Department of State
Privacy Act of 1974; System of Records
AGENCY: Department of State
ACTION: Notice of a Modified System of Records.

SUMMARY: This system of records compiles information used in the adjudication of U.S. visas.
DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records notice is effective upon publication.
ADDRESSES: Questions can be submitted by mail, email, or by calling Eric F. Stein, the Senior Agency Official for Privacy, on (202) 485-2051. If mail, please write to: U.S Department of State; Office of Global Information Systems, A/GIS; Room 1417, 2201 C St., N.W.; Washington, DC 20520. If email, please address the email to the Senior Agency Official for Privacy, Eric F. Stein, at Privacy@state.gov. Please write "Visa Records, State-39" on the envelope or the subject line of your email.
FOR FURTHER INFORMATION CONTACT: Eric F. Stein, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS; Room 1417, 2201 C St., N.W.; Washington, DC 20520 or by calling (202) 485-2051.
SUPPLEMENTARY INFORMATION: The purpose of this modification is to make substantive and administrative changes to the previously published notice. This notice modifies the following sections of State-39, Visa Records: System Location, Categories of Individuals Covered by the System, Categories of Records in the System, Record Source Categories, and Administrative, Technical, and Physical Safeguards. In addition, this notice makes administrative updates to the following sections: Record Access Procedures, Contesting Record Procedures, Notification Procedures, and History. These changes reflect new visa adjudication procedures, the movement to cloud storage, updated contact information, and a notice publication history.
SYSTEM NAME AND NUMBER: Visa Records, State-39.
SECURITY CLASSIFICATION: Unclassified and Classified.
SYSTEM LOCATION: Department of State ("Department"), located at 2201 C St., N.W., Washington, DC 20520; Visa Office, Department of State, Annex 17, 600 19th St., N.W., Washington, DC 20006; National Visa Center, 32 Rochester Avenue, Portsmouth, NH 03801; Kentucky Consular Center, 3505 N. US Hwy 25 W., Williamsburg, KY 40769; U.S. embassies, consulates general, consulates, and Department of State Enterprise Server Operations Centers (henceforth referred to as the Department of State). Records may also be located within a government-certified cloud provided by a cloud-based service provider.
SYSTEM MANAGER(S): Deputy Assistant Secretary for Visa Services, Room 6811, Department of State, 2201 C St., N.W., Washington, DC 20520-4818; Director, National Visa Center, 32 Rochester Avenue, Portsmouth, NH 63801; Director, Kentucky Consular Center, 3505 N. US Hwy 25 W., Williamsburg, KY 40769. All system managers can be contacted with this email address PRA_BurdenComments@state.gov. When emailing system managers, include the phrase "SORN" in the email subject line. At specific locations

abroad, the on-site manager is the consular officer responsible for visa processing.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301 (Secretary of State's authorities with respect to Management of the Department of State); 22 U.S.C. 2651a (Organization of the Department of State); 22 U.S.C. 3921 (Management of the Foreign Service); 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended).

PURPOSE(S) OF THE SYSTEM: The Visa Records system maintains information used to assist the Bureau of Consular Affairs and consular officers in the Department and abroad in adjudicating visas and Certificates of Identity. It is also used in dealing with problems of a legal, enforcement, technical, or procedural nature that may arise in connection with a U.S. visa or Certificate of Identity.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Visa Records may include the following individuals when required by a visa application or a Certificate of Identity application: U.S. petitioners, U.S. persons applying for returning residence travel documentation, and visa and Certificate of Identity applicants who subsequently become documented as U.S. persons. The Privacy Act defines an individual at 5 U.S.C. 552a (a)(2) as a U.S. citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: Visa Records maintains visa applications and related forms; Certificate of Identity applications or portions thereof; documents of identity; biometric information; social security numbers; national identity numbers; photographs; financial information; gender, birth, marriage, death and divorce certificates; interview worksheets; biographic information sheets; affidavits of relationship; medical examinations and immunization reports; police records, criminal and legal information; educational and employment records; petitions for immigrant status and nonimmigrant status; bank statements; social media handles and information gathered from social media; communications between the Visa Office, the National Visa Center, the Kentucky Consular Center, U.S. embassies, U.S. consulates general and U.S. consulates, other U.S. government agencies, international organizations, members of Congress, legal and other representatives of visa applicants, relatives of visa applicants, and other interested parties where such communications are, or may be, relevant to visa adjudication; and internal Department of State correspondence and notes relating to visa adjudication. Visa Records may also contain information collected regarding applicants' or petitioners' U.S. family members; U.S. employers; and other U.S. persons referenced by the applicant or petitioner.

RECORD SOURCE CATEGORIES: These records contain information that is primarily obtained from the individual who is the subject of the records; attorneys/agents representing these individuals; relatives; sponsors; petitioners; members of Congress; U.S. Government agencies; foreign government agencies, international organizations; local sources at posts; and anyone else with information that is, or may be, relevant to a U.S. visa application.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The principal users of this information outside the Department of State may include, when consistent with Section 222(f) of the Immigration and Nationality Act:

A. The Department of Homeland Security for uses within its statutory mission, including to process, approve or deny visa petitions and waivers, as well as for law enforcement, counterterrorism, transportation and border security, administration of immigrant benefits, critical infrastructure protection, fraud prevention, or employment verification purposes.
B. Public or private employers seeking to confirm the authenticity of the visa when it is presented as evidence of identity and/or authorization to work in the United States;
C. The Department of Justice, including the Federal Bureau of Investigation (and its National Crime Information Center), the Terrorist Screening Center, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. National Central Bureau (Interpol) and the Drug Enforcement Administration, for purposes of law enforcement, criminal prosecution, representation of the U.S. government in civil litigation, fraud prevention, counterterrorism, or border security.
D. The Department of the Treasury for uses within its statutory mission, including the enforcement of U.S. tax laws, economic sanctions, and counterterrorism.
E. The National Counterterrorism Center, the Office of the Director of National Intelligence and other U.S. intelligence community (IC) agencies, for uses within their statutory missions, including intelligence, counterintelligence, counterterrorism and other national security interests.
F. The Department of Defense, for uses within its statutory mission including for purposes of border security, homeland defense, force protection, law enforcement and counterterrorism.
G. The Department of Labor for uses within its statutory mission including the administration and enforcement of U.S. labor laws.
H. Congress, for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States.
I. State, local, and tribal government officials for law enforcement, counterterrorism, or border security purposes.
J. Interested persons (such as the visa applicant, the applicant's legal representative or other designated representative) inquiring as to the status of a particular visa case (limited unclassified information may be released when appropriate).
K. Courts provided the Secretary of State has determined that release is appropriate, and the court has certified it needs such information in the interest of the ends of justice in a case pending before the court.

L. Foreign governments for purposes relating to the administration or enforcement of the immigration, nationality, and other laws of the United States, or in the Secretary's discretion and on the basis of reciprocity, for the purpose of preventing, investigating, or punishing acts that would constitute a crime in the United States or, pursuant to an agreement with a foreign government, to enable such government to consider whether the record indicates a person would be inadmissible to the United States when it determines whether to deny a visa, grant entry, authorize an immigration benefit, or order removal of such person.

M. The Centers for Disease Control and Prevention, for uses within its statutory mission, including its role relative to the physical and mental examination of aliens under immigration laws.

N. Appropriate agencies, entities, and persons when (1) the Department of State suspects or has confirmed that there has been a breach of the system of records; (2) the Department of State has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of State (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of State efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

O. Another Federal agency or Federal entity, when the Department of State determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

The Department of State periodically publishes in the Federal Register its standard routine uses that apply to all of its Privacy Act systems of records. These notices appear in the form of a Prefatory Statement (published in Volume 73, Number 136, Public Notice 6290, on July 15, 2008). All these standard routine uses apply to Visa Records, State-39.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored both in hard copy and on electronic media. A description of standard Department of State policies concerning storage of electronic records is found in the Department's Foreign Affairs Manual (https://fam.state.gov/FAM/05FAM/05FAM0440.html). All hard copies of records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved through individual data fields including but not limited to: Applicant personal data; biometrics and namecheck data; case data; and visa data.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The retention period for visa records depends on the nature of the information and disposition of the visa adjudication. Some files related to issued immigrant visas are destroyed six months after issuance. In some instances, files with historical significance are permanent records. Most files related to Certificates of Identity are retained for twenty-five years after closure. These records are retired and destroyed in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA), and a complete list of the Department's schedules can be found on its Freedom of Information Act (FOIA) program's website (https://foia.state.gov/Learn/RecordsDisposition.aspx). More specific information may be obtained by writing to the following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street, N.W.; Room B-266; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All Department of State network users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet network users are required to take the Foreign Service Institute's distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to Visa Records, a user must first be granted access to the Department of State network system.

Department of State employees and contractors may remotely access this system of records using non-Department owned information technology. Such access is subject to approval by the Department's mobile and remote access program and is limited to information maintained in unclassified information systems. Remote access to the Department's information systems is configured in compliance with the Office of Management and Budget Circular Memorandum A-130 multifactor authentication requirements and includes a time-out function.

All Department of State employees and contractors with authorized access to records maintained in this system of records have undergone a background security investigation. Access to the Department of State, its annexes and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. While the majority of records covered in Visa Records are electronic, all paper records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of

access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

The safeguards in the following paragraphs apply only to records that are maintained in government-certified cloud systems. All cloud systems that provide IT services and process Department of State personally identifiable information (PII) must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy.

Information that conforms with Department-specific definitions for FISMA low, moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Department's Cloud Management Office and the Department of State Authorizing Official. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) and Department of State policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally-approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Department of State Authorizing Official. High FISMA impact risk level systems will additionally be subject to continual auditing and monitoring, multifactor authentication mechanisms utilizing Public Key Infrastructure (PKI) and NIST 800-53 controls concerning virtualization, servers, storage and networking, as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

RECORD ACCESS PROCEDURES:

Individuals who wish to gain access to or to amend records pertaining to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C St., N.W.; Room B-266**;** Washington, DC 20520. The individual must specify that he or she wishes the Visa Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; email address; telephone number; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Visa Records include records pertaining to the individual. Detailed instructions on Department of State procedures for accessing and amending records can be found at the Department's FOIA website (https://foia.state.gov/Request/Guide.aspx).

However, in general, visa records are confidential and may not be released

under section 222(f) of the Immigration and Nationality Act, except that, the Department of State may consider requests for records that originated with, or were sent to, a requesting visa applicant or someone acting on such applicant's behalf to be releasable thereto.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest record procedures should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C St., N.W.; Room B-266; Washington, DC 20520.

NOTIFICATION PROCEDURES: Individuals who have reason to believe that this system of records may contain information pertaining to them may write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C St., N.W.; Room B-266; Washington, DC 20520. The individual must specify that he or she wishes the Visa Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; email address; telephone number; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Visa Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 5 U.S.C. 552a (k)(1), (k)(2), and (k)(3), records contained within this system of records are exempted from 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f). See Department of State Rules published in the Federal Register, under 22 CFR 171.26.

HISTORY: This SORN was previously published at 83 FR 28062 (June 15, 2018).