
ISSM:	Information Systems Security Manager
KST:	Known or Suspected Terrorist
MOU:	Memorandum of Understanding
OMB:	Office of Management and Budget
ORI:	Originating Agency Identifier
PII:	Personally Identifiable Information
SBU:	Sensitive But Unclassified
SORN:	System of Records Notice
US-VISIT:	United States Visitor and Immigrant Status Indicator Technology