Privacy Impact Assessment
for the

DHS S&T Staff Management System

February 2, 2006

Contact Point
Jackie Bowman
Human Capital
Science and Technology
202-254-5614

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

The Department of Homeland Security, Science & Technology (S&T) Staff Management System (SMS) is a web based Intranet application that maintains information regarding S&T personnel and contractors.

Introduction

The purpose of S&T Staff Management System is to, maintain information regarding DHS S&T staffing positions, the details regarding DHS S&T Staff (as defined below in section 1.2), and resources used by S&T Staff such as offices and government issued equipment. The system will assist in developing workforce plans, facilities plans, equipment acquisition plans, and future-year budgets. Currently each office within the S&T Directorate maintains information about positions and staffing management processes through individual spreadsheets. No comprehensive staff management system is currently maintained or standard processes enforced. This web application does not replace or replicate the information management system currently in place for financial management (Federal Financial Management System/National Finance Center/Prism) or the upcoming human resources management system (MAXhr). This tool will provide S&T Directorate the ability to augment those supporting systems by automating and standardizing the currently manual processes employed in reconciling the data received from those systems.

The system is hosted in a DHS facility, connected to an existing Sensitive But Unclassified DHS infrastructure and available to authorized users through the DHS network. The application uses a web-based interface, which users on the DHS network will access through Internet Explorer available on the user workstation. No additional clients are required to access the application. Users will be authenticated through the existing DHS Network Active Directory structure, and are assigned roles within the system which are appropriate for the functionalities they perform in their current support duties. Users must have an active DHS network account as well as be assigned roles within the SMS application in order to access the application.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The system will collect information related to personnel who support the DHS S&T Directorate, both Federal employees and contractors. The information collected will include: name, birth date, telephone numbers, email address, work mailing address, education and training records, pay grade information (for Federal employees), social security numbers, security clearance level, and passport numbers.

1.2 From whom is information collected?

For the purposes of this document, S&T Staff refers to personnel occupying S&T positions, occupying S&T facilities, or using S&T resources. The information that will be included in SMS is currently collected for S&T staff during hiring, in-processing, and throughout the tenure as a member of the DHS S&T staff. Information stored and processed by the SMS has already been collected by the S&T Human

Resources, Facilities Management, Security, and CIO staffs, as well as members of the various management staffs. At the present time staffing information resides in a variety of databases, spreadsheets, and on paper managed by organizational offices such as S&T HR and Facilities, as well as the specific offices the staff member supports. The information will be consolidated from the existing management sources and imported into the SMS. Offices currently using the existing ad-hoc sources have been included throughout the software development lifecycle to address their requirements in the system. All new data generated (new staff members, and updates to existing information), will be collected and managed in the system by the S&T SMS user responsible for that information (e.g. HR, Facilities, CIO, etc.).

1.3 Why is the information being collected?

The information is being collected to:

- Maintain information regarding S&T staff
- Support the day to day management of S&T resources
- Routine office purposes
- Allow for the projection of salary budgets for federal staff members
- Reporting of S&T resources

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

SMS maintains information that S&T has already been authorized to collect and manage for S&T staff in accordance with SORN OPM/GOVT-1 as well as the Privacy Act 5 USC 522 (a) (b) (1)(2) and (3). No additional personal information beyond what is already being managed by S&T is being collected. This system will further restrict access to personal information, and provide an auditable record of access to that information. The SMS only serves as S&T's central repository and tracking tool for this type of information and captures this information in a standardized format for internal S&T use only.

S&T was given authorization to develop SMS by the S&T Human Capital group who are required to manage the processes supported by the SMS. S&T is also authorized to develop support systems compliant with DHS policy and procedures to assist with day-to-day business operations of the organization

This system will replace manual processes currently used for personal data management, and SMS will be managed and supported by the S&T Human Capital office, at the direction of the S&T Deputy Chief of Staff.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The aggregation of the data in the SMS was evaluated to determine the sensitivity of the system for Certification and Accreditation purposes, and was discussed at length with representatives from the DHS S&T CIO Information Systems Security Management office. Of specific concern was the aggregation of personal information about S&T staff into a single database system, the potential visibility of personal financial & security clearance information in a single location, and the potential for causing personnel to become targets for identify theft or being pursued to compromise classified information.

Risks of data exposure have been mitigated by limiting system access to only approved users on the DHS SBU network with the need to access data in the performance of their duties. Users have access to personal data only to the extent as is required by their outlined job function. This need for access has been reviewed and approved by the Deputy S&T Chief of Staff and any additional access request to SMS will require the same approval.

To further protect the confidentiality and integrity of the information, all users will be trained on how to handle and protect the information contained in SMS prior to being granted access. Auditing is enabled on all system components to capture user actions and weekly audit reviews by the SMS Information System Security Officer will assist in detecting abnormal system usage.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

As outlined in section 1.3, the information will be used to manage S&T staff SMS provides S&T the ability to effectively manage S&T support staff information that is required for the day-to-day operations of the organization.

Social Security Numbers (SSN) will be used to uniquely identify staff in the system, and will be masked at all times, except to the S&T Security Office and S&T Human Capital Office.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

The system does not provide the facility to perform data or data pattern analysis. It is meant as a data repository and process management tool, rather than a data mining tool. Users are able to narrow datasets based on search parameters; however, no facility for intelligent analysis is provided.

Aggregated reporting is provided by the SMS. Examples of reports are: Staff Phone Lists, Work Location, Education and Training, and Essential Personnel. Human Capital, the Financial Office, and specific senior Federal leadership have access to Financial Reports containing pay grade details for Federal Employees. These details do not provide true salaries, but provide Office of Personnel Management data table mappings for the Federal position held by an individual. This provides approximate salaries for future staff planning and budget forecasting purposes.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Personal data collected in the system are provided by individuals through the DHS hiring process, known as the S&T on-boarding which include security clearance verification. The information is captured and verified manually by S&T Human Capital and Security offices before it is entered into the system. In addition application controls such as pre-populated drop down menus ensure information entered is accurate and properly formatted. The S&T Human Capital office generate validation reports regularly to ensure accuracy, and information is updated by the specific program office responsible for maintaining the accuracy of that data.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Controls are in place in the form of administrative policies and procedures, as well as technical controls outlined in section 8.8, which ensure information is used in accordance with the above described uses. Access to personal information is limited to system users who have been approved and assigned a system role authorizing access to information required to perform their job functions. The ability to perform data mining, query directly against the database, or create data reports other than those authorized for their user role is controlled through technical access controls on the SMS.

User's that are granted access to the SMS have signed a DHS Rules of Behavior and Non-Disclosure Agreement that outline the roles and responsibilities while accessing a government system and consequences of misbehavior are also defined. Additionally, a standard DHS warning banner is displayed on the SMS homepage to inform users that they are about to access a DHS owned computer system:

> **This is a Department of Homeland Security (DHS) computer system. DHS computer systems are provided for the processing of Official U.S. Government information only. All data contained on DHS computer systems is owned by DHS and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on DHS computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.**

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

SMS Data is retained in accordance with General Records Schedule 1, item 18 (a). SMS staff is currently working with the DHS Records Management Office to ensure that records are not retained longer than is required. When a staff member is no longer associated with the organization their record is marked as "archived". Report generation includes an "include archived record" selection, should that information be desired. Data back-up and long-term storage is performed by DHS S&T OCIO network support staff.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes. A data retention schedule has already been established by the NARA pertaining to the type of information stored and processed by SMS. Reference GRS-1 item 18 (a).

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The system owner desires to store a subset of non-personnel data (e.g. excluding the SSN, DOB, Name, etc.) for the purpose of long-term budgets and staffing analysis and forecasting.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Information in the SMS is used only within the DHS S&T organization and no information sharing occurs with any other internal DHS organization outside of the S&T Component. Information contained in SMS is entered directly into SMS by authorized representatives from the S&T Security Office, S&T Human Capital Office and S&T Facilities Office.

S&T Human Capital and the Security Office are involved in all facets of the hiring process and are authorized SMS users responsible for updating and maintaining information in SMS that is relevant to their Office areas of responsibility.

4.2 For each organization, what information is shared and for what purpose?

The information in the system may be shared with an internal DHS employee's parent organization upon request.

4.3 How is the information transmitted or disclosed?

When information is requested by the internal DHS parent organization, it will be provided in report form through the existing communication methods between S&T and the DHS parent organization.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The same risks that exist for the system (see section 6.4) exist for internal sharing.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Information is not shared with any external organizations.

5.2 What information is shared and for what purpose?

Not applicable.

5.3 How is the information transmitted or disclosed?

Not applicable.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Not applicable.

5.5 How is the shared information secured by the recipient?

Not applicable.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Not applicable.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

There are no external information sharing partners.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

All current DHS S&T staff will be notified via e-mail that their information will be stored in SMS for S&T staff tracking and management purposes and be given an opportunity to decline. New DHS S&T employees will be notified of data collection and storage during their new hire orientation.

SMS stores and tracks information that S&T has already been authorized to collect during the hiring processes for all S & T staff and no additional personal information is being collected that does not already exist in the individual's personnel file. The personal information contained in this system is covered under System of Record Notice OPM/GOVT-1.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Information contained in SMS has already been voluntarily provided by the individuals during the DHS S&T on-boarding processes. Individuals have the right to decline to provide the information during the on-boarding process. SMS will only store information that is provided to the S&T Human Capital Office, S&T Security Office and other S&T Management Offices by the individual.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The information stored in SMS is standard S&T Human Capital information and is required to fulfill the functions of the S&T Human Capital office, which uses this system in support of their duties. Individuals are notified that the data will be used for managing S&T staff. In accordance with SORN OPM/GOVT-1, this information can be used by government agencies to manage the day-to-day operations of the organization without further notice to the individual.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

As an S&T Human Capital management support system, SMS will store certain personal information that is currently collected by S&T support offices. While both Federal and Contractor data will be stored in the system, they are treated differently in the system. Contractors are given the opportunity to decline to provide personal information beyond what is required for employment and to manage security clearances.

They are notified during the on-boarding process that additional information may be collected by S&T Human Capital to support staff management within S&T.

Due to the nature of the information stored by the system, certain privacy risks were identified to include; unauthorized access to the information (intentional / unintentional). These risks have been mitigated through management, operational and technical controls. Detail is provided in section 8.8.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals cannot access the system directly, but may request and be provided with a paper copy of their information by contacting the S&T Human Capital Office. All individuals will be instructed to contact the Human Capital office to verify that their information is correct.

7.2 What are the procedures for correcting erroneous information?

Every individual has the right to challenge any information contained within the SMS that they consider incorrect personal information. If the individual detects erroneous information, they are required to notify the S&T Human Capital Office and or Security Office who is responsible for working with the individual to correct the information

DHS S&T contractors who detect erroneous information are directed to contact the security officer of their hiring company who will work with the S&T Human Capital office to correct the information.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are directed to report incorrect personal information to their supervisor, the S&T Human Capital staff, corporate security officer, or the S&T organization responsible for the information.

7.4 If no redress is provided, are alternatives are available?

Any redress necessary will be considered by the S&T Human Capital Office.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Individuals have a right to obtain a copy of their personal information stored in SMS and this request is honored by the S&T Human Capital Office, the S&T Security office, or the office responsible for managing that information.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

Access to SMS is limited to:

- Authorized staff who support the S&T on-boarding and human capital management processes
- DHS S&T CIO IT Operations Group
- DHS Network administrators
- Approved system developers participating in software roll-outs

8.2 Does the system use "roles" to assign privileges to users of the system?

Yes, role based access controls is enforced on the SMS application. Roles are defined by the position the user holds within DHS S&T and limits computing resources. Role based access control is used within the SMS environment because it is a method for controlling what information computer users can use, the programs that they can run, and the modifications that they can make. The method of access was chosen for SMS because user membership into roles can be revoked easily and new memberships established as job assignments dictate. Role associations can be established when new operations are instituted, and old operations can be deleted as organizational functions change and evolve.

8.3 What procedures are in place to determine which users may access the system and are they documented?

Documented policy and procedures are in place for approving users to have access to the system, at the direction of the Chief of Staff, DHS S&T. The users of this system who have access to personal information are: the S&T Office Directors/Deputies, S&T Security, S&T Human Capital, and S&T CFO.

The system has pre-determined user access roles based upon the support functions performed by the assigned user. The office director or supervisor will determine a user's need for access to the system. Once determined, the director will submit in writing a request for access to SMS to the S&T Chief of Staff. The Chief of Staff will direct the SMS administrator to create the appropriate user account and provide training to the new user.

The steps that need to be taken to add a new administrator/user account to the SMS Application are as follows.

- A member of the S&T Office Management staff notifies S&T Chief of Staff Office that a new user needs to be added to the SMS system.

- The Office Manager verifies the user's need for access to the system, gathers the new user's personal information, first name, last name, email address, phone number and provides the user information and access requirements to the SMS system administrator.

- The new user account is added to the website by the SMS System Administrator, and an e-mail is sent to the new user stating that their credentials have been changed/modified.

8.4 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Each account that is created on the system is supported by system access request forms signed an approved by the requester's supervisor and S&T Deputy Chief of Staff. User accounts are reviewed by the Information System Security Officer (ISSO) and the S&T Deputy Chief of Staff on a quarterly basis.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Audit and accountability policies and procedures have been developed, documented and maintained to ensure that risks, vulnerabilities and threats are properly identified; analyzed, documented, and significant risks are adequately managed. The policies and procedures encompass user activity during the operational and maintenance phase of the SMS.

Audit trails for a variety of system related events and activities are logged to allow the system administrator and system ISSO to check for associated security issues. The items recorded provide an accurate representation of the actions taking place, the user or host responsible for initiating the action, as well as the date and time.

Additionally the level of logging user activity has been tailored to the needs of the SMS system, with specific focus upon the Program Management and Reviewer users, who have access to sensitive information. Each time an attempt is made to login to the system with an invalid username, the system logs the username, date/time and IP address of the computer trying to gain access. These logs are reviewed weekly by the SMS ISSO to determine the appropriate course of action. The SMS audit facility logs insert, update, and delete operations to the system log file and to the database audit tables including identification of: DHSNET username (associated with SMS user session), date/time, database table, database operation performed, and specific content modified.

8.6 What privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Access to the system is limited to specific individuals who currently handle this information in accordance to Federal privacy regulations. Additional privacy training will be provided during SMS user training, prior to providing access to the system.

All employees receive training regarding appropriate use and management of personal information. All new employees receive introductory privacy training at orientation. The personal information accessed by system users is the same information being accessed and handled in their current job position.

8.7 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes, Certification and Accreditation activities were completed on the system on 11 January 2006 in accordance with the Federal Information System Management Act (FISMA). SMS has been assessed based on the Confidentiality, Integrity and Availability of the information system.

8.8 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

S&T identified four privacy risks during the risk assessment for SMS: unauthorized access to the information; unauthorized modification of the information; threats from External sources (Internet access); misuse of information.

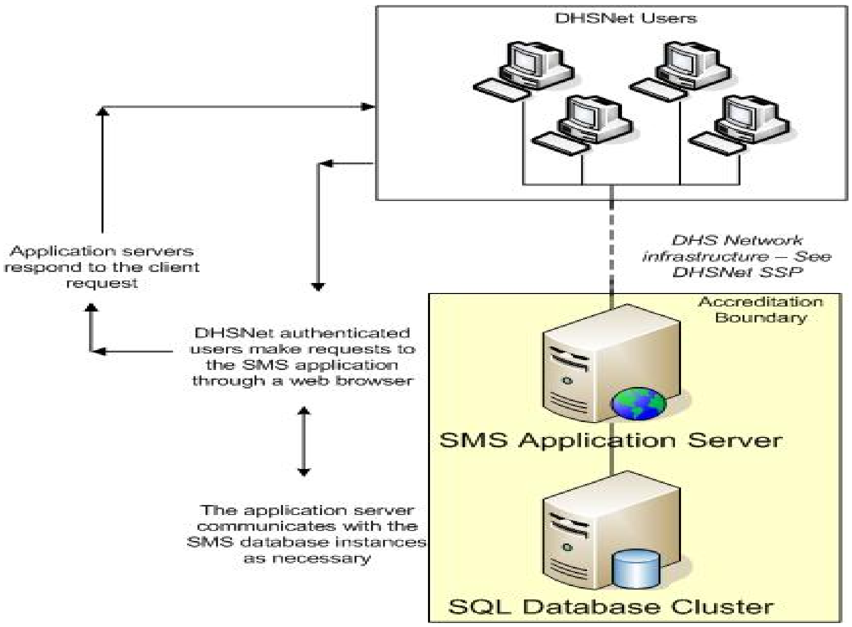
S&T has taken several discrete steps aimed at mitigating the identified risks. Some of the below steps work to protect against more than one identified risk.

- Role based access controls are implemented, providing access to the specific data required by an individual to perform their job functions.
- SMS is an internal S&T application, which is not accessible via the Internet.
- Individuals are instructed as the appropriate use and protection of information through annual security awareness training, and specific SMS user training.
- Boundary protection devices (firewalls) are used to prevent unauthorized access to the DHS network and SMS.
- Intrusion detection capabilities are installed at the network level to detect system and network anomalies.
- Virus protection is installed and updated regularly on servers hosting SMS
- Limited administrative accounts, and separation of roles and responsibilities between the network administrator who manages the server and related network components from the system administrator who manages the application are also implemented.
- 128-bit SSL encryption is used to securely transmit data between the user's web browser and SMS server to mitigate risk of data compromise while in transit.
- Clear operating instructions for user's and administrators are documented and available to all users.
- Weekly reviews of the audit logs performed by the ISSO

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The SMS application was built from the ground up. It is a custom Intranet web-based application that uses a J2EE framework to enable platform independence and deployment configuration flexibility. The SMS components are hosted on two machines, a database server and an application server. The system is designed for use on the DHS Local Area Network (LAN). User access is accomplished through an Internet Explorer browser. SMS interfaces with existing Microsoft Active Directory (LDAP) and Microsoft Exchange (Email) servers within DHSNET. Below is a data flow diagram that illustrates how the application processes information:


DHSNet Users
DHS Network infrastructure – See DHSNet SSP
Accreditation Boundary
Application servers respond to the client request
DHSNet authenticated users make requests to the SMS application through a web browser
SMS Application Server
The application server communicates with the SMS database instances as necessary
SQL Database Cluster

9.2 How were data integrity, privacy, and security analyzed as part of the decisions made for your system?

Data stored by the system was assessed using FIPS 199, NIST 800-60 and Department of Homeland Security Functional Business Requirements Matrix. Confidentiality, Integrity and Availability were independently assessed based on the impact on the DHS mission and day-to-day operations. Data integrity and security considerations have been made throughout the software development lifecycle. Privacy decisions have been made based upon the data currently collected and managed by the existing staff management processes, and the data requirements of the involved organizations. SSN access is limited to the Human Capital and Security offices.

9.3 What design choices were made to enhance privacy?

The system was designed with role-based user access in order to limit users to specific sets of data and system functionality to that required to perform the duties of their positions. Further design and implementation choices are detailed above in section 8.8.

Conclusion

Throughout the software development lifecycle of SMS, the protection of personal information has been considered a priority. In order to assess the privacy risks of SMS effectively and accurately, and because the program enhances a current S&T business process, this PIA was carried out and performed in accordance with Department of Homeland Security Privacy Office guidelines and policy, and OMB guidelines and policy. In the process of conducting the PIA for SMS, DHS S&T identified the need to examine the privacy and security aspects of the existing SORNs and implement on an ongoing basis any necessary additional strategies to ensure the privacy and security of SMS data.

Additional privacy requirements will be re-assessed should any new processes be developed, and on an ongoing basis as needed.

Responsible Official

Jackie Bowman
Human Capital
Science and Technology
Department of Homeland Security

Approval Signature

___________________________________ February 2, 2006

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security