DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Security Incident Management Analysis System (SIMAS)
April 3, 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)
Email: pia@state.gov

A. 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".**

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 both of the following e-mail addresses: **pia@state.gov.**

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

YES _ X _ **NO**___

System Name Diplomatic Security Records **Number** STATE-36

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

The Security Incident Management and Analysis System (SIMAS) is a worldwide Bureau of Diplomatic Security (DS) web-based application, whose major purpose is to serve as a repository for all suspicious activity and crime reporting from U.S. Diplomatic Missions abroad. SIMAS reports typically contain a detailed narrative description of the suspicious activity prompting the report, available suspicious person(s) and vehicle descriptors, and other identification data as may be available (e.g. photographs). Reports also indicate date, time and location of suspicious activity, and may include amplifying comments from relevant Bureau offices.

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

The legal authorities as documented in STATE-36, Diplomatic Security Records.

B. DATA IN THE SYSTEM:

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

Present and former employees of the Department of State including Diplomatic Security Special Agents; applicants for Department employment who have been or are presently being investigated for security clearance; contractors working for the Department; interns and detailees to the Department; individuals requiring access to the official Department of State premises who have undergone or are undergoing security clearance; some passport and visa applicants concerning matters of adjudication; individuals involved in matters of passport and visa fraud; individuals involved in unauthorized access to classified information; prospective alien spouses of American personnel of the Department of State; and individuals or groups whose activities have a potential bearing on the security of Departmental or Foreign Service operations.

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

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

Information may be obtained directly from the suspicious individual, from Department personnel at post responsible for reporting suspicious activities, or from third parties, including domestic law enforcement agencies and host country government agencies, as well as confidential sources. Information is not always sourced directly from the suspicious individual because the suspicious individual may not be able to be interdicted and questioned before departing the area, or they be the subject of counter-surveillance or under investigation and purposely not be interdicted to protect the integrity of the larger investigation.

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

SIMAS allows users to input “events” consisting of suspicious or potentially threatening incidents gathered from observations in the vicinity of a post. It provides a means for collecting detailed characteristics of persons, vehicles, and other entities associated with a particular incident. It also allows users to download digital images to an event. SIMAS enables DOS staff to recognize trends and patterns of hostile surveillance directed against U.S. mission personnel and property. The system links suspicious entities to other suspicious entities and/or event components.

3) Accuracy, Timeliness, and Reliability

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

The agency or source providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by DS include, among other things, maintaining the system as a live feed, allowing the information to be updated/edited at any time, and cross referencing information. A SIMAS working group meets on a daily basis to review and analyze all SIMAS events (received by cable and via SIMAS) submitted by posts over the previous 24 hour period to identify correlation and trends, track the status of incidents, ensure appropriate follow-up action, and to provide timely dissemination within DS and other actionable government agencies. This working group is chaired by ITA and is comprised of representatives from CI, IP, ITA, OPO, and PII.

b. How will data be checked for completeness?

Completeness of data will be checked through investigations and/or through personal interviews of the source of the information.

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).

Reports are entered within 72 hours of the event (suspicious activity) which prompted them. Information (data) entered is derived from eye-witness accounts, and possibly from the interdiction and questioning of the suspicious individual(s). Reports are reviewed by Department personnel within 24 hours of their entry. Compliance with this requirement ensures the regional security officer's perspective on the significance of an incident is available, as soon as is reasonable, to the leadership and to analysts at every level. Investigations and/or personal interviews will confirm accuracy and currency of information. DS/IP/ITA representatives lead a daily review.

C <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?

Yes, SIMAS allows users to input "events" consisting of suspicious or potentially threatening incidents gathered from observations in the vicinity of a post. It provides a means for collecting detailed characteristics of persons, vehicles, and other entities associated with a particular incident. It also allows users to

download digital images pertaining to an event. SIMAS enables DOS staff to recognize trends and patterns of hostile surveillance directed against U.S. mission personnel and property. The system links suspicious entities to other suspicious entities and/or event components.

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?

Possibly. If this was to occur, the new/previously unavailable data would be added to/entered in the report; or, depending on its significance and sensitivity, recording/dissemination may be warranted through some other channel/means.

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 in and of itself will make no determinations. Department and other law enforcement or intelligence analysts make all determinations.

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

Yes, the information will be placed in either the existing investigated file or in an existing background security file.

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

Verification will be made through law enforcement and intelligence community investigations and/or personal interviews. Reliability of sources is assessed. Inquiries concerning redress of records in this system may be directed to the Director, Office of Information Resource Management , Programs and Services.

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.

Data can be retrieved in several ways, including use of event descriptors (e.g., event number, date of event, post location) as well as by personal identifiers (e.g., name, passport number, license plate numbers, etc.).

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

The database will be used to produce descriptive reports containing a narrative description of suspicious activities, including any known details on the person(s) involved in the activity. Reports provide a means for collecting detailed characteristics of persons, vehicles, and other entities associated with a particular incident. These reports assist Department staff in recognizing trends and patterns of hostile surveillance directed against U.S. mission personnel and property. The system can also link suspicious entities and/or event components.

Diplomatic Security employees and contractors with an official purpose will have access to the information. Other federal agency personnel with an official law enforcement interest may also be provided access to the information as prescribed by agreements between the agencies.

D. 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?

SIMAS is operated and its servers are located at State Annex-20 (SA-20) only. System is accessible through the Department's worldwide OpenNet (SBU) network accessible at all posts abroad. Worldwide users are issued accounts through the DS/ISSO to access the system, and comment on reports.

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

The retention period of data is consistent with established Department of State Policies and Guidelines as documented in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11.

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?

The retention period of data is consistent with established Department of State Policies and Guidelines as documented in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11.

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

No. Current system security restrictions are in place and followed.

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

There is no new or additional technology that would affect privacy. Yes, appropriate access restrictions are in place.

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?

N/A

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

N/A

8) Are there forms associated with the system? YES ___ NO X

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)?

ACCESS TO DATA:

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

Access to the data in the system is on an "official purpose" basis and/or under routine use criteria as explained in STATE-36.

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

A criterion for gaining access to the system is based on an official purpose. Criteria, procedures, controls, and responsibilities regarding access are all documented.

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

Access will be restricted on "a need to know basis," specific to work related responsibilities. Full access may be granted when necessary.

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)

The system provides a means of limiting access to areas within the application based on user ID, password, and "a need-to-know." Moreover, the Bureau of Diplomatic Security employees and contractors must follow the System Behavior Rules established by the Department.

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

If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? YES

Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended? YES

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?

Not currently occurring, but future sharing agreements with other agencies such as the National Counterterrorism Center (NCTC) are expected, given the Information Sharing Environment (ISE) mandate. Specific legal authority to share terrorism information lies, for example, in the following documents:

- Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458; and
- Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect Americans.

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?

Other agencies will not have direct access to the data, absent an agreement between the agencies. The data may be shared with an agency upon request from the agency if that agency is listed as a routine user in STATE-36. The use of the data by the other agency will be restricted to the same purpose for which the data was originally collected.

8) Who is responsible for assuring proper use of the SHARED data?

The agency receiving the information is responsible for adhering to lawful restrictions.