Tactical High Threat Operational Response

1. Contact Information

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

2. System Information

(a) Name of system: Tactical High Threat Operational Response
(b) Bureau: Diplomatic Security
(c) System acronym: DS THOR
(d) iMatrix Asset ID Number: 203353
(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):
   DS THOR currently does not collect or maintain any PII of U.S. Persons and is limited to collecting and maintaining data of foreign nationals. We are updating this PIA to reflect the collection and maintenance of PII of U.S. Persons both Outside Contiguous United States (OCONUS) and in the Contiguous United States (CONUS) by this system.

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?
   DS THOR has authorization to operate (ATO) until May 30, 2019. Any significant changes to the system will be reviewed for their effect on the ATO.

(c) Describe the purpose of the system:
   Diplomatic Security Tactical High-Threat Operation Response (THOR) is a client-server application used by Diplomatic Security to acquire, collect and maintain identification, criminal identification, crime and other records. The information collected within DS THOR is shared externally with various law enforcement and intelligence agencies to establish and verify an individual’s identity.
DS THOR is responsible for the collection of biographical and biometric information (such as fingerprints, irises and images for facial recognition) of an individual and the submission of the information collected.

The information collected within THOR is shared internally within the Department of State to facilitate base access, for established vetting processes, and in support of existing law enforcement and investigative efforts.

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

DS THOR collects and stores the following information:

- Applicant’s full name
- Date of birth
- Country or place of birth
- Country of Citizenship
- Gender
- Physical description (hair and eye color, height and weight)
- Passport number
- Race
- Global Unique Identifier (GUID)
- Telephone numbers
- Email Address
- Office of employment
- Social Security Number or other national identification numbers
- Driver’s license number
- Biometric data: Fingerprints, Irises and facial templates/images.

However, as PII collected from non-U.S. citizens is not covered by the provisions of the Privacy Act and the E-Government Act, the remainder of this PIA addresses the PII collected and maintained by DS THOR on U.S. persons only. DS THOR also collects and maintains the responses received from external agencies.

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


Additional authorities are as follows:
- 26 Code of Federal Regulations (CFR) 601.017, Criminal Investigation Functions, April 1, 2007

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

☒ Yes, provide:
- SORN Name and Number: See Below
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): See Below

  - STATE-31, Human Resources Records, July 19, 2013

☐ 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)): See Below
- Length of time the information is retained in the system: See Below
- Type of information retained in the system: See Below

<table>
<thead>
<tr>
<th>Schedule Number</th>
<th>Length of Time</th>
<th>Type of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-11-012-01 Criminal Investigative Case Files</td>
<td>Disposition: TEMPORARY. Cut off after case closes. Retire to RSC 10 years after closure for transfer to WNRC. Destroy 30 years after case closes.</td>
<td>Description: Headquarters, Field Offices and Overseas Files. 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 consists of correspondence, reports, funds spent/received information, affidavits, subpoenas, search/arrest warrants, sworn statements, sentencing documents, evidence/property receipts, photos, copies of drivers licenses, birth and death certificates, passports, and other related documentation. Note that materials gathered during the execution of a search warrant may be in in these files.</td>
</tr>
<tr>
<td>A-11-025-01a Threat - Case Files - Contains correspondence, reports and other</td>
<td>Disposition: PERMANENT. Retire to the Records Service Center</td>
<td>Description: a. Cases concerning diplomats, American citizens, Department personnel or families, Department facilities or property, and cases of an unusual nature.</td>
</tr>
<tr>
<td>Documentation on terrorist, criminal, and other specific threats or actions taken against individuals or property. Arranged by country.</td>
<td>(RSC) when no longer needed for use in the office. Transfer to the Washington National Record Center 1 year after received by the RSC. Transfer to the National Archives when 25 years old in a format acceptable at that time.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>A-11-025-01b Threat - Case Files - Contains correspondence, reports and other documentation on terrorist, criminal, and other specific threats or actions taken against individuals or property. Arranged by country.</strong></td>
<td>Disposition: Destroy/delete when 10 years old.</td>
<td>Description: b. All other cases.</td>
</tr>
<tr>
<td><strong>A-11-027-01a DOS Clearance System</strong></td>
<td>Disposition: N/A</td>
<td>The DOS Clearance System (DOSC) is the personnel security and suitability processing system and archive. The DOSC contains the security and suitability case files with their associated forms, reports, analysis, memoranda, worksheets, authorizations, etc. It tracks the various processing steps and activities involved with investigations and the determinations made regarding security clearances, public trust certifications and suitability. The system covers the entire process and interfaces with other external databases for information.</td>
</tr>
<tr>
<td><strong>A-11-027-01a(4) Department of State Personnel Security Master Case File</strong></td>
<td>Disposition: Temporary. If not hired, destroy when 7 years old. If hired, transfer to employee files.</td>
<td>Description: Applicant Files (1) Security Clearance granted. [Supersedes N1-059-94-43, item 81b (1) (A-11-004-31(b))]</td>
</tr>
<tr>
<td><strong>A-11-027-01a(5) Department of State Personnel Security Master Case File</strong></td>
<td>Disposition: Temporary. Destroy when 7 years old.</td>
<td>Description: Applicant Files (2) Security Clearance or other requested access NOT granted.</td>
</tr>
</tbody>
</table>
| B-08-002-01a(2) Local Personnel Investigative Files | Disposition: Destroy three years after termination of employment. | Description: This covers both Department of State Non-American employees and other U.S. Government agency Non-American employees - when post security office conducts investigation.

a. Locals who were certified for employment.

(2) Regional Security Office copy. |
|---|---|---|
| B-08-002-01b(2) Local Personnel Investigative Files | Disposition: Note card and destroy. | Description: b. Locals who were refused certification for employment on the basis of information of record.

(2) Regional Security Office copy. |
| B-08-002-01c(2)(a) Local Personnel Investigative Files | Disposition: Destroy when 5 years old. | Description: c. Locals who were investigated, but who abandoned their application.

(2) Regional Security Office copy.

(a) File containing derogatory information. |
| B-08-002-01c(2)(b) Local Personnel Investigative Files | Disposition: Destroy when 1 year old. | Description: c. Locals who were investigated, but who abandoned their application.

(2) Regional Security Office copy. |
| B-08-002-01d(2) Local Personnel Investigative Files | Disposition: Destroy 5 years after termination, except for certain reporting required by security regulations | Description: d. Locals and local applicants who were terminated for cause.

(2) Regional Security Office copy. |
| B-08-002-03a Security Case Files | Disposition: Card and destroy 1 year after case is closed. | Description: Security investigative files involving attempted penetration, fraud, loss of diplomatic pouches, and other cases not pertaining to investigations of individuals who are or may be employed by the Department or other Federal agencies. The record copies of these cases are retained by the Office of Security. |
| B-08-002-03b Security Case Files | Disposition: Permanent. Retire to RSC one year after case has been closed | Description: Case files involving terrorist groups, unsolved or significant murders, or special events. Contains information from |
or designated inactive. Transfer to WRNC when 5 years old. Transfer to NARA when 30 years old.

newspaper clippings, reports, correspondence with local authorities, cables, etc.

<table>
<thead>
<tr>
<th>B-08-002-04 Security Investigation Case Files - Foreign Nationals, escapees, exchanges, refugees, and visa applicants</th>
<th>Disposition: Cut off when case is closed and reported to the Department, requesting post, or other agency. Destroy case 1 year after cut-off date.</th>
<th>Description: Security investigation case files conducted for the Department, other posts, and other agencies. Correspondence, reports, and other documentation on security investigations conducted at the request of the Department, other posts, or other agencies in order to determine eligibility of escapes, refugees, and other foreign nationals for assistance, employment, exchange programs, or visas covering: criminal investigations, law enforcement agencies, offenses, visa fraud, and other related subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-08-002-05b Security Investigation Card Files</td>
<td>Disposition: Destroy 20 years after transfer to the inactive file</td>
<td>Description: Regional Security Office - Card files on security investigations conducted at post. Cards record basic data on cases of: Foreign Service Nationals certified for employment, including initial and subsequent investigations; Foreign Nationals refused employment; Foreign Nationals who abandoned an employment application after the security investigation was conducted; U.S. Government employees for whom overseas investigation is required; Non-American citizens being investigated for employment elsewhere, for a visa or other assistance, or for participation in an exchange program; Individuals involved in incidents such as attempted penetration, fraud, or loss of diplomatic pouches.</td>
</tr>
</tbody>
</table>

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒ Yes  ☐ No

- If yes, under what authorization?
(c) How is the information collected?
  Authorized individuals obtain biometric (fingerprints, irises and facial images) data using fingerprint and iris/facial capture devices. The biographical information is entered by the authorized individual. All data entered/uploaded into DS THOR by authorized individuals is part of their official duties.
(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?
  Authorized Personnel will review the initial documentation and identification forms provided to them and validate against proper identification (i.e., embassy badging or national identification card). Any changes to biographical data thereafter will require a new enrollment of the individual, if authorized personnel wish to resubmit the information.

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 checking and quality 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.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
  The biographical information is as current as the information received from the data source. All biometric information that is collected is current as of the collection.
(g) Does the system use information from commercial sources? Is the information publicly available?
  N/A
(h) Is notice provided to the individual prior to the collection of his or her information?
  Yes, both civil and criminal subjects are notified prior to the collection of his or her information.
(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?
  Civil applicants may decline to submit biometric and biographical data; however the background check is often a prerequisite for employment.
- If no, why are individuals not allowed to provide consent?
  Criminal subjects are under lawful criminal supervision or investigation.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The collection of PII is limited to the required components of a civil and criminal investigation.

5. Use of information

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

DS THOR is used by authorized individuals to facilitate base access, for 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 civil or criminal investigation.

An individual’s personal and biometric information is collected and shared internally with other Department of State applications as well as 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 THOR. Law enforcement and intelligence agencies return results to authorized users.

Data can be retrieved in DS THOR by keyword searches, such as applicant name, global unique identifier (GUID), transaction control number (TCN).

(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. It was designed for identity assurance and investigative purposes.

(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?
Authorized DS agents, investigators and analysts are able to retrieve data based on text queries. All related data is maintained in the DS THOR system in order to provide a centrally indexed repository.

(2) Does the analysis result in new information?
Yes, the analysis can result in new information about the individual based upon the results that are returned from external agencies. Individual’s records can be updated to reflect the findings of the investigation.

(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.

Internally, DS THOR may share information with Department of State systems and
offices with criminal, investigative and intelligence responsibilities. This includes but is
not limited to:

- Identity Management System (IDMS)
- DS Post Applicant Submission System (DS PASS)
- Supplemental Authentication & Monitoring (SAM)

Externally the information may be shared with:

- A Federal, State, or local agency, or other appropriate entities or individuals, or
  through established liaison channels to selected foreign governments, in order to
  enable an intelligence agency to carry out its responsibilities under the National
  Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive
  Order 12333 or any successor order, applicable national security directives, or
  classified implementing procedures approved by the Attorney General and
  promulgated pursuant to such statutes, orders or directives.

That includes but is not limited to:

- Department of Homeland Security (DHS)
- Department of Defense (DoD)
- Department of Justice (DoJ)
- Other agencies and entities involved in national security; U.S. border
  security, official government business or federal law enforcement

(b) What information will be shared?

Electronic Biometric transmission (EBT) files contain all information collected within the
system defined in Section 3d of this document. DS THOR shares an EBT file with all
internal or external agencies defined in Section 6a of this document.

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

The purpose for sharing the information collected within DS THOR is to establish and
verify a person’s identity.

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

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

All external agencies that share information with DS THOR are required to sign an MOU or MOA, which generally define a set of responsibilities and requirements. Items generally covered in an MOU or MOA include but are 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.

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

The privacy concerns are with regard to the collection of PII that is used for employee screening and support for criminal investigations. These concerns are addressed by identifying the likelihood the information is disseminated to unapproved external entities. In the case of DS THOR, only authorized personnel will have access and the network the application rests upon is configured to comply with DS-approved network safeguards.

7. Redress and Notification

(a) **What procedures allow individuals 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 Notice (SORN) STATE-31 and STATE-36, and in rules published at 22 CFR 171.31 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 171.32.

(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 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 available only 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.

(c) By what means are individuals notified of the procedures to correct their information?
The mechanism for requesting correction of information is specified in State SORN 36, 22 C.F.R. Part 171. 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 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) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.
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 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 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 DS THOR components, for changes to the DoS mandated security controls.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
DS THOR is monitored by inherited security controls of the OpenNet general support system. Controls built into OpenNet include routers and Network Intrusion Detection System (NIDS). These controls provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties. In addition, the application is placed behind a virtual firewall to further limit access to system data. Additionally, DS THOR has built in system audit trails that are automatically generated and regularly analyzed and reviewed to deter and detect unauthorized access.

(d) Explain the privacy training provided to authorized users of the system.
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 Cybersecurity Awareness Training on an annual basis and must acknowledge in place policies by signing user agreements. 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.

(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.
Because PII is present in the application, FIPS 140-2 encryption is in place for all sessions. Users are only allowed access to data required for their particular task.

(f) How were the security measures above influenced by the type of information collected?
The DS THOR application system is categorized as a “High” risk system in accordance with FIPS 199. In light of this, NIST SP 800-53, Rev. 4 “High” security controls were applied in accordance with OMB to ensure the security of the application as a whole, including the protection of PII.

9. Data Access

(a) Who has access to data in the system?
Access to the THOR Client is limited to authorized Department of State users that have a justified need to access the information. The installation of the THOR Client is limited to machines that have been identified to be used by authorized individuals. Access to the
THOR Portal is role-based and response handling is limited to cleared DS agents, investigators and analysts.

(b) How is access to data in the system determined?
Access to the THOR Client and Portal is limited to authorized Department of State users that have a justified need to access the information in order to perform official duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
DS THOR data is role-based and configured with the SQL database. All users will not have access to all data within the system. PII is restricted to authorized personnel. Users are only allowed to access data required to complete particular tasks. Response handling is restricted to cleared DS agents, investigators, and analysts.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
Role based access control is in place to prevent the misuse of data by users who have access to the data. The role based access is configured for “least privilege”, which establishes separation of duties (e.g. IT personnel have limited access to enrollment data). In addition, DS THOR has built in system audit trails that are automatically generated to deter and detect the misuse of data by authorized users.