Overseas Security Advisory Council (OSAC)

1. Contact Information

Privacy Office
A/GIS Deputy Assistant Secretary
Bureau of Administration Global Information Services

2. System Information

(a) Name of system: Overseas Security Advisory Council (OSAC) Web

(b) Bureau: Diplomatic Security

(c) System acronym: OSAC

(d) iMatrix Asset ID Number: 781

(e) Reason for performing PIA:

☐ New system

☒ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Moving current infrastructure over to a Cloud solution, which is due to occur by or around March 2018.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

The system is undergoing assessment with an anticipated completion date by February 2018.

(c) Describe the purpose of the system:

The Overseas Security Advisory Council (OSAC) website (OSAC Web) is a web-based database which collects information (including PII) via a web-based form for the purpose of creating new user accounts. Users come from any of 30 private-sector and/or four public-sector OSAC member organizations (including U.S. businesses, non-governmental organizations, faith-based groups, and universities), DoS, and DS. Users accessing OSAC Web gain access to vital security-related information (i.e. risk, forecasting, and innovation information), which helps them to remain competitive and secure within the

global environment. OSAC Web is the medium for exchanging unclassified information between DoS, other government agencies, and the U.S. private sector on security-related incidents and threats abroad, such as:

- 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

OSAC Web is also used to grant access to attendees to events held at DoS locations, in which case, DL, and/or passport numbers are collected.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Username
- Password
- E-mail address
- First Name
- Last Name
- Office Title
- Office Phone
- State/Province
- Country

In addition, the PII listed below is collected and temporarily stored in the database during event registration, whenever OSAC holds an event that is located at a DoS location:

- Date of Birth
- Passport Number, Driver's License (DL) Number, and Issuing State ID

PII is collected to register a new constituent organization and/or user. This information is not shared outside of OSAC. The collection of DL, or passport number 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 access to the attendees).

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

The legal authorities 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)
- Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: State-36
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): December 15, 2015

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☒Yes ☐No

Language is currently being added to State-36 to ensure that it covers the cloud usage of this system.

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-11-024-02
- Length of time the information is retained in the system: DOB, Driver's License, and Passport numbers are hard deleted from the database the day after the DoS-hosted event occurs.
- Type of information retained in the system:
  No information is stored anywhere in the system after the hard delete.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No

- If yes, under what authorization?

The legal authorities 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)

Executive Order 13526; Title 5 U.S.C. 552a(e)(10); Title 44 U.S.C. chapters 21 and 33; Title 40 U.S.C. chapter 318a; and Title 41 CFR section 102–81.10 and 81.15; 22 U.S.C. 4802(a).

(c) How is the information collected?
PII for a new constituent organization is collected via a web-based form. Organizations have the ability to either transmit documentation related to the organization's status as a US-based entity via a scanned document in an e-mail or by fax. Individuals are also able to attach a file to their application to submit this information. The level of sensitivity of information in OSAC is sensitive but unclassified (SBU).

(d) Where is the information housed?
☒ Department-owned equipment
☒ FEDRAMP-certified cloud (Will be moved here approximately spring 2018.)
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?
The agency or individual 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.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Users with an OSAC.gov account are encouraged to periodically review their user profile and verify that the information is current.

(g) Does the system use information from commercial sources? Is the information publicly available?

The PII that is collected does not come from commercial sources nor is it publicly available. Users voluntarily submit their information to OSAC via the OSAC website.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
Enrollment/registration by an entity on the OSAC website is completely voluntary.
- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The data collected carries inherent risks of being inadvertently or knowingly revealed to those without user authority; therefore, 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.

To mitigate this risk this system incorporates the highest degree of privacy and security controls. Based on the nature of the PII collected and maintained, the system was given a SCF rating of "moderate" and OSAC established specific privacy and security controls commensurate with this rating. The controls are subject to rigorous testing and a formal certification and accreditation process.

5. Use of information

(a) What is/are the intended use(s) for the information?
The collection of PII such as a DL or passport number is used for the purpose of granting access to OSAC events to attendees and to create new user accounts.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes. Please refer to 5(a).

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?
The OSAC Web system analyzes the user's email address to authenticate access to the website at login, as well as for password retrieval in cases where the user forgets their password. This is more an "authentication process" than analysis.

(2) Does the analysis result in new information?
A new password may result in the analysis of the user's email address, if they have forgotten their original password.

(3) Will the new information be placed in the individual's record? ☒Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities that require accessing and/or using the information, i.e. verifying individuals that are permitted to attend DoS facility events.

(b) What information will be shared?
PII such as Driver's License Number or Passport Number is shared when OSAC holds an event that is located at a DoS facility.

(c) What is the purpose for sharing the information?
To grant access to attendees.

(d) The information to be shared is transmitted or disclosed by what methods?
User and event attendee information is accessed via the OSAC website. Authorized users with assigned roles are able to view this information as well as export it to an Excel spreadsheet. The information is then sent via email to DS.

(e) What safeguards are in place for each internal or external sharing arrangement?
Authorized users have a username and password to login to the system with roles assigned to them specific to their functional use and strong segregation of duties is applied.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities that require access to, and use of, attendee information. No other internal disclosures of the information within the DoS are allowed.

Internal sharing of the PII collected by OSAC carries the risk of involuntarily disclosure by those outside of OSAC who review and analyze the information to those who are not authorized to have knowledge of the data. This risk is mitigated by internal OSAC procedures which mandate sharing of PII be conducted only by those officials within DoS with a legitimate need to access it.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Users can correct their own information after logging onto the system with their username and password.

Alternatively, individuals are entitled to avail themselves of the procedures outlined in 22 C.F.R. Part 171 in order to seek access to their own information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals may directly access their information by using the application and can amend it, should they identify errors of fact or omission. For individuals without direct access, to the extent that material contained in OSAC is subject to the Privacy Act (5 U.S.C. 552a), individuals can request amendment of material in the system under the procedures set forth in 22 C.F.R. Part 171. This amendment procedure may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Inaccurate or erroneous information in criminal investigative files will only be subject to amendment or correction at the request of the federal law enforcement agency which originated the material.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Sufficient notice of the purpose, uses, and authority of the collection of the personal information is described to a participating OSAC entity in the disclaimer on the OSAC website. The publication of State-36 informs record subjects of the type of collection occurring in OSAC.

8. Security Controls

(a) How is the information in the system secured?

The internal network/systems are only accessible from outside the physical boundary using a Virtual Private Network (VPN) through the Cisco ASA 5510 firewall. Once authenticated through the VPN additional logon credentials will be needed to access any of the servers or equipment. All Windows Server and Center Server access will need an Active Directory account with sufficient permissions. Access to the storage array, storage switches, network switches and firewall will all require use of accounts that are managed on those devices.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

The following DoS policies establish the requirements for restricting access to information to those with a legitimate need to know/access:

- 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

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The system maintains a log of system use and events. Back-up information is stored at an appropriately secured location in accordance with 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 back-ups are additionally maintained on a hard drive and retained at the primary site in Sterling, VA and the back-up site in McLean, VA.

(d) Explain the privacy training provided to authorized users of the system.

DS/CTO in coordination with DS/DSS/TIA/OSAC will identify key personnel associated with its contractor (CVP and MetroStar Systems) 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 are both responsible for system and security administration of OSAC servers. DS/SI/CS also has a Departmental Security Awareness program in place. In addition, all employees must pass the annual Cybersecurity Awareness course.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

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 OSAC Executive Office as well as OSAC RISC analysts will be required to use two-factor authentication in order to login to the website and, therefore, to access PII contained within the system.

(f) How were the security measures above influenced by the type of information collected?

As outlined in 5(a), Driver's License and Passport numbers are retained for only 24 hours in the system. This allows for better control of the information and ensures that the data is not retained indefinitely.

9. Data Access

(a) Who has access to data in the system?

Access to the system requires a password and is based on a "need to know" and user roles. 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.

(b) How is access to data in the system determined?

Please refer to 9(a).

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Please refer to 9(a).

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

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 or PKI token, and a "need-to-know." DS employees, contractors, and OSAC members must follow the system rules of behavior established by the DoS.