PRIVACY IMPACT ASSESSMENT

Security Incident Management and Analysis II (SIMAS II)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: July 2022
(b) Name of system: Security Incident Management and Analysis II
(c) System acronym: SIMAS II
(d) Bureau: DS
(e) iMatrix Asset ID Number: 6177
(f) Child systems (if applicable) and iMatrix Asset ID Number: None
(g) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The Security Incident Management and Analysis System (SIMAS) II is a worldwide Bureau of Diplomatic Security (DS) web-based application, which serves as a repository for all suspicious activity, crime, and incident reporting from U.S. Diplomatic Missions abroad (all U.S. embassies and consulates) and Department of State domestic facilities. Department of State personnel, including Diplomatic Security personnel, regional security officers, and cleared foreign nationals, enter incident records into SIMAS II as a central repository for all physical security incidents affecting Department of State interests. Incident records contain a detailed narrative description of the suspicious or

criminal activity prompting the report, available suspicious person(s) and vehicle descriptors, and other identification data as may be available (e.g., photographs). Incident records also indicate date, time, and location of suspicious activity, and may include amplifying comments from relevant bureau offices.

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

SIMAS II 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 being directly or indirectly involved in or associated with suspicious activities and/or criminal allegations near U.S. Government property. All types of information may not be collected on each specific group of individuals. However, in some instances all PII elements to be collected on an individual.

All data types below are not required but are collected if applicable due to the nature of the incident.

• Citizenship Status and Related Personal Information (source-documents)
• Biographic (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 personal information collected (source: personal interviews by authorities)
- Name
- Personal Address
- Personal email address
- Place of birth
- Citizenship status
- Date of Birth
- Personal and/or Work Telephone Number(s)
- Father’s Name
- Mother’s Name
- Associate’s Full Name

Though SIMAS II collects PII from both U.S.-persons and non-U.S.-persons, the remainder of this PIA will only address the PII collected from U.S.-persons.

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

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to SIMAS II, 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)
- Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans)

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

☒Yes, provide:

- SORN Name and Number:
  Systems Records Notices STATE-36: Security Records

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  06/15/2018

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

(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 Office 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 (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  A-11-021-07

- Disposition Authority Number:
  DAA-0059-2018-0003-0007

- Length of time the information is retained in the system:

25

- Type of information retained in the system:
  Suspicious activities including possible surveillance and other crime-related information.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

U.S. Diplomatic Missions abroad - information on suspicious activities (and other incidents affecting US security), and potential information on individuals involved, are entered into SIMSA II by the general users (specified in 8b). Local host nations police or security forces may in certain instances provide the Department extensive information on an individual or group(s) through their own respective investigation and interviews, this information will also be entered into SIMAS II by general users.

Department of State domestic facilities - information on suspicious individuals or incidents may be collected and entered in the system through investigations or interviews by either a Department of State employee (such as a special agent or a uniformed protection officer (UPO)), or by local police or other reporting entity. Every host nation provides the information in different formats to the RSO. There is no standardized format for collecting the information.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Department Regional Security Officers (RSO) are responsible for verifying the accuracy of the collected information prior to approving the incident record submission. Each post or location that uses SIMAS II has their own SOP tailored to the location's unique circumstances and assets available for vetting accuracy of data entered into SIMAS II. SIMAS II records are updated as new information about an incident becomes available.

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

Information is current at the time it is entered into SIMAS II. SIMAS II is a world-wide incident reporting system with multiple new entries daily. Notable incident records which receive Bureau of Diplomatic Security (DS) investigative activity are updated by the reviewing DS supervisors (who may obtain more accurate data from their investigative activity to supplement the SIMAS II incident records).

(h) Does the system use information from commercial sources? Is the information publicly available?

No, this system does not use information from commercial sources; the information is not publicly available.

(i) How was the minimization of PII in the system considered?

Given the sensitive nature of collecting, processing, and protecting of PII, SIMAS II only obtains what is necessary to achieve the mission.

Privacy concerns were paramount; each item of PII collected was scrutinized to determine whether the system did indeed require the information to process the requests each application manages. We realize that the information collected by SIMAS II could be used for nefarious purposes, so all applicable Department approved risk mitigation techniques and IT security safeguards were applied to the system. The application of Department approved risk mitigation processes and technologies will significantly reduce the likelihood of compromise of the system's information.

5. Use of information

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

SIMAS II is a data repository for all suspicious activity, demonstrations, and other security-related incidents and reporting from U.S. Diplomatic Missions abroad (all U.S. embassies, consulates, and other Chief of Mission facilities) and potentially affecting domestic Department of State facilities. The PII, and other information collected by SIMAS II, is used for analysis of suspicious activities and criminal investigations.

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

Yes, SIMAS II is being used according to its designed function, which is to support analysts in performing data analysis of suspicious activities and criminal investigations.

(c) Does the system analyze the PII stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the PII?
The system links suspicious entities to other suspicious entities and/or event components.
The information in SIMAS II is leveraged 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 within SIMAS II.

(2) Does the analysis result in new information?
Trends and patterns may be identified that leads to supporting mission activity, but no new information on the record subject is produced.

(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

(d) If the system will use test data, will it include real PII?
☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal: Though not routine, in some instances, SIMAS IIs' PII is shared with other offices within the Department such as Office of the Inspector General (OIG), Bureau of Intelligence and Research (INR), Bureau of Counterterrorism (CT), Consular

Affairs (CA), Bureau of Management (M), and various Regional Bureaus.

External: SIMAS shares information with National Counterterrorism Center (NCTC).

(b) What information will be shared?

Internal:
There are no instances of routine, direct data sharing. When shared, the information includes all PII listed in 3d.

External:
All PII listed in 3d is shared with NCTC.

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

Internal: SIMAS II shares information with the bureaus mentioned above with the purpose of crime and terrorism prevention and/or review and auditing purposes.

External:
SIMAS II shares information with NCTC to prevent crime and terrorism.

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

Internal: Information is shared via Unclassified Department cable, email, or hard copy for all offices/bureaus listed in 6a.

External:
The data is exported from SIMAS into XML files. The files are transported to NCTC on an encrypted hard drive and delivered by hand via a certified courier from NCTC. Files are shared with NCTC in accordance with the signed MOA (Memorandum of Agreement Between Bureau of Diplomatic Security and National Counterterrorism Center on Security Incident Management and Analysis System Information Sharing).

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

Internal: Data is shared via cable, encrypted email, or hard copy. When PII is delivered in hard copy, it is carried in a locked bag.

External:
Files are shared with NCTC in accordance with the signed MOA (Memorandum of Agreement Between Bureau of Diplomatic Security and National Counterterrorism Center on Security Incident Management and Analysis System Information Sharing).

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Due to the nature of record subjects being involved or associated with law enforcement investigations, notice is not provided to the record subjects. Further, SIMAS II is not a record subject facing system.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

SIMAS II is not accessible to record subjects. In cases where collection is part of an active investigation, notice is not provided to the record subject.

(c) What procedures allow record subjects to gain access to their information?

SIMAS II is not accessible to record subjects. As a criminal law enforcement and suspicious activity information repository owned by the Bureau of Diplomatic Security, SORN State-36, which covers SIMAS II, discusses exclusions from the access and redress provisions of the Privacy Act that apply to SIMAS II in order to prevent harm to law enforcement investigations or interests.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

To the extent that material contained in SIMAS II is subject to the Privacy Act (5 USC 552a) individuals can request amendment of material in the system under procedures set forth in SORN State-36. The procedures to allow a record subject to correct inaccurate or erroneous information are published in the system of records State-36, Security Records, and in rules published at 22 CFR 171.5.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Procedures for redress are published in the system of records notice State-36 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 if permissible.

8. Security Controls

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

As a system, SIMAS II is protected by a layered defense in depth approach that limits user access to the system and the associated data. SIMAS II defense starts with it being placed on OpenNet, which is not accessible from the public internet.

SIMAS II data is stored in an Oracle database, which is protected by role-based access controls configured with the concept of least privilege. The data-at-rest for SIMAS II is protected via encryption.

SIMAS II 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. Further, Diplomatic Security 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 II components, for changes to the DoS mandated security controls.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Application Administrators: Primarily responsible for configuring the options available in the various drop-down menus, and other domain-related settings (as opposed to technical configuration). This role creates accounts that access this system. Application administrators have logon identifications associated with their name that allows for user auditing. Users in this role do not have access to PII.

General Users: Access to this system is restricted to cleared Department of State (DoS) direct hire, contractor employees, and Locally Employed Staff. Once access is obtained, they can view all PII mentioned in 3(d) as needed for their assigned posts and job duties. As part of daily assigned job requirements, general users have access to PII relative to their specific job duties and/or geographic assignment within SIMAS II.

System Administrators: Primarily responsible for configuring technical aspects of the system (e.g., mail server information). This role does not have access to PII. This role is responsible for the daily maintenance, upgrades; patch/hot fix application, backups, and configuration to the database.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

The Business Owner for this application is the Threat Investigations and Analysis Directorate (DS/TIA).

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. These access restrictions are managed via role-based access controls. 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.

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

(d) How is access to data in the system determined for each role identified above?

User access to SIMAS II is role-based. System access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. A representative from DS/TIA/ITA has final approval for all account requests. All account requests are submitted via AccessDS application. Account request procedures are in place in AccessDS to determine what access users need.

All roles and accounts must be approved by the user's supervisor and the Information System Security Officer.

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

System accounts are maintained and reviewed on an annual basis. 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.

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

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Each user must complete the course titled PS800, which is Cybersecurity Awareness Training. A quiz is administered as part of PS800, prior to receiving access to a Department network. This briefing is an annual requirement. Additionally, all users are required to take the biennial privacy course, PA318 Protecting Personally Identifiable Information.