Security Records Tracking System (SRTS)

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 Records Tracking System

(b) Bureau: Diplomatic Security

(c) System acronym: SRTS

(d) iMatrix Asset ID Number: 194, 654

(e) Reason for performing PIA:

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

(f) Explanation of modification (if applicable): Not applicable

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.
Not applicable; SRTS is a child system under DS CAGE, whose SCF covers all child systems.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The RMF Steps 1–3 A&A documentation is being prepared for delivery to IRM/IA later this month.

(c) Describe the purpose of the system:
SRTS is a collection of specialized server components for Microsoft Internet Information Server (IIS), engineered specifically for use within government agency environments. SRTS supports secure, accessible web applications and web services that solve mission-critical requirements for the Bureau of Diplomatic Security (DS). SRTS itself does not collect, store, or process personally identifiable information (PII); however, some web applications and services that will be supported by SRTS will do so. Those applications

and services will be added in the future to this PIA as "child systems". Presently, there is one application to be added, which is the NISP Manager:

National Industrial Security Program Manager (NISP Manager)
The NISP Manager supports the domain models and business processes pertaining to:

- authorizations for non-DoS personnel to visit DoS facilities (handled now by the Visitor Security Clearance Tracking System (VSCTS), which will be formally retired when SRTS and NISP Manager attain authorization to operate (ATO));
- Contract security classification specifications (i.e., DD Form 254).

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

NISP Manager

- First name
- Middle name
- Last name
- SSN
- Date of birth
- Place of birth
    - City
    - U.S. state
    - Country
-

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

The legal authorities as documented in System of Records Notice (SORN) STATE-36, Security Records, specific to SRTS, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended)
- Pub.L. 107-56 Stat.272, 10/26/2001 (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)
- DoD 5220.22-M National Industrial Security Program Operating Manual

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

☒Yes, provide:

- SORN Name and Number: Security Records, STATE-36
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): 5/9/2013

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

Not applicable

(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)): See table below.
- Length of time the information is retained in the system: See table below.
- Type of information retained in the system: See table below.

Schedule No.	Length of Time of Retention	Information Type
NISP Manager		
A-11-038-12a	Temporary. Destroy 6 years after password is altered or user account is terminated.	User Identification, Profiles, Authorizations, and Password Files – EXCLUDING records relating to electronic signatures
A-11-038-12b	Temporary. Destroy when business use ceases.	User Identification, Profiles, Authorizations, and Password Files (Routine systems, i.e., those not covered by item 6a.)
[future systems added to SRTS]		

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?
NISP Manager

Collection of SSNs is required for validating personnel security clearances because each SSN is unique to one individual. A security clearance cannot be validated without the individual's SSN.

This collection of SSNs is authorized under Executive Order 9397. Relevant to this system, the Department may collect SSNs under the following STATE-36 categories:

- **Categories of Individuals Covered by the System** specifically include
  - visitors to the Department of State (the Harry S Truman Building), to its domestic annexes, field offices, missions on official business requiring access to classified information; and
  - contractors working for the Department performing on contracts requiring access to classified information.
- **Categories of Records in the System** specifically include numeric identifiers, giving SSNs as one example.

[Next system added to SRTS]

(c) How is the information collected?
SRTS uses web applications; for each application, users input the applicable information into a web-based form that is specific to that application.

(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.

Not applicable

(e) What process is used to determine if the information is accurate?

NISP Manager

- For visitor access requests, the end user is responsible for the accuracy of the information provided.
- For contractor clearances, the end user is responsible for the accuracy of the information provided.
  For security classification specifications (DD Form 254), the end user for SRTS is responsible for the accuracy of the information provided. The end user for SRTS is the person(s) that perform data entry, data validation and the Industrial Security Specialist.

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

NISP Manager

- For visitor access requests, the information is used once per access request per visitor; it must be current only at the time of the request.
- For contractor clearances, the system users are responsible for ensuring the accuracy of the information in the system. The system validates information against syntactical and logical constraints, but the users are expected to validate semantic content against other sources.

- For security classification specifications (DD-254), the system users are responsible for ensuring the accuracy of the information in the system. The system validates information against syntactical and logical constraints, but the users are expected to validate semantic content against other sources.

(g) Does the system use information from commercial sources? Is the information publicly available?
SRTS does not use information from commercial sources, nor is any of the information publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?
NISP Manager
Yes. The individual is notified that he/she must provide the information in order to receive authorization to visit DoS facilities. Users that are contractors are notified that their information is required to receive access to DoS facilities. However, if information is obtained from a 3rd party source, those individuals may not be notified. In all cases, it is the responsibility of the Facility Security Officer (FSO) to provide the notification.

(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?
NISP Manager
Consent is granted through acceptance of a position requiring access to classified information. The individual may decline to provide the information; this will, however, be grounds for automatic denial of the individual's request. The individual may not consent to some uses but not others; such a stipulation would be grounds for automatic denial of the individual's request.
- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?
NISP Manager
Privacy concerns were paramount; each item of PII collected by the VSCTS (the software systems being replaced by SRTS) was scrutinized to determine whether the new system did indeed require it to process access authorizations to visit DoS facilities, access automated information systems, participate in classified meetings, or perform on-site contracts requiring access to classified information.

5. Use of information

(a) What is/are the intended use(s) for the information?
NISP Manager
The information is used to determine whether an individual fits the criteria to be allowed the access that he/she is requesting.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
NISP Manager
Yes; the system's purpose is to collect the information required to allow DoS officials to be able to authorize visitors to DoS facilities, access automated information systems,

participate in classified meetings, or perform on-site on contracts requiring access to classified information; the information collected is used for exactly that purpose.

(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?

NISP Manager

Not applicable

(2) Does the analysis result in new information?

NISP Manager

Not applicable

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

NISP Manager

Not applicable

(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

NISP Manager

The information will determine whether an individual is eligible for access to classified information consistent with the purpose of the visit.

6. Sharing of Information

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

NISP Manager

As part of the clearance verification process, BizTalk can query NISP Manager for clearance information, and NISP Manager responds with any matching records. BizTalk is the application used to process user network account requests.

(b) What information will be shared?

NISP Manager

SRTS data is accessed based by approved parties with an established "need to know", which includes Federal, State, local agency or other appropriate entities for the purpose of executing the responsibilities listed under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, and Executive Order 12333.

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

NISP Manager

Once the information is input via SRTS, the PII is not shared outside of DS.

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

NISP Manager

Once the information is input via SRTS, the PII is not shared outside of DS.

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

NISP Manager

Once the information is input via SRTS, the PII is not shared outside of DS.

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

NISP Manager

Once the information is input via SRTS, the PII is not shared outside of DS.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
SRTS contains information covered by the Privacy Act; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records STATE-36, Security Records, and in rules published at 22 CFR 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

The procedures in the two documents in 7(a) above inform individuals about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their records.

If a request submitted to an application within SRTS is denied because information was entered incorrectly, the authorizing individual may allow the information to be corrected and the request to be resubmitted.

If no, explain why not.

Not applicable

(c) By what means are individuals notified of the procedures to correct their information?
Procedures for notification and redress are published in SORN STATE-36, Security Records, and in rules published at 22 CFR 171.31. The procedures inform individuals about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their records.

8. Security Controls

(a) How is the information in the system secured?
SRTS users are required to have a minimum security clearance of "Secret" to access the system. Access within the system is controlled by membership in user groups, which model roles.

(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.
User authentication in SRTS is accomplished through integration with Active Directory for OpenNet. Therefore, a user must have a valid OpenNet account to access SRTS.

User access to SRTS is role-based. System access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Access control lists for SRTS, which define who can access the system, are regularly reviewed, and inactive accounts are promptly disabled. Additionally, the system audit

trails that are automatically generated are regularly analyzed and reviewed to detect unauthorized uses. (An audit trail provides a record of which particular functions a given user performed or attempted to perform on an information system.)

(d) Explain the privacy training provided to authorized users of the system.
Every user of any DoS system must attend a security briefing, which also includes privacy orientation, before receiving access to DoS networks and access to DoS facilities. Each user must also complete Cybersecurity Awareness Training annually and sign a user access agreement form certifying that access is needed for the performance of official duties. System administrators and privileged users are required to complete a separate security awareness briefing given by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding form and Rules of Behavior statement. Additionally, DS/CTO/CPA/CGB identifies key personnel within DS/CTO that need to attend the Department's mandated Information Assurance training for system administrators.

(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.
SRTS is accessible via OpenNet, so an active OpenNet account is required for access to SRTS. In order to access SRTS, the user must first authenticate to OpenNet. Authentication is handled via Windows Authentication (mixed mode). Authorization is done on an individual user basis. Users are assigned one or more roles, which are used to determine the exact access each user has in the system. The end user account credentials are then matched with system-specific account information. This provides additional account profile information relevant to operation of SRTS. Local user account information is managed through the application framework.

(f) How were the security measures above influenced by the type of information collected?
Strong security measures were put into place because the PII that is collected may come from U.S. Government employees (and also, by extension their family members), U.S. citizen contractor employees, and members of the U.S. public.

9. Data Access

(a) Who has access to data in the system?
SRTS users consist of Department of State direct hires and cleared contractors possessing security clearances relative to the positions held. Both the application users and system administrative staff must be U.S. citizens and have a minimum clearance of Secret. The system and database administrators are the only accounts with direct access to the database for the purpose of performing maintenance.

(b) How is access to data in the system determined?
User access to SRTS is role-based. System access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

(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.
User access to data within the SRTS system boundary is restricted by the roles that users

are assigned, such as system administrator or database administrator. User access is controlled by the OpenNet authentication process and then by the rules governing the role to which the user is assigned.

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

Security for SRTS is based on user access levels, with discreet access control allowed at the web page level. The user interface is adaptive based on the account. All edits, deletions, and system management actions are tracked through an auditing system. Every user action executed is documented, and no records are completely removed from the system.