PRIVACY IMPACT ASSESSMENT

Diplomatic Security – Training Management System

1. Contact Information

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

2. System Information

(a) Name of System: Diplomatic Security – Training Management System
(b) Bureau: DS
(c) System Acronym: DS-TMS
(d) iMatrix Asset ID Number: 272773
(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): Not Applicable (N/A)

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?

The DS-TMS application is currently operational and under a conditional one (1) year ATO that expires on 4/30/2021. The Assessment and Authorization (A&A) process is in RMF Step 4 with an estimated completion date of March 2021.

(c) Describe the purpose of the system:

The Diplomatic Security-Training Management System (DS-TMS) is a cloud-based application that provides robust tracking of budgets, training, projects, and resources resulting in better management visibility. DS-TMS focuses on the four (4) key elements of training courses: (1) Training Development and Execution; (2) Budgeting; (3) Workflows; and (4) Logistics and Inventory.

(d) Describe the Personally Identifiable Information (PII) that the system collects, uses, maintains, or disseminates:

There are two (2) groups of individuals from whom PII is collected, used, maintained, and/or disseminated by the DS-TMS application.

(1) *DS/T/FASTC Employees and Instructors* are U.S. citizens who have access to the DS-TMS application:

- First Name
- Last Name
- Business Contact Information (Work Email, Work Phone Number, Work Address, Work Title)
- Personal Phone Number
- Personal Email Address
- Personal Address
- Date of Birth
- Social Security Number
- Substantive Individual Personnel Information
  - Gender
  - County
  - Driver's License Number
  - Driver's License State
  - Emergency Contact Name
  - Emergency Contact Phone
  - Emergency Contact Alternate Phone
  - Emergency Contact Address
  - Emergency Contact City
  - Emergency Contact State
  - Emergency Contact Zip Code
  - Sending Organization (or Sponsor)
  - Training Category
  - Dietary Restrictions
  - Health/Medical/Vision Issues
  - Non-Housing Accommodations
  - Date and Time Only for Last Medical Screening
  - Date and Time Only for Last Suitability Check.
- Substantive Individual Educational Information:
  - Date and Time Only for Certifications and Qualifications
  - Professional Licenses

Employee and Instructor roles include: Program Managers, System Administrators, and Accreditation & Evaluation, Course Coordinator, Division Chief, Facilities Manager, Facility Scheduler, Firearms Scheduling, Fleet Management, Instructional Designer, LMS Manager, Mobile Device Manager, Multimedia/Programming Specialist, Office Director (FASTC), Registrar, Resource Manager (DS/T), Resource Manager (FASTC), SECD Instructor, Special Assistant (FASTC), System Security Consultant, Visitor (Envisage), and Visitor (FASTC).

(2) *Students* are U.S. citizens and non-U.S. citizens. Students <u>do not</u> have access to the DS-TMS application:

- First Name
- Last Name
- Gender

- Date of Birth

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

The legal authorities are as documented in State-36 regarding Security Records:

- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. § 4802,as amended"); and
- Foreign Assistance Act, 22 USC § 2349aa et. seq.

(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): 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 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)):

Schedule Number	Schedule Title	Schedule Disposition Number
A-11-008-12	Training Activities Support File	N1-059-07-01, Item 20b
A-11-009-14	Curriculum Development Records	N1-059-07-01, Item 1
A-11-009-15	Curriculum Review Records	N1-059-07-01, Item 2
A-11-009-16	Course Execution Records	N1-059-07-01, Item 3
A-11-009-17	Course Evaluation Records	N1-059-07-01, Item 4
A-11-009-18	Class Records	N1-059-07-01, Item 5
A-11-009-19	Student Training Records	N1-059-07-01, Item 6
A-11-009-20	Course Administrative Records	N1-059-07-01, Item 7
A-11-009-21	Department of State Staff Training Records	N1-059-07-01, Item 8
A-11-009-22	Training Policy and Procedures Records	N1-059-07-01, Item 9
A-11-009-23	Accreditation Records	N1-059-07-01, Item 10
A-11-009-32a	Reports Files - Registrar	N1-059-07-01, Item 19a
A-11-009-32b	Reports Files - Registrar	N1-059-07-01, Item 19b

Schedule Number	Schedule Title	Schedule Disposition Number
A-11-009-33a	Course Files - Register	N1-059-07-01, Item 20a
A-11-009-33b	Course Files - Register	N1-059-07-01, Item 20b
A-03-005-05	Intermediary Records	DAA-GRS-2017-003-0002 (GRS 5.2, Item 020)

- Length of time the information is retained in the system:

Schedule Number	Schedule Disposition Number	Length of Time Information is Retained
A-11-008-12	N1-059-07-01, Item 20b	TEMPORARY: Destroy five (5) years after departure from Department of State.
A-11-009-14	N1-059-07-01, Item 1	TEMPORARY: Cut-off file upon conclusion of first course review, which is conducted after 5 (five) years. Retain original course development materials for 5 (five) years after cut-off and destroy (Supersedes N1-059-94-43, Items 94a and 97a).
A-11-009-15	N1-059-07-01, Item 2	TEMPORARY: Cut-off file upon conclusion of a subsequent course review, which is conducted after 5 (five) years. Retain Curriculum Review materials for 5 (five) years after cut-off and destroy.
A-11-009-16	N1-059-07-01, Item 3	TEMPORARY: Cut-off file when course is discontinued. Destroy 10 (ten) years after cut-off (Supersedes N1-059-94-43, Items 94b, 97b, and 2(a)).
A-11-009-17	N1-059-07-01, Item 4	TEMPORARY: Cut-off file upon completion of a scheduled course review, which is after 5 (five) years. Destroy 1 (one) year after cut-off.
A-11-009-18	N1-059-07-01, Item 5	TEMPORARY: File materials at the conclusion of each class. Cut-off file upon completion of a course review, which is after 5 (five) years. Materials for 10 (ten) years after cut-off and destroy (Supersedes N1-059-94-43, Item 100).
A-11-009-19	N1-059-07-01, Item 6	TEMPORARY: Cut-off file at termination of employment with Department. Retire 1 (one) year after cut-off date. Destroy 5 (five) years after cut-off date (Supersedes N1-059-94-43, Item 99).
A-11-009-20	N1-059-07-01, Item 7	TEMPORARY: Cut-off file at the end of each calendar year. Destroy when 2 (two) years old or when no longer needed, whichever is sooner.
A-11-009-21	N1-059-07-01, Item 8	TEMPORARY: Destroy 5 (five) years after departure from assignment within Department of State.
A-11-009-22	N1-059-07-01, Item 9	TEMPORARY: Cut-off at the end of each calendar year. Retire 5 (five) years after cut-off date. Destroy when 30 (thirty) years old.

Schedule Number	Schedule Disposition Number	Length of Time Information is Retained
A-11-009-23	N1-059-07-01, Item 10	TEMPORARY: Cu- off at the end of each calendar year. Retire 5 (five) years after cut-off date. Destroy when 30 (thirty) years old.
A-11-009-32a	N1-059-07-01, Item 19a	TEMPORARY: Destroy when 20 (twenty) years old or when superseded, whichever is later.
A-11-009-32b	N1-059-07-01, Item 19b	TEMPORARY: Destroy/delete within 180 (one hundred and eighty) days after recordkeeping copy has been produced.
A-11-009-33a	N1-059-07-01, Item 20a	TEMPORARY: Retire to records storage center when 1 (one) year old. Destroy when 5 (five) years old (Supersedes N1-059-94-43, Item 58).
A-11-009-33b	N1-059-07-01, Item 20b	TEMPORARY: Destroy/delete within 180 (one hundred and eighty) days after recordkeeping copy has been produced.
A-03-005-05	DAA-GRS-2017-003-0002 (GRS 5.2, Item 020)	TEMPORARY: Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. (Supersedes GRS 4.3, Item 010; GRS 4.3, Item 011; GRS 4.3, Item 012; GRS 4.3, Item 020; GRS 4.3, Item 030, and GRS 4.3, Item 031).

- Type of information retained in the system: The PII retained in the system is identified in Section 3(d).

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. citizens or Legal Permanent Residents [LPRs])

☒ 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? (1) Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. § 4802, as amended, and (2) Foreign Assistance Act, 22 USC § 2349aa et. seq.

(c) How is the information collected?

DS/T/FASTC Employees and Instructors: Employee and Instructor PII is collected directly from the individual via the DoS OpenNet Global Access List (GAL). The GAL obtains the PII from the myProfile application. It is a Department mandate to complete the myProfile form.

Students: Student PII is collected directly from the individual via the DS-TMS Student Application Portal. Students enter their own PII in the DS-TMS Student Application Portal, as students do not have authorized access to the DS-TMS application itself.

(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.

PII is housed in two (2) FedRAMP-Certified Clouds; Amazon Web Services Government Cloud (AWS GovCloud) as the Infrastructure-as-a-Service (IaaS), and Envisage Technologies Corporation as the Software-as-a-Service (SaaS), as well as on Department-Owned equipment running on the DoS OpenNet, Global OpenNet (GO), or GO Browser networks.

(e) What process is used to determine if the information is accurate?

DS/T/FASTC Employees and Instructors: PII is manually inputted by the employees and instructors themselves into the myProfile application (which feeds the GAL), thus ensuring that the PII is accurate. In addition, the PII is reviewed and approved by DS/T/FASTC Program Managers.

Students: Student PII is manually inputted into the DS-TMS Student Application Portal by the students themselves. In addition, the PII is reviewed and approved by DS/T/FASTC Program Managers. If a student finds that their PII is inaccurate, the student must contact their DS/T/FASTC instructor via @state.gov email or telephone, and the DS/T/FASTC Instructor will manually correct the error in the DS-TMS application for the student.

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

DS/T/FASTC Employees and Instructors: Yes, the PII in the application is current, and to ensure the PII remains current, DS/T/FASTC employees and instructors review the PII on a periodic basis, with updates performed as necessary.

Students: Yes, the PII in the application is current, and to ensure the PII remains current, students provide their PII updates to DS/T/FASTC instructors whenever changes are necessary.

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

No, DS-TMS does not use information from commercial sources, and the information in DS-TMS is not publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?

DS/T/FASTC Employees and Instructors: Employees and instructors are notified prior to the collection of their PII. PII is obtained for employees and instructors from the GAL and the GAL obtains the PII from the myProfile application. Notice that PII that is being collected is the responsibility of the myProfile application. It is a Department mandate to complete the myProfile form.

Students: Students are notified prior to the collection of their PII. When the student goes to the DS-TMS student application portal URL, the log-on page (Form DS-7800) displays a Privacy Act Statement that PII is being collected by the DS-TMS application.

(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?

DS/T/FASTC Employees and Instructors: Yes, employees and instructors can decline to provide their PII, or to consent to particular use of the PII. If employees or instructors decline to provide information, they will not be authorized access to the DS-TMS application.

Students: Yes, students can decline to provide their PII or can consent to particular use of the information. If a student declines to provide their PII, or to consent to particular uses of the PII, the student will not be authorized access to the DS-TMS Student Application Portal. The DS-TMS Student Application Portal is used for the student to enroll (register) for a course, access the virtual course, and receive notifications of future courses available to them.

- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The DS-TMS System Owner performed due diligence and made a conscientious decision to use the minimum amount of PII necessary to achieve the objective of the DS-TMS application. Social security numbers are collected so that DS/T/FASTC employees and instructors can properly distinguish between non-U.S. and U.S. individuals, as well as to synchronize data with the Foreign Service Institute (FSI), via non-automated mechanisms. The 'Date and Time of Last Medical Screening' is collected by the DS-TMS application to ensure personal safety of the DS/T/FASTC employees, instructors, and students.

5. Use of Information

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

The intended use of the PII in the DS-TMS application is to enroll students, track training requirements, manage training resources, and certify completed training. The PII is used to document course assignments, instructors' attendance at their required course, and the students' attendance at the course.

(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, the use of PII in DS-TMS is relevant to the purpose for which the DS-TMS application is designed. The purpose of DS-TMS is to enroll students, track training requirements, manage training resources, and certify completed training.

(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.

There is no sharing of PII, internally or externally.

(b) What information will be shared? N/A

(c) What is the purpose for sharing the information? N/A
(d) The information to be shared is transmitted or disclosed by what methods? N/A
(e) What safeguards are in place for each internal or external sharing arrangement? N/A
(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed? N/A

7. Redress and Notification

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

DS/T/FASTC Employees and Instructors: DS/T/FASTC employees and instructors are authorized access to DS-TMS using their PIV card and password. The application authenticates them as authorized users, and the employees and instructors can access all PII on employees, instructors, and students.

Students: The instructor prints out the student PII at the start of the training session for the students to review. If the PII requires any changes, it will be manually updated by the DS/T/FASTC instructor in the DS-TMS application.

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

☒Yes ☐No

If yes, explain the procedures.

DS/T/FASTC Employees and Instructors: DS/T/FASTC employees and instructors are authorized access to the DS-TMS application, and there are procedures in-place to allow the PII to be corrected. Employees and instructors correct the inaccurate or erroneous PII in the DS-TMS application.

Students: Students are not authorized access to the DS-TMS application; however there are procedures in-place to allow the students' PII to be corrected. The PII will be updated by the DS/T/FASTC Instructor who manually corrects any errors in the DS-TMS application for the Student.

- If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

DS/T/FASTC Employees and Instructors: DS/T/FASTC employees and instructors are notified periodically to review and correct their PII in DS-TMS, if appropriate.

Students: The DS/T/FASTC Instructor informs the students to provide any updates to their PII to the instructor. The DS/T/FASTC instructor manually corrects any errors in the DS-TMS application for the student.

8. Security Controls

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

The PII in the DS-TMS application is secured with the following safeguards:

- Connection to the DS-TMS application is first through the use of HyperText Transfer Protocol (HTTP) via the Internet;
- The HTTP port then automatically routes the user through the use of HyperText Transfer Protocol Secure (HTTPS) to the DS-TMS application;
- All network traffic is HTTPS-encrypted using Federal Information Processing Standards (FIPS) approved encryption and uses Transport Layer Security (TLS) 1.2;
- The database is stored on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) volumes that are encrypted in place with FIPS-approved AES-256 level encryption;
- Annual training is taken by DoS Users and Non-DoS Users which includes data privacy topics;
- DoS Users: DoS users will access the OpenNet network via the use of HSPD-12 and FIPS 201-compliant Personal Identity Verification (PIV)-Authenticators or an IRM issued RSA Token Authentication GO device (e.g., fob that generates time-based one-time passwords). The use of Security Assertion Markup Language (SAML) Single Sign-On (SSO) allows integration and meets the requirements for Access Controls (AC) and Identification and Authentication (I&A) for DoS users to safely access the Acadis TMS web interface to authenticate to the DS-TMS application.
- Non-DoS Users: Non-DoS (External) users will be authenticated through the use of an IRM Okta. Okta is the State Enterprise – Identity Credential and Access Management (SE-ICAM) solution for implementing Multi-Factor Authentication (MFA) for cloud-based applications. Okta supports Security Assertion Markup Language (SAML) type authentication mechanism and is generated by IRM. Okta uses DoS Active Directory (AD) and meets the requirements for Access Control (AC) and Identification and Authentication (I&A) for Non-DoS (External) users and accepts Federal Identity Credential and Access Management (FICAM)-approved third-party credentials for Other Government Agencies (OGAs) to safely access the Acadis TMS web interface to authenticate to the DS-TMS student application portal.
- Safeguards of the DoS OpenNet, DoS OpenNet GO, or DoS GO Browser networks allow authentication to the DS-TMS and DS-TMS Student Application Portal;
- Inherited security controls from the DoS OpenNet, DoS OpenNet GO, or DoS GO Browsers networks;
- Inherited security controls from the Envisage (SaaS) software;
- Inherited security controls from the AWS-GovCloud (IaaS) network, as well as physical security controls; and
- A Standard Operating Procedure (SOP) for DS-TMS System Owner & System Administrator has been established to provide guidance on downloading PII.

(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 DoS Users identified in Section 3(d)(1) as DS/T/FASTC employees and instructors have been granted access rights to all PII that is necessary to perform their official duties. The System Owners and System Administrators determine which access rights are granted to employees and instructors based on their particular role and job function; see Section 9(b) for a list of user access.

The Non-DoS users identified in Section 3(d)(2) as students have been granted limited access rights to the DS-TMS Student Application Portal. As students, they do not have access to the DS-TMS application itself.

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

DS-TMS is subject to monitoring, recording, and auditing safeguards that are provided by AWS-GovCloud (IaaS) and Envisage (SaaS). A Monthly Vulnerability Report is reviewed by the DS-TMS System Administrators for potential security risks and this information is forwarded to the DS-TMS System Owner for remediation.

DS-TMS System Administrators will run a local query on a monthly basis that shows monitoring, recording, and auditing records of DS-TMS employee, instructor, and student activities, and that output is reviewed each month by the System Administrators.

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

DoS users (employees and instructors) must attend a security briefing prior to receiving access to DoS networks and receiving a PIV card for building access. This briefing is sponsored by DS Security Infrastructure, Office of Information Security (DS/SI/IS) and includes a discussion of the Privacy Act of 1974.

DoS users (employees and instructors) must take PS800 'Cybersecurity Awareness', which has a privacy component, and pass a quiz prior to receiving access to a DoS network. This briefing is an annual requirement.

Non-DoS users (students) who do not have OpenNet access to Course PS800 (e.g., restricted users) are provided the 'Annual Cybersecurity Awareness for Users with Restricted Access' briefing by the ISSO within 10 business days of initial system logon, when required by system changes, and annually thereafter.

DS-TMS users (employees and instructors) must also take PA318 'Protecting Personally Identifiable Information' within 90 days of their start date, and every two (2) years thereafter.

All DoS employees (which includes DS-TMS employees and instructors) that access the DoS Intranet – DoS OpenNet, DoS OpenNet GO, or GO Browser networks – must

review and sign a 'Security Briefing for DS Network and Application Users', which has a privacy component, before they are given access to the DoS networks.

DS-TMS System Administrators must follow the DoS-mandated Security Awareness Program that is in-place for IT professionals. In order to gain access as a DS-TMS System Administrator function, an individual must attend the 'Information Assurance Training for System and Security Administration' course, which has a privacy component, and obtain a certificate of completion.

(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 PII in the DS-TMS application is secured by the security controls and safeguards listed in Section 8(a) and therefore unusable to unauthorized users.

(f) How were the security measures above influenced by the type of information collected?

Security measures were influenced by the PII collected and stored by DS-TMS. With the determination of the PII necessary for the system, the DS-TMS System Owner performed due diligence to use the minimum amount of PII necessary and secured that PII as required. The rating of 'moderate' impact level of all PII data types collected and stored by DS-TMS means strict security measures are in place, based on guidance by Federal Information Processing Standards (FIPS) 199 and the National Institute of Standards and Technology (NIST SP) 800-60.

9. Data Access

(a) Who has access to data in the system?

DS/T/FASTC Employees and Instructors: Employees and instructors have access to PII in the DS-TMS application.

Students: Students can only enter their own PII in the DS-TMS Student Application Portal.

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

DS/T/FASTC Employees and Instructors have access to PII in the DS-TMS application based on the four (4) types of role-based user access approved by the System Owner and the System Administrator:

- To *view* PII in DS-TMS requires the ***Read*** role, all roles identified in Section 3(d)(1) have these rights necessary to perform their duties;
- To *enter* PII in DS-TMS requires the ***Write*** role, all roles identified in Section 3(d)(1) have these rights necessary to perform their duties;
- To *edit* PII in DS-TMS requires the ***Edit (Modify)*** role; all roles identified in Section 3(d)(1) have *Edit* rights necessary to perform their duties; and
- To *troubleshoot* issues with PII in DS-TMS requires the ***Delete*** role, only System Administrators have the *Delete* rights necessary to perform their duties.

Students do not have access to data in the DS-TMS application but do have access to the DS-TMS Student Application Portal to enter their own PII. Students' user access is determined by the System Owner, and the System Administrator is only allowed to provide students with *Read* and *Write* roles.

(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/T/FASTC employees and instructors have access to all PII in the DS-TMS application as needed to perform their duties, and as determined by the System Owner and System Administrator; therefore their access is not restricted.

Students do not have access to the DS-TMS application and PII within it; therefore their access is restricted.

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

DS/T/FASTC employees and instructors are familiar with the requirements for protecting PII and to ensure they are trustworthy, they:

- Are thoroughly screened for suitability prior to their employment with DoS;
- Sign Non-Disclosure Agreements; and
- Pass an annual computer security briefing entitled 'Security Briefing for DS Network and Application Users'.