

SMSe PIA

1. Contact Information

A/GIS/IPS Director

Bureau of Administration

Global Information Services

Office of Information Programs and Services

2. System Information

(a) Name of system: Security Management System enterprise

(b) Bureau: DS/C/ST

(c) System acronym: SMSe

(d) iMatrix Asset ID Number: 886

(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): [Click here to enter text.](#)

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?
Currently authorized and in the process of reauthorization.

(c) Describe the purpose of the system:

The Mission of the Security Management System enterprise (SMSe) is the worldwide integration of selected technical security systems, with data availability to DS staff at post and to remote DS monitoring centers, for the purpose of better protecting people, information, facilities, and operations.

SMSe provides real-time and historic data by integrating technical security sub-systems at Foreign Service posts, then networking those posts via the SMSe Network (SMSeNet), a private, encrypted VPN through OpenNet or the Internet. This data is available to Regional Security Officers, Security Engineering Officers (SEOs) and Marine Security

Guards (MSG) at post, to regional Engineering Service Center staff, and to the Washington-metro area DS Command Center (DSCC) and the SMSe Network Operations Center (NOC) located at SA 24.

- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
Names and pictures of users for badging and system event purposes.
- (e) What are the specific legal authorities and/or agreements that allow the information to be collected?
1. 5 USC 301; Federal Information
 2. Executive Order 10450 – Security Requirements for Government Employees:
 3. Executive Order 10865 – Safeguarding Classified Information Within Industry
 4. Executive Order 12958 – Classified National Security Information
 5. Executive Order 12968 – Access to Classified Information
 6. Executive Order 12829 – National Industrial Security Program
 7. Homeland Security Presidential Directive 12 – Personnel Identification Verification
- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
- Yes, provide:
- SORN Name and Number: STATE-36, SECURITY RECORDS
 - SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): May 9, 2013
- 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 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.) DS/C/ST will be submitting a records retention schedule to NARA through the DS Records Management Office. The disposition will replicate the scheduled followed for AlarmNet which is as follows:

[A-11-014-15a](#) **AlarmNet General Support System (GSS)**

Description: Master File:

An electronic tracking system that utilizes information collected by the Bureau's Identity Management System (IDMS) to build access profiles and give individuals access to facilities within the Department of State nationwide. The information is required to grant access clearances, and to provide the Department's Diplomatic Security Uniformed Protective Officers (UPO) the information necessary to protect Department assets. AlarmNet supports the Bureau of Diplomatic Security (DS/FSE/DME) mission requirements for providing physical intrusion detection, access control security, and monitoring from central locations, for all domestic Department facilities nationwide on a 24x7 basis. AlarmNet provides the connectivity for the Department's Domestic Access Control and Intrusion Detection System.

Disposition: Temporary. For maximum security facilities, records of access are destroyed when 5 years old unless retained for specific ongoing security investigation.

DispAuthNo: GRS 18, item 17a

[A-11-014-15a\(1\)](#) **AlarmNet General Support System (GSS)**

Description: Master File:

An electronic tracking system that utilizes information collected by the Bureau's Identity Management System (IDMS) to build access profiles and give individuals access to facilities within the Department of State nationwide. The information is required to grant access clearances, and to provide the Department's Diplomatic Security Uniformed Protective Officers (UPO) the information necessary to protect Department assets. AlarmNet supports the Bureau of Diplomatic Security (DS/FSE/DME) mission requirements for providing physical intrusion detection, access control security, and monitoring from central locations, for all domestic Department facilities nationwide on a 24x7 basis. AlarmNet provides the

connectivity for the Department's Domestic Access Control and Intrusion Detection System.

Disposition: Temporary. Destroy Personal Identity Verification cards within 30 days after death, separation, or transfer of employee. Destroy all other records upon notification of death or no later than five years after separation or transfer of employee, whichever is applicable.

DispAuthNo: DAA-0059-2012-0001-0001

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): [Click here to enter text.](#)
- Length of time the information is retained in the system: [Click here to enter text.](#)
- Type of information retained in the system:
[Click here to enter text.](#)

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? N/A – system does not collect SSNs.

(c) How is the information collected?

An employer or sponsor enters information into an online infopath form used by this application only, requesting USG facility access for new employees, expanded physical access for existing employees, or an ID badge for an eligible family member. Once the RSO makes a decision on the level of access permitted, a picture ID badge is made through the GLID system. The name and picture from the badge is then stored in the C CURE database. Office of Security Technology staff are working with A Bureau Directives Management to create a DS 1838 version for overseas, which will supersede this form.

(d) 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.

[Click here to enter text.](#)

- (e) What process is used to determine if the information is accurate?
Information that is collected is verified with the user prior to being entered into the system.
- (f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Information obtained is static (Picture and name of badge holder) and is, therefore, current.
- (g) Does the system use information from commercial sources? Is the information publicly available?
No
- (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?

[Click here to enter text.](#)

- If no, why are individuals not allowed to provide consent?

The SMSe workstation is the basis for the overseas post identification - Global Identification (GLID) badge system. To gain access to Department of State facilities at any given post, an individual is given an ID badge made with the GLID system. All information requested is necessary to grant the ID badges.

- (j) How did privacy concerns influence the determination of what information would be collected by the system?
Each Regional Security Officer (The special agent assigned to secure the Department facility overseas – RSO) determines the information to be collected at post. Default is the name and photo of the individual who will be issued the ID badge. SMSe only collects the bare minimum of required data so that it known who is accessing which area and where.

5. Use of information

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

The purpose of the SMSe system is to tie physical access through monitored compound access control locations to a monitoring station at either the Marine security Guard position at post, and also the network operations center at SA 24. When the badge holder swipes their badge to gain physical access to the facility, their photo and name is briefly displayed against the monitor. This feature allows MSGs to visually match the person they see entering the facility to the photographic image of the individual recorded in the C Cure database and authorized access to the facility.

- (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

- (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?

[Click here to enter text.](#)

- (2) Does the analysis result in new information?

[Click here to enter text.](#)

- (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.

SMSe is provided to the user population who require access and is not shared with external entities.

- (b) What information will be shared?

Name of individual badge holder and the individual's photographic image.

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

To identify who is accessing which area of the Department of State Facility overseas.

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

Information is displayed on the SMSe console which is monitored by the Marine Security Guard at the individual post, available to RSO staff members and on an as needed basis, to the network operations center in SA 24.

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

SMSe staff are instructed to handle the information as sensitive but unclassified.

- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The console is provided and restricted to cleared American security personnel at post who use it to monitor individuals that access government facilities. The information displayed is name and photo, for immediate verification by the individual monitoring facility access. This limitation of the scope of the PII used in SMSe ensures that only those with a need-to-know are able to view the information contained within SMSe.

7. Redress and Notification

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

Individual users at post will not typically have access to SMSe records. The information collected and available for display is limited to picture and name.

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

Yes No

If yes, explain the procedures.

User notifies his or her superior and it is then corrected by SMSe staff.

If no, explain why not.

[Click here to enter text.](#)

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

They are instructed to verify their information and notify their superiors for any incorrect information.

8. Security Controls

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

SMSe is a closed network, accessible only via SMSe connected workstations and servers. The aforementioned workstations and servers are protected at the SBU level.

(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.

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. Below is an excerpt from said guide showing which users should be given access to which data/applications:

	SMSe Support (Personal)	SEO/STS (Personal)	RSO/ARSO/OMS (Personal)	TOG (Personal)	ESC/ESO (Generic)	MSG (Generic)	RSO (Generic)	LGF (Generi
SMSIDOM	X	X	X	X	X	X	X	X
Local Badge CCure Server		X	X					
Local Velocity		X	X					
Local Windows (non-domain badging machines)		X	X					
VSOC	X			X	X	X	X	X

Regional CCure server	X	X						
Solarwinds	X				X			
CCure Central	X							

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

SMSe is a closed network and only accessible via SMSe connected workstations and servers. The aforementioned workstations and servers are protected at the SBU level. Data sent over SMSe is encrypted on both sides. SMSe uses an application called Splunk log management software to monitor.

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

All SMSe users are required to complete the PS800: Cybersecurity Awareness training for OpenNet Plus.

(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.

SMSe is a closed network and only accessible via SMSe connected workstations and servers. SMSe is also encrypted on both ends. Users are required to meet password complexity standards as well as password age requirements.

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

SMSe security measures were implemented to secure all SMSe data and not just the information collected and stored on individuals with access to the network.

9. Data Access

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

SMSe Watchstander staff, SMSe management personnel, and SMSe system administrators.

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

Access to SMSe data is determined by SMSe management staff. User access is also determined by least privilege.

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

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

From the SMSe SSP: The SMSe User Guide outlines the process for authorizing user access to the system based on need to know or job requirements, and the limiting of user

access to one of least privilege on data files. The guide outlines the permissions for both Windows and the other permissions-based applications that reside on the network.

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

SMSe is governed by the National Institute of Standards and Technology which identifies controls to ensure information in government systems is protected and secured. Among those controls are controls governing who has access to the information within the system, specifically:

AC-6: This control requires that the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-6(1): This control requires that the organization explicitly authorizes access to [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information].

AC-6(2): This control requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.