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: April 8, 2011

(b) Name of system: Security Management System enterprise

(c) System acronym: SMSe

(d) IT Asset Baseline (ITAB) number: 886

(e) System description (Briefly describe scope, purpose, and major functions):

SMSe provides near real time monitoring, control and reporting capabilities of persons who enter post facilities overseas. SMSe generates records of the person's system generated card number, door ID, and the date/time. The system provides a real time display at the Marine Security Guard (MSG) post of access control activity and indicates whether access was granted or denied based on user access rights to enhance security of the post facility. SMSe is the global integration of security systems and devices to provide both local and remote monitoring and control capabilities, centralized archiving and dissemination of data to dispersed user groups.

The platform used to integrate the various security systems is a Boeing product called Visual Security Operations Console (VSOC) which uses 3D modeling of each facility to provide improved situational awareness for security and maintenance staff. VSOC also includes a database that contains the integrated reporting from the various security systems such as access control and alarm systems.

Responsibility for monitoring security events is divided between the Washington based Diplomatic Security Command Center (DSCC) staff and regionally based MSGs. MSG staff are responsible for monitoring security events at their home post as well as other designated regional posts that do not have an MSG guard force.

(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): N/A

(h) Date of previous PIA (if applicable): 17 April 2009

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?

Several elements of personally identifiable information (PII) are collected from authorized persons requiring regular access to the facility, such as employees, facility staff and family members. These persons are required to provide PII for use in conjunction with a magnetic swipe card. The elements of PII collected consist of:

- Last name, first name and middle initial;
- Title (Mr,Mrs,Ms,Dr);
- Family designation (Sr/Jr);
- Work area within the mission;
- A PIN number selected by the user; and
- A digital image of themselves.

The SMSe system integrates information from discreet security systems. One of these systems provides access control. Authorized persons requiring regular access to the facility, such as employees and family members are required to provide PII for use in conjunction with a magnetic swipe card. This allows identity confirmation whenever the card (and PIN where required) is used to access a door in the facility controlled by a card reader and keypad that forms part of the access control system. The SMSe system also creates a new record each time a user attempts to access a door controlled by the access control system. The system can be programmed to allow entry by card swipe only or by a combination of card swipe and PIN entry for each door. The scope of the record produced ranges from the username, door accessed and date/time on the access control system, to a more complete record on the Visual Security Operations Console (VSOC) platform that also includes the user's image.

It should be noted that visitors' PII taken for admittance to the facility is not used to produce individual access control cards. Instead, generic visitor cards are produced and the visitors' PII is recorded external to the SMSe system.

b. How is the information collected?

An applicant's information is obtained directly from the individual who is also prompted to enter a PIN number which is attached to his or her record. The PIN number does not appear on the screen when entered. A digital camera attached to the badging station equipment is used to enter the image of the applicant into the access control system where the image is associated with a system generated badge number which is encoded onto the magnetic stripe of an access control card. This card can either be an existing Department of State domestic access control card or can be generated at post. For post generated cards the card color also indentifies the status (cleared or uncleared) of the card holder.

Access control records are stored by both the Access Control System as well as the Visual Security Operations Console (VSOC) database. Access control records are maintained

both centrally in Washington, DC and at each site, while the main integrated VSOC database is located only in Washington, DC.

The level of sensitivity of the unclassified information accessed, processed, stored, and transmitted on SMSe is sensitive but unclassified (SBU). SMSe processes privacy data as defined by the Privacy Act of 1974.

c. Why is the information collected and maintained?

The information collected and maintained is the minimum required to provide identity confirmation for access control to U.S. overseas missions and facilities.

Access control records are combined with data from other security systems in the Visual Security Operations Console (VSOC) database. The collection of this information is deemed necessary to facilitate improved maintenance of security systems and to enhance the security of the facilities.

d. How will the information be checked for accuracy?

The regional security officer (RSO) at each post is responsible for verifying and approving forms submitted by all employees, family members, and locally engaged staff (LES). This coupled with the user entering their own PIN helps to authenticate any records generated by the system that contain PII. In the case of locally generated cards, the user image is also attached to the card. Specific methodologies for verification employed by the Bureau of Diplomatic Security (DS) include maintaining the system as a live feed, allowing the information to be updated/edited at any time.

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

The legal authority for the collection of information as documented in Public Notice 6039 State-36, Security Records, specific to SMSe, 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 PII collected is considered minimal considering the extent of the PII collected amounts to the name and image of each person. There is no aggregation of additional information which would provide sufficient information for any form of identity theft. The SMSe system has several mitigating factors protecting this information. The system is a closed system that cannot be accessed via the internet. Access to the system is controlled and only granted to cleared Department employees with an operational need and who possess a minimum SECRET clearance. Physical access to the SMSe hardware is also limited.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National

Institute of Standards and Technology (NIST). These controls include regular security assessments, physical protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, information integrity protection (e.g., antivirus software, and audit reports).

The nature of the PII collected and maintained resulted in a security categorization of "moderate" for the system with 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.

When a user attempts to access an overseas mission using their post generated swipe card (and PIN number where required) a record is created in SMSe that consists of the system generated card number, door ID, and the date/time. The system provides a real time display at the MSG guardpost of access control activity and indicates whether access was granted or denied based on user access rights. In this way, the security of the facility is enhanced.

Each access control event is included as part of the Visual Security Operations Console (VSOC) database that also includes alarm system status. The system allows reports to be generated to assist maintenance and security staff to confirm security equipment operation and to assist with analysis of unexplained security events.

b. What types of methods are used to analyze the data? What new information may be produced?

Details of successful as well as unauthorized access attempts are recorded for real time display for security staff, such as the DSCC staff in Washington, DC and by regional Marine Security Guards (MSGs) who monitor facility security. Historical records are also generated for later analysis should an unexplained security event require investigation. The system allows standardized as well as user defined reports from the Visual Security Operations Console (VSOC) database that can be subject based – for example the time and dates when a particular person accessed a door. The report(s) generated are, therefore, a subset of the information held on the VSOC database.

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

The system does not use any commercial information, publicly available information, or information from other Federal agency databases.

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

SMSe is a U.S. Government-owned system that is maintained and supported by U.S. Government employees and contract employees.

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.

The only privacy impact concern would be the association of system generated reports with an ongoing security or criminal investigation. The relevant authorities specified in STATE-36 that would produce or have access to such reports have well established systems in place to limit distribution and protect data used in ongoing investigations.

SMSe is a U.S. Government-owned system. It is supported by contract employees, who support U.S. Government employees in their maintenance of the system.

Contractors who support SMSe are subjected to a background investigation by the U.S. Government for pertinent facts bearing on the loyalty and trustworthiness of the individual. In addition, access to the system is controlled and is only granted to cleared Department employees with an operational need who possess a minimum SECRET level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

5. Retention

a. How long is information retained?

The retention period of three years for data is consistent with established Department of State policies and guidelines for Countermeasures and Counterintelligence Central Monitoring Systems as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

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

The limited depth of PII (name and image) in the badging data as well as that in the access records means there is little risk to an individual. The main risk from long term storage of any PII would be the unintentional disclosure of information at the time of disposal of redundant equipment. SMSe follows the procedures established by the Department for the secure disposal of redundant equipment which mitigates this risk.

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?

The historic integrated Visual Security Operations Console (VSOC) database records (which include access control records) are made available to areas of the Bureau of Diplomatic Security (DS) responsible for analysis of unexplained security events at overseas missions.

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

The internal organization mentioned in 6(a) above has direct access to the SMSe system. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening.

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

The main perceived privacy threat would be the unintentional release of system records associated with an ongoing investigation that could cause embarrassment to a user. This risk is mitigated by the well established procedures and classifications used when dealing with ongoing investigations and approved disposal methods once the investigation is complete.

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?

Other agencies do not have direct access to the data, but the data may be shared with an agency upon request provided that the agency requesting the data is listed as a routine user in STATE-36. The use of the data by the other agency will be restricted to the same purpose for which the data was originally collected.

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

This information could be shared in either hard or soft copy. Any reporting derived from SMSe data would be classified at a minimum at the *Sensitive but Unclassified (SBU)* level. This is a sensitivity marker for material that warrants/requires administrative control and protection from public or other unauthorized disclosure for reasons other than national security. The PII held in SMSe falls within the definition of SBU. There are currently various equivalent designations to SBU used throughout the Federal Government. Safeguards in place for the sharing arrangements are through statute and regulation, as well as through Department and agency policy stating that each agency is obliged to follow to provide appropriate safeguarding of SBU material to prevent unauthorized or unintended disclosure.

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

The privacy risk associated with external sharing and disclosure would be from the unintentional release of the records associated with a possible security or criminal investigation. Any external agency granted access to the data for this purpose already has well established limited distribution procedures in place to protect data used in ongoing investigations and for storage and disposal of the records once the investigation is complete.

8. Notice

The system:

☒ contains information covered by the Privacy Act, detailed in *State-36, Security Records*.

☐ does NOT contain information covered by the Privacy Act.

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

Notice of the purpose, use, and authority for collection of information submitted are described in the System of Records Notice titled STATE-36, Security Records. Additionally, the individual is present at the time the swipe card is created and their personal data is recorded in the system.

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

An individual may decline to provide the limited privacy information required for the issuance of an ID card. Without the required information, the Department of State will be unable to issue the employee or family member his or her access card.

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 stated in the Department of State's Disposition of 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.

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.

The notice offered is reasonable and adequate in relation to the system's disclosed purposes and uses.

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?

SMSe contains Privacy Act covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above and in rules published at 22 CFR 171.31. The procedures fully inform individuals on how to inquire about the existence of records, how to request access to records, and how to request an amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a record on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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 information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A user is granted access to the system by requesting access from the SMSe website. The user completes a new user application which is forwarded to SMSe Management for approval. The SMSe information system security officer (ISSO) or designate, approves or disapproves access to the SMSe system based upon security clearance, the DS employee and his or her need to access the system. If the ISSO cannot determine these factors, the regional security officer (RSO) at post is asked to verify the demonstrated need for access. A system use notification ("warning banner") is displayed before log-on is permitted, stating the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

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

Prior to receiving system access, all users of SMSe must complete the SMSe System Access Request form where they acknowledge that they have read and understood the SMSe rules and regulations included as part of the Access Request form.

In addition, all users are required to undergo computer security and privacy awareness training prior to accessing the Department of State OpenNet system, and must complete refresher training yearly in order to retain access.

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.

Several steps are taken to reduce residual risk related to system and information access. Access control lists defining who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system's audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

11. Technologies

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

Identity management system technology is used in the form of the badging station and associated equipment used to encode the system generated user ID number on the access control card magnetic strip which enables the identity of the user to be confirmed when the individual attempts to enter an area controlled by card reader technology.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the 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); and following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the 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?

SMSe was granted Full Accreditation at the Sensitive But Unclassified (SBU) level for a period of 36 months in February 2008. Reauthorization of SMSe is currently pending and is expected by April of 2011 for an additional 36 months.