PRIVACY IMPACT ASSESSMENT

Security Records Tracking System (SRTS)

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 Records Tracking System
(c) System acronym: SRTS
(d) Bureau: Diplomatic Security
(e) iMatrix Asset ID Number: 194654
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(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:

Security Records Tracking 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 through the SRTS components that are maintained under the boundary of this system. The components of SRTS help to solve mission-critical requirements for the Bureau of Diplomatic Security (DS). SRTS contains the following components:

- Industrial Security Management System (ISMS) supports the Office of Industrial Security DS/SI/IND in preparing the Contract Security Classification Specification (DD 254) for classified contracts and task orders. The DD254 does not contain any PII. ISMS also supports the managing of Visitor Access Requests (VAR), to include the level of classified information access, for contract employees working on the Department's contracts. The VAR does contain PII.
- Domestic Workers Management System (DWMS) supports Department of State Office of The Chief of Protocol mission requirements for record keeping of domestic workers (non-U.S. persons) attached to foreign diplomats coming into the United States. DWMS also keeps records of foreign diplomats' compliance with US labor regulations and laws when they employ domestic workers.

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

The PII in SRTS comes from its components as listed below.

ISMS:
- First name
- Middle name
- Last name
- Social Security Number (SSN)
- Date of birth
- Place of birth
- City
- U.S. state
- Country

DWMS:
- First name
- Middle name
- Last name
- Date of birth
- Place of birth
- City
- Country

Note: DWMS only collects information on foreign workers who are non-U.S. persons. The remainder of this PIA will only focus on the PII in SRTS pertaining to U.S.-persons.

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

- 22 USC 4802 et seq. (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended)
- Executive Order 12829 (National Industrial Security Program, as amended)
- Executive Order 12968 (Access to Classified Information, as amended)
- Executive Order 13467 (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, as amended)

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

☒Yes, provide:

- SORN Name and Number:
  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)):
  Please see table below

- Disposition Authority Number:
  Please see table below

- Length of time the information is retained in the system:
  Please see table below

- Type of information retained in the system:
  Please see table below

Schedule No.	Disposition Authority Number	Length of Time of Retention	Information Type
A-11-029-04a	DAA-0059-2011-0016-0004	Temporary. Destroy 20 years after cessation of contract performance on DoS contracts.	a. Master File: Contains data extracted from forms DD Form 254 (Contract Security Classification Specifications) issued to companies and included in their contracts since 1990s.
A-11-029-04b	DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)	Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. (Supersedes GRS 4.3 item 010; GRS 4.3, item 011; GRS 4.3, item 012; GRS 4.3, item 020; GRS 4.3, item 030; and GRS 4.3, item 031)	DD Form 254 Database records which includes hard copy and electronic input documents, or forms designed and used solely to create update or modify the records in an electronic medium and not required for audit or legal purposes (such as need for signatures) and not previously scheduled for permanent retention in NARA-approved agency records schedule. Also includes adhoc reports output for reference purposes or to meet day-to-day business needs.
A-11-029-04f	GRS 3.2, item 040	Temporary. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later. (Supersedes GRS 24, item 4a[1]).	f. System Backups and Tape Library Records. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.
A-11-029-07	N1-059-95-43, item 40	Temporary. Destroy 2 years after all contracts with firm have been closed out.	**Industrial Security Facility Files** Documentation on facility security clearances and contracts involving contracting firms either bidding on or awarded DOS classified and/or Sensitive But Unclassified (SBU) Contracts, signed copies of Contract Security Classification Specification (DD Form 254), Reports on adverse information, Security Violation Reports, requests/approvals for contractor access to COMSEC, and assorted security clearance documentation.

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?
  - 22 USC 4802 et seq. (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended)
  - Executive Order 12829 (National Industrial Security Program, as amended)
  - Executive Order 12968 (Access to Classified Information, as amended)
  - Executive Order 13467 (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified Information, as amended)

(d) How is the PII collected?

On behalf of the contractor, the Facilities Security Officer (FSO) submits the contractor's PII as part of the Visit Authorization Request (VAR) sent to the Department. Once received and processed by DS/SI/IND, an ISMS user will enter the information from the VAR into ISMS.

(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.

N/A

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

DS/SI/IND validates the information provided about the contractor in the VAR by cross referencing it with the information stored in the Department of Defense "Defense Information Security System" (DISS). If there are no discrepancies between the information on the VAR and the information stored in DISS, the information is entered into ISMS.

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

The information in the system is only as current as the most recent submission of information for that record. ISMS is current as of the VAR submission for the contractor. For Domestic Workers, the information is current as of the most recent interview.

(h) 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.

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

Given the sensitive nature of collecting, processing, and protecting PII, SRTS 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. Only PII that is directly relevant and necessary is collected.

5. Use of information

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

The information is used to determine whether an individual fits the criteria to be allowed the access that the contractor is requesting.

(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, the system's purpose is to collect the information required to allow Department of State officials to be able to authorize visitors to Department of State 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 PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(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: There is no internal sharing.

External: There is no external sharing.

(b) What information will be shared?

Internal: There is no internal sharing.

External: There is no external sharing.

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

Internal: There is no internal sharing.

External: There is no external sharing.

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

Internal: There is no internal sharing.

External: There is no external sharing.

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

Internal: There is no internal sharing.

External: There is no external sharing.

7. Redress and Notification

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

No. Notice is not provided to the record subject. The contract company is responsible for collecting the PII and providing to the Department.

(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?
The record subject's employer provides the PII to the Department on the record subject's behalf.

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

No, record subject cannot gain access to their information because SRTS it is not a user facing system.

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

☒Yes ☐No

If yes, explain the procedures.

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.

In the case of a VAR being denied because information was entered incorrectly, the authorizing individual may allow the information to be corrected and request the contract company to resubmit the VAR with the correct information.

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 SORN State-36, Security Records, and in rules published at 22 CFR 171.23. The procedures inform individuals about how to request amendment of their records.

In addition, record subjects can reach out to their contracting company to correct their information.

8. Security Controls

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

The system uses defense in depth layers of security, including management, data at rest encryption, encryption in transit, auditing, firewalls, physical security, and continuous monitoring. This system maintains an Authorization To Operate (ATO) that was issued in accordance with the FAM/FAH.

Access to applications is controlled at the application level with additional access controls at the database level.

(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).

Industrial Security User Administrator: has access to only create or delete users from the system and does not have access to PII.

Industrial Security Administrator: has access to modify certain aspects of how the application functions, such as editing the contents of dropdown lists, modifying workflows within the application, or adding/removing entities modeled in the application. These users do not have access to PII just configuration items within the application to make it function.

General Users: General Users have read and/or write permissions to access specific application screens. Examples of such functions are data entry, data review, and workflow approval.
General Users are restricted to only entering/viewing PII available to them based on their job duties, enforced via Access Control Lists within the application.

- The Industrial Security Specialist access enables a General User read/write privileges to enter and update records in the system.

- The Industrial Security Read Only access enables a General User read-only access to records in the system and cannot make any changes to PII.

System Administrators: This category is generally restricted to Tier 1/2/3 operational support personnel who may also have Privileged User access to the host operating system and/or database system. They do not have access to PII.

(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.

All requests must be approved by a supervisor or Information Systems Security Officer (ISSO) and is based on need-to-know. Once access is granted, a user's specific access to PII is restricted via Role Based Access controls within each component, only allowing a user access to PII based on their role.

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

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. A representative from DS/SI/IND 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?

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 is documented, and no records are completely removed from the system.

(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 a course titled PS800, which is Cybersecurity Awareness Training. This briefing is an annual requirement. Additionally, all users are required to take the biennial privacy course, PA318 Protecting Personally Identifiable Information.

Users must also sign a user access agreement form certifying that access is needed for the performance of official duties.