**DEPARTMENT OF STATE**

**PRIVACY IMPACT ASSESSMENT**

**State Messaging and Archive Retrieval Toolset (SMART)**

**Updated October 3, 2008**

**Conducted by:**
**Bureau of Administration**
**Information Sharing Services**
**Office of Information Programs and Services**
**E-mail: pia@state.gov**

**A. Who is the Agency Privacy Coordinator who is conducting this assessment?**

Ms. Margaret Grafeld, Director
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

**B. GENERAL INFORMATION ABOUT THE SYSTEM**

**(1) Does this system collect, maintain, or disseminate personally identifiable information (PII) about individuals?**

No. SMART is a message management infrastructure not a business application having as its primary mission purpose to collect and maintain information about defined categories of individuals. A message managed by SMART may coincidentally contain information embedded in the message body about an individual.

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

SMART does not comprise a Privacy Act system of records.

**(3) What is the purpose of the system?**

SMART replaces several Department messaging systems with a modern, secure, and integrated messaging system that supports dynamic archiving and information sharing. SMART integrates email messages, cables, and memos on an easy-to-use, commercial software platform.

**(4) What legal authority authorizes the purchase or development of this system?**

The authority for the operation of this system is 5 U.S.C. 301-302 (Management of the Department of State)

**C. DATA IN THE SYSTEM:**

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

SMART is a message management infrastructure not a business application having as its primary mission purpose to collect and maintain information about defined categories of individuals. A message managed by SMART may coincidentally contain information embedded in the message body about an individual.

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

Messages managed by SMART originate as email messages, cables, or internal memoranda.

**(3) What type of information is collected from the source of the information?**

SMART is a message management infrastructure and does accomplish the collection of personal information from individuals as its primary mission purpose.

**(4) Accuracy, Timeliness, and Reliability**

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

SMART is a message management infrastructure and does accomplish the collection of personal information from individuals as its primary mission purpose. If the originator of an email, cable, or memorandum includes personal information in such documents, it is the responsibility of the originator to ensure the accuracy of the information.

**b. How will data be checked for completeness?**

SMART is a message management infrastructure and does accomplish the collection of personal information from individuals as its primary mission purpose. If the originator of an email, cable, or memorandum includes personal information in such documents, it is the responsibility of the originator to ensure the completeness of the information.

**c. Is the data current?**

SMART is a message management infrastructure and does accomplish the collection of personal information from individuals as its primary mission purpose. If the originator of an email, cable, or memorandum includes personal information in such documents, it is the responsibility of the originator to ensure that the information is as current as required to constitute a correct Department communication.

**D. <u>INTENDED USE OF THE DATA:</u>**

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

The originator of messages managed and archived by SMART are responsible for ensuring that any personal information included in a message is relevant and necessary to that communication.

**(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 new data is created or derived by SMART from the messages that are managed and archived by it.

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

No such determinations are made by SMART based on the messages managed and archived by it.

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

Not applicable.

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

Not applicable.

**(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.**

SMART does not provide for searches of archived messages based upon personal identifiers.

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

No compilation, analysis, or interpretation of archived messages is performed by the system in relation to personal information that may coincidentally be embedded in the messages.

## 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 be maintained in all sites?**

SMART systems, operations, and maintenance policies are consistent at all sites.

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

The retention period of messages managed and archived by SMART depends on the record control schedule for the particular category of message, e.g. emails, cables, internal memorandums.

**(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?**

SMART was jointly developed with NARA to ensure that it properly integrates with and supports the objectives of the OMB-sponsored, cross-agency e-records management initiative. Removal of records from SMART adheres to NARA guidance and to both Department and National Security guidance regarding the handling of federal records.

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

SMART does not employ any technology considered to increase privacy risk to individuals.

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

Not applicable because SMART employs no such technology.

**(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?**

Not applicable because SMART employs no such monitoring technologies.

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

Not applicable because SMART is not a Privacy Act system of records.

**(8) Are there forms associated with the system?**

No forms (hard copy or web forms) for the purpose of collecting personal information directly from individuals are employed in SMART.

## F. ACCESS TO DATA:

**(1) Who will have access to the data in the system?**

Access to the messages in SMART is provided to Department of State staff having authorized clearances and a need-to-know. Department authorized users can access (search) the SMART archive but are subject to security controls. Other agency personnel residing outside of Department of State facilities may be recipients of messages managed by SMART but will not have direct access to the SMART message archive.

**(2) What are the criteria for gaining access to the system?**

Access is governed by a role-based access control methodology that enforces security clearance and need-to-know access policies for SBU and classified information. These

procedures, controls, and responsibilities regarding access are documented in the Department Foreign Affairs Handbook, the Foreign Affairs Manual, and the SMART Business Guide.

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

Access for individuals is governed by a role-based access control methodology that enforces security clearance and need-to-know information access policies for SBU and classified information.

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

SMART does not provide for searches of archived messages based upon personal identifiers. SMART utilizes controls required by the Foreign Affairs Handbook, Foreign Affairs Manual, and the SMART Business Guide.

**(5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**?

Contractors are involved in the design, implementation, operation, use, and maintenance of the system. Training for contractors is equivalent to employee training with regard to accessing and conveying official information. Necessary and appropriate Privacy Act clauses are contained in all SMART support contracts.

**(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 other government systems share information with SMART or have access to the messages in the SMART archive.

**(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?**

Federal government email systems external to the Department of State may originate messages that are received by the Department of State and are consequently managed and archived by SMART. Agencies outside Department of State do not have access to the SMART archive.

**(8) Who is responsible for assuring proper use of such shared data?**

Not applicable because outside agencies do not have access to the SMART archive.