Submit the completed PIA to
Privacy's SharePoint Customer Center

SMART-SBU

1. Contact Information

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

2. System Information

(a) Name of system: State Messaging and Archive Retrieval Toolkit

(b) Bureau: IRM/MSO/OPS

(c) System acronym: SMART

(d) iMatrix Asset ID Number: 2743

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Importing information into new PIA template

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?

Authorized to Operate as subsystem of OpenNet ATO expired 3/31/2017; the new ATO is expected to be granted in September 2017.

(c) Describe the purpose of the system:

SMART-SBU (hereafter called "SMART") replaces existing Department of State unclassified email and cable systems with a Microsoft Outlook-based system. SMART manages three message 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).

SMART supports the Messaging Systems Office (IRM/OPS/MSO) mission requirements for managing unclassified messaging systems for the Department of State that allows effective communications among all elements of the Department of State. SMART is designed to be a simple, secure, and user-driven system that will meet Department of State (DoS) messaging, archiving, and information sharing needs by integrating several Commercial-Off-the-Shelf (COTS) products with customized applications and components. Within SMART, the Core Messaging project comprises a majority of messaging functionality, providing the capability to send and receive formal Department of State messages, interest profiling (also referred to as "Alert Me," based on the user-selection in the SMART Client software), message archiving, organizational profiling, role-based access control (RBAC), cross-enclave messaging, message tracking, and taxonomy searching and profiling.

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

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. The SMART system includes all cables, record emails, and working emails created, sent, and received by State Department employees and contractors. Messages contained in the SMART repository could contain personal data (names of individuals, birthdates of individuals, SSN or other identifying numbers, individual ID number from other sources, address/phone or similar information, images, email address of individuals, biometric IDs, or any other individually identifying item about individuals).

SMART is not designed to collect, nor does it explicitly collect, information about individuals. SMART facilitates the transmission of information, which may include personal data. SMART will not be used to explicitly collect Privacy Act information from employees or the public. 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

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

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

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

☒Yes, provide:

- SORN Name and Number: Email Archive Management Records, STATE-01

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): May 2, 2017

☐No, explain how the information is retrieved without a personal identifier.

Click here to enter text.

(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 .)

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:

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 ☒N/A

- If yes, under what authorization?

(c) How is the information collected?

SMART is a message management infrastructure. It is not a business application intended to uniformly collect information, to include PII. A SMART message may coincidentally incorporate PII in its subject line, body text, or attachments. The SMART system includes all cables, record emails, and working emails created, sent, and received by State Department employees and contractors.

(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?

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.

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

Messages are continuously archived; therefore the archive is kept current with new messages. The timeliness of the information contained in the messages is the responsibility of the SMART users. SMART does not incorporate features to check the timeliness 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.

(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?

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

(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?

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 any IT system that originally compiled the PII sent by individuals would describe any options available to record subjects at time of collection.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

Privacy risk related to type of information applies to any IT system that may have originally compiled 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.

5. Use of information

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

SMART archives messages, created by SMART users, which contain the information. Messages in the archive can be searched and retrieved. Access to the messages is restricted by Role Based Access Controls (RBAC). A user's role (defined by system administrators when user accounts are created) determines what the user can retrieve from the archive.

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

SMART archives messages that contain the information. The only use of that information is in the search function. Users can search messages in the archive via searchable fields where they can enter key words.

(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.

Information is shared with those to whom the user addresses the message and the markings, captions, and tags applied to the message. Messages are shared internally and to other government agencies based on the RBAC rules explained in 5(a). The administrators of SMART-SBU do not share information in the system internally or externally.

(b) What information will be shared?

SMART does not share the information, but provides controlled access to the messages, created by the users, that contain the information. The specific information shared is determined by the user who creates the message.

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

This is determined by the user who creates the message.

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

Messages are transmitted electronically with appropriate network infrastructure safeguards.

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

SMART messages are Sensitive But Unclassified (SBU) information. SMART operates under the Department network authorized for the processing of any SBU information. All State employees and contractors with a SMART account can search the SMART Archive.

There are systems external to the Department which interface with SMART and provide a means to exchange messages. However these interfaces only allow for the direct addressing of messages to known users. There are currently no plans for any system, internal or external to the Department, to directly access the SMART repository. To control risk and liability associated with the distribution of sensitive or incorrect information, information owners strictly enforce the same clearance and need-to-know restrictions imposed by the system within the Department. There is no requirement for explicit State Department policy restrictions regarding general reuse of the information by other agencies. The USG employs a consistent security clearance and need-to-know privacy policy throughout the Executive Branch, although they may be administered differently from within other agencies.

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

When sending a message, users are prompted with a dialogue box, which requires them to choose a sensitivity level for the message. One of the options is "Official – Privacy/PII." 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.

7. Redress and Notification

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

Role-based access controls restrict who can see specific messages.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☐Yes ☒No

If yes, explain the procedures.

Click here to enter text.

If no, explain why not.

SMART is a message archiving system. The archive is made up of PDF versions of email messages. Once in the archive the messages cannot be altered. If there is incorrect

information in a message, it is still part of the archive. An individual would have to contact the sender or receiver of the information to correct any mistakes.

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

NA

8. Security Controls

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

All servers are secured using DOS security configuration guidelines. Access to the message archive is restricted using Role Based Access Control. SQL databases holding the message archive are secured by DOS security configuration guidelines.

(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.

Access to messages in the archive is restricted based on captions and tags added to the message when it was created. Access is based on Department of State logon account.

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

All access to the message archive is logged. All actions taken in SMART system are also logged.

(d) Explain the privacy training provided to authorized users of the system.
All Department of State employees and contractors are required to participate in yearly training on PII

(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.

Two-factor authentication into the Department of State network is required.

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

The information in the SMART message archive is SBU. Messages marked by the message originator as containing PII are restricted to users with the rights to certain captions.

9. Data Access

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

Access is restricted to users of the Department of State network with specific access to the SMART system. Access is further restricted by use of captions and tags set by the originator of the message

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

Access is based on a users' job responsibility and which captions or tags they have been granted access to by their supervisor

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

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

Access to messages in the archive is restricted based on captions and tags added to the message when it was created.

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

Role Based Access controls based on a users' Department of State logon.