DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Security Management System-enterprise (SMSe)

Conducted by:
Bureau of Administration
Information sharing and Services
Office of Information Programs and Service
Privacy Office
Email: pia@state.gov

The Department of the State
FY 2008 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

Department of State
FY 2008 Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:

- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/ISS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also please complete the certification page at the end of this document. Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION:

1) Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public?**

YES _X_ NO___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to the following e-mail address: pia@state.gov .

2) Does a Privacy Act system of records already exist?

YES __X_ NO ___

If yes, please provide the following:
System Name _____ Number ___36____

If no, a Privacy system of records description will need to be created for this data.

3) What is the purpose of the system/application?

The Security Management System enterprise (SMSe) is a program of the Office of Security Technology, Bureau of Diplomatic Security (DS/C/ST). SMSe is the world wide 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. The goal of SMSe is to improve security for all posts, and especially to better protect national information at Classified Lock & Leave posts. The Global Identification (GLID) Program (*Blue DOS ID Badge) was responsible for deploying ID badges to all US Posts abroad. The GLID badging workstation has since been integrated into the SMSe network (SMSeNet).

4) What legal authority authorizes the purchase or development of this system/application?

- Government Information Security Reform Act of 1999
- OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," updated in 1996.
- Department of State's Automated Information Systems Security Policy Requirements (12 FAM 600)
- The Omnibus Diplomatic Security and Antiterrorism Action of 1986

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

The categories maintained in the system include: first name, last name, photo and account privileges (and associated access control PIN codes, if issued) of embassy USG/PSC or contractor employees, their family members (*who require access to the Mission), and Foreign Service Nationals. This data is used to produce Department of State Identification (ID) badges for identification and access control purposes. If a mission/post has an Automated Access Control System (AACS) then the person's ID badge is encoded with the appropriate access control privilege based upon their job function and access requirements.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

The information was directly obtained from the individual and the individual is required to select and enter a PIN into CCURE. This PIN is hashed and therefore cannot be seen when entered.

b. What type of information is collected from the source of the information?

The categories maintained in the system include: first name, last name, the person's photo, whether the person has a CCURE user account, and their access control PIN (if applicable).

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The regional security officer (RSO) at post verifies and approves the forms submitted by all employees, family members, and locally engaged staff (LES).

b. How will data be checked for completeness?

The RSO is responsible for verifying the completeness of these records before issuing ID badges.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The first and last name information categories collected will not change. If a person's appearance alters and they can no longer be recognized by the picture on their ID badge, it is the responsibility of the RSO to ensure an updated photo is taken and a new ID badge is produced. The old ID badge would be properly destroyed and disposed IAW the policies stated in the FAM/FAH.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Yes. The use of the data collected is relevant and necessary to ensure the security of post. The data collected directly corresponds to the data that is presented on an individual's ID badge, when it is produced. ID badges are used to verify a person's identify before they are granted access to a facility.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

No. No new data will be collected for existing personnel. Only the information categories mentioned above are collected and maintained.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

No. The system does not make such determinations.

4) Will the new data be placed in the individual's record?

No. New data will not be collected for existing personnel. Only the info categories mentioned above will be collected and maintained for existing personnel (USG, PSC, contractors, or LES), new post personnel (USG, PSC, contractors, or LES) or family members that require access to post.

5) How will the new data be verified for relevance and accuracy?

The regional security officer (RSO) at post verifies and approves the data submitted by all employees, family members, and locally engaged staff (LES).

6) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

The data is maintained in a database on SMSeNet. First and last name identifiers can be used to retrieve the data. Access to the SMSeNet is controlled and is only granted to cleared-Americans with an operational need that possess a minimum Secret clearance. Access to the CCURE application is also controlled, through user authentication. Each user is given a specific level of privileges based upon their job function.

7) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Facility access records can be extracted for users at sites by security managers (RSOs) using the access control system. This data may be used by the RSO to investigate alarm or access anomalies.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data are maintained in all sites?

This data is maintained locally at each post with a badging capability and is automatically replicated to a central site.

2) What are the retention periods of data in this system?

The personnel data is retained indefinitely, or until manually purged by a posts badging operator or RSO.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Personnel reports are destroyed after use or in accordance with local RSO or post policy.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No. This is simply an evolution of existing access control and badging / identification technologies.

5) How does the use of this technology affect public/employee privacy and does it restrict access to the system?

Access to SMSeNet and the databases is restricted to security and technical support personnel who are SECRET cleared U.S. citizens.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

The types of information that are collected about post personnel or family members are the location of where they were granted/denied access and the date and time of where this access occurred. The CCURE application requires user authentication and only specific individuals are given monitoring privileges.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No. Any system modifications would strictly be procedural, hardware, or software based and would not add to the current information types that are maintained about post personnel and their family members.

8) **Are there forms associated with the system? YES _X_ NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (e.g., contractors, users, managers, system administrators, developers, other)

All SMSe program personnel (Ops Support Staff, Integrators, System Administrators, Management and ISSO, including FS, GS, PSC and contractors) have access to this data. Selected FS users overseas also have access to maintain and support the systems.

2) **What are the criteria for gaining access to the system?** Are criteria, procedures, controls, and responsibilities regarding access documented?

All cleared-American individuals who have an operational need for access to SMSeNet are required to complete the SMSeNet System Access Request form found on the SMSe Intranet Website. This form requires that the person submitting the request review and acknowledge the Rules & Regulations of the network. Once the request is submitted, SMSe Ops Support personnel confirm that the request is legitimate before the account is created. The ISSO is 'cc' on each SMSeNet System Access Request form submission and these requests are archived.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access to SMSeNet and the CCURE application is restricted through user authentication and uniquely assigned permissions for both domain and application user accounts.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access?** (Please list processes and training materials)

Only those individuals who have an operational need to access this data are given this privilege. Typically users are only able to access their local records. Technical support personnel are able to access the global database. Unauthorized access to this data is prevented through physical controls (workstations are installed in LAA or CAA spaces and alarmed) and software controls via the use of user authentication and user account privileges within the CCURE application.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Yes. The majority of Washington based SMSe support personnel are contractors, of whom play a key role in the design and development of the system, as well as the maintenance. Support staff overseas are Foreign Service personnel.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

No. SMSeNet is an encrypted VPN that does not have connectivity with other systems.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

No.

8) **Who is responsible for assuring proper use of the SHARED data?**The SMSe ISSO is responsible for assuring the confidentiality, integrity and availability of the data; however this data is not shared.

ADDITIONAL COMMENTS: *(optional)*