SENSITIVE BUT UNCLASSIFIED

RELEASE IN PART B7(E)

MEMORANDUM OF AGREEMENT BETWEEN THE UNITED STATES DEPARTMENT OF STATE AND THE UNITED STATES DEPARTMENT OF DEFENSE FOR LIMITED ACCESS TO PASSPORT RECORDS

ARTICLE I PURPOSE

The purpose of this Memorandum of Agreement (MOA) is to establish the terms and conditions under which the U.S. Department of State, Bureau of Consular Affairs, Passport Services (hereinafter Consular Affairs or CA) will provide the Department of Defense Executive Agent (EA) for Passport and Passport Agent Services (DoD/) limited access to Passport Records, in order to provide designated DoD/ personnel with the capability to check the status of no-fee passport applications submitted to CA by DoD personnel and eligible family members. B7(E)

B7(E)

ARTICLE II BACKGROUND

CA's mission 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 is committed to protecting the integrity of the U.S. passport as proof of U.S. citizenship domestically and internationally. CA is also committed to balancing border security needs while encouraging travel to and from the United States. CA is responsible for issuing all U.S. passports pursuant to the terms of Title 22 of the U.S. Code and the Immigration and Nationality Act.

B7(E)

, is the Executive Agent (EA) for the Department of Defense (DoD) Passport Agent Services. Through an agreement with the Department of State, the DoD EA is charged with providing passport and visa services to military members, Defense civilians, and their eligible family members. B7(E)

B7(E)

carries out these EA duties. executes official, no-fee, and diplomatic passport applications; executes applications for foreign visas; partners with SIA to train and certify DoD Passport Acceptance Agents; answers customer service inquiries from DoD Passport Agents worldwide; and operates a mail room for the receipt and distribution of completed passport and/or visa applications. B7(E)

B7(E)

B7(E)

ARTICLE III RELEVANT LEGAL AUTHORITIES

The Parties enter this MOA based on the following authorities:

A. Consular Affairs Authorities.

- Title 22 of the United States Code, Chapter 4, Section 211a, which grants the Secretary of State the authority to allow for passports to be granted, issued, and verified.
- The Privacy Act of 1974, 5 U.S.C. § 552a and the routine uses thereunder, including the routine uses discussed in the Department of State's System of Records Notice (SORN) for Passport Records [State-26, published at 76 Fed. Reg. 39466-39470 (July 6, 2011)].

B. Department of Defense Executive Agency for Passports and Passport Agent Services Authorities.

DoD Directive 1000.21, which designates the Secretary of the Army as the DoD EA for DoD Passport and Passport Agent Services and applies to all DoD Components.

C. Compliance with Applicable Authorities

The Parties acknowledge that any sharing by CA of Passport Records with DoD/[ ] and use thereof by DoD/[ ], must be consistent with State-26 System of Records Notices and the provisions of this MOA. B7(E)

B7(E)

ARTICLE IV
DATA TO BE ACCESSED

CA will provide DoD/[ ] limited access to Passport Records system agnostic to check the status of passport applications of DoD personnel and eligible family members for official, diplomatic, and no-fee regular passports. DoD/[ ] will access Passport Records through the Consular Consolidated Database (CCD), which contains built-in audit functions. Any changes to the method by which DoD/[ ] accesses passport data will require amendment to this MOA. B7(E)

B7(E)

B7(E)

[redacted]

ARTICLE V
DISCLOSURE BY DOD/LSW

DoD/[ ] may only share the passport application status with the passport applicant, passport acceptance agents, and DoD personnel involved in the procurement, control, and accountability of official, diplomatic, and no-fee regular passports. Only status information such as "pending" "in process" "it has been mailed" "issued" or "not issued" may be released to the persons above. B7(E)

SENSITIVE BUT UNCLASSIFIED

Any other information requires an executed Privacy Act waiver. Any other inquiries regarding information on a passport application or other details about adjudication, other than a status check, must be referred to the Special Issuance Agency (SIA).

DoD/ shall not provide, reproduce, transmit, copy, or otherwise disclose any records or information from Passport Records, including but not limited to form DD-1056, Authorization for a No-Fee Passport Book, to any party. DoD/ will refer all third-party requests (including Congress, the General Accounting Office, courts, and the general public) for passport database information to the for decision and/or assistance. DoD/LSW will not furnish or make accessible any passport information to any such third party. B7(E) B7(E) B7(E) B7(E)

ARTICLE VI
PRIVACY SECURITY/SAFEGUARDS

The Parties recognize that sharing of passport records is subject to Federal law, including relevant provisions of the Privacy Act of 1974, and that established Privacy Act exemptions and "routine uses" allow for release or sharing of information contained in these records only under certain conditions.

At the time of signing, DoD/ will have in place safeguards and procedures designed to prevent and detect unauthorized use or disclosure of information obtained under the terms of this MOA. DoD/ hereby agrees to take action to penalize the misuse, alteration, deletion, or unauthorized access or storage of the data by DoD employees, contractors, detailees, and agents under applicable civil and criminal laws; and to ensure compliance with the Privacy Act of 1974. B7(E) B7(E)

A. **General Conditions of Access and Security Administration**

1. DoD/ will be responsible for the setup and maintenance of user accounts subject to consultation with CA on requirements. B7(E)

2. CA and DoD/ will inform each other of the name and title of their respective Information Systems Security Officers (ISSOs), Certifying Authority, and Oversight Authority Officials. B7(E)

3. CA and DoD/ will ensure that all information obtained under the terms of the MOA 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 access, alter, or delete any such records by means of computer, remote terminal, or other means. B7(E) B7(E)

4. DoD/ will use its system of oversight to ensure that DoD/ access to CA's Passport Records system and DoD/ use, dissemination, storage, and deletion of information and records from the Passport Records system is in accordance with the MOA and all relevant laws, regulations, and policies. B7(E) B7(E)

SENSITIVE BUT UNCLASSIFIED

5. DoD/ will be responsible for implementing oversight to ensure that connection to CA's Passport Records system is only performed on a federal government computer and located in a federal government facility. Accessing CA's Passport Records system outside a government facility is prohibited. B7(E)

6. DoD/ will be responsible for preventing and detecting unauthorized access, use, alteration, storage, or deletion of the information contained in CA's passport records by DoD/ personnel or contractors. B7(E) B7(E)

7. DoD/ will restrict access to CA's passport data and information obtained under the terms of the MOA to individual DoD/ employees, contractors, and detailees who require access to the information described in this MOA to perform their official duties for DoD/ . When an individual no longer has a need to access CA's passport records, access will be promptly disabled. CA will be notified immediately of any changes regarding DoD/ users' access to the Passport Records system. B7(E) B7(E) B7(E) B7(E) B7(E)

8. DoD/ will grant authorization to individual users and require its passport data users to follow standard operating procedures established by DoD/ in consultation with CA and as described below, including any training requirements and signing of briefing acknowledgment forms. B7(E) B7(E)

9. DoD/ shall ensure that all DoD/ employees and contractors with access to passport data will be properly advised of the rules governing the handling of passport data, including specialized handling necessary for data on U.S. persons covered under the Privacy Act. B7(E)

B7(E)

B. Standard Operating Procedures for Passport Data Sharing

1. DoD/ and CA will designate staff members to manage this program, answer related questions, and field technical questions. CA will assist DoD/ through these designated staff members with periodic inquiries on particular U.S. passport data. CA will assist DoD/ in the interpretation of records, citizenship questions, and with any requests for additional information. B7(E) B7(E) B7(E)

2. DoD/ will designate employees referred to as Certifying Authority Officials, who will be responsible for identifying and verifying that users are in positions that require access to the passport record system. B7(E)

a. DoD/ will bi-annually identify and validate all Certifying Authority Officials (Certifying Authorities). B7(E)

SENSITIVE BUT UNCLASSIFIED

b. DoD/ will notify CA when Certifying Authorities have changed so that CA can ascertain appropriate levels of access and authorization are maintained and accounts are properly updated. B7(E)

c. DoD/ Certifying Authorities will undergo initial training provided by or approved by CA regarding the responsibilities of users and of Certifying Authorities, including verifying user information prior to granting access to passport record systems, and disabling user access immediately when access is no longer merited. B7(E)

d. DoD/ Certifying Authorities shall provide annual certifications that they are aware of and will diligently fulfill their responsibilities under the Privacy Act as it relates to access to passport data provided to DoD/ under this MOA. B7(E) B7(E)

3. DoD/ Certifying Authorities will bi-annually verify the accuracy, completeness, and official business need for all DoD/ user accounts. The verification will ensure that: B7(E) B7(E) B7(E)

a. Users and Oversight Authorities are in positions that merit their access to passport record systems;

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 the user's supervisor;

d. DoD/ will identify accounts that have been inactive for 90 days or more or accounts with incomplete or unknown identification information and determine whether any of these accounts are valid and have a current need for access. B7(E)

4. DoD/ will designate employees referred to as Oversight Authority Officials, who will be responsible for confirming whether access of passport records is for official purposes; for knowing how and when passport data is used at the user's location; for reviewing all monitor questionnaires completed by DoD/ users; for determining whether access to a record by a DoD/ user was valid; and, along with the Certifying Authority Officials, for reporting any unauthorized use of the system under the terms of this agreement to CA. The Oversight Authority must be in a supervisory position. B7(E) B7(E) B7(E) B7(E)

a. DoD/ through the role of the Certifying Authorities will bi-annually identify and validate all Oversight Authority Officials (Oversight Authorities). B7(E)

b. Oversight Authorities will be responsible for validating DoD/ user access to passport records when requested to do so by automated questionnaires on passport record systems, or directly by representatives of CA. B7(E)

SENSITIVE BUT UNCLASSIFIED

c. Oversight Authorities will ensure that both the user in question and the Oversight Authority have responded completely to the questionnaire within 24 hours and 120 hours, respectively.

d. Oversight Authorities should have a comprehensive understanding of the utilization of passport data by DoD/ users in order to responsibly validate record access. B7(E)

5. Training:

a. DoD/ users with access to passport data, including Certifying Authorities and Oversight Authorities, will complete an approved yearly CA training course on passport data security awareness prior to initial and renewed access. B7(E)

b. CA will provide training data to DoD/ . No actual passport data, including passport record database data, may be used for training sessions; only simulated data may be used for training. B7(E)

c. DoD/ users will 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)

6. Tiered Access for Passport Records

a. B7(E)

B7(E)

7. Protection of Passport Data

a. The Parties agree that any unauthorized access, use, disclosure, storage, or deletion of passport data by a DoD/ Certifying Official, Oversight Official, or user is to be reported immediately to appropriate officials in DoD/ as well as in CA, specifically, to B7(E)

B7(E)

B7(E)

b. Access Alerts

i. CA has identified and developed a Monitor List of certain passport records meriting an enhanced auditing regime.

ii. If a user tries to access a record on the Monitor List, the user must complete a questionnaire and provide an explanation of the purpose of viewing the record *prior* to accessing it. The user's Oversight Authority will be notified to verify the purpose of access, and must provide his/her response within 120 hours. Failure on the part of the user to respond to CA within 24 hours could result in a suspension of the user's access to passport record systems. If the supervisor, the Oversight Authority, and CA determine the access was justified as work

SENSITIVE BUT UNCLASSIFIED

related, any access that was suspended will be restored. If the access to the passport record was not authorized for official purposes, the user's access will be disabled until the Monitor Committee determines if disciplinary action will be recommended or access will be returned.

iii. 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 for access to a Monitor List record, nor inappropriate use of the system, users and Oversight Authorities must fully complete the questionnaire following the established procedure.

iv. DoD/ undertakes to assist CA with investigations of all access alerts when so requested. B7(E)

c. Unauthorized Access:

i. DoD/ and CA acknowledge that the term "unauthorized activity" includes (but is not limited to) unauthorized accidental or intentional access, use, disclosure, storage, or deletion of CA's passport data. B7(E)

ii. DoD/ acknowledges that it will be responsible for preventing, detecting, reporting, and responding to unauthorized activity by DoD/ personnel, including employees and contractors, in accordance with the Privacy Act, other applicable federal guidance, and this MOA. Such responsibility shall include the establishment of oversight mechanisms so as to detect unauthorized activity. B7(E) B7(E)

iii. DoD/ will promptly take appropriate disciplinary or remedial action and notify CA when an unauthorized activity has occurred. B7(E)

B7(E)

iv. DoD/ will report in writing any suspected or confirmed data breach involving CA's passport data to . DoD/ shall also provide such information to CA immediately. Notification to CA will be sent to the B7(E) B7(E) B7(E) B7(E) B7(E) B7(E) B7(E)

v. DoD/ acknowledges that CA will respond with certain minimum actions, such as deactivation of access for identified Certifying Authorities, Oversight Authorities, and/or users who either commit an unauthorized activity or authorize unnecessary levels of access. B7(E)

SENSITIVE BUT UNCLASSIFIED

vi. DoD/ will conduct an investigation in the event of potential suspicious unauthorized activity related to passport data, and share the results of that investigation with CA. B7(E)

d. Audits

i. DoD/ will conduct periodic privacy compliance audits, both random audits and trend audits, to enhance detection of unauthorized activity related to passport data transmitted by CA to DoD/ and maintained in its systems. B7(E) B7(E)

ii. CA also reserves the right to conduct audits of user activity (both random and user specific) to enhance the prevention and detection of unauthorized activity.

8. Return, Transfer, Destruction of Personal Passport Information.

a. Upon completion of its use of personal information obtained from passport databases, DoD/ will, when lawful to do so, routinely destroy such information, using appropriate methods in consultation with CA. B7(E)

b. Upon CA's written request, or upon termination of the MOA, DoD/ shall follow CA's written instructions concerning the return, transfer, and/or destruction of all information provided by CA, except as prohibited by law. B7(E)

c. DoD/ shall furnish CA with written confirmation that it has complied with CA's written request within fourteen (14) calendar days of receipt of CA's written instructions. B7(E)

9. Limitations on Searches of Passport Data

a. Random, unspecific reviews of records for purposes of quality assurance or training are expressly prohibited. These activities are presumptively improper and constitute unauthorized access that the privacy and security protocols in this MOA, along with other information security measures undertaken by CA and DoD, are designed to prevent.

ARTICLE VII
RECORD REVIEWS

CA's Administrator will have the right to perform record reviews at DoD/ upon reasonable notice, or other reviews to ensure that adequate safeguards are maintained by DoD/ with regard to the access to information provided under this MOA. B7(E) B7(E)

SENSITIVE BUT UNCLASSIFIED

ARTICLE VIII
PROGRAM ADMINISTRATOR FOR EACH AGENCY

The Program Administrators will have the authority to ensure implementation of the provisions of this MOA pertaining to security at their respective agencies, and will act as agency contacts for that purpose.

On behalf of CA, the Administrator will be the [redacted] of the Bureau of Consular Affairs. B7(E)

On behalf of the DoD/[redacted], the Administrator will be the Director, [redacted], a designated representative of the Department of Defense. B7(E)

ARTICLE IX
DISPUTE RESOLUTION

B7(E)

Any disagreement between the Parties regarding the interpretation, application, or implementation of this MOA will be resolved by consultation between the Parties.

ARTICLE X
FUNDING

This MOA is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed in writing, each Party shall bear its own costs in relation to this MOA. Expenditures by each Party will be subject to budgetary processes and the availability of funds pursuant to relevant law, regulations, and policies.

ARTICLE XI
NO THIRD PARTY RIGHTS OR BENEFITS

This MOA is not intended to create any right or benefit, substantive or procedural, enforceable by law or otherwise, for any third party.

ARTICLE XII
INTERPRETATION AND SEVERABILITY

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

SENSITIVE BUT UNCLASSIFIED

ARTICLE XIII
AMENDMENT OR TERMINATION

This MOA will be reviewed every three years or at the request of either party to ensure its accuracy. Either Party hereto may request amendment of this MOA at any time. Any request will be in writing, from the Administrator of the proposing Party, as identified under Article VIII, to the Administrator of the other Party, as similarly identified, and will enter into effect only when both Parties have concurred in writing.

Either Party may terminate this MOA by written notice to the other Party. Termination will occur no sooner than 30 days after receipt of a written notice to terminate.

ARTICLE XIV
EFFECTIVE DATE AND PERIOD OF AGREEMENT

This MOA, which consists of fourteen numbered sections, will become effective when signed by both Parties and will remain in effect unless terminated or amended per Article XIII.

SIGNED IN TWO ORIGINAL COPIES:

U.S. DEPARTMENT OF DEFENSE

Gerald B. O'Keefe
Administrative Assistant
to the Secretary of the Army
U.S. Department of Defense

DATE: 26 Dec 2019

U.S DEPARTMENT OF STATE
BUREAU OF CONSULAR AFFAIRS

Michele T. Bond
Acting Assistant Secretary
Bureau of Consular Affairs
U.S. Department of State

DATE: 12/2/19

epic.org EPIC-18-10-12-DOS-FOIA-20200131-Interim-Production 000159