SIMAS II - PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Security Incident Management and Analysis II

(b) Bureau: DS

(c) System acronym: SIMAS II

(d) iMatrix Asset ID Number: 6177

(e) Reason for performing PIA: Update to a previous PIA

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

(f) Explanation of modification (if applicable): Click here to enter text.

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?
SIMAS went through an Annual Controls Assessment (ACA), which was reviewed and approved by IRM/IA in March 2016. The SIMAS application is categorized as a High system.

(c) Describe the purpose of the system:
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, 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 Suspicious Activity Reports (SARs) and other incident data into SIMAS as a central repository for all physical security

incidents affecting Department of State interests. SIMAS Reports typically 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). Reports 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 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 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 Related Personal 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(s)
  - Father's Name
  - Mother's Name
  - Associates
  - Travel and lodging arrangements
  - Group and personal associates and associations

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

☒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): December 15, 2015

☐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)): A-11-021-07
- Length of time the information is retained in the system: 25 years
- 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) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No

- If yes, under what authorization?

(c) How is the information collected?
In the overseas environment, suspicious (and other incidents affecting US security) information (and potential individuals involved) are passed to local (host nation) security or police forces for review. These local host nation police or security forces may obtain extensive information from an individual or group(s) through their own respective investigation and interviews. In the domestic (USA) environment, information on suspicious individuals or incidents may be gained through investigation 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.

(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?
Department personnel review the incident entries and approve for publication.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Information is current. SIMAS is an world-wide incident reporting system with multiple new entries daily. Notable SIMAS incidents which receive DS investigative activity are updated by reviewing DS supervisors (who may obtain more accurate data from their investigative activity to supplement the SIMAS record). DS may open a case in the DS Investigative Management System (IMS) with further details which will refer to the SIMAS entry, and the DS officer should note in the SIMAS entry if additional information is available in IMS.

(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?
Varies by geographic location and host nation rules. Also exemptions J2 and K2 in the 1974 Privacy Act cover law enforcement with the purposes of identifying individual criminal offenders or alleged offenders

(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?

Local police address the matter – in some jurisdictions, you must provide identification to law enforcement.

- If no, why are individuals not allowed to provide consent?

Exemptions J2 and K2 in the 1974 Privacy Act cover law enforcement with the purposes of identifying individual criminal offenders or alleged offenders

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

Privacy was highly considered with the CTO project and programming offices to be built in as SIMAS was redesigned and fielded. Because personally identifiable information would be collected in some instances and that data would be used to identify potential terrorist trends and persons of interest, privacy concerns dictated the level of access to the information more than the type of information to be collected. Only those DS employees with need to know have access permissions (including direct hires, contractors, and locally hired employees abroad).

5. Use of information

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

SIMAS 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 Dept. of State facilities.

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

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

(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?

The system links suspicious entities to other suspicious entities and/or event components.

The information in SIMAS 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.

(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
The information collected and maintained by SIMAS is shareable with other Department of State offices with criminal investigative or intelligence responsibilities, the National Counterterrorism Center (NCTC) and other Intelligence Community and Executive Departments (with criminal investigative missions) for the purpose of preventing crime and terrorism.

(b) What information will be shared?
Reports that may communicate global physical security incidents, descriptions of suspicious activity, persons, vehicles, and artifacts (e.g. photographs).

(c) What is the purpose for sharing the information?
Preventing crime and terrorism.

(d) The information to be shared is transmitted or disclosed by what methods?
Information is shared internally to bureaus outside of DS in the form of a report via cable-mail or hard copy (classified and/or law enforcement sensitive) . Information shared outside of DS is shared on a "need to know" basis with executive offices and bureaus which require the information in order to fulfill their criminal investigative or intelligence community mission.

(e) What safeguards are in place for each internal or external sharing arrangement?
Access to SIMAS is discretionary, based on "need to know", and is shared externally via secure transmission.

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

7. Redress and Notification

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

As a criminal law enforcement and suspicious activity information repository owned by the Bureau of Diplomatic Security, SORN State 36, 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. However, access requests are considered on a case-by-case basis if made in writing to the Department of State at Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW; Washington, DC 20522-8100, as specified in the SORN, State 36.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

The procedures are the same as those outlined in Question 7a.

If no, explain why not.

Click here to enter text.

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

Procedures for notification and 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 the information in the system secured?

The safeguards native to DS unclassified and classified information systems are relied upon to protect the PII information. In addition, SIMAS information is available (via secure transmission) for the NCTC for review, in accordance with the signed MOA.

(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.

The Business Owner for this application is the Threat Investigations and Analysis Directorate (DS/TIA). DS/TIA approves and authorizes the overall use of the SIMAS system by agencies, offices, and others with a need for access to SIMAS data. Individual requests for SIMAS accounts are vetted by DS direct-hire employees through the DOS New Account Request system. System accounts are maintained and reviewed on a regular basis.

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.

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.

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

DS/TIA approves and authorizes the overall use of the SIMAS system by agencies, offices, and others with a need for access to SIMAS data. Individual requests for SIMAS accounts are vetted through the DOS New Account Request system.

System accounts are maintained and reviewed on a regular 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.

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.

(d) Explain the privacy training provided to authorized users of the system.

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.

(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 is required using a DOS issued badge.

(f) How were the security measures above influenced by the type of information collected?
The security controls required by NIST SP-800-53 are in place as prescribed by FISMA and the systems security categorization level. An Authorization to Operate (ATO) has been issued for the system.

9. Data Access

(a) Who has access to data in the system?
Manager approved personnel with a "need to know" are granted access.

(b) How is access to data in the system determined?
Access is determined by mission criteria based on a "need to know".

(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.
Only approved users will have access to SIMAS. 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.

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