Diplomatic Security Evidence and Property System (DSEPS)

1. Contact Information

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

2. System Information

(a) Name of system: Diplomatic Security Evidence and Property System

(b) Bureau: Diplomatic Security

(c) System acronym: DSEPS

(d) iMatrix Asset ID Number: 4492

(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): Reauthorization

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?
DSEPS is undergoing reauthorization with an estimated completion date in January 2019.

(c) Describe the purpose of the system:

The data entered into DSEPS is used to support DS investigations by recording the details of seized property items (documents, firearms, currency, etc.; see (h) below for a more complete listing of file contents) under the case number identifier.

Most of the activities in the system relate to the management of property items: chain of custody and disposition using an internally generated Evidence Control File number which is associated with a Case Number and subjects.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
DSEPS collects and maintains PII on the subjects of investigations, which includes Department employees, contractors, members of the U.S. public, and foreign nationals. This information may include:

- Name
- Birthday
- Address
- Phone Number
- Email Address
- Office Location (ex: Miami, FL; Phoenix, AZ; Washington, DC)

(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, Security Records, specific to DSEPS, 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)

(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): December 15, 2015

☐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 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)): N1-059-10-011, item 1
- Length of time the information is retained in the system: TEMPORARY. Cut off after case closes. Retire to RSC 10 years after closure for transfer to WNRC. Destroy

30 years after case closes. (Supersedes NARA Job No.: N1-059-97-4, item 1a(1), 1a(2), 1b, 2a(1), 2a(2), and 2b).

- Type of information retained in the system:
  Files contain information on investigations that range from passport and visa fraud to smuggling, assault, and acts of terrorism, and they cover any investigations undertaken by DS, including, but not limited to, investigations internal to the Department of State. Files also consist of correspondence, reports, funds spent/received information, affidavits, subpoenas, search/arrest warrants, sworn statements, sentencing documents, evidence/property receipts, photos, copies of driver's licenses, birth and death certificates, passports, and other related documentation. Note that materials gathered during the execution of a search warrant may be in these files.

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 Not applicable—DSEPS does not collect SSNs.

- If yes, under what authorization?

Not applicable—DSEPS does not collect SSNs.

(c) How is the information collected?

Data entered into DSEPS is acquired or seized by DS investigators, technical support, administrative and criminal investigations personnel. Evidence acquired and seized may consist of, but is not limited to, paper documents (records), narcotics, currency, videotapes, audiotapes, digital video reporting, hard drives, and other forms of electronic media.

All data is manually entered on a record-by-record basis by designated DS users using a web-based application framework. Some data elements are also stored in the Investigation Management System (IMS) and are manually replicated during entry to provide reference (e.g., case number, title, subject, crime). The level of sensitivity of the unclassified information accessed, processed, stored and transmitted on DSEPS is sensitive but unclassified (SBU).

(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.

(e) What process is used to determine if the information is accurate?
The DSEPS user interface uses drop menus for item selection, and it extracts specific (minimal) case information from IMS. Some entries are freeform (e.g.; serial numbers, notes, etc.) and can only be verified by the check-in process via the Evidence Custodian(s) or during Supervisor 90 day evidence reviews.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
The system provides the ability to edit or delete all records (with auditing) so that errors can be corrected, with a record of the changes. Property managed by the system is entered into DS custody and requires a confirmation between users, which creates an additional workflow that reinforces data input accuracy.

(g) Does the system use information from commercial sources? Is the information publicly available?
The answer to both questions is "No."

(h) Is notice provided to the individual prior to the collection of his or her information?
Notice of the purpose, use and authority for collection of information submitted is described in the System of Records Notice titled STATE-36, Security Records. Additionally, the publication of this PIA will provide notice of this collection. Any direct notice could hinder DS investigations.

(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?

- If no, why are individuals not allowed to provide consent?
Individuals are not allowed to provide consent because of the nature of the confidentiality needed for DS investigations. The information is collected by DS law enforcement officers in the course of criminal investigations; DS law enforcement officers are authorized to collect the information under the following authorities:
  - 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)

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Privacy concerns influenced information stored in DSEPS by limiting data collection to what is necessary for facilitation of investigations. Privacy concerns also led to ensuring compliance with DS approved information safeguards and procedures.

5. Use of information

(a) What is/are the intended use(s) for the information?
Most of the activities in the system relate to the management of property items: chain of custody and disposition using an internally generated Evidence Control File number which is associated with a Case Number and subjects. This information is used in furtherance of DS investigations regarding the property catalogued in DSEPS.

(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. When evidence is seized in relation to an investigation, it is logged into DSEPS (which replaces paper forms and logbooks) along with information identifying the owner or possessor of the evidence. This information can be used, for example, to track the progress of the case or provide data on related cases.

(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?

(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Printouts, reports, PDF files etc., derived from DSEPS are shared internally (DS Legal and DO Finance), and may be shared with Law Enforcement Agencies (LEA), such as the FBI, as appropriate and legal and following all DS procedures therein.

(b) What information will be shared?
Printouts, reports, etc., derived from DSEPS may be shared with LEAs such as FBI etc. as appropriate and legal.

(c) What is the purpose for sharing the information?
Shared information is used to facilitate processes needed for completing criminal investigations.

(d) The information to be shared is transmitted or disclosed by what methods?
Information derived from DSEPS may be shared with users via paper printouts.

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

Overall, the primary safeguard in place is user training in handling the various data in a legal manager. The reports are labeled with the appropriate classification label for that particular content, which abides by regulation. Those receiving the information within DS and external (e.g. LEAs) are trained to handle the information in a secure manner by legal requirements.

Administratively, audit logs are used to provide accountability of personnel who access DSEPS and all associated activities conducted by that user in the system. These logs are available for management review. Access to DSEPS is limited to authorized users who are trained and held accountable to use the system according to design and policy requirements.

Information shared with external entities is addressed on a case-by-case basis, and the following applies:

(1) Any information that is actually part of an "item" of evidence, the evidence management rules would apply (e.g.; return to owner, destroy and provide destruction certification, etc.)
(2) Any information that is derived from the raw data of the system (reports, etc.) a letter with instructions that when no longer needed, to return to us or destroy and provide proof of destruction.
(3) For sensitive cases, approval would first be obtained from our legal department, and again, a letter would be provided with end of use instructions.

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

As with any system, the concern is the appropriate use of the information contained. Users with access to DSEPS are vetted first to include only trusted persons and reduce the risk of unacceptable behavior. Users are held accountable for activity per DSEPS rules of behavior.

7. Redress and Notification

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

The records contained in DSEPS are exempt from the notification, access, and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(j)(2). Notwithstanding the applicable exemptions, the Bureau of Diplomatic Security will review all such requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the U.S. or activities related to any investigatory material contained within

this system, the applicable exemption may be waived at the discretion of the Bureau of Diplomatic Security, and in accordance with procedures and points of contact published in the system of records notice identified in section 3(f) above, and in rules published at 22 CFR 171.31.

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

☒Yes ☐No

If yes, explain the procedures.

To the extent that material contained in DSEPS is subject to the Privacy Act (5 U.S.C. 552a), individuals can request amendment of material in the system under the procedures set forth in 22 C.F.R. Part 171. This amendment procedure may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Inaccurate or erroneous information in criminal investigative files will only be subject to amendment or correction at the request of the federal law enforcement agency which originated the material.

Procedures for individuals to request correction of their information are published in 22 CFR 171.33. Generally speaking, CFR 171.33 (b) states the following instructions: "Requests to amend records must be in writing and mailed or delivered to the Information and Privacy Coordinator, at the address given in Sec. 171.5, who will coordinate the review of the request with the appropriate offices of the Department. The Department will require verification of personal identity as provided in Sec. 171.32(b) before it will initiate action to amend a record. Amendment requests should contain, as a minimum, identifying information needed to locate the record in question, a description of the specific correction requested, and an explanation of why the existing record is not accurate, relevant, timely, or complete. The requester should submit as much pertinent documentation, other information, and explanation as possible to support the request for amendment."

Sec. 171.5 states the following: "(a) Requests for records in accordance with this chapter may be made by mail addressed to the Information and Privacy Coordinator, U.S. Department of State, SA-2, 515 22nd Street, NW., Washington, DC 20522-6001. Facsimile requests under the FOIA only may be sent to: (202) 261-8579. E-mail requests cannot be accepted at this time. Requesters are urged to indicate clearly on their requests the provision of law under which they are requesting information. This will facilitate the processing of the request by the Department. In any case, the Department will process the request under the provision of law that provides the greatest access to the requested records."

(b) If no, explain why not.

N/A

(c) By what means are individuals notified of the procedures to correct their information?
Because of the nature of this information collection during a law enforcement investigation, this PIA and the respective SORNs serve as notice to individuals. Procedures for notification and redress are published in the system of records notice identified in section 3(f) above, 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?
Access control lists, 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.)

(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 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.

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

Activity by authorized users is monitored, logged, and audited. The business owner, DS/ICI/CR/CIR, approves and authorizes use of the DSEPS 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 3 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. 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 DSEPS components, for changes to the DoS mandated security controls.

The DSEPS system is accessible via OpenNet. In order to access DSEPS, user must first authenticate to OpenNet. The end user account credentials are then matched with system-specific account information. This will provide additional account profile information relevant to DSEPS operation (ex. user access type = field/custodian/supervisor).

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

- PA459, Protecting Personally Identifiable Information (PII)—Mandated in 13 FAM 361, Training Mandatory for Department Employees; FSI distance learning course; one-time mandatory requirement for ALL Department of State Foreign Service (FS) and Civil Service (CS) employees. Locally Employed Staff (LES) who handle PII are also required to take the course. At this time, contractors are NOT required to take this course.
- PS-800, Cyber Security Awareness Course—Available online via the Foreign Service Institute; contains training on handling PII. All users of DoS computer systems are required to pass this course annually.

(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.

The DSEPS system is accessible via OpenNet, so an active OpenNet account is required for DSEPS access. In order to access DSEPS, the user must first authenticate to OpenNet. DSEPS 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 will

provide additional account profile information relevant to DSEPS operation (ex. user access type = field/custodian/supervisor). Local user account information is managed through the application framework.

DSEPS provides three basic user types that can be further refined using the Access Scope tool. These levels have predefined sets of assigned functions. They are the following:

- Field: The "Field" role enables all users to have access to the application.
- Custodian: The "Custodian" role only applies to Evidence Control (EC) level users. This role is granted the "Field" roles privileges in addition to specific functions such as inventory, process, log, and scan functions.
- Supervisor: The privileges granted to the "Supervisor" role are similar to privileges granted to the Custodian role with the exception that the "Supervisor" role is granted to individuals responsible for the supervision of employees.

DSEPS 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.

(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?

DSEPS 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 primary users of the DSEPS are all Special Agents (SAs) and personnel directly involved in support of DS criminal investigations. There are approximately 1,100 registered active users currently in DSEPS.

(b) How is access to data in the system determined?

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.

(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 as managed via the access control lists (ACL) will have access to the system and data. Access is determined by a user's role, so all users don't have access to all data.

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

DSEPS uses role based access controls (RBAC) that limits access to the system to specific job functions that require specific levels of access and must first be approved by management.

The access levels are: (1) user access, (2) discreet access.

Security is based on user access levels, with discreet access control allowed at the web page level.

To further enhance control over misuse, all edits, deletions, and system management actions are tracked through an auditing system. Every action executed is documented, and no records are completely removed from the system.