

## Security Incident Management Analysis System (SIMAS)

### 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: January 5, 2010
- (b) Name of system: Security Incident Management Analysis System
- (c) System acronym: SIMAS
- (d) IT Asset Baseline (ITAB) number: 798
- (e) System description (Briefly describe scope, purpose, and major functions):

The Security Incident Management and Analysis System (SIMAS) is a worldwide Bureau of Diplomatic Security (DS) web-based application, which serves as a repository for all suspicious activity and crime reporting from U.S. Diplomatic Missions abroad (all U.S. embassies and consulates). Department of State personnel, including Diplomatic Security personnel, regional security officers, and cleared foreign nationals, enter Suspicious Activity Reports (SARs) into SIMAS as a central repository for all physical security incidents overseas. 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.

- (f) Reason for performing PIA:
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security re-certification
- (g) Explanation of modification (if applicable): Certification & Accreditation
- (h) Date of previous PIA (if applicable): October 26, 2009

### 3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

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

SIMAS collects and maintains the following types of PII on members of the public, foreign nationals, U.S. government employees, and contractors who are identified as

## ***Security Incident Management Analysis System (SIMAS)***

being directly or indirectly involved in or associated with suspicious activities and/or criminal allegations near USG property. All types of information may not be collected on each specific group of individuals. However, it may be possible for all forms of PII to be collected on an individual.

- Citizenship Status and Information (source-documents)
  - DSP-11 (Passport Application)
  - OF-156 (VISA application)
- Biometric Information (source-observation and photography)
  - Gender
  - Race
  - Height
  - Weight
  - Eye Color
  - Skin Tone
  - Hair Color
  - Hair Style
  - Images
  - Age or Estimated Age
  - Body Type (Build)
  - Scars, Marks, & Tattoos
- Other (source-personal interview by authorities)
  - Name
  - Address
  - DOB
  - Telephone Number
  - Father's Name
  - Mother's Name

### **b. How is the information collected?**

SIMAS allows Department of State (DOS) personnel 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.

### **c. Why is the information collected and maintained?**

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. Regional security officers (RSOs) submit telegrams concerning surveillance detection incidents judged high-probability of terrorism nexus per existing instructions. All information in SIMAS is visible to headquarters and to RSOs with SIMAS access worldwide.

### **d. How will the information be checked for accuracy?**

The agency or source providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by the Bureau of Diplomatic Security (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

## ***Security Incident Management Analysis System (SIMAS)***

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 U.S. government agencies. This working group is chaired by ITA and is comprised of representatives from CI, IP, ITA, OPO, and PRV. Completeness of data will be checked through investigations and/or through personal interviews of the source of the information.

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

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to SIMAS, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986), as amended;
- Pub.L. 107-56 Stat.272, 10/26/01 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

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

SIMAS collects the minimum amount of personally identifiable information (PII) necessary to complete its statutorily mandated functions. SIMAS collects a significant amount of personally identifiable information to positively identify individuals who have jeopardized the safety of U.S. missions abroad. This collection of PII is justified due to the need to protect personnel at U.S. missions and share information about security incidents abroad with other U.S. Government agencies.

As SIMAS does collect sensitive PII, there are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

## **4. Uses of the Information**

### **a. Describe all uses of the information.**

SIMAS allows direct communication of suspicious activity and crime information between posts and headquarters. It centralizes the data from all posts for analysis, and allows RSOs to also view events entered by other posts in their regions or globally.

## ***Security Incident Management Analysis System (SIMAS)***

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

DS investigators and analysts are able to retrieve data based on text queries and then use the data to conduct terrorist and criminal investigative analysis based on data collected and stored in SIMAS. The information in SIMAS is then used in connection with other intelligence and law enforcement information that is collected through other means such as Motor Vehicle Records, Law Enforcement Only restricted databases (i.e. NCIC, TECS, etc.), and other outside sources. No new information on the record subject is produced with in SIMAS.

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

Information contained within SIMAS is collected from overseas sources such as foreign local police departments and from subjects themselves through interdiction by local police which results in personal biographical data such as names, dates of birth, or information captured directly by the SD team i.e. photos, record of license plates. The system does not use other federal databases. An analyst may utilize the raw data from SIMAS in concert with intelligence from other federal agencies in compiling an intelligence product outside of SIMAS, but it does not make its way back into the SIMAS database.

### **d. Is the system a contractor used and owned system?**

SIMAS is a U.S. Government owned system which was primarily designed and developed by contractors under the guidance and management of U.S. Government employees. All contractors abide by regulatory guidelines established as part of their contractual arrangement with the U.S. Government and have signed and follow DS rules related to the protection and handling of sensitive information. All employees (FS, GS, and contractor) are required to be trained annually on the protection of information as part of the DOS Information Security Program. These records are maintained centrally and by DS as well.

### **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.**

SIMAS collects and processes sensitive PII and performs significant analysis and matching against other U.S. Government databases for the purpose of suspicious activities and crime reporting but does not create new information about the record subject. Accounts assigned to users are issued on a need-to-know basis which is determined by the office of assignment. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein, with the passage of time, PII is used for purposes for which the public was not given notice. Information within SIMAS is used for a specific purposes only, suspicious activities and crime reporting, thereby mitigating any privacy risk associated with the collection of sensitive PII.

## ***Security Incident Management Analysis System (SIMAS)***

### **5. Retention**

#### **a. How long is information retained?**

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11, Countermeasures & Counterintelligence, A-11-003-21a&b.

Information on cases that reflect distinctive Department activities, attract media or Congressional interest, or are otherwise historically significant are kept permanently. All other case information is reviewed every five years and destroyed 20 years after determination date that the case no longer has any security interest.

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

SIMAS collects and maintains personally identifiable information (PII). There are inherent risks associated with maintaining this type of information. Records within SIMAS are only retained in accordance with the Diplomatic Security records disposition schedule; they are not used for purposes outside of terrorist or criminal investigations and are properly disposed of according to their records disposition schedule.

### **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?**

The information collected and maintained by SIMAS is shared with the Office of Counter Terrorism (C/ST) and the Office of Intelligence and Research (INR) as well as various regional desk and senior DOS offices for the purpose of preventing crime and terrorism.

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

In order for an employee of the Bureau of Diplomatic Security to obtain access to SIMAS, they must complete the required training to gain access to OpenNet and the SIMAS application; have their manager's approval; pass the proper security checks; and request and be granted access.

Information is shared internally to bureaus outside of DS in the form of a report via classified cable. Information shared outside of DS is shared on a "need to know" basis with offices and bureaus which require the information in order to fulfill their mission.

Numerous management operational and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to: annual security training, separation of duties, least privilege, and personnel screening.

## ***Security Incident Management Analysis System (SIMAS)***

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

It is possible for a DOS employee with authorized access SIMAS to retrieve an individual's PII and use this information in an unauthorized manner. In order to mitigate this risk all DOS employees are required to undergo computer security and privacy awareness training prior to accessing SIMAS, through which the information is shared, and must complete refresher training yearly in order to retain access. A system of records is maintained all access to SIMAS files.

## **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?**

There is external sharing of PII from SIMAS to the intelligence and security communities through classified telegram/cable dissemination when warranted for life or safety issues, and criminal or terrorist investigative purposes. There is a signed memorandum of agreement (MOA) with the National Counterterrorism Center (NCTC).

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

PII collected and maintained in SIMAS is shared with several departments and agencies through classified cable traffic for purposes of mitigating terrorist action. This includes:

- Central Intelligence Agency
- Federal Bureau of Investigation
- Department of Agriculture
- Department of Defense
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Justice
- Department of Treasury
- National Geospatial-Intelligence Agency
- Nuclear Regulatory Commission
- US Capital Police

The safeguards of the classified system are relied upon to protect the PII information. In addition, SIMAS information is available for the NCTC for review, in accordance with the signed MOA.

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

PII collected and maintained in SIMAS is currently shared through classified cable means when necessary. Risk is mitigated by the use of the classified network and PII within SIMAS is protected during transfer through the integrity of DOS classified programs. Other external sharing is covered through an MOA between DOS and the NCTC. The MOA limits and protects the use of PII with the agency.

## **Security Incident Management Analysis System (SIMAS)**

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information by personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text) and the use of un-secure connections are also a serious threat to external sharing. Numerous operational and technical management controls are in place to reduce and mitigate the risks associated with external sharing and disclosure including, but not limited to formal memorandums of agreement/understandings (MOA/MOU), service level agreements (SLA), annual security training, separation of duties, least privilege and personnel screening.

### **8. Notice**

The system:

- Contains information covered by the Privacy Act.  
Provide number and name of each applicable system of records.  
(visit [www.state.gov/m/a/ips/c25533.htm](http://www.state.gov/m/a/ips/c25533.htm) for list of all published systems):  
STATE-36
- Does NOT contain information covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information are described in the System of Records Notices STATE-36, Security Records.

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

No. Due to the nature of the information collected and maintained by SIMAS, individuals may or may not have the opportunity or right to decline the collection of information. Some of the information collected and maintained by SIMAS includes observational information such as height, weight, hair color, gender, and build collected through photography.

#### **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?**

No. The utility of the information in the system about a particular individual will not extend beyond the allotted time in the Department of State's Disposition of Records Schedule, as defined in Diplomatic Security Records, Chapter 11. Moreover, there is negligible privacy risk as a result of the degradation of information quality over an extended period of time.

#### **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.**

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

## ***Security Incident Management Analysis System (SIMAS)***

### **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?**

SIMAS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above and in rules published at 22 CFR 171.31. The procedures inform the individual how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

The notification and redress mechanisms, outlined in the Notice section above and 22 CFR 171.31, offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

### **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?**

The Business Owner DS/DSS/ITA approves and authorizes use of the SIMAS system. System accounts are maintained and reviewed on a regular basis. The following DOS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of three consecutive invalid access attempts by a user during a 15 minute time frame. After 20 minutes of inactivity, a session lock control is implemented at the network layer.

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.



## **Security Incident Management Analysis System (SIMAS)**

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

The Bureau of Diplomatic Security (DS) uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the SIMAS components, for changes to the DOS mandated security controls.

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

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order 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.**

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed, or attempted to perform on an information system.)

## **11. Technologies**

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

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. SIMAS has been designed to minimize risk to privacy data.

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

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

## **12. Security**

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

The C&A for SIMAS was completed November 30, 2009, and received a 36 month authorization to operate (ATO). The new ATO expires November 30, 2012.