

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

RELEASE IN
PART B7(E)

**MEMORANDUM OF UNDERSTANDING
BETWEEN**

**THE U.S. DEPARTMENT OF STATE
BUREAU OF CONSULAR AFFAIRS**

AND

THE

FOR

THE PROVISION OF ACCESS TO PASSPORT RECORDS SYSTEM DATABASES

B7(E)

**ARTICLE I
PURPOSE**

The purpose of this Memorandum of Understanding (MOU) is:

To establish the conditions under which the United States Department of State, Bureau of Consular Affairs, Passport Services, (hereinafter Consular Affairs or CA) will provide access to the Passport Records System database to the [REDACTED]

collectively "the Parties," to assist [REDACTED]

B7(E)
B7(E)
B7(E)
B7(E)
B7(E)
B7(E)

**ARTICLE II
BACKGROUND**

Fundamental to the mission of 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 and U.S. passports. CA specifically is committed to balancing border security needs with encouraging travel to and from the United States. Within CA, Passport Services is responsible for issuing U.S. passports that enable U.S. nationals to travel internationally. Implementing the Immigration and Nationality Act, designated U.S. Department of State employees, both in domestic agencies and at consulates and embassies abroad, are responsible for issuing all U.S. passports. CA is committed to protecting the integrity of the U.S. passport as proof of U.S. citizenship at home and around the world.

The [REDACTED]

B7(E)
B7(E)

-

B7(E)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ARTICLE III RELEVANT AUTHORITIES

The Parties enter into this MOU based on the following authorities:

A. Consular Affairs Authorities.

The Department of State, Bureau of Consular Affairs, relies upon the authorities found at Title 22 of the United States Code, Chapter 4, Section 211a, which grants the Secretary of State the authority to cause passports to be granted, issued, and verified; the Privacy Act of 1974, 5 United States Code, Section 552a and the routine uses provided for thereunder, including the routine use discussed in the Department of State's Systems of Record Notice (SORN) for Passport Records [State-26, published at 76 Fed. Reg. 39466, 39466-39470 (July 6, 2011)] and the Department of State's Prefatory Statement of Routine Uses [76 Fed. Reg. 39466, 39466-39470 (July 6, 2011)].

B.

B7(E)

-
-
-
-
-
-
-

B7(E)

C. Compliance with Applicable Authorities.

The Parties acknowledge that any sharing by CA of passport records with under this MOU must be consistent with the State-26 System of Record Notice or the "Prefatory Statement of Routine Uses" (76 Fed. Reg. 39466, 39466-39470 (July 6, 2011)) and that any use by of those passport records must be consistent with the provisions of this MOU.

B7(E)

B7(E)

ARTICLE IV PERIOD OF AGREEMENT

This MOU is effective when signed by the Parties' respective representatives and will continue indefinitely, unless terminated or amended as provided by Article XIV.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ARTICLE V
CA DATA TO BE ACCESSED BY [REDACTED]

Consular Affairs will provide [REDACTED] with electronic access to the [REDACTED],
 which allows [REDACTED].

B7(E)
 B7(E)
 B7(E)
 B7(E)

B7(E)

The Parties to this MOU will comply with the provisions of the U.S. Constitution and all applicable laws, executive orders, and policies, including the Privacy Act of 1974 with respect to information in the databases. Information described in this Article will only be accessed by [REDACTED] pursuant to the authorities outlined in Article III of this MOU for use in the verification of employment eligibility and/or the issuance of a security clearance as described in Article I. No "roaming" activity or general open access is permitted.

B7(E)

ARTICLE VI
ROLES, FUNCTIONS AND RESPONSIBILITIES OF THE PARTIES

A. [REDACTED] Certifying Authority Officials

B7(E)

1. [REDACTED] will designate employees referred to as Certifying Authority Officials, who will be responsible for identifying/verifying that users are in positions that merit access to the passport record system. [REDACTED] agrees to:
 - a. Identify and validate all Certifying Authority Officials quarterly;
 - b. Notify CA via the [REDACTED] when Certifying Authority Officials have changed;
 - c. Ensure that [REDACTED] Certifying Authority Officials undergo initial training provided by or approved by CA regarding the responsibilities of users and of Certifying Authority Officials, including verifying user information prior to granting access to the passport records system, and disabling access/deactivating users' accounts immediately when access is no longer merited; and,
 - d. Require annual certifications from Certifying Authority Officials that they are aware of and will diligently fulfill their responsibilities under the Privacy Act.

B7(E)

B7(E)

B7(E)
B7(E)SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED**B. [] Certifying Authority Official' Responsibilities regarding [] Users**B7(E)
B7(E)

1. [] Certifying Authority Officials will bi-annually verify the accuracy, completeness, and business (official) need for all [] user accounts. The verification will ensure that:
 - a. User and Certifying Authority Officials are in positions that merit their access to the passport records system;
 - b. Users are U.S. citizens or U.S. nationals;
 - c. Active accounts determined to be valid are updated with complete, correct and current user contact and access information, including contact information for each user's supervisor; and
 - d. Accounts that have been inactive for 90 days or more, or accounts with incomplete or unknown identification information, are identified and a determination made whether any of these accounts are valid and have a current need for access.

B7(E)
B7(E)**C. [] Oversight Authority Officials**

B7(E)

1. [] will designate employees referred to as Oversight Authority Officials, who will be responsible for determining the official purpose of passport records searches; knowing how and when passport data is used at the user's location; reviewing all Access Alert record questionnaires submitted by [] users at []; making a decision concerning access to a record by an [] user; and, along with the Certifying Authority, reporting any unauthorized use of the system to CA under the terms of this agreement. [] agrees to:
 - a. Identify and validate all Oversight Authority Officials quarterly.
 - b. Notify CA when Oversight Authority Officials have changed so that CA can deactivate and remove unnecessary accounts from [] oversight capabilities.
 - c. Arrange annual training provided by or approved by CA regarding the responsibilities of users and of Oversight Authority Officials concerning passport data handling and security; and
 - d. Require annual certifications from Oversight Authority Officials that they are aware of and will diligently fulfill their responsibilities under the Privacy Act.

B7(E)
B7(E)
B7(E)
B7(E)
B7(E)

B7(E)

D. Passport Data Security Awareness Training for [] users

B7(E)

1. All [] users with access to passport data will complete a training course on passport data security awareness, including specialized handling necessary for data on U.S. citizens covered under the Privacy Act, prior to access.
2. [] will cover any potential costs associated with completing this training.
3. All [] users must complete training annually and be recertified before access is renewed.

B7(E)

B7(E)

B7(E)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

4. No actual passport data, including [] database data, may be used for training sessions; only simulated data, provided by CA when available, may be used for training. B7(E)
5. Passport data security awareness training provided by the [] requires that [] users certify that they understand their obligations under the Privacy Act and other applicable requirements to safeguard passport records and the privacy of passport applicants and passport holders. B7(E)
B7(E)

E. The Parties will:

1. Maintain an office, desk or designate a point of contact to answer questions arising from access of passport records; and,
2. Notify each other at least two weeks prior to the submission for publication for notice and comment of a new System of Records Notice (SORN) or an amendment to the existing SORN regarding: (1) new uses or users of passport data, (2) new uses or users of passport data obtained from the other Party, or (3) new uses or users of data of mutual interest to the Parties' respective responsibilities.

F. CA will:

1. Provide [] direct electronic access to the databases described in Article V, or successor systems; B7(E)
2. Assist [] in the use of the databases described in Article V; B7(E)
3. Assist [] with periodic inquiries on particular U.S. passport data; and, B7(E)
4. Assist [] in the interpretation of applications, citizenship questions and the possible need for other records, including such other questions that may arise relevant to [] use of the databases. B7(E)

G. [] will:

1. Restrict access to all CA data and systems to those personnel who have received the appropriate clearances required for all government and contractor personnel accessing [] data and systems; B7(E)
2. Restrict the use of CA data and systems to the verification of employment eligibility and/or the issuance of a security clearance as described in Article I; and,
3. Notify the Bureau of Consular Affairs, [] B7(E)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ARTICLE VII PRIVACY REQUIREMENTS

In accordance with privacy of information law and applicable U.S. code sections, the Parties' responsibilities to safeguard information from the passport databases described in Article V of this Agreement are as follows:

A. Re-disclosure.

[] will refer all third party (including Congress, the General Accounting Office, courts, and the general public) requests for passport database information described in Article V to CA for decision and/or assistance. [] will not furnish or make accessible any such information to any third party without the prior written consent of CA.

B7(E)

B7(E)

B7(E)

To the extent that information or records from the databases described in Article V are incorporated into [] records, [] is permitted to share such information in accordance with the provisions of the Privacy Act of 1974, as amended (5 U.S.C. §552a); Department of State's SORN for Passport Records (State-26, published at 76 Fed. Reg. 39466, 39466-39470 (July 6, 2011)); the Department of State's Prefatory Statement of Routine Uses [published at 76 Fed. Reg. 39466, 39466-39470 (July 6, 2011)]; and [] will not otherwise disseminate information or records from the databases described in Article V.

B7(E)

B7(E)

B7(E)

[] shall keep an accurate accounting of each disclosure of information or records obtained from the databases described in Article V as required by 5 U.S.C. § 552a(c) and provide documentation of such accounting to CA upon request.

B7(E)

B. Return, Transfer or Destruction of Personal Information.

[], upon completion of its use of personal information obtained from passport applications, will routinely destroy such information pursuant to its authorized records schedules per [] or upon CA's written request based upon a legal obligation to direct such destruction, or upon termination of this MOU. [] shall follow CA's written instructions concerning the return, transfer and/or destruction of all personal information. [] shall furnish CA with written confirmation of actions taken within 14 calendar days of receipt of CA's written instructions. Notwithstanding the foregoing, if the information has been incorporated into an [] record, it will be destroyed pursuant to [] retention schedule.

B7(E)

B7(E)

B7(E)

B7(E)

B7(E)

B7(E)

B7(E)

B7(E)

ARTICLE IIX SECURITY/SAFEGUARDS

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

At the time of signing, will have in place appropriate safeguards and procedures designed to protect against unauthorized use and disclosure of information obtained under the terms of this MOU.

B7(E)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED**A. Prevention of Misuse**

[] hereby agrees to take appropriate action to penalize misuse, alteration, deletion or any other unauthorized access of the data by [] personnel under applicable civil and criminal laws and assure compliance with the protections provided by the Privacy Act of 1974.

B7(E)

B7(E)

B. Access Authorization

1. [] users will access and use the information obtained under the terms of the MOU in a manner that prevents, or in the alternative, detects access to or use of the information contained in the databases referenced in Article V in a manner that is not authorized by this MOU.
2. CA and [] will provide points of contact and will inform each other of the name and title of their respective Certifying Authority Officials.
3. [] will be responsible for establishing measures reasonably designed to prevent and detect unauthorized access to or use of the information contained in CA's passport records by [] personnel.

B7(E)

B7(E)

B7(E)

B7(E)

C. Access Controls

1. [] is responsible for the set up and maintenance of user accounts, regarding access to the databases referenced in Article V, subject to consultation with CA on requirements. [] personnel shall securely log onto the Department of State network prior to accessing the databases described in Article V.
2. **CA's Passport Record Monitor Program:**
 - a. If a user accesses a record on the Monitor List, the user must complete a questionnaire, to provide an explanation of the purposes of the access. The user's Oversight Authority Official will then be notified and must validate the reasons given by the user. Failure to respond to CA in a timely manner will result in a suspension of the user's and/or Oversight Authority Official's access to the passport records system. If the oversight authority and CA determine the access was justified as an official use, any access that was suspended will be restored. If access to the passport record was not justified, the user's access will be disabled.
 - b. As part of the Monitor Program, a percentage of all passport records system searches will randomly trigger the questionnaire, outside the Monitor List records. While it does not denote a request to a Monitor List record, nor inappropriate use of the system, users and Oversight Authority Officials must fully complete the questionnaire following the established procedure.
 - c. CA also reserves the right to unilaterally conduct audits of user activity, and will notify [] if an audit suggests an [] user may have mis-used his or her access privileges.

B7(E)

B7(E)

B7(E)

B7(E)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED**D. Unauthorized Access:**

1. [] and CA acknowledge that the term "unauthorized activity" includes (but is not limited to) unauthorized or accidental access, use for purposes other than the verification of employment eligibility and/or the issuance of a security clearance, dissemination, disclosure, storage, or disposal of CA's passport data. B7(E)
2. [] acknowledges that it will be responsible for preventing, detecting, reporting, and responding to unauthorized activity by [] personnel, including employees, contractors, and detailees from third agencies, in accordance with the Privacy Act, other applicable federal guidance and this MOU. B7(E)
B7(E)
3. [] will promptly take appropriate disciplinary or remedial action and notify CA when it learns that an unauthorized activity has occurred. B7(E)
4. [] acknowledges its requirement to report any suspected or confirmed data breach involving CA's passport data to []
[] B7(E)
B7(E)
B7(E)
5. [] acknowledges that CA will respond with certain minimum actions, such as deactivation of access, for identified Certifying Authority Officials, Oversight Authority Officials, and users who either commit an unauthorized activity or authorize unnecessary levels of access. B7(E)
6. [] undertakes to assist CA with investigation of unauthorized activity related to passport data, and will conduct an investigation in the event of potential suspicious unauthorized activity related to passport data. B7(E)
7. [] will report to CA the final outcome of any investigation of a breach or improper disclosure of information, including disciplinary action taken against [] users who commit unauthorized activity. B7(E)
B7(E)

E. Data Transmission Requirements

In transmitting data under this MOU, [] and CA will utilize mutually acceptable technical specifications and security protocols. B7(E)

F. Records Storage

[] shall store all information from the databases described in Article V in systems that ensure protection of the information. B7(E)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

**ARTICLE IX
DOCUMENT AUTHENTICATION**

[redacted] may request further information, and authenticated copies of passport records for official or judicial purposes by written request to the [redacted]

B7(E)

B7(E)

B7(E)

**ARTICLE X
PROGRAM ADMINISTRATORS FOR EACH AGENCY**

In the case of CA, the Administrator will be the [redacted]

B7(E)

B7(E)

In the case of [redacted], the Administrators will be the [redacted]

B7(E)

B7(E)

**ARTICLE XI
ENTRY INTO FORCE**

This MOU, which consists of fifteen (15) numbered sections, will enter into force when signed by both parties.

**ARTICLE XII
NO THIRD PARTY RIGHTS OR BENEFITS**

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 associated personnel thereof. This agreement is not intended to be enforceable in any court or administrative forum. The parties will seek to resolve any disputes regarding the agreement by mutual consultation.

**ARTICLE XIII
FUNDING**

This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of the understanding between the parties hereto of the tasks and methods for performing tasks described herein. Unless otherwise agreed in writing, each party shall bear its own costs in relation to 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,

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

**ARTICLE XIV
AMENDMENT OR TERMINATION**

A. Amendment

Either Party hereto may request amendment of this MOU at any time. It is understood that any request will be in writing and that any amendment will enter into effect only when both parties have concurred in writing.

Requests to amend this MOU will be sent, in writing, from the Administrator(s) of the proposing Party to the Administrator(s) of the other Party. The Administrator(s) for the Parties are set forth in Article X of this MOU.

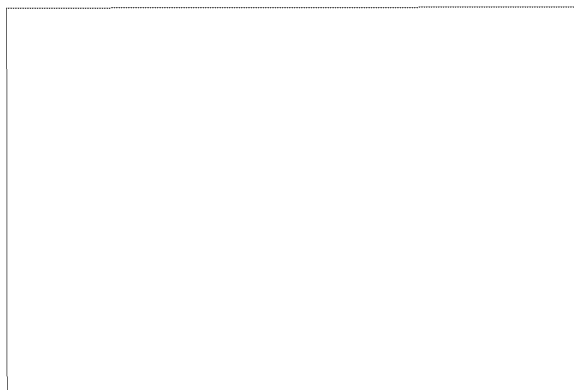
B. Termination

Either Party hereto may terminate this MOU with 30-days written notice to the other Party's Administrator(s). All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of all information received during a Party's participation in this MOU shall survive any termination.

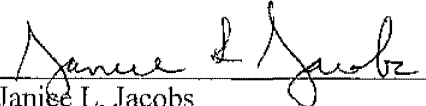
**ARTICLE XV
INTERPRETATION AND SEVERABILITY**

Nothing in this agreement is intended to conflict with current law or regulation. If a term of this agreement is inconsistent with such authority, then that term shall be invalid to the extent of the inconsistency, but the remaining terms and conditions of this agreement shall remain in full force and effect.

SIGNED:



CONSULAR AFFAIRS


Janice L. Jacobs
Assistant Secretary
Bureau of Consular Affairs
U.S. Department of State

B6
B7(E)

SENSITIVE BUT UNCLASSIFIED