Security Management Systems enterprise (SMSe)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 03/2022
(b) Name of system: Security Management Systems enterprise
(c) System acronym: SMSe
(d) Bureau: Diplomatic Security (DS)
(e) iMatrix Asset ID Number: 886
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The mission of the Security Management System enterprise (SMSe) is to protect people, information, facilities, and operations. SMSe supports physical access to post and its facilities by providing badges to all government employees, government contractors, and visitors.

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

SMSe collects PII from government employees/government contractors, SMSe users, and visitors to facilitate mission needs. SMSe users have access to both the post (through the badge) and the SMSe system, whereas the Government employee/contractor badge holder only has access to physical post. Each Regional Security Officer (RSO) has the discretion to determine additional information types to be collected at their respective post based on the security needs of each location.

Government employee/contractor badge holders: PII is collected to provide an SMSe badge. SMSe government employees/contractors are cleared U.S. citizens.

- Name
- Picture
- Iris scan

SMSe users: Those government employees and government contractors who also require SMSe access (SMSe users) will receive additional privileges to the SMSe system. SMSe users are cleared U.S. citizens.

- Name
- Picture
- Iris scan

Visitors: Visitors are locally employed staff and family members who may be U.S. Citizens or Non-U.S. Citizens. SMSe collects PII to provide an SMSe badge which is required of all visitors at post:

- Name
- Picture

Short-term and/or one-time visitors are not badged by SMSe. Rather, they are escorted by authorized personnel.

The remainder of the PIA will focus on the PII of U.S. citizens.

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

5 U.S.C. 301; Departmental Regulations

Executive Order 10450 – Security Requirements for Government Employees:

Executive Order 10865 – Safeguarding Classified Information Within Industry

Executive Order 12958 – Classified National Security Information

Executive Order 12968 – Access to Classified Information

Executive Order 12829 – National Industrial Security Program

Homeland Security Presidential Directive 12 – Personnel Identification Verification

22 U.S.C. § 4802, Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended

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

☒Yes, provide:

- SORN Name and Number:
  Security Records, STATE-36

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  June 15, 2018

☐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

If yes, please notify the Privacy Office 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 (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  See below.

- Disposition Authority Number:
  See below

- Length of time the information is retained in the system:
  See below.

- Type of information retained in the system:
  See below.

DoS Records Schedule/Disposition Authority Number	Disposition	Description
Security Projects and Special Programs, (View Details**)** **Disposition Authority Number:** DAA-0059-2018-0003-0007 **Applies To:** DS/C DS/DO DS/HTP DS/IP DS/TIA	Temporary. Cut-off at end of calendar year of final action. Destroy/delete 5 years after cut-off but no later than 30 years if required for business use.	Records documenting technical and physical security upgrades/improvements of embassy, consulate, and U.S. occupied buildings, communications equipment, computers, defensive equipment, armored vehicles, and security countermeasures. This schedule also covers records of special programs, operations, and events relating to security threats, incidents, or actions taken against individuals or property. Records include, but are not limited to, specifications for the test and evaluation of vendor products, design drawings, floor plans, inspections, standards, certification/non-certification letter, tracking and control information on equipment, including make, model, serial number, maintenance, distribution, and shipping, historical documentation of purchase, requisition, inventory, planning, research, funding, testing, training, storage, and destruction, status reports, technical reports, statistical data, engineering, installations, penetration, security technology, surveillance, surveys, technical services, visits, assessments, evaluations, threat lists, intelligence summaries, trends overseas, and other related subjects.
Personal Identification Credentials and Cards, (View Details) **Disposition Authority Number** DAA-0059-2018-0003-0007 **Applies To:** DS/C DS/DO DS/HTP DS/IP DS/TIA	Temporary. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.	Records about credential badges (such as smart cards) that are (1) based on the HSPD12 standards for identification cards issued to Federal employees, contractors, and affiliates, and (2) used to verify the identity of individuals seeking physical access to Federally controlled Government facilities, and logical access to Government information systems. Also referred to as Common Access Cards (CAC) cards, Personal Identity Verification (PIV) cards, and Homeland Security Presidential Directive 12 (HSPD-12) credentials. Exclusion: Records of certain classes of Government employee identification cards, such as those covered under special-risk security provisions or 44 U.S.C. Section 3542, are covered by agency-specific schedules.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐ No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

Government employee/contractor badge holders: The record subject's name is verified and collected from the two forms of government identification provided to the badge issuer. The picture of the record subject is taken by a camera and a badge issuer uploads it into SMSe. Then the badge issuer prints the badge from a printer that is connected to their workstation. Iris scans are obtained via the iris scanner device after badges are issued. The iris scans are stored within SMSe.

SMSe Users: In addition to the badge requirements above, SMSe users complete the DS-7804 form "SMSe User Account Request." Once management approval is received, the information from the user account request is manually entered into system by an SMSe staffer.

Visitors: The visitor must provide proof of identification by providing two forms of government identification and have their picture taken by the badge issuer. The badge issuer uploads the visitor's picture into SMSe. The badge issuer also enters the information from the documentation into SMSe.

(e) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

(f) What process is used to determine if the PII is accurate?

SMSe government employee/contractor badge holders: The badge issuer verifies the information collected from the subject against the two forms of government identification provided. The subject's government clearance is also verified for accuracy and to ensure proper access is granted.

SMSe users: The badge issuer verifies the information collected from the subject against the two forms of government identification provided, and government employees/government contractors complete the DS-7804 form to establish their user account.

Visitors: The badge issuer verifies information collected by SMSe at the time the visitor applies to establish their building access. The visitor must provide proof of identification by providing two forms of government identification.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

SMSe government employees/contractors badge holders and SMSe Users: The information is deemed current at the time it is collected. It is the responsibility of the SMSe government employee/contractor or user to inform the RSO of any information changes.

Visitors: It is the responsibility of the visitor to inform the RSO or designated representative of any information changes.

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

No, SMSe does not use information from commercial sources. The information contained in SMSe is not publicly available.

(i) How was the minimization of PII in the system considered?

SMSe only requests the minimum required PII to regulate and track physical access to post and its facilities. Default information for the system is the name and photo of the individual who will be issued the ID badge and/or provided access to the SMSe system (SMSe users).

Each RSO has the discretion to determine, and will control, any additional information types collected at their respective post based on the security needs of each location

5. Use of information

(a) What is/are the intended use(s) for the PII?

The intended use of the PII in the SMSe system is to manage physical access to post and its facilities by providing badges.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the use of the PII is relevant to the design of SMSe. The system leverages the PII and helps the RSOs determine if the individual in question should be granted physical facility access and/or an SMSe user account.

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

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(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

(d) If the system will use test data, will it include real PII?
☐Yes ☐ No ☒ N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:
There is no internal sharing of PII.

External:
There is no external sharing of PII.

(b) What information will be shared?

Internal:
There is no internal sharing of PII.

External:
There is no external sharing of PII.

(c) What is the purpose for sharing the information?

Internal:
There is no internal sharing of PII.

External:
There is no external sharing of PII.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
There is no internal sharing of PII.

External:
There is no external sharing of PII.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
There is no internal sharing of PII.

External:
There is no external sharing of PII.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

SMSe government employee/contractor badge holders: There is presently no notice provided to record subjects. However, DS is currently working to update procedures, to include a Privacy Act statement shared at the time of collection of PII, via broadcast message that will provide notice to badge holders at all posts.

SMSe users: Notice is provided via the SMSe User Account Request form DS-7804.

For visitors: There is presently no notice provided to record subjects. However, DS is currently working to update procedures, to include a Privacy Act statement at the time of collection of PII.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII? ☐Yes ☒No

If yes, how do record subjects grant consent?
Click or tap here to enter text.
If no, why are record subjects not allowed to provide consent?

For SMSe government employees/contractors badge holders: May decline to provide the PII but doing so will result in them not receiving a badge and/or physical access to post.

For SMSe users: Users may decline to provide the PII but doing so will result in them not receiving an account.

For visitors: Visitors who decline to provide the PII will not gain physical access to the post.

(c) What procedures allow record subjects to gain access to their information?

Records subjects may follow the procedures for access to their information as outlined in the system of records State-36, Security Records.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

If records subjects need to correct inaccurate or erroneous information, they must notify the RSO to facilitate update of their information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

For SMSe government employees/contractors badge holders, SMSe users, and visitors: The badge issuer verifies that the information is correct and informs the badge holder that they should notify the RSO, or their designee, of any information that needs to be corrected.

8. Security Controls

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

SMSe is a closed network, accessible only via SMSe connected workstations and servers. Access control lists limit the accessibility of SMSe to only authorized personnel. The workstations and servers are protected at the Sensitive But Unclassified (SBU) level in accordance with National Institute of Standards and Technology (NIST) requirements. All SMSe Data-at-rest and data-in-transit are encrypted.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

The "SMSe User Accounts Guide Version 3.3, February 2020" details procedures on configuring SMSe user accounts based on the role the system user fulfills and is strictly limited to role-based access. The following table per the SMSe guide depicts the SMSe user roles and their respective PII data access:

SMSe Role	General User Category	PII Data Access
Engineering Service Center (ESC)	End User	• Name • Picture
Regional Engineering Service Center (RESC) staff	End User	• Name • Picture
Regional Security Officers (RSO): 3 Types • Engineering Security Officer (ESO) • Regional Security Officer (RSO) • Technical Security Officer (TSO)	End User	• Name • Picture • Iris scans
Security Engineering Officers (SEO)	End User	• Name • Picture
SMSe Network Operations Center (NOC) located at SA-24	System Administrators	• Name • Picture
Washington-Metro area DS Command Center (DSCC)	End User	• Name • Picture

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

SMSe is a standalone network with no connections to other networks. SMSe users are placed in appropriate AD user groups based on region and post; therefore, access to SMSe is also limited based on the region and post in which they are assigned.

(d) How is access to data in the system determined for each role identified above?

The following roles must meet the following criteria in order to access the data in the system: Have an OpenNet account in good standing, a minimum of a secret security clearance, a completed SMSe user request form, and SMSe ISSO approval.

- Regional Security Officers (RSO)
- Security Engineering Officers (SEO)
- SMSe Network Operations Center (NOC) staff located at SA-24
- Washington-metro area DS Command Center (DSCC)

The SMSe User Accounts Guide details procedures on configuring SMSe user accounts based on the role the system user fulfills and is strictly limited to role-based access.

New users must complete the online SMSe User Account Request form located on the links section of the SMSe Field Site on OpenNet. The request is routed for approval to the requestor's supervisor. Upon approval, the request is automatically sent to the Security Technology Operations Center (STOC). A new work order (WO) is generated and the information in the WO is used to create the new SMSiDOM (the network domain name for SMSe) account in Active Directory (AD). If any of the information appears incorrect, the STOC will contact the Senior Watch Officer (SWO) or NOC Manager before proceeding.

The process for authorizing and controlling user access to the system is based on need to know, job requirements, and limiting of user access to one of least privilege on data files. Apart from some central admin groups, some permissions are post-specific. For example, a user with Regional Security Officer (RSO) permissions for Frankfurt does not have RSO permissions for Tokyo.

Only authorized, cleared direct-hire and contractor employees having a need-to-know are granted an SMSe user account. Users of the SMSe application fall into two general categories: End Users and System Administrators.

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

NIST security controls help ensure the information contained in SMSe is protected, secured, and the likelihood of misuse is reduced. SMSe data-at-rest and data-in-transit

are protected via encryption and user role-based access controls including the concept of "least privilege".

Splunk log management software facilitates monitoring system events, overall status, and provides auditable information for detecting and reposting any irregularities and potentially malicious activities. Additionally, SMSe maintains audit logs of badge administration activity.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All SMSe users are required to complete the PS800: Cybersecurity Awareness training for OpenNet. In addition, SMSe users who are Department employees and contractors must take the Department's on-line privacy course, PA318: Protecting Personally Identifiable Information.