1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Information Sharing Services,
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: August 6, 2008

(b) Name of system: Overseas Security Advisory Council

(c) System acronym: OSAC

(d) IT Asset Baseline (ITAB) number: 781

(e) System description:

The Overseas Security Advisory Council, which falls under the auspices of the Bureau of Diplomatic Security (DS), is an active partner of U.S. businesses and universities, helping them to remain competitive and secure in a global environment through the dissemination of vital security-related information. OSAC, established in 1985, is comprised of 30 private sector and four public sector member organizations that represent specific industries or agencies operating abroad. OSAC country councils are an overseas extension of OSAC, and provide a forum for effective communication between the U.S. embassy and the U.S. private sector in a given country. There are currently over 100 OSAC Country Councils operating globally. OSAC objectives are to:

- Establish continuing liaison and provide for operational security cooperation between Department of State security functions and the private sector;
- Provide for regular and timely interchange of information between the private sector and the Department of State concerning developments in the overseas security environment;
- Recommend methods and provide material for coordinating security planning and implementation of security programs; and,
- Recommend methods to protect the competitiveness of U.S. businesses operating worldwide.

OSAC Committees are as follows:

- Threats and Information Sharing;
- Country Council and Outreach; and
- Security Awareness and Innovation.

The OSAC website (www.osac.gov) is the focal point for exchanging unclassified information between the Department of State (DOS), other government agencies, and the U.S. private sector on security-related incidents and threats abroad. Some of the information accessible from the website includes:

- Department travel advisories;

- Public announcements;
- Daily security related news articles;
- Events;
- Reports on security and crime incidents abroad;
- Country council information;
- Terrorist group profiles;
- Significant anniversary dates;
- General crime information for cities and countries;
- Locations and contacts at Department posts abroad; and
- Updates on new or unusual situations.

(f) Reason for performing PIA:

□ New system

□ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification: Not applicable.

(h) Date of previous PIA: April 24, 2007

3. Characterization of the Information

The system:

□ does NOT contain PII.

☒ does contain PII.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

OSAC recipient data is information that populates the data fields in the application database. PII collected includes:

- Username;
- Password;
- Email address;
- First Name;
- Last Name;
- Office Title;
- Office Phone;
- State/Province;
- Country; and
- One of the following elements for the badge process: Social Security Number, Driver's License Number, or Passport number. This information is maintained in the OSAC database for a period no longer than 60 calendars days once a year.

The sources of the information are DS/DSS/OSAC and its business partners.

b. How is the information collected?

Information can be obtained directly or indirectly from an individual or individuals and/or the Bureau of Diplomatic Security (DS) personnel.

c. Why is the information collected and maintained?

Information collected is the minimum required to meet OSAC's business objectives to effectively protect against and manage international threats as it relates to U.S. Interests.

d. How will the information be checked for accuracy?

The agency or source providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by DS include maintaining the system as a live feed, allowing the information to be updated/edited at any time, and cross-referencing information with the DS/DSS/OSAC analyst or surrogates.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to OSAC, are as follows:

- Pub.L. 99-399(Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended;
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The information collected is the minimum required to meet the business objectives of OSAC in order to effectively protect and manage international threats as they relate to U.S. interests. No adverse determination may result from the information collected causing the denial of a right benefit, or privilege owed the record subject. This system incorporates the highest degree of privacy and security controls.

The nature of the PII collected and maintained resulted in a security categorization of “moderate” for the system and established specific privacy and security controls. The controls are subject to rigorous testing and a formal certification and accreditation process; authority to operate is authorized by a senior agency official. System controls are reviewed annually and accredited every three years or sooner if the system has implemented major changes.

4. Uses of the Information

a. Describe all uses of the information.

The information is used by U.S. private and public sector administrators and analysts to participate in the coordination of the International Threats Advisory to maintain accurate and timely information. No non-production usage of the information is permitted.

b. What types of methods are used to analyze the data?

Analysis of the information is limited to non-subject-based statistical information such as the level and number of threats by country.

What new information may be produced?

None.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

OSAC may collect information from commercial and public sources. The OSAC Council is comprised of 30 private sector and four public sector member organizations, representing a broad range of economic sectors or agencies operating abroad. Private sector members are selected from the Council's constituency and normally serve for two-four year terms. Member organizations designate a representative to work on the Council. Under OSAC leadership, annual goals and objectives are discussed, evaluated, initiated, and assigned. The Council is co-chaired by the Director, Diplomatic Security Service (DS/DSS) and a selected representative from the private sector.

d. Is the system a contractor used and owned system?

The system is owned/operated by the Department of State, Bureau of Diplomatic Security Services, Overseas Security Advisory Council (DS/DSS/OSAC) and is maintained by contractors.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Appropriate use is regulated by automated controls in the system and by the system rules of behavior. Instructions on use of the system are periodically refreshed and re-issued as appropriate. The system does not allow any flexibility of features that could potentially create a vulnerability to function creep.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The utility of the information in the database about a particular threat will not extend over the allotted time defined in the Department of State's Disposition Schedule of Diplomatic

Security Records. Moreover, over an extended period of time there is negligible privacy risk as a result of a degradation of information quality.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Internal organizations with which the information is shared include the originating office and the individuals with work-related responsibility for the creation, maintenance, and monitoring of the information in the database.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The system does not interface with any other government system. Its information is not transmitted to any other system. Information is available only to authorized users of the system. Authorized users have roles assigned to them specific to their functional use and strong segregation of duties is applied.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the Department of State are allowed.

7. External Sharing and Disclosure

a. With which external organizations is the information shared?

OSAC shares information with Diplomatic Security employees, contractors, and OSAC members. However, Personally Identifiable Information data is not shared outside the Bureau.

What information is shared?

International threats, by country.

For what purpose is the information shared?

Possible international threats.

b. How is the information shared outside the Department?

Via the OSAC website.

What safeguards are in place for each sharing arrangement?

Safeguards are user name and password with network perimeter defense.

c. Privacy Impact Analysis:

A risk to any online application is unauthorized access; however, the OSAC application provides a means of limiting access to areas within the application based on user ID/password or PKI token, and a “need-to-know.” Diplomatic Security employees, contractors, and OSAC members must follow the system rules of behavior established by the Department of State.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

The information in this system is covered by STATE-36, Security Records, last amended December 26, 2007 at 72 FR 73057-73060.

□ does not constitute a system of records covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Yes, notice is provided to non-combative individuals and groups. OSAC is exempt from the Paperwork Reduction Act in accordance with the “certifications” exemption permitted at 5 CFR 1320.2

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes, enrollment/registration by an entity at the OSAC website is completely voluntary

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information?

Yes, enrollment/registration by an entity at the OSAC website is completely voluntary; “right to consent” is not applicable in this system.

If so, how does the individual exercise the right?

Conditional consent is not applicable to the official purpose of the system.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Sufficient notice of the purpose, uses, and authority of the collection of the personal information is described to a participating OSAC entity, based on the rules of behavior, specific to the use of the system. Individuals who have reason to believe that Diplomatic Security may have membership records pertaining to them, should write to the Director, Office of Information Programs and Services, A/ISS/IPS, SA–2, Department of State, Washington, DC 20522–6001. The individual must specify their desire to have their Security Records checked. At a minimum, the individual must include: username; password; e-mail address; first name; last name; office title; office phone number; state/province; country; and a brief description of the circumstances that may have caused the creation of the record. Individuals who wish to gain access to or amend records pertaining to them should write to the Director, Office of Information Programs and Services (address above).

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals may directly gain access to their information by using the application and amend their personal information should they identify errors of fact or omission. Individuals who have reason to believe that Diplomatic Security may have security/investigative records pertaining to them should write to the Director, Office of Information Programs and Services, A/ISS/IPS, SA–2, Department of State, Washington, DC 20522–6001. The individual must specify that they request Security Records to be checked. At a minimum, the individual must include: username; password; e-mail address; first name; last name; office title; office phone number; state/province; country; and a brief description of the circumstances, which may have caused the creation of the record. Individuals who wish to gain access to or amend records pertaining to them should write to the Director, Office of Information Programs and Services (address above).

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

There is no risk associated with notification and redress.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access?

The following Department of State policies establish the requirements for access enforcement:

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

Access to the system is based on a “need to know” and user role. Policies and procedures regarding access are all documented. Diplomatic Security employees and contractors must follow the system rules of behavior established by the Department of State.

What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The system maintains a log of system use and events.

b. What privacy orientation or training for the system is provided authorized users?

Every Department user must attend a security briefing prior to receiving access to Department of State networks and getting a badge for facility access. This briefing is sponsored by DS/SI/IS and includes a overview of the Privacy Act of 1974. Users must also take a Departmental information system security briefing and be tested on it prior to receiving access to a Department of State network.

DS/CTO/SMD/SEC regularly updates the user acknowledgment agreement that all users must sign in order to have access to Department of State networks. DS/SI/CS also has a Departmental Security Awareness program in place.

DS/CTO identifies key personnel within DS/CTO/SMD/OPS and DS/CTO/SMD/SEC who need to attend the Department of State's mandated Information Assurance training for system administrators. DS/CTO/SMD/OPS and DS/CTO/SMD/SEC are responsible for system and security administration of DS-owned servers.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

No such residual risk is anticipated.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

If any privacy risk exists, it would be related to the relational database; however, there are several safeguard in place, such as antivirus protection, intrusion protection, patch management updates, and other commonly known technologies implemented within the DS computing environment. Thus, no special risk exists.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No such risk is anticipated.

12. Security

What is the security certification and accreditation (C&A) status of the system?

OSAC Version 01.01.15 was authorized to operate on May 1, 2007, via the certification and accreditation process. The authorization will expire on May 31, 2010.