DEPARTMENT OF STATE

[**Public Notice: 12000]**

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a New System of Records.

SUMMARY: Information in Special Presidential Envoy for Hostage Affairs and Related Records is used to support diplomatic and consular efforts to secure the recovery of and provide assistance and support services to individuals taken hostage or wrongfully detained abroad.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records notice is effective upon publication, with the exception of the routine uses that are subject to a 30-day period during which interested persons may submit comments to the Department. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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 "Special Presidential Envoy for Hostage Affairs and Related Records, State-60" 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: None

SYSTEM NAME AND NUMBER: Special Presidential Envoy for Hostage Affairs and Related Records, STATE-60.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Department of State, including overseas at U.S. embassies, U.S. consulates, and U.S. consular agencies and within a government cloud provided, implemented, and overseen by the Department's Enterprise Server Operations Center (ESOC), 2201 C Street NW, Washington, DC 20520.

SYSTEM MANAGER(S): The Special Presidential Envoy for Hostage Affairs (SPEHA), Special Assistant, Office of the Special Presidential Envoy for Hostage Affairs; U.S. Department of State, 2201 C Street NW, Washington, DC 20520, phone: 202-647-4611.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

(a) 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and providing assistance to other agencies);

(b) 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);

(c) 22 U.S.C. 1732 (Release of citizens imprisoned by foreign governments);

(d) 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance);

(e) 22 U.S.C. 2715a (Responsibility to inform victims and their families regarding crimes against U.S. citizens abroad);

(f) 22 U.S.C. 2715b (Notification of next of kin of death of U.S. citizens in foreign countries);

(g) Sec. 599C of Public Law 101-513, 104 Stat. 1979, as amended (Claims to benefits by virtue of hostage status) (Benefits ended, but applicable to past records);

(h) Presidential Executive Order 13698 (Hostage Recovery Activities) (June 29, 2015);

(i) Presidential Policy Directive 30 (U.S. Nationals Taken Hostage Abroad and Personnel Recovery Efforts) (June 24, 2015);

(j) Section 302(c) of the Robert Levinson Hostage Recovery and Hostage-taking Accountability Act (Div. FF, Title III, Subtitle A of the Consolidated Appropriations Act, 2021, P.L 116-260) (Hostage and Wrongful Detention Recovery Efforts and Codifying the Special Presidential Envoy for Hostage Affairs) (December 27, 2020); and

(k) Presidential Executive Order 14078 (Bolstering Efforts to Bring Hostages and Wrongfully Detained United States Nationals Home) (July 19, 2022).

PURPOSE(S) OF THE SYSTEM: The information in the Special Presidential Envoy for Hostage Affairs and Related Records system of records is used to support diplomatic and consular efforts to secure the recovery of and provide assistance and support services to individuals taken hostage or wrongfully detained abroad.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who are, may be, or were previously taken hostage, detained but unacknowledged by a foreign government, subject to coercive travel restrictions, or detained unlawfully or wrongfully by a foreign government (hereinafter, for purposes of this notice, "individuals taken hostage or wrongfully detained abroad") and such individuals and offices involved in or engaging on their cases, including family members, congresspersons, third party intermediaries, and attorneys,

who receive assistance or engage with the Office of the Special Presidential Envoy for Hostage Affairs (SPEHA) or other offices or bureaus in the Department of State. The Privacy Act defines an individual at 5 U.S.C. 552a(a)(2) as a United States citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: Records related to individuals who are taken hostage or wrongfully detained abroad. These records may include biographic and contact information, such as name, place of birth, current mailing address, zip code, email address, phone number, Social Security number, title, date of birth, gender, passport information, photographs, video recordings, health information, and employment information; information related to the individual's detention or treatment by a foreign government or non-state actor and actions by the United States government and other actors in relation to their case ; information about foreign, personal, family, emergency contacts; and information about third party intermediaries and their engagement. These records may also include communications to and from U.S. embassies, U.S. consulates, and consular agencies; foreign, federal, state, and local government agencies, including law enforcement agencies; members of Congress; U.S. and foreign courts; U.S. and foreign nongovernmental organizations; the United Nations and other international organizations; and the subject(s) of the records, their family members, and other interested parties. Certain records in this system are consular records that are also maintained pursuant to the Office of Overseas Citizen Services (OCS) System of Records Notice (State-05) (81 FR 62235), available at https://www.state.gov/system-of-records-notices-privacy-office/.

RECORD SOURCE CATEGORIES: These records contain information that is obtained from the individual who is the subject of the records, their family members, their attorneys, and

third-party intermediaries. Information may also be obtained from federal, state, local and foreign government authorities and nongovernmental entities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: The information in the Special Presidential Envoy for Hostage Affairs and Related Records may be disclosed to:

(a.) Federal agencies and federal interagency bodies in connection with the recovery of and investigation and prosecution of cases involving individuals taken hostage or wrongfully detained abroad;

(b.) Domestic, international, and foreign law enforcement agencies in connection with law enforcement issues and health, safety, welfare and related matters involving individuals taken hostage, or wrongfully detained abroad;

(c.) Foreign governments and international organizations to facilitate resolution of cases involving individuals taken hostage or wrongfully detained abroad;

(d.) Federal, state, and local agencies in connection with the administration of U.S. federal, state, or local benefits or foreign benefits for individuals taken hostage or wrongfully detained abroad;

(e.) Federal, state, foreign, and local agencies responsible for investigating and/or prosecuting hostage and wrongful detention cases or assisting those who have been taken hostage or wrongfully detained abroad and/or their family members;

(f.) Federal, state, and foreign courts where the information is relevant and necessary to litigation involving an individual who has been taken hostage or wrongfully detained abroad;

(g.) Family members of an individual who has been taken hostage or wrongfully detained abroad;

(h.) The individual's employer when the disclosure is for the benefit of an individual who has been taken hostage or wrongfully detained abroad;

(i.) Congressional offices and Congressional committees when the disclosure is for the benefit of an individual who has been taken hostage or wrongfully detained abroad;

(j.) Third parties designated by a family member of an individual taken hostage or wrongfully detained abroad when the disclosure is for the benefit of an individual who has been taken hostage or unlawfully or wrongfully detained abroad;

(k.) Attorneys when the individual to whom the information pertains has been taken hostage or wrongfully detained abroad, and that individual is the client of the attorney making the request, or when the attorney is acting on behalf of some other individual to whom access is authorized under this notice;

(l.) The news media or the public where such disclosure is in furtherance of the Special Presidential Envoy for Hostage Affairs' mission, and where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy or to have an undue adverse effect on either the subject or individuals associated with the subject, and where there is a legitimate public interest in the information disclosed.

(m.) To 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.

(n.) To 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 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 Special Presidential Envoy for Hostages Affairs and Related Records system, State-60. Records in this system that are also consular records are subject to the routine uses identified in the Overseas Citizen Services Records and Other Overseas Records system of records notice STATE–05, as well as those in this notice.

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 here 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 only.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: By individual name, birth date, passport number, or other personal identifier, such as country/location of detention, if available.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: 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 outlined here https://foia.state.gov/Learn/RecordsDisposition.aspx. The range of disposition for records maintained in the system is one to twenty years. 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 users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet users are required to take the Foreign Service Institute 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 Special Presidential Envoy for Hostage Affairs and Related Records, a user must first be granted access to the Department of State computer 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 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 OMB Circular 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 thorough 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. 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 information 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 Federal Information Security Management Act (FISMA) low, moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Department's Cloud Program 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, The Federal Risk and Authorization Management Program (FedRAMP), OMB regulations, National Institute of Standards and Technology's (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 mechanism 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 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 Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that they wish Special Presidential Envoy for Hostage Affairs and Related Records to be checked. At a minimum, the individual must include: full name and any other names used; current mailing address and zip code; date and place of birth; 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 Special Presidential Envoy for Hostage Affairs and Related Records includes records pertaining to them. Detailed instructions on Department of State procedures for accessing and amending records can be found on the Department's FOIA website at https://foia.state.gov/Request/Guide.aspx.

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 Street, 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 Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that the Special Presidential Envoy for Hostage Affairs and Related Records should be checked. At a minimum, the individual must include: full name and any other names used; current mailing address and zip code; date and place of birth; 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 Special Presidential Envoy for Hostage Affairs and Related Records include records pertaining to them.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 5 U.S.C. 552a(k)(1), records subject to the provisions of section 552(b)(1) are exempted from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Pursuant to 5 U.S.C. 552a(k)(2), records that consist of investigatory material compiled for law enforcement purposes are exempted from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

HISTORY: None.

Eric F. Stein,

Deputy Assistant Secretary,

Global Information Services (A/GIS),

Department of State.

Billing Code 4710-AD