Privacy Impact Assessment

for the

CISA Overseas Support Program

DHS Reference No. DHS/CISA/PIA-039

November 4, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Stakeholder Engagement Division (SED) has created the CISA Overseas Support Program (OSP) to serve as a focal point for international collaboration between CISA, host country government officials, and other federal agency officials to enhance our national security, promote the resiliency of critical infrastructure, and address risks vital to U.S. interests. The program is responsible for deploying attachés, liaison officers (LNO), and technical advisors internationally to support CISA's mission. CISA is conducting this Privacy Impact Assessment (PIA) due to the collection of personally identifiable information (PII) of the agency's personnel and their dependents for permanent change of station (PCS) and temporary duty assignment (TDY) overseas deployments.

Overview

CISA, as part of its mission, identifies and implements U.S. government cyber and infrastructure security objectives through expanded global partnerships, ensuring that its international engagement and related operations reflect broader U.S. national security, economic, and foreign policy goals. To meet these objectives, overseas CISA personnel advance CISA's mission by appropriately and securely sharing information, mitigation advice, and best practices. The CISA Overseas Support Program, which is responsible for deploying and providing support to attachés, liaison officers, and technical advisors overseas, sustains CISA's international mission.

The CISA Attaché Offices will serve as focal points for international collaboration between CISA, host country government officials, and other U.S. government officials. Enhancing CISA's work with foreign partners by establishing the Overseas Support Program will build CISA's capacity and capability to defend against cyber incidents globally, improve the security and resiliency of critical infrastructure, identify and address the most significant risks to national critical functions, and provide seamless and secure emergency communications. The CISA Attaché Offices advance CISA's missions in cybersecurity, critical infrastructure protection, and emergency communications and leverage the agency's global network to promote CISA's four international strategic goals:

- *Advancing operational cooperation,*
- *Building partner capacity,*
- *Strengthening collaboration through stakeholder engagement and outreach, and*
- *Shaping the global policy ecosystem.*

CISA attachés provide on-site representation and expert and authoritative advice on all aspects of policies and programs related to CISA's mission. Each CISA attaché is a member of the

U.S. embassy's country team and works closely with and advises the U.S. ambassador and mission staff on new and potentially adverse information involving CISA's mission. CISA attachés serve as the official point of contact (POC) for CISA headquarters and the embassy on all CISA related matters, including providing expertise and advice on all CISA efforts in-country and engaging, as appropriate, with the counterparts from the United States, host country, and other foreign governments; private sector entities; and non-governmental organizations, in conjunction with and in support of the CISA and DHS missions.

Liaison officers are CISA employees who are responsible for interacting directly with CISA's counterpart organization in the country to which they are assigned, on behalf of CISA. Liaison officers work with CISA's foreign counterpart agencies to communicate and coordinate activities on matters of mutual concern; oversee engagements with foreign partners; expand, strengthen, and develop partnerships; and recommend new engagements and partnerships to CISA senior leadership. Liaison officers do not have the authority to advise or make decisions on behalf of CISA without first seeking CISA leadership approval.

CISA employees serving as technical advisors are embedded in the operational arm of foreign organizations and execute responsibilities for national computer network defense, cyber incident response, and communications resiliency. Technical advisors work with the foreign partner government to improve collaboration and coordination between the United States and the host government on technical issues of mutual importance. Technical advisors do not have the authority to advise or make decisions on behalf of CISA without first seeking CISA leadership approval.

In its role of deploying and supporting CISA personnel overseas, the Overseas Support Program will collect information from CISA employees and their accompanying eligible family members (EFM) to track permanent change of station and temporary duty assignment deployments and ensure employee and eligible family members' safety and accountability while assigned overseas. This repository of information, both reference and personal information of CISA employees and their dependents, will be stored on a secure agency collaboration Microsoft SharePoint site where only employees assigned to the Overseas Support Program who need to know will have access to the collected information. The SharePoint site displays visual cues indicating that Sensitive Personal Identifiable Information (SPII) is authorized to be posted, and the SharePoint site is managed accordingly.

Reference information and forms (Standard Operating Procedures (SOP), Handbooks, How-to-Guides, Checklists, Frequently Asked Questions (FAQ)) as well as general program information—including the names of the CISA attachés, liaison officers, and technical advisors—will be available to the CISA workforce through the agency's intranet.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The authorities below permit the collection and use of information for the Overseas Support Program:

- 6 U.S.C. § 652(c)(2);
- 6 U.S.C. § 652(c)(11);
- 6 U.S.C. § 659(c)(8); and
- U.S. Department of State Foreign Affairs Handbook, 2 FAH-2 H-110 et seq.[1] (noting requirements for personally identifiable information collection for overseas staffing).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information collected by the Overseas Support Program can be retrieved by a personal identifier, and pursuant to the Privacy Act, a System of Records Notice (SORN) is required. The Overseas Support Program is covered by the following System of Records Notices:

- DHS/ALL-032 Official Passport Application and Maintenance Records,[2] which covers the collection of passport information from CISA employees and members of their families.
- DHS/ALL-040 DHS Personnel Recovery Information System of Records,[3] which covers all other personally identifiable information.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Information collected by the Overseas Support Program will be retained on a Microsoft SharePoint site with appropriate access controls restricted only to those individuals assigned to the Overseas Support Program who also need to know the information. Microsoft SharePoint is an employee collaboration tool documented in DHS/ALL/PIA-059 DHS Employee Collaboration

[1] *See* U.S. Department of State Foreign Affairs Handbook, 2 FAH-2 H-110 et seq., *available at* https://fam.state.gov/FAM/02FAH02/02FAH020110.html.

[2] *See* DHS/ALL-032 Official Passport Application and Maintenance Records, 76 Fed. Reg. 8755 (February 15, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.

[3] *See* DHS/ALL-040 DHS Personnel Recovery Information System of Records, 82 Fed. Reg. 49407, (October 25, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

Tools.[4] As a content management tool, it is assessed for security compliance and maintains privacy compliance documentation describing purpose, use, and types of personally identifiable information stored within the site as a part of the inventory maintained by CISA for all Microsoft SharePoint sites that retain personal information.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Records collected and retained by the Overseas Support Program are covered under General Records Schedule (GRS) Employee Management Records 2.2,[5] Item 010 - Employee Management Administrative Records. To ensure compliance, the Overseas Support Program will conduct annual audits of all records that are retained by the program to dispose of/delete them in accordance with General Records Schedule 2.2, Item 010.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information is not being collected or solicited directly from the public; therefore, the Paperwork Reduction Act (PRA) does not apply to the information collected by the Overseas Support Program.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The Overseas Support Program will collect the following personal information to track information related to permanent change of station and temporary duty assignment deployments:

From CISA Attachés, Liaison Officers, and Technical Advisors:

- First Name
- Middle Initial
- Last Name

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR DHS EMPLOYEE COLLABORATION TOOLS, DHS/ALL/PIA-059 (2017), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[5] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, GENERAL RECORDS SCHEDULE, RECORDS SCHEDULE NUMBER 2.2, EMPLOYEE MANAGEMENT RECORDS, *available at* https://www.archives.gov/files/records-mgmt/grs/grs02-2.pdf.

- Gender (Male/Female)
- Date of Birth
- Place of Birth (City, State, and Country)
- Dual Citizenship (Yes/No)
    - Country/Countries of Citizenship
- Marital Status
- Personal Identity Verification (PIV)[6] Card Expiration Date
- Personal Email Address
- Personal U.S. Mobile Phone Number
- Home Phone Number
- Home Address
    - City, State, Zip Code
- Work Email Address
- Desk Phone Number
- Work Mobile Number
- Current Grade Level
- Current Series
- Current Step
- Current Duty Station
- Current Supervisor
- Current Supervisor’s Title
- Current Supervisor’s Email Address
- Home Office
- Current Security Clearance Level
- Government Travel Card (Yes/No)

[6] For more information on Personal Identity Verification cards, visit https://www.idmanagement.gov/university/piv/.

- Official Passport (Yes/No)
  - Official Passport Number
  - Issuance Date
  - Expiration Date
- Language Proficiency Skills
- Prior Overseas Deployment (Yes/No)
  - Summary
- Dates Unavailable for Pre-Deployment Training
- Department of State Medical Identification Number

From or on Behalf of Eligible Family Member(s)/Dependent(s) (Adult):

- Are Dependents Accompanying Employee Deployed Overseas (Yes/No)
  - If Yes, How Many Dependents Will be Accompanying Employee
- Spouse/Domestic Partner Information
  - First Name
  - Middle Initial
  - Last Name
  - Gender (Male/Female)
  - Date of Birth
  - Place of Birth (City, State, and Country)
  - Dual Citizenship (Yes/No)
  - Countries of Citizenship
  - Personal Phone Number
  - Personal Email address
  - Ever Held US Passport (Yes/No)
  - Department of State Medical Identification Number

From Eligible Family Member(s)/Dependent(s) (Minors):

- First Name

- Middle Initial
- Last Name
- Gender (Male/Female)
- Date of Birth
- Place of Birth (City, State, and Country)
- Dual Citizenship (Yes/No)
  - Countries of Citizenship
- Ever Held US Passport (Yes/No)
- Current Education Grade Level if in School
- Individual Development Plan (IDP) (Yes/No)
- Department of State Medical Identification Number
-

From Emergency Point of Contact/Next of Kin in United States:

- First Name
- Middle Initial
- Last Name
- Relationship to Employee
- Home Phone Number
- Personal Phone Number
- Email Address

The Overseas Support Program will also collect contact information (e.g., work email address and phone numbers) from the Department of State Regional Security Officers (RSO) and post housing points of contact related to the location of deployed personnel.

2.2 What are the sources of the information and how is the information collected for the project?

CISA employees are provided the CISA Deployment Request Form to complete and submit information to the Overseas Support Program. The form requests only required information from the employee and dependents to process a permanent change of station or temporary duty assignment overseas. Personal data about the CISA employees and their overseas assignments are collected directly from these individuals. Dependent information is collected from the CISA employee on behalf of their dependents and submitted to the Overseas Support Program to retain.

Contact information for the Department of State Regional Security Officers and post housing point of contacts related to the location of deployed personnel is collected directly from the embassy or consulate.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The Overseas Support Program does not use any information from commercial sources or publicly available data. All information is obtained directly from CISA personnel or the Department of State.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the information collected by the Overseas Support Program is ensured by collecting information directly from involved CISA personnel through their completion of the Deployment Request Form. CISA personnel may update responses and make changes to the information retained by the program to ensure that the information remains accurate and up to date throughout their overseas assignment.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more information will be collected from individuals than necessary.

Mitigation: This risk is mitigated. CISA uses the Deployment Request Form, which has been reviewed and approved by the CISA Office of Privacy, Access, Civil Liberties and Transparency (PACT), CISA Office of the Chief Counsel, and the DHS Privacy Office, to ensure the information is collected in a standardized format. The information that is being collected is limited to only the information needed for employees and their dependents to deploy overseas successfully. Any change to the program or to the program purpose that would require the collection of additional information may necessitate an update to this Privacy Impact Assessment.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The Overseas Support Program is responsible for deploying CISA employees and their dependents to serve on Permanent change of station or Temporary duty assignments overseas. Employees serving permanently overseas are assigned for three to five years, while employees temporarily assigned overseas may be deployed from a few weeks to a year.

In preparation for an overseas assignment, a variety of personal information must be collected to assist employees and their dependents in obtaining a diplomatic passport, diplomatic title, privileges, and immunities; identifying housing and schooling; and enrolling in mandatory pre-deployment training. Most of the information collected is used internally within CISA to ensure the employee has the correct security clearance for the overseas position, to update the employee's personal identity verification (PIV) card to ensure it does not expire while overseas, to process any personnel actions reflecting the change in duty station, and to issue relocation orders.

The Overseas Support Program also provides CISA employees and their dependents with the necessary medical forms for submission to the Department of State for their medical clearance. All medical information required by the Department of State to obtain medical clearance is submitted directly to Department of State, and no medical information is used or retained by the Overseas Support Program. If medically approved, the CISA employee will send their medical clearance approval email (and that of their dependents, if applicable) to the Overseas Support Program for its records to track and maintain the Medical ID number given to the individual by the Department of State, the clearance date, and the type of medical clearance (world-wide or post specific). The Overseas Support Program will use this information to notify individuals when medical clearance updates are required when there is a change in duty station or if the medical clearance expires. Individuals are then responsible for submitting requisite medical forms directly to the Department of State to be issued a subsequent medical clearance approval email to be retained by the Overseas Support Program, including only data related to the issuance of the medical clearance.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. The Overseas Support Program does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. No other DHS components will have assigned roles or responsibilities or have access to the system/program. Access to the system is restricted to employees assigned to the Overseas Support Program who need to know.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information, such as employee or eligible family member's medical information, may be misused or for a purpose other than the one for which it was initially collected.

Mitigation: The risk is mitigated. CISA employs access controls to mitigate this risk. Employees assigned to the Overseas Support Program who have access to the collaboration tool where the collected information is retained are trained on both DHS and CISA procedures for handling and safeguarding personally identifiable information. The collaboration tool employs strict access controls to the information; access is provided only to those individuals with a valid need to know, view, and use the information for its specified purpose. Personnel receive privacy training and are required to take annual refresher training. In addition, CISA maintains standard operating procedures, information handling guidelines, and practices for identifying sensitive information and the proper handling, safeguarding, and minimization of personally identifiable information. CISA also defines the terms of use for specifically identified roles and responsibilities.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Information is collected directly from CISA personnel or Department of State Regional Security Officers and post housing points of contact. The Deployment Request Form includes a Privacy Act Statement stating, "All information contained in this form is being used solely for the purpose of your permanent change of station or temporary duty assignment overseas. Information contained in this form will be shared only with those who have a role in your overseas deployment process. Failure to provide the required information may result in the inability to deploy."

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

CISA employees who voluntarily apply for an overseas assignment are required to comply with all mandatory pre-deployment requirements. Failure to comply with the mandatory pre-deployment requirements may result in the employee being unable to deploy. The Privacy Act Statement on the Deployment Request Form, and the requirements listed in the vacancy announcement, provides the employee with notice of what information is required for an overseas assignment. The employee has the option to either apply or not apply for the position. In addition, this Privacy Impact Assessment also provides notice to employees and their dependents of what information will be collected and how it will be used.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an employee's dependents may not be provided with adequate notice as to how their personally identifiable information will be used.

Mitigation: The risk is partially mitigated. The Deployment Request Form provides direct notice to the CISA employee. The Privacy Act Statement added to the Deployment Request Form provides the CISA employee with notice describing what information is necessary to be collected for the purposes of an overseas assignment and whether to continue with the application. CISA expects that employees requesting deployment will provide notice to their spouses and dependents when providing their information in preparation for an overseas relocation. Additional notice is also provided to individuals upon the publication of this Privacy Impact Assessment, describing to the employees and their dependents the purpose of the program, what information will be collected, and how the collected information will be used.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

The Overseas Support Program will retain the personal information collected on the Deployment Request Form for the duration of the employee's overseas assignment. Upon completion of the overseas assignment, the information will be archived in Microsoft SharePoint in accordance with CISA's record and retention policy. During an annual review of the records, if applicable, the Overseas Support Program will dispose of/delete archived records in accordance with General Records Schedule 2.2, Item 010.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that collected information may be retained longer than necessary and as stipulated in the retention schedule.

Mitigation: This risk is mitigated. As documented in its standard operating procedures, the Overseas Support Program will conduct annual audits of all records that are retained by the program to dispose of/delete in accordance with General Records Schedule 2.2, Item 010.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The information collected by the Overseas Support Program is shared outside of DHS with the Department of State as a part of its normal programmatic operations. The Department of State is responsible for issuing or providing diplomatic passports, medical clearances, diplomatic titles, privileges and immunities, housing, and schooling at post. The Overseas Support Program will share only the information required to complete the aforementioned items, and retain email correspondence regarding these items with the Department of State as a part of normal programmatic operations.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The System of Records Notices stated in Section 1.2 of this Privacy Impact Assessment contain routine uses that allow for the sharing of records outside of DHS. These uses are limited to specific circumstances that are a part of normal business operations as they pertain to the Overseas Support Program and personnel deployment overseas.

6.3 Does the project place limitations on re-dissemination?

Information is shared only with those individuals at the Department of State who have a need to know and who are involved in the overseas deployment process. The Overseas Support Program will verify the contact information for the points of contact prior to transmitting personal information to ensure that the information is submitted to the correct point of contact and to limit the need for the information to be re-disseminated.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The Overseas Support Program maintains a copy of the emails submitted to the Department of State as a part of normal programmatic operations.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be shared with Department of State personnel lacking the need to know or uninvolved with normal Overseas Support Program operations.

Mitigation: The risk is mitigated. Access to information shared by the Overseas Support Program is restricted to only those individuals at the Department of State who have a need to know how to perform program responsibilities. CISA personnel receive annual privacy and cybersecurity training and are required to ensure personally identifiable information is only sent to the correct Department of State points of contact. CISA also maintains standard operating procedures and information handling guidelines and practices for the identification of sensitive information and for the properly handling, disseminating, and safeguarding of personally identifiable information.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

The Overseas Support Program allows employees to request and/or update their and their dependents' information collected during the deployment process by emailing overseassupportprogram@cisa.dhs.gov.

Individuals can also access information collected by the program by submitting a Freedom of Information Act (FOIA) or Privacy Act request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/Privacy Act request at https://www.dhs.gov/freedom-information-act-foia, or by writing to:

The Privacy Office
Privacy Office, Mail Stop 0655
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, D.C. 20528-065

Individuals may also make information inquiries to FOIA@hq.dhs.gov. The release of information is subject to standard FOIA exemptions.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals will follow the same procedures listed in Section 7.1. to correct and/or update their information.

7.3 How does the project notify individuals about the procedures for correcting their information?

Guidance on how employees can correct their information is listed on the Deployment Request Form, discussed with the employees during the pre-deployment training, and outlined here in this Privacy Impact Assessment and the applicable System of Records Notices.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not understand the redress procedure to correct any of their information and their dependents' information.

Mitigation: The risk is mitigated. Guidance on how employees can correct their information and their dependents' information is described on the Deployment Request Form at the point of collection of this information, discussed with the employees during the pre-deployment training, and outlined here upon the publishing of this Privacy Impact Assessment. In addition, monthly programmatic check-ins by the program are held with the employee, a reminder is provided to the employee to contact overseassupportprogram@cisa.dhs.gov if any updates and/or changes are needed to their information and/or their dependents' information.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CISA has well-established and comprehensive information handling processes to enhance information security and eliminate possibilities for inappropriate sharing, misuse, and/or loss, including the information handling processes described in the Department's Handbook for Safeguarding Sensitive Personally Identifiable Information.[7]

The Overseas Support Program has also submitted to the CISA Office of Privacy, Access, Civil Liberties and Transparency (PACT) compliance documentation regarding its Microsoft SharePoint site, where program information is retained, all information that is maintained on the site, and appropriate access controls to that information. Access controls include the ability to show who accessed the site, when they accessed the site, and the date any modifications were made to the site. Access is routinely monitored by the Overseas Support Program section chief to ensure that only those individuals in the program with a valid need to know have the ability to access and use the information as a part of their duties. When employees depart the program, the section chief promptly removes their access to the site.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Personnel assigned to the Overseas Support Program are required to complete annual privacy training covering identifying, retaining, safeguarding, and using personally identifiable information during daily work activities. Individuals who have not completed the required privacy training will have their access to the Microsoft SharePoint site, where the Overseas Support Program information is maintained, and suspended until they complete assigned privacy training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Employees assigned to the Overseas Support Program will receive access to the Microsoft

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSITIVE PII, PRIVACY POLICY DIRECTIVE 047-01-007, REVISION 3, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

SharePoint site upon completing all DHS and CISA onboarding training requirements, such as DHS Privacy Training and DHS Records Management Training. The Overseas Support Program section chief will have administrative access to the Microsoft SharePoint site and the ability to add and/or remove an employee's access to the site. The employees assigned to the program will have "edit" access only (not administrative access), allowing them to enter information from the Deployment Request Form into the Microsoft SharePoint site.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The Overseas Support Program does not have any information sharing agreements or Memoranda of Understanding (MOU). However, should any agreement be developed for this program, it will be reviewed by all appropriate parties (e.g., privacy, legal).

Contact Official

Jasmyn Hurry
Section Chief, Operational Support Program
CISA International Affairs, Stakeholder Engagement Division
operationalsupportprogram@cisa.dhs.gov

Responsible Official

Kaitlin Jewell
Associate Director
CISA International Affairs, Stakeholder Engagement Division

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Deborah T. Fleischaker
Chief Privacy Officer (A)
U.S. Department of Homeland Security
Privacy@hq.dhs.gov