Privacy Impact Assessment: FSI Cornerstone FSI-Learn

1. Contact Information

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

2. System Information

(a) Name of system: Cornerstone (CSOD) FSI-Learn

(b) Bureau: Foreign Service Institute (FSI)

(c) System acronym: FSICS

(d) iMatrix Asset ID Number: 302080

(e) Reason for performing PIA: Click here to enter text.

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

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?
This is a new system that is currently under assessment, and is expected to be completed October 2020.

(c) Describe the purpose of the system:
FSICS is a cloud SAAS platform providing online Learning experiences, particularly online training courses. The user base consists primarily of Department of State, Department affiliates', and other Agencies' staff requiring online training courses. FSICS does not collect any PII directly but imports required PII from a separate Department of State system called Student Training Management System (STMS).

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The FSICS only uses and maintains the following PII:

- Last Name
- First Name
- Personal email address only for non-State Department users (e.g. Department Employee family member).
- Official email address (for Department or other Agency Employees or Contractors)

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
22 USC Section 4021 (Institution for Training)
Executive Order 13434
5 USC 301, Departmental Regulations

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☐Yes, provide:
- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

☒No, explain how the information is retrieved without a personal identifier.

FSICS does not retrieve any information by personal identifier. It only serves as a platform to allow access to online learning materials.

(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:
- Schedule number (e.g., (XX-587-XX-XXX)): A-09-001-03a(1)
- Length of time the information is retained in the system: Destroy when 5 years old or no longer needed, whichever is sooner
- Type of information retained in the system:
Correspondence, reports and other documentation on organization and enrollment of classes.

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?

Click here to enter text.

(c) How is the information collected?

FSICS does not collect any PII directly from an individual; rather, it imports required PII from the Student Training Management System (STMS).

(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.

The PII information is housed inside Cornerstone (CSOD) SAAS Cloud

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

The FSICS System imports PII from the Student Training Management System (STMS) and implements functional error-checking to ensure data are imported accurately during the import process.

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

The FSICS System imports PII from STMS, and the data are wholly dependent on STMS updates. Updates occur as needed. There is no fixed schedule.

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

No.

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

No notice is provided to the individual prior to the collection of his or her information, since FSICS only receives PII from STMS and does not gather PII directly from users.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?
No information is collected directly from individuals.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The FSICS is a Cloud Learning Management system that requires the minimum PII needed for conducting online training. There are no highly sensitive PII elements collected, such as social security numbers, and FSICS does not directly collect PII but obtains it from STMS.

5. Use of information

(a) What is/are the intended use(s) for the information?
In FSICS any PII is dedicated to online training-related record keeping such as course enrollments, course completions, and certificate generation. Email addresses could potentially be used to communicate with students regarding their coursework.

(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

(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.

FSICS PII information is not shared internally or externally with any other information system.

(b) What information will be shared?

FSICS PII information is not shared internally or externally with any other information system.

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

FSICS PII information is not shared internally or externally with any other information system.

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

FSICS PII information is not shared internally or externally with any other information system.

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

FSICS PII information is not shared internally or externally with any other information system.

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

FSICS PII information is not shared internally or externally to any other information system.

7. Redress and Notification

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

Users have access to their information directly by logging into the system and viewing their student profile which shows their email address and course enrollments..

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

☒Yes ☐No

If yes, explain the procedures.

Individuals may contact FSICS Help Desk to initiate corrections, the Help Desk is available via e-mail.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
FSICS contains directions for users to seek assistance to correct any PII data issues or solve any other problems they encounter. A dedicated FSICS System Help Desk provides user support.

8. Security Controls

(a) How is the information in the system secured?
FSICS is a SAAS cloud platform and is certified at FedRamp moderate impact level. A range of security controls ensuring confidentiality, integrity, and availability are employed per FedRamp Authorization requirements. Some of the controls include TLS secure communications, multi-factor authentication, injection protections, and incident response procudures.

(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.
PII in FSICS is accessible to only authorized staff at the Department of State. FSICS implements role-based access controls to implement the principles of least privilege, separation of duties, and need to know. Higher privilege roles with PII access are Registrar and Administrator.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
FSICS enforces multi-factor user access control through the Department of State Enterprise Identity, Credential and Access Management (SE-ICAM) and has rigorous system audit trails to deter and detect any unauthorized activity. SE-ICAM services include threat monitoring of FSICS user login activities thereby adding another defense in depth layer to FSCIS security posture.

(d) Explain the privacy training provided to authorized users of the system.
FSCIS privileged users are all Department of State employees or contractors who are mandated to take biennial privacy training through the course PA-318: Protecting Personally Identifiable Information. Personnel must also take the annual PS-800 CyberSecurity Course, which has a privacy component.

(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.
All FSICS PII is encrypted at rest and transmission in accordance with cloud FEDRAMP moderate authorization specifications that ensures proper compliance with Federal regulations. Authentication occurs through Department of State SE-ICAM OKTA Multi-

Factor authentication. FSICS is security monitored by the cloud provider in accordance with FEDRAMP monitoring controls.

(f) How were the security measures above influenced by the type of information collected?
Because the loss of confidentiality, integrity, or availability could have a serious adverse effect on organizational operations, organizational assets, or individuals, the system was categorized as a moderate system and the appropriate FedRamp security controls, verifications, and authorizations were undertaken for FSICS. All security measures are a result of implementing said security controls commensurate with FedRamp moderate baseline.

9. Data Access

(a) Who has access to data in the system?
FSICS access is controlled through role based security. These roles are Student, Registrar and Administrator.

(b) How is access to data in the system determined?
Typical student access to the system depends on being registered for online courses in FSICS through the Student Training Management System. The Administrator and Register roles are based on job description.

(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.
FSICS implements role based security, so student roles only have access to their own information. While the higher privilege Administrator or Registrar roles have greater access, their activities are audited (audit trail) and functions are restricted depending on the role.

(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 controls prevent users from having access to data other than that which they have a business need to access. Security clearance background checks undertaken prior to onboarding personnel and logging and auditing all significant higher privilege actions mitigates misuse risks.

Lower privilege roles are prevented from accessing higher privilege sections through browsing restrictions enforced at the FSICS server.