

## **MEMORANDUM OF UNDERSTANDING**

### **BETWEEN**

**THE DEPARTMENT OF STATE,  
BUREAU OF CONSULAR AFFAIRS**

### **AND**

**THE DEPARTMENT OF THE TREASURY  
OFFICE OF INTELLIGENCE AND ANALYSIS**

#### **I. PURPOSE**

The purpose of this Memorandum of Understanding (MOU) between the Department of State, Bureau of Consular Affairs (State/CA), and the Department of the Treasury, Office of Intelligence and Analysis (Treasury OIA), hereinafter referred to as the Parties, is to facilitate interagency information sharing of State/CA nonimmigrant and immigrant visa data and Treasury OIA intelligence and counterintelligence information.

#### **II. AUTHORITY**

State/CA enters into this MOU under the authority provided by 8 U.S.C. §§ 1104-05. Treasury OIA enters into this MOU to share information pursuant to the National Security Act of 1947, Executive Order 12333, Executive Order 13388, The Intelligence Reform and Terrorism Prevention Act 2004, and the Implementing Recommendations of the 9/11 Commission Act of 2007.

#### **III. BACKGROUND**

Fundamental to the mission of State/CA is to protect and assist U.S. citizens abroad, enhance U.S. border security, and facilitate legitimate international travel for persons eligible for U.S. visas. State/CA specifically is committed to balancing border security needs with encouraging travel to the United States. State/CA has the responsibility for visa operations worldwide, the adjudication of visa applications, and the issuance of visas and other travel documents.

(b)(7)(E)

(b)(7)(E)

Treasury OIA supports the greater mission of the Department of Treasury by providing expert analysis and intelligence products on financial and other support networks for terrorist groups, proliferators, and other key national security threats. Treasury OIA provides timely, accurate, and focused intelligence support on the full range of economic, political and security issues.

Specifically, Treasury OIA is a component of the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence (TFI). TFI organizes the Treasury's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, proliferators of weapons of mass destruction (WMD), money launderers, drug kingpins, and other national security threats.

**IV. RESPONSIBILITIES OF THE PARTIES**

In order to further the interests of national security, the Parties hereby agree to share information relevant to supporting and enhancing each other's mission and operations:

- A. State/CA shall provide Treasury OIA access to relevant visa data including, but not limited to, information on adjudications, issuances, and refusal records, in a Sensitive but Unclassified (SBU) form, via query access to the Consular Consolidated Database (CCD). (See the Reports and Users Attachment annexed to and constituting a part of this MOU.)
- B. Treasury OIA shall provide State/CA, in accordance with Treasury information management requirements, with information relevant to State/CA's mission, (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

## V. TECHNOLOGY STANDARDS

The Parties are committed to updating the information technologies employed to implement this MOU and to ensure that the relevant systems remain efficient as data volumes increase and more advanced technologies become available.

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

- A. Visa records are considered confidential under section 222(f) of the Immigration and Nationality Act (INA), 8 U.S.C. § 1202, which reads in part:

*The records of the Department of State and of diplomatic and consular offices of the United States pertaining to the issuance or refusal of visas or permits to enter the United States shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States except that –*

\*\*\*\*\*

*(2) The Secretary of State, in the Secretary's discretion and on the basis of reciprocity, may provide to a foreign government information in the Department of State's computerized visa lookout database and, when necessary and appropriate, other records covered by this section related to information in the database-*

*(A) With regard to individual aliens, at any time on a case-by-case basis for the purpose of preventing, investigating, or punishing acts that would constitute a crime in the United States....*

*(B) With regard to any or all aliens in the database, pursuant to such conditions as the Secretary of State shall establish in an agreement with a foreign government in which that government agrees to use such information and records for the purposes described in subparagraph (A) or to deny visas to persons who would be inadmissible to the United States.*

- B.** The Parties recognize that the visa data and other information that State/CA is to provide under this MOU constitute visa records within the scope of section 222(f) of the INA. Such records, including extracts from and portions of such records, must be treated in accordance with the disclosure restrictions as described in that section and may be used “only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States,” as determined by State/CA.
- C.** The Parties further recognize that a visa bearer’s immigration status may change from that of nonimmigrant to immigrant, lawful permanent resident, or U.S. citizen. In recognition that the records of lawful permanent residents and U.S. citizens are subject to Privacy Act requirements under 5 U.S.C. § 552a, the Parties may follow their internal policies for meeting those requirements.
- D.** To ensure the proper handling and protection of visa records:
- 1.** State/CA shall:
    - a.** Designate representatives to authorize Treasury OIA to share visa data, if necessary and appropriate, with other U.S. government entities or foreign governments; and
    - b.** Train designated Treasury OIA users on effective and appropriate use of the CCD. Training will include, but not be limited to, an explanation of the interface, data fields, and queries, as well as applicable laws, regulations and procedures pertaining to safeguarding the information contained therein. Training will be conducted in close coordination with designated Treasury OIA information systems security officers.
  - 2.** Treasury OIA shall:
    - a.** Limit CCD access to personnel who have a need-to-know such information in the performance of their official duties;
    - b.** Require all personnel having access to the CCD, including contractors and detailees from third-party U.S. government agencies, to be appropriately trained and briefed by designated

staff on the proper handling and protection of visa data prior to allowing access. Upon completion of the training, personnel shall be required to sign an acknowledgement statement affirming they understand the visa data confidentiality requirements;

- c. Refer to State/CA any requests for information on the visa decision process received from third parties (including, but not limited to, inquiries from any U.S. government agency, any state or local government agency, Congress, courts, the media, and the general public), for a determination of whether such information may be released;
- d. Not disclose, reproduce, transmit, or copy a visa record, or any portion of information from a visa record, for sharing with any third party (including, but not limited to, any other U.S. government agency or office, any state or local government agency or office, Congress, the Government Accountability Office, courts, the media, and the general public), unless Treasury OIA has first notified State/CA of its intent to share such records with a third party and obtained State/CA consent prior to any sharing – except as provided in paragraph (e) below;
- e. State/CA provides advance consent to Treasury OIA to share visa records, or any portion of information in a visa record, with the following U.S. government agencies: DHS, (b)(7)(B), (b)(7), DIA, FBI, (b)(7)(B) and ODNI, provided that such disclosure is for the purpose of administering and enforcing U.S. law within the meaning of INA section 222(f). State/CA has previously determined that disclosure of visa records to the federal government agencies named in this paragraph is consistent with INA section 222(f) as these agencies require the data for administering or enforcing U.S. laws related to counterintelligence, counterterrorism, and other national security-related operations and activities;
- f. Not disclose, reproduce, transmit, or copy for disclosure a visa record, or any portion of information from a visa record, for display on the Treasury website or in any other Treasury publication or notification that is open to the public; including

but not limited to, disclosing or displaying any portion of visa data solely derived from a visa record used for the purpose of a Treasury administrative sanctions designation;

- g. Obtain State/CA consent before disclosing, reproducing, transmitting, or copying for disclosure a visa record, or any portion of information from a visa record, to a foreign government;
- h. Annotate any visa records, or any portion of information from a visa record, approved for disclosure under this MOU with instructions that it is protected under INA 222(f), and may not be further disseminated; and
- i. Provide points of contact to act as information systems security officers to administer user accounts and carry out MOU requirements regarding the disclosure and use of CCD information and training for Treasury OIA personnel who are to be given access to relevant visa data.

## **VII. ACCESS CONTROLS AND SAFEGUARDS FOR DEPARTMENT OF STATE VISA RECORDS**

### **A. General**

1. Treasury OIA will ensure that users of State/CA visa records and their supervisors are familiar with the requirements of the MOU.
2. Treasury OIA will certify and provide documentation to State/CA, on a periodic basis, to the contacts listed in Section XIII A. of this MOU that Treasury OIA has fully complied with all access controls and safeguards in the MOU.
3. Treasury OIA understands that certain access may be denied or deactivated and a certifying authority withdrawn if State/CA determines that Treasury OIA or a Treasury OIA user has failed to comply with any of the provisions of the MOU.

## **B. Access Authorization, Control, and Oversight.**

- 1. Treasury will be responsible for the setup and maintenance of user accounts subject to consultation with State/CA on requirements.**
- 2. Treasury OIA will use its established system of oversight to ensure that access to State/CA visa records/systems and Treasury OIA use, dissemination, storage, and disposal of State/CA information is in accordance with the MOU, and other relevant laws, regulations, and policies.**
- 3. Treasury OIA shall have the responsibility for preventing and detecting unauthorized access to or use of the information contained in State/CA visa records. Information will be accessed only for official purposes, and only by authorized users in accordance with the MOU. Authorizations must be kept current in light of actual job responsibilities of individual users. When an individual no longer has a need to access State/CA visa records, access will be promptly terminated.**
- 4. Treasury OIA will ensure that all Treasury employees, including contractors and detailees from third agencies with access to the information, will be properly advised of the rules governing the handling of data including specialized handling necessary for data on U.S. citizens, U.S. nationals, and lawful permanent residents covered under the Privacy Act, as well as the law pertaining to confidentiality of visa records.**

## **C. Security Administration**

- 1. State/CA and Treasury OIA will provide points of contact and will inform each other of the name and title of their respective Information Systems Security Officers (ISSOs), who will have the authority to administer passwords, enforce the provisions, and carry out the requirements of the MOU relating to security, and the disclosure and use of information and training for Treasury OIA personnel who access State/CA records.**

2. All information obtained under the terms of the MOU will be processed and accessed under the direct supervision and control of authorized personnel of the Parties, in a manner that will protect the records and ensure that unauthorized persons cannot retrieve, alter, or delete any such records by means of computer, remote terminal, or other means.

#### **D. System Security/Safeguards**

##### **1. Unauthorized Activity**

- a. Treasury OIA and State/CA acknowledge that the term “unauthorized activity” includes (but is not limited to) unauthorized access, use, dissemination, disclosure, storage, or disposal of State/CA visa data.
- b. Treasury OIA will be responsible for preventing, detecting, and reporting all unauthorized activity including breaches of visa data to State/CA. If Treasury OIA determines that there has been or may have been unauthorized access, use, dissemination, storage or disposal of State/CA visa records, or any other breach of the confidentiality relating to State/CA visa records, and as otherwise required in compliance with applicable laws, regulations, and policies, Treasury OIA will promptly take appropriate disciplinary or remedial action and notify State/CA in accordance with applicable law.
- c. In addition to any disciplinary or other action taken by Treasury OIA, State/CA may give a written warning against further unauthorized access, suspend and/or terminate access to State/CA data for Treasury OIA employees (including contractors and detailees from third agencies) who have or are suspected of having engaged in unauthorized activity.

#### **E. Data Accuracy**

- a. Should a Treasury OIA user discover an error in any of State/CA visa records/data, Treasury OIA will report such error to State/CA.





**XIII. POINTS OF CONTACT**

**A. State/CA/Visa Office:**

Director  
Information Management and Liaison  
Office of Visa Services

(b)(6)

**B. Treasury/OIA/ICI:**

Director  
Office of Reports and Requirements

(b)(6)

**XIV. COMMENCEMENT AND TERMINATION**

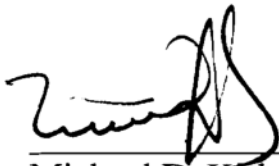
- A.** Cooperation under this MOU may commence upon signature.
- B.** Either Party may discontinue its participation in this MOU by giving at least 30 days advance written notice to the other Party. However, all provisions regarding the protection of visa data or other shared information remain in effect as long as either Party remains in possession of any such records or any information derived therefrom.

**XV. FINAL PROVISIONS**

- A.** This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the Parties, their parent agencies, the United States, or the officers, employees, agents, or other associate personnel thereof.
- B.** Nothing in this MOU is intended to conflict with current law or regulation or the directives of the Parties. If a term of this MOU is inconsistent with such authority, then the term is to be invalid, but the remaining terms and conditions of this MOU are to remain in full force and effect.

The foregoing represents the understanding reached by State/CA and Treasury OIA.

Signed in duplicate.



\_\_\_\_\_  
Michael D. Kirby  
Acting Assistant Secretary  
Bureau of Consular Affairs  
Department of State

Date July 9, 2010

(b)(6)  


Date 14 JUL 10

Michael P. Madon  
Deputy Assistant Secretary for Intelligence Community Integration  
Office of Intelligence and Analysis  
Department of the Treasury

(b)(7)(E)

