PRIVACY IMPACT ASSESSMENT

Tactical High Threat Operational Response

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 02/2022
(b) Name of system: Tactical High Threat Operational Response
(c) System acronym: DS THOR
(d) Bureau: Diplomatic Security
(e) iMatrix Asset ID Number: 203353
(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):

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:

Diplomatic Security Tactical High-Threat Operation Response (DS THOR) is a client-server application used by Diplomatic Security to acquire, collect, and maintain records related to crime and criminal and non-criminal identification. The information is used for embassy vetting of existing employees and new (potential) permanent or temporary hires. Existing employees are vetted annually to ensure that workforce integrity is as high as possible and tactical risks are reasonably low.

The information collected within DS THOR is shared externally with law enforcement and intelligence agencies to establish and verify an individual's identity.

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

DS THOR collects PII from non-U.S. persons and U.S. persons. U.S. persons applies to new and existing federal employees, new and existing federal contractors, as well as temporary construction and maintenance workers. DS THOR also collects and maintains the responses received from external agencies. DS THOR collects and stores the following information below:

Information collected on both U.S. persons and non-U.S. persons (used for enrollment)

Biometric Information:

- Fingerprints (Images and templates)
- Iris scans (Images and templates)
- Facial (Images)

Biographic Information**:**

- Applicant's full name
- Gender
- Race
- Hair Color
- Eye Color
- Height
- Weight
- Date of Birth
- Country of Birth
  - Optional: Birth state/province/city village
- Primary Citizenship
- Secondary citizenship
- Occupation

Information collected on U.S. Persons

Passport Information (Mandatory for U.S. Citizens):

- Passport Type

- Surname
- Given Name(s)
- Passport Number
- Issuing Country
- Issuing Authority
- Issuing date and expiration date

Permanent Resident Card (Mandatory for non-Citizens)

- Given name
- Surname
- United States Citizenship and Immigration Services (USCIS) number
- Gender
- Date of Birth
- Card Expiration Date
- Green Card Eligibility Categories

Information collected on Non-U.S. Persons
Passport Information (Optional):

- Passport Type
- Surname
- Given Name(s)
- Passport Number
- Issuing Country
- Issuing Authority
- Issuing date and expiration date

National ID:

- National ID Issuing Country
- National ID Number

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

- The Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended, 22 U.S.C. § 4802, et seq., (Pub. L. 99-399)
- Executive Orders 13488 and 13467, as amended by Executive Order 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters (2017)
- Federal Information Security Act, 5 U.S.C. § 301 (Pub. L. 104-106, Section 5113)

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

☒Yes, provide:

- SORN Name and Number:
    - STATE-31, Human Resources Records
    - STATE-36, Security Records

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
    - July 19, 2013
    - 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):

- Schedule number (e.g., (XX-587-XX-XXX)):
  Please see below table.
- Disposition Authority Number:
- Length of time the information is retained in the system:
- Type of information retained in the system: .

DoS Records Schedule/Disposition Authority Number	Disposition	Description
Other Case and Investigative Files View Details Disp Auth Number: DAA-0059-2018-0003-0003 Applies To: **DS/DO, DS/SI**	Temporary. Cut-off at the end of calendar year of case closure. Destroy 100 year(s) after cutoff.	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 drivers' licenses, birth and death certificates, passports, and other related investigative information
High Profile Case Files View Details Disp Auth Number: DAA-0059-2018-0003-0002 Applies To: **DS/SI, DS/TIA**	Permanent. Cut-off at end of calendar year of case closure. Transfer to the National Archives 25 years after cut-off	Records relating to personnel security and suitability of top echelon officials; reflecting distinctive department activities or attract media or congressional interest; concerning terrorist, criminal and other specific threats or actions taken against diplomats, American citizens, Department personnel, families, facilities or property; or documenting programs that prevent, disrupt and resolve acts of international terrorism.
Personnel Security and Access Clearance Records General Operations Support View Details Disp Auth Number:	Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use. (Supersedes GRS 18, item 22a)	Records of people not issued clearances. Includes case files of applicants not hired. Records about security clearances, and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes: • questionnaires • summaries of reports prepared by the investigating

DAA-GRS-2017-0006-0025 (GRS 5.6, item 181) Applies To: N/A		agency • documentation of agency adjudication process and final determination Note: GRS 3.2, Information Systems Security Records, items 030 and 031, covers Information system access records. Exclusion: Copies of investigative reports covered in items 170 and 171. Disp Auth Number: DAA-GRS-2017-0006-0025 (GRS 5.6, item 181) Applies To: All
Intermediary Records General Operations Support View Details Disp Auth Number: DAA-GRS-2017-0003-0002 (GRS 5.2, item 020) Applies To: All	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)	Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record. To qualify as an intermediary record, the record must also not be required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Records include: • non-substantive working files: collected and created materials not coordinated or disseminated outside the unit of origin that do not contain information documenting significant policy development, action, or decision making. These working papers do not result directly in a final product or an approved finished report. Included are such materials as rough notes and calculations and preliminary drafts produced solely for proof reading or internal discussion, reference, or consultation, and associated transmittals, notes, reference, and background materials. • audio and video recordings of meetings that have been fully transcribed or that were created explicitly for the purpose of creating detailed meeting minutes (once the minutes are created) • dictation recordings • input or source records, which agencies create in the routine process of creating, maintaining, updating, or using electronic information systems and which have no value beyond the input or output transaction: o hardcopy input source documents where all

		information on the document is incorporated in an electronic system (See Exclusion 1 and Note 1) o electronic input source records such as transaction files or intermediate input/output files • ad hoc reports, including queries on electronic systems, whether used for one-time reference or to create a subsequent report • data files output from electronic systems, created for the purpose of information sharing or reference (see Exclusion 2) Exclusion 1: This item does not allow destruction of original hardcopy still pictures, graphic materials or posters, aerial film, maps, plans, charts, sound recordings, motion picture film, or video recordings once they are digitized. Agencies must follow agency-specific schedules for these records. If the records are unscheduled, the agency must submit a schedule for them. Exclusion 2: This item does not include the following data output files (agencies must follow agency-specific schedules for these records, except for the final bullet, which the GRS covers in another schedule): • files created only for public access purposes • summarized information from unscheduled electronic records or inaccessible permanent records • data extracts produced by a process that results in the content of the file being significantly different from the source records. In other words, the process effectively creates a new database file significantly different from the original • data extracts containing Personally Identifiable Information (PII). Such records require additional tracking and fall under GRS 4.2, item 130 (DAA-GRS-2013-0007-0012) Note 1: An agency must submit a notification to NARA per 36 CFR 1225.24(a)(1) prior to destroying hardcopy input records previously scheduled as permanent. An agency must schedule the electronic version of unscheduled hardcopy input records prior to destroying the input record. Legal citations: 36 CFR 1225.22 (h)(2); 36 CFR 1225.24 (a)(1)

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?

All data are gathered via a locally created advisory statement and then entered/uploaded into DS THOR, through a desktop client interface (thick client computer) and a generic external biometric capture device by authorized individuals called enrollers. The advisory statement informs the enrollee and the enroller of the PII required by DS THOR. Enrollers are authorized personnel using DS THOR to enter information about enrollees e.g., a Foreign Service National Investigator (FSNI). The enroller facilitates one enrollment at a time and sends it to the server. Data are sent to the server in a format called an Electronic Fingerprint Transaction (EFT) file, which contains all DS THOR PII. The data sent to the server are deleted once the transmission is completed and are not retained on the desktop client.

The EFT contains data that adhere to the Electronic Biometric Transmission Specification (EBTS) standards, which were created for national security, federal, state, and local law enforcement. EBTS defines the composition of the data that agencies must adhere to when electronically encoding and transmitting biometric image, identification, and arrest data.

Additionally, a system called DS PASS is used in Iraq to gather the required biographic information, which is downloaded into DS THOR. DS THOR does not send or share data to DS PASS.

(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?

At the discretion of the Regional Security Officer (RSO) data are gathered using a locally created advisory statement (initial documentation and identification credentials) and then are entered/uploaded into DS THOR, through a desktop client interface (thick client computer) and a generic external biometric capture device by authorized individuals called enrollers. The enrollers review the advisory statements and validate the required information against proper identification (i.e., embassy badging or national identification card) to check for accuracy. Any changes to biographical data thereafter will require a new enrollment of the individual.

In addition, DS THOR has built-in data validation controls to include validity checks to ensure all mandatory information has been collected before completion. Sequence and quality checking are conducted against the biometric data collected to ensure proper fingerprints have been collected and the quality of iris/fingerprint data is compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-76, and Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011 NIST SP 500-290.

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

The biographical and biometric information collected from a record subject is used for identity verification via DS THOR and is current at the time the information is obtained during each encounter. An "encounter" is each occurrence when the record subject's information needs to be obtained for identity verification. After the initial encounter, encounters happen on a yearly basis. All information collected is current at the time of each encounter and is updated only during subsequent encounters.

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

The information used for the system is not from commercial sources. The information contained is not publicly available.

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

During the requirements analysis phase of the system, it was determined that DS THOR would use the minimum amount of PII required to fulfill the system's function. The only PII collected are the minimum necessary data points to identify individuals and their respective unique characteristics and attributes to facilitate embassy/consulate employee vetting for access.

5. Use of information

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

PII collected via DS THOR is used by authorized individuals to facilitate access, follow established vetting processes, and in support of existing law enforcement and investigative efforts. DS THOR is used to record information for fingerprint matching, iris matching, and other searches to verify the identity of individuals in a non-criminal investigation.

Individuals' personal and biometric information is shared externally with law enforcement and intelligence agencies. Once the information is shared, it is matched against data repositories to establish or verify the identity of the individual processed in DS THOR. Law enforcement and intelligence agencies return results to authorized users.

(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 use of PII is highly relevant to the functionality of DS THOR because the system exists to facilitate identity assurance and investigative activities that involve screening persons of interest. To support these efforts, PII is collected as a part of conducting internal biometric matching requests for the Department of State and external biometric matching requests such as those submitted to Department of Defense (DoD), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) to facilitate embassy/consulate employee vetting.

(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?

The collected biometric data undergoes a biometric matching process, which is supported by DS THOR. The collected biometric information (iris scans and fingerprints) is compared via algorithm against the biometric template datastore.

(2) Does the analysis result in new information?

Yes, the biometric matching results in a pool of match candidates that supports the verification of individuals and a consolidation of any derogatory information (DEROG) that may exist.

(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:

DS THOR shares information externally with:

- Department of Defense (DoD) – DoD Automated Biometric Identification System (ABIS)
- Department of Homeland Security (DHS) – Automated Biometric Identification System (IDENT)
- Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division - Integrated Automated Fingerprint Identification System (IAFIS)

(b) What information will be shared?

Internal:
There is no internal sharing.

External:

All external systems are forwarded the Electronic Fingerprint Transaction (EFT) file which contains all DS THOR PII indicated in 3(d).

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

Internal:
There is no internal sharing.

External:

The purpose for sharing DS THOR data with all external agencies in 6a is to establish and verify a person's identity. Upon verifying a person's identity, DS THOR facilitates checking for a subject's known associated DEROG, which is the negative information about the subject e.g., criminal charges, criminal infractions, suspicious behaviors, associated with terrorists etc. Externally sharing the information collected helps to increase the accuracy of the subject's identity, by checking the larger community of other law enforcement agencies, and entities that support national security. A broader search allows for a more comprehensive identity validation to reducing risks. After identifying possible matches, info goes to a biometric analyst and an adjudication is conducted.

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

Internal:

There is no internal sharing.

External:

Information is shared externally via secure e-mailing of the EFT. The EFT is a trusted method used to transmit or disclose identity history, biographic, and criminal or non-criminal identification by external law enforcement agencies.

The EFT contains data that adheres to the EBTS standards. EBTS defines the composition of the data that agencies must adhere to when electronically encoding and transmitting biometric image, identification, and arrest data.

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

Internal:

There is no internal sharing.

External:

A Memorandum of Understanding (MOU) between DS bureau, DoD, and FBI was signed in 2013. The MOU defines the responsibilities and requirements for each entity that includes, but is not limited to: Trusted Behavior Expectations, User Community, Access Controls, Audit Trail Responsibility, Data Ownership, Security Parameters, Incident Handling and Reporting, Antivirus and Security Training and Awareness.

The information collected is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

Safeguards:

- EFTs (protected by encryption)

- Database (protected by encryption)
- Data in Transit is protected using Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security 1.2

7. Redress and Notification

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

U.S. person enrollees are informed via a local advisory statement of their rights for redress and notification by the enroller during the enrollment process.

(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?

The enroller works with the enrollee to gather data, which is entered/uploaded into DS THOR, through a desktop client interface and a generic external biometric capture device by authorized individuals as part of their official duties. All data are gathered via a locally created advisory statement and then are entered/uploaded into DS THOR. Consent is obtained when the enrollee agrees to provide the necessary PII and consents to its submission. Without this information the required background checks cannot be completed, and the enrollee will not be able to be hired for employment.

If no, why are record subjects not allowed to provide consent?

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

DS THOR contains Privacy Act-covered records. Notifications and redress are, therefore, rights of record subjects. Procedures for notification and redress are published in the Privacy Act System of Records Notices (SORNs) STATE-31 and STATE-36, and in rules published at 22 CFR 171.20-26 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.20-26.

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

☒Yes ☐No

If yes, explain the procedures.

To the extent that material contained in DS THOR is subject to the Privacy Act (5 USC 552a), individuals can request amendment of material in the system under procedures set forth in STATE-36. This amendment procedure is limited to information on non-criminal investigations. All information pertaining to criminal investigations is excluded from the Privacy Act under 5 USC 552a (j)(2). Inaccurate or erroneous information in DS THOR 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?

The mechanism for requesting correction of information is specified in State-36 and 22 CFR 171.20-6. 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 all of the information in the system secured?

Access controls are in place for the back-end SQL database, which are based upon role-based permissions configured for “least privilege”. The review process establishes segregation of duties for the application. Authentication to the application is established via windows authentication using single sign-on via OpenNet. Once a user logs into OpenNet and is authenticated, the end user is granted access to the DS THOR system.

(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).

DS THOR User Role	System Access Description	Potential Type of PII
Enroller	Basic access to thick client with “entry only” access, which allows the person to enter biometric and biographic data into the system for the enrollment listed in Section 3d. Once they submit the information, it is not retained on their system.	All listed in 3d, however, the system does not let them search on or retrieve this type of data. This is point of entry only. The

		system provides only empty fields to facilitate the collection of information about the enrollee. After the enrollment data collection is complete, they have no persistent access to this data.
Enrollment Data Reviewer (limited to individual posts)	Read only view of a simplified set of enrollment data for all enrollment data collections only at their post.	Passport Information • Citizenship Status • Applicant's full name • Date of birth • Country or place of birth • Country of Citizenship • Gender • General Identity Information • National identification numbers • Global Unique Identifier (GUID) • Physical description (hair and eye color, height and weight) • Race • Office of employment
RSO Staff	Full data view for their post. Write access to some data for their post only.	All listed in 3d
Watchdesk Officer	Global read access. No write access.	All listed in 3d
Biometric Analyst	E.g., Counterintelligence and Counterterrorism Vetting Division (CCV), has full read access and applicable write access to all posts	All listed in 3d
User Admin	Access to create, modify, and expire user accounts except for their own. This role does not have data access.	None
System Admin	Access to perform configuration and maintenance to the application as a whole. This role does not have data access.	None

Data Admin	Read only access to all data. Only role able to delete data entries, which are audited. Data admins work on troubleshooting and general maintenance of the data through the graphical user interface.	All listed in 3d

The system administrator is not a role within DS THOR (*Note*. In DS THOR this is not the same as "System Admin"). The system administrator has access to the DS THOR servers and its file system data stores. The database administrator (DBA) is a system administrator that has access to administer the SQL Server instance that hosts the DS THOR databases. DBAs have access to all the data in the DS THOR databases to ensure they are functionally properly, but do not manage the data.

(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.

DS ACCESS is the user account request and access system used to request access to DS THOR. Based on job role, access is requested and approved by the supervisor and/or the Regional Security Officer (RSO). The table below summarizes DS THOR roles, type of system access, and type of data access in the system. The RSO assigns roles to users as needed.

DS THOR Application Roles	Type of System Access	Type of Data Access
Enroller (DS Agent, FSN, Cleared U.S. citizen staff at post not in one of the other roles, investigator, analyst)	Thick client Data Entry Only	• Sees PII for persons they specifically are processing
Enrollment Data Reviewer (FSN, Cleared U.S. citizen staff at post not in one of the other roles)	Web client	• Read only enrollment data • Post restricted • Sees the PII that all enrollers at the same post sees
RSO Staff (DS Agent) • Cleared U.S. citizen only	Web client	• Read – enrollment and responses • Write – comments (RSO data) • Modify – comments (RSO data) • No delete access • View and modify data to facilitate operations that may contain PII • Post restricted • See the PII that Enrollment Data Reviewers see, RSO data (e.g. data entered by other RSOs at post and the responses)

Watchdesk Officer (Investigator) • Cleared U.S. citizen and headquarter staff	Web client	• Read access to all data within the DS THOR • Able to see all data data form RSOs, but in read only format
Biometric Analyst (Analyst) • Cleared U.S. citizen and headquarter staff	Web client	• Must be in the Program Office • Global role that requires special approval • Read access to enrollment and responses • View and modify data to facilitate operations that may contain PII • Access • Able to see all data from RSOs • Able to edit data that is eligible (e.g., data about encounters is not eligible)
Data Admin (Cleared U.S. citizen, Administrator, CTO roles)	Web client	• Read and Access delete access to all data • Same data access as Watchdesk officer, but with the ability to delete • Access to data is only for troubleshooting purposes
User Admin (Cleared U.S. citizen, Administrator, CTO roles)	Web client	• No data access, cannot see PII
System Admin (Cleared U.S. citizen, Administrator, CTO roles)	Web client	• No data access, cannot see PII

Access to the DS THOR application is restricted to Department of State employees and contractors as noted in the completed and approved Network Access Request (NAR) form.

The application and database administrators are the only users with elevated privileged access to the database, and only for express purposes of troubleshooting and performing routine maintenance. Additionally, all access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. System accounts are maintained and reviewed on a regular basis. The following Department policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies Apply to Web servers)
- 12 FAM 623.2-1 Access Controls

DS THOR 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 determines and 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. 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 DS THOR components, for changes to the Department's mandated security controls.

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

Access to the DS THOR Client and Portal is limited to authorized Department of State users that have a justified need to access the information to perform official duties.

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

The application is placed behind a virtual firewall to further limit access to system data. Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Activity by authorized users is monitored, logged, and audited. DS THOR has built in system audit trails that are automatically generated and regularly analyzed and reviewed to deter and detect unauthorized access. Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

(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.

Department users are required to attend a security briefing before access to Department systems is granted. This briefing also includes privacy orientation. Users are also required to complete PS 800 Cybersecurity Awareness Training, which includes a privacy component, on an annual basis and must acknowledge in place policies by signing user agreements. Users are also required to complete the FSI course PA318, Protecting Personally Identifiable Information, biannually.

System administrators and privileged users are required to complete a separate security awareness briefing provided by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding and Rules of Behavior statement. The ISSO awareness briefing includes a privacy component.