PRIVACY IMPACT ASSESSMENT

Diplomatic Security Evidence and Property System (DSEPS) PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: December 2022
(b) Name of system: Diplomatic Security Evidence and Property System
(c) System acronym: DSEPS
(d) Bureau: Diplomatic Security (DS)
(e) iMatrix Asset ID Number: 4492
(f) Child systems (if applicable) and iMatrix Asset ID Number: Not Applicable
(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):

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:

DSEPS is used to support the U.S. Department of State, Bureau of Diplomatic Security (DS) investigations by recording the details of seized property items (documents, firearms, currency, etc.;) under the case number identifier. Details recorded in DSEPS include the PII identifying the owner or possessor of the evidence.

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 individuals undergoing investigations (e.g., criminal investigations), which includes Department employees, contractors, members of the U.S. public, and foreign nationals. This information may include:

- Name
- Date of birth
- Home address/ Search warrant location
- Personal Phone Number
- Personal Email Address
- Office Location (ex: Miami, FL; Tucson, AZ) Possible in REMARKS or NOTES but not a dedicated field unless subject to a Search Warrant.

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

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)
- 22 U.S.C. 4802 (Responsibility of Secretary State)

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

☒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):
  June 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):

- **Disposition Authority Number** (e.g., (XX-587-XX-XXX)):
  DAA-0059-2018-0003-0003

- **Length of time the information is retained in the system:**
  Temporary. Cut-off at the end of calendar year of case closure. Destroy 100 year(s) after cutoff.

- **Type of information retained in the system**:
  Other Case and Investigative Files

- **Description**:
  Records documenting a wide range of cases and investigative programs and activities to include, but are not limited to, passport and visa fraud; smuggling; assault; acts of terrorism; counterintelligence and espionage; and workplace allegations of violence, theft, fraud, computer misuse, and substance abuse. Records include, but are not limited to, background, evidence, analysis, reports, interviews, funds, affidavits, subpoenas, warrants, sworn statements, sentencing documents, evidence/property receipts, photos, copies of driver's licenses, birth and death certificates, passports, and other related investigative 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?

Information collected by DSEPS is collected through direct interviews conducted by DS Law Enforcement Investigators, uploading of documents or images, and through DS Law Enforcement investigative and analytical activities. DS Law Enforcement Investigators complete form DS-1857 with record subject information and then manually enter it into DSEPS.

(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?

There are two processes that determine if PII is accurate. First, assigned personnel validate data through cross-checking various U.S. Agencies (federal and state) databases and through interviews. Access to these disparate databases is at each posts' disposal. Second, if, through investigations, assigned personnel find the data in DSEPS is inaccurate, it is the DS Law Enforcement Investigators responsibility to update the PII.

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

Investigators review profiles and update the records as new information is identified. Property managed by the system is entered into DS custody and requires a confirmation between users, which creates an additional workflow that reinforces that data, including PII, is current.

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

No, the system does not use information from commercial sources nor is it publicly available.

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

DSEPS collects PII that is directly relevant and necessary to accomplish the specified purpose(s) and takes measures to reduce the collection and storage of PII. During the requirements analysis phase of the DSEPS design, it was determined that social security number is not required. As such, the application was able to minimize the amount of PII collected to the minimum needed to fulfil the application's function.

5. Use of information

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

The intended use of the PII in DSEPS is related 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 PII 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 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:
DSEPS shares PII with the U.S. Attorney's office and, as part of joint investigation and task forces. It also provides PII to any federal, state, and local authorized law enforcement entities with a need to know.

(b) What information will be shared?

Internal:
There is no internal sharing.

External:
All PII listed in 3d is provided to the U.S. Attorney's office for litigation.

In cases where there is a need-to-know, PII listed in 3d is provided to federal, state, and local authorized law enforcement entities based on the active investigation.

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

Internal:
There is no internal sharing.

External:
The purpose for sharing information with the U.S. Attorney's Office and federal, state, and local authorized law enforcement entities is for investigation and law enforcement purposes.

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

Internal:
There is no internal sharing.

External:
When sharing with the U.S. Attorney's Office and federal, state, and local authorized law enforcement entities, PII is shared via encrypted email or delivered in hard copy.

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

Internal:
There is no internal sharing
External:
All PII provided to the U.S. Attorney's Office and federal, state, and local authorized law enforcement entities is properly marked with the appropriate Classification. PII is shared

via encrypted email. When PII is delivered in hard copy, it is carried in a locked bag as required.

7. Redress and Notification

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

No. Due to the nature of record subjects being involved or associated with criminal allegations and fraudulent activities, the records subjects are not afforded any notice prior to data collection per 5 U.S. Code § 552a (j)(2).

(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?

Due to the nature of record subjects being involved or associated with criminal allegations and fraudulent activities, the record subjects don't provide consent.

(c) What procedures allow record subjects 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, DS 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 security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of DS, 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.

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

☐Yes ☒No

If yes, explain the procedures.

All DSEPS records are associated with criminal investigations. All information pertaining to criminal investigations is excluded from the Privacy Act under 5 U.S.C. § 552a (j)(2). 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.

If no, explain why not.

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

There is no means by which record subjects are notified of the procedures to correct their information due to the fact that DSEPS records are associated with criminal investigations and are excluded from the requirement to provide the procedure as identified in the Privacy Act.

8. Security Controls

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

DSEPS's 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 DSEPS is protected via Oracle TDE encryption.

DSEPS 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. The evidence custodian is responsible for monitoring accounts and deactivating accounts of individuals who no longer need access.

(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).

DSEPS Roles	Description of System Access	PII Access
System Administrators	A limited number of System Administrators have access to the system to conduct standard administrative activities including hardware updates/maintenance, software updates/maintenance, and general troubleshooting. System Administrators have limited access to the application for troubleshooting activities but are not authorized to create files or work cases.	All PII listed in 3d
Developers	A limited number of Developers have access to the system to conduct general troubleshooting activities. Developers have no system administrative privileges. Developers have limited access to the application for troubleshooting activities but are not authorized to create files or work cases.	All PII listed in 3d

End Users	Field: The Field role enables all users to have access to DSEPS. This role is able to access all files they have created. They also have access to files created by other users in which they have been granted access.	All PII listed in 3d
	Custodian: The Custodian role has access to PII associated with cases they have access to.	All PII listed in 3d
	Supervisor: The Supervisor role has access to PII for all cases within their office.	All PII listed in 3d

(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 DSEPS system uses role-based access controls and limits users to specific roles as required to complete their task. The access control lists, which defines 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) How is access to data in the system determined for each role identified above?

All users identified in 8b request access via the AccessDS application. The system Information System Security Officer (ISSO), and their supervisor is included in the approval chain for these privileged accounts.

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

Activity by authorized users is monitored, logged, and audited. The business owner, DS/INV/CR/SIS, approves and authorizes use of the DSEPS system. System accounts are maintained and reviewed on a regular basis.

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.

(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.

Users are required to complete the PS800 Cybersecurity Awareness Training on an annual basis and must acknowledge in place policies by signing user agreements. Users are also required to complete the PA318, Protecting Personally Identifiable Information, biennially.