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: July 26, 2010

b. Name of system: State Messaging and Archive Retrieval Toolset-Unclassified

c. System acronym: SMART-SBU

d. IT Asset Baseline: 2743

e. System description:

SMART-SBU (hereafter called "SMART") replaces existing Department of State unclassified email and cable systems with a Microsoft Outlook-based system. SMART manages three messages types – working emails, record emails, and cables. It allows users to control archiving and retrieval of messages by adding internal sensitivity labels to a message. One sensitivity label indicates the message contains personally identifiable information (PII).

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: To describe privacy-enhancing features now incorporated in SMART-SBU.

h. Date of previous PIA: October 2008

3. Characterization of the Information

The system:

- ☐ does NOT contain PII.
- ☒ does contain PII.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

SMART is a message management infrastructure. It is not a business application intended to uniformly collect PII. A SMART message may coincidentally incorporate PII in its subject line, body text, or attachments.

b. How is the information collected?

Information compiled by SMART originates as email messages or cables key-entered by Department staff into government-furnished computer equipment in the course of official business.

c. Why is the information collected and maintained?

The specific reason for incorporating PII in a message will vary. PII usually appears in SMART messages related to certain channels, i.e., program areas that require special handling of messages. The following channels commonly have PII in their cables or emails:

- MED Channel for medically sensitive information
- DIRGEN, HR, and EEO Channels for sensitive personnel matters
- AGRÉMENT Channel for approval by a receiving state of the appointment of a new Chief of Mission
- DISSENT Channel for dissent on official policy

d. How will the information be checked for accuracy?

SMART does not incorporate features to check accuracy of PII contained in a cable or email because accuracy of the message is the responsibility of the originator. The free-text nature of messages prevents any additional error checking by SMART.

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

5 U.S.C. 301-302 (Management of the Department of State)

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

SMART does not collect PII directly from individuals. It manages messages that may incorporate PII in the conduct of Department programs. Evaluation of privacy risk resulting from the collection of the PII is accomplished under the PIA of the IT system that originally collects the PII for a purpose authorized by statute.

4. Uses of the Information

a. Describe all uses of the information.

Uses of the PII relate to the purpose of the SMART message containing the PII. The specific reason to incorporate PII in a message may vary significantly; however, the PII usually relates to one of the programmatic channels listed in section 3.b. of this PIA.

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

SMART incorporates no functionality to manipulate PII in messages or to recompile for analysis the PII in the messages in the SMART Archive. No new PII is created by SMART through automated functions.

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

With respect to the PII that may be in SMART messages, SMART does not incorporate any commercial information, publicly available information, or information from other Federal agency databases so as to alter the character of the PII.

d. Are contractors involved in the uses of the PII?

Contractors were involved in the development of SMART. Contractors assist Federal employees in maintaining and operating SMART. Contractors are subject to the same personnel screening procedures and access controls as Government employees. Governing contracts include required Federal Acquisition Regulation privacy clauses.

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.

SMART does not collect PII directly from individuals. It manages messages that may incorporate PII in the conduct of Department internal operations. Evaluation of privacy risk resulting from use is accomplished under the PIA of the IT system that originally collects the PII for a particular purpose. Procedures outlined in Section 10 of this PIA describe how SMART messages with PII are safeguarded by SMART and how their retrieval from the SMART Archive is limited to those individuals with the appropriate clearance level and having an authorized need to know.

5. Retention

a. How long is information retained?

Retention of SMART messages depends on whether a message is a working email, a record email, or a cable, and whether the message is deemed a Federal record. It is the responsibility of the sender and the person who receives an email to determine whether or not the message meets the criteria of a Federal record.

If the email is determined to be a Federal record, SMART allows the sender to designate it as record email so that it is automatically stored in the SMART Archive. Cables managed by SMART are considered equivalent to record emails, and are automatically stored in the SMART Archive without requiring designation as such by the originator. Record emails and cables are retained under the record disposition policy that applies to other records in the same programmatic area.

Working emails are considered to be transitory in nature and to have no long-term record value. Working emails are stored and managed in the SMART user's mailbox and local Microsoft Exchange email servers; however, they are not stored in the SMART Archive and cannot be retrieved using SMART search capabilities. SMART users are expected

to delete, store, and manage working emails in accordance with Department policies the same as they would if there were no SMART message management.

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

Record retention may be associated with privacy risk from several standpoints:

- Sensitive PII is at some risk of exposure for the duration it is retained in an active state; therefore, a shorter retention naturally lessens risk of exposure.
- Records originally compiled for biographic and demographic purposes become outdated and unreliable as they age into semi-active and inactive states
- Records maintained outside the structure of enforced disposition schedules create problems for record searches related to disclosure inquiries
- The accessibility and usability of records can depend on the continued viability of the storage and retrieval technologies applied to the records.

The privacy risk related to retention of messages managed by SMART is considered negligible because official record disposition schedules apply; because the messages are not used as the subject's authoritative biographic or demographic source; and because the storage technologies used in SMART are deemed resistant to industry obsolescence.

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?

When a message containing PII is prepared in SMART, the sender adds an internal sensitivity marking of Privacy/PII that will restrict subsequent retrievals from the SMART Archive. Even if only one portion of a message contains PII, the entire message is considered to carry the Privacy/PII sensitivity label. The Privacy/PII marking is displayed in both electronic and printed versions of the message. Role-based access controls apply to all messages in the SMART Archive to limit internal sharing to only those individuals authorized and having an official need to know.

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

SMART messages are Sensitive But Unclassified (SBU) information. SMART operates under the Department network authorized for the processing of any SBU information.

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

Insiders present a threat to Department systems in that they are capable of gaining direct access to sensitive information through the access rights they have been assigned. The insider threat can include, but is not limited to, acts of maliciousness, carelessness, ignorance of security policies, and improper information system use. However, all Department employees and contractors have been screened and cleared prior to being granted access to Department systems and security controls are in place to identify users and audit the activities they perform while logged on to a Department system. Also, all

employees and contractors must successfully complete mandatory security awareness training and are required to sign a “Rules of Behavior” agreement prior to operating any Department systems.

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?

SMART does not inherently share PII information with external organizations.

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

Any disclosure outside the Department of a message with the Privacy/PII sensitivity label would be made under the authority of a condition of disclosure in the Privacy Act applicable to the system of records that the PII is part of.

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

Because SMART messages containing PII would be subject to the controls on disclosure required by the Privacy Act, the privacy risk related to external sharing is negligible.

Once it leaves the Department’s network, the level of risk does increase slightly, as the Department is no longer in complete control over the electronic space in which the PII now resides. However, the Department has Memoranda of Agreement and Information Security Agreements in place with the external agencies in addition to layered defense-in-depth technical security controls,

8. Notice

Information in the subject line, body text, or attachments of SMART do not constitute a separate Privacy Act system of records. PII incorporated in some SMART messages may be subject to the provisions of the Privacy Act. The governing Privacy Act system of records is described by the PIA for the IT system that originally compiles the PII.

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

Notice at time of collection is not directly applicable to SMART messages. PII in some messages may be subject to the notice provisions of the Privacy Act. The PIA for the IT system that originally compiles the PII describes means of notice to the record subject at time of collection.

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

Notice of opportunity and/or right to decline provision of information is not directly applicable to SMART messages. The PIA for the IT system that originally compiles the PII would describe opportunities and rights available to the record subject at time of collection.

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?

Opt-in/opt-out choices available to subjects of the PII in some SMART messages do not bear on the privacy risk of SMART itself. The PIA for the IT system that originally compiles the PII describes any options available to record subjects at time of collection.

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.

Privacy risk related to notice applies to the IT system that originally compiles the PII that may later appear in a SMART message. Consequently, the PIA of that system will address privacy risk related to notice.

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?

Notification and redress are not directly applicable to SMART messages. The PIA for the IT system that originally compiles the PII would describe procedures for notification and redress. If the PII is subject to the provisions of the Privacy Act, formal procedures for notification and redress must exist and would be described in the Privacy Act system of records pertaining to the PII.

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

Privacy risk related to notification and redress applies to the IT system that originally compiles the PII that may later appear in a SMART message. Consequently, the PIA of that system will address privacy risk related to notification and redress.

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?

Access to SMART requires an OpenNet logon request approved by the individual's supervisor. To get access to OpenNet, the user must sign a Department user access agreement acknowledging OpenNet terms of use. The individual's supervisor must also sign the agreement certifying that access is needed by the individual to perform their official duties.

Department rules of behavior for handling PII describe the individual's responsibility to safeguard PII and to avoid prohibited activities such as curiosity browsing of databases. A system use notification ("warning banner") is displayed at time of logon and restates the restrictions on use. Activity by authorized users is monitored, logged, and audited.

Role-based access control is invoked when cables and record emails are searched in the SMART Archive. Records having the Privacy/PII sensitive label is only available through searches to those few staff provisioned for access to that category of messages.

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

All users are required to undergo Department-standard computer security awareness training (CSAT) at the time of issuance of an OpenNet user account. Users must annually complete CSAT refresher training 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.

Safeguards for access are commensurate with the security categorization of SMART. Residual risk is considered to have been remediated and mitigated to an acceptable (low) level by the Designated Approving Authority (DAA).

11. Technologies

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

SMART does not incorporate any technologies that would increase the risk of compromise or unauthorized exposure to PII.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Role-Based Access Controls (RBAC) and mandatory annual Cyber Security Awareness Training, along with “Tips of the Day” information security reminders, help to reinforce good habits and prevent inadvertent PII disclosures.

12. Security

What is the security certification and accreditation (C&A) status of the system?

SMART successfully completed C&A and obtained full Authorization to Operate (ATO) in September 2008.