1. Contact Information

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

2. System Information

(a) Date PIA was completed: October 7, 2010

(b) Name of system: Overseas Security Advisory Council

(c) System acronym: OSAC

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

(e) System description (Briefly describe scope, purpose, and major functions): The Overseas Security Advisory Council (OSAC), 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. Established in 1985, OSAC 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 more than 100 OSAC Country Councils operating globally. OSAC objectives are to:

- Establish a continuing liaison and provide for operational security cooperation between Department of State (DoS) security functions and the private sector;
- Provide for regular and timely interchange of information between the private sector and the DoS 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 among the 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 reauthorization

(g) Explanation of modification (if applicable):

The OSAC environment has evolved into a Next Generation platform, which encompasses new hardware, updated software, and a changed location. The current development and staging environments of the new OSAC.gov, is housed at an outside vendor facility in McLean, Virginia. The production environment will be hosted at a Qwest facility in Sterling, Virginia. The go live date is scheduled in November 2010. Until that time, the current OSAC.gov website is housed within a Department of State facility.

(h) Date of previous PIA (if applicable): January 10, 2010

3. Characterization of the Information

The system:

□ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

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;
- E-mail 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 calendar days once a year.

The sources of the information are the Department of State, Bureau of Diplomatic Security Services, Overseas Security Advisory Council (DS/DSS/OSAC) and its business partners. PII is collected to register a new constituent organization and user. This information is not shared outside of OSAC. The collection of SSN, DL, or PPN only occurs when OSAC holds an event that is located at a DoS location; an example would be the annual briefing every November where this information is collected and shared with DS for purposes of granting facility access to the attendees. PII data is hard deleted from the database shortly after the event occurs. No information is stored anywhere in the system after the hard delete.

When the new OSAC.gov goes live, backups of user- and system-level information contained in the OSAC information system will be conducted daily and weekly; and backup information will be stored at an appropriately secured location in accordance with the NIST SP 800-34.

Back-ups are performed daily during weekdays. One full back-up on tape is completed once a week and incremental tape back-ups are performed for each week day. Historical backups are additionally maintained on a hard drive and retained, at the primary site in Sterling, VA and the backup site in McLean, VA.

b. How is the information collected?

PII for a new constituent organization is collected via a web-based form in the system. Organizations have the ability to either transmit documentation relating to the organization status of being a U.S. based entity via a scanned document in an e-mail or via fax. In the new system individuals will also be able to attach a file to their application to submit such information. This process of submitting documentation will be the preferred method going forward. The DoS employees collect the information that OSAC maintains through established DoS documents. The level of sensitivity for OSAC is sensitive but unclassified (SBU). OSAC processes privacy data as defined by the Privacy Act of 1974.

c. Why is the information collected and maintained?

The 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 OSAC's business objectives to effectively protect against and manage international threats as it relates 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.

U.S. private and public sector administrators and analysts use the information 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? What new information may be produced?

Analysis of the information is limited to non-subject-based statistical information, such as the level and number of threats by country. New information is not produced.

No data mining is used to analyze the information contained in OSAC.

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 to 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. Are contractors involved in the uses of the PII?

DS/DSS/OSAC owns and operates the system, and contractors maintain the system at an offsite vendor location.

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 DoS policies and guidelines as documented in the DoS Disposition Schedule of Diplomatic Security Records:

Overseas Security Advisory Council (OSAC) File Description:

Correspondence, memorandums, telegrams and publications on overseas security problems covering businesses, business information, the charter of OSAC, classified information, coordination, corporations, council members, emergency planning, enterprises, exchange of information, facilities, families, liaison, meetings, other agencies, personnel, private organizations, private sector, programs, protective security, questionnaires, security awareness, terrorism, threats, vulnerabilities, and other related subjects.

All other OSAC records.

Disposition:
Destroy 3 years after cutoff date or when no longer needed for reference, whichever is sooner.

DispAuthNo:
N1-059-94-43, item 86b

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

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

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?

Only the OSAC staff has access to the information on users to the system that includes all PII.

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 U.S. government employees or contractors on the OSAC staff with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the DoS are allowed.

7. External Sharing and Disclosure

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

OSAC shares information with DS employees, contractors, and OSAC members. However, personally identifiable information is not shared outside the Bureau of Diplomatic Security.

Information regarding international threats, by country, is shared.

The only purpose for which information is shared is for possible international threats.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

To find how information is shared outside of DoS use the OSAC website, whereby one can review the OSAC Newsletter, Events Calendar, and Country Councils Reports.

Safeguards are user name and password with a network perimeter defense.

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

Unauthorized access is a risk to all online applications; however, the OSAC application provides a means of limiting access to areas within the application based on user ID/password and a “need-to-know.” DS employees, contractors, and OSAC members must follow the system rules of behavior established by the DoS.

8. Notice

The system:

☒ contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records.
Security Records. STATE-36:

□ does NOT contain information 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 in accordance with membership rights. OSAC is exempt from the Paperwork Reduction Act in accordance with the “certifications” exemption permitted at 5 CFR 1320.3(h).

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? If so, how does the individual exercise the right?

No. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State’s Disposition Schedule, as defined in Diplomatic Security Records, Chapter 11. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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 DS may have membership records pertaining to them, should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA–2, Department of State, Washington, DC 20522–6001. The individual must specify his or her desire to have his or her 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 DS may have security/investigative records pertaining to them should write to the Director, Office of Information Programs and Services, A/GIS/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 minimal 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? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The following DoS 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.

The system maintains a log of system use and events.

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

DS/CTO in coordination with DS/DSS/TIA/OSAC will identify key personnel associated with its contractor (TMS); to determine who needs to attend the Department of State’s mandated Information Assurance training for system administrators. DS/DSS/TIA/OSAC along with its contractor TMS are both responsible for system and security administration of OSAC servers. DS/CTO/SMD/SEC regularly updates the user acknowledgment agreement that all users must sign to have access to DoS networks. DS/SI/CS also has a Departmental Security Awareness program in place.

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.

Residual risks are not anticipated.

11. Technologies

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

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. The OSAC system has been designed to minimize risks to privacy data.

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

No technologies that are known to elevate privacy risk are employed in OSAC; however, numerous management, operational, and technical controls are in place to mitigate any unanticipated risks. Applying security patches and hot-fixes, continuous monitoring, checking the NVD, following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

12. Security

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

OSAC Version 2.0 is under certification and accreditation review currently. The authorization is undetermined as the application is under C&A review.