Privacy Impact Assessment (PIA)

for the

Federal Tax Information (FTI) Student Aid Internet Gateway (SAIG)

October 31, 2023

Point of Contact

Contact Person: Alisa Anderson
Title: SAIG Business Technical Lead
Email: Alisa.Anderson@ed.gov

System Owner

Name: Reza Venegas
Title: Business Owner/Program Manager
Principal Office: Federal Student Aid

Submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

FY 2022

*Please complete this **Privacy Impact Assessment (PIA)**, which describes how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The U.S. Department of Education (Department) Student Aid Internet Gateway (SAIG) system is a store-and-forward[1] mailbox system that enables the secure, electronic exchange of Higher Education Act of 1965, as amended (HEA) Title IV data over the Internet. In December of 2019, Congress passed the Fostering Undergraduate Talent by Unlocking Resources for Education Act (FUTURE Act) to allow the Internal Revenue Service (IRS) to disclose certain Federal Tax Information (FTI) to the Department for the purposes of:

- Determining eligibility for, or repayment obligations under, income-driven repayment (IDR) plans; and
- Determining eligibility for, and amount of, Federal student financial aid.

A new instance of SAIG, FTI-SAIG, will be implemented to handle the transmission of FTI pursuant to security requirements of the FUTURE Act and IRS Publication 1075, "Tax Information Security Guidelines for Federal, State and Local Agencies."

1.2. How does the IT system function to support the project or program as described in Question 1.1?

FTI-SAIG is being implemented to allow transmission of FTI, which is part of the Institutional Student Information Record (ISIR), in a highly secure environment.

Once a Free Application for Federal Student Aid (FAFSA) has been processed, an ISIR is created that contains data provided by the applicant and all contributors (e.g., parents and spouses of applicants, third party preparers) on the FAFSA along with the following:

[1] Store and forward is a data communication technique in which a message transmitted from a source node is stored at an intermediary device before being forwarded to the destination node.

- FAFSA Processing System (FPS) data (results of matches[2], rejects[3], eligibility indicators[4])
- National Student Loan Data System (NSLDS) data (loan/grant statuses and detailed information on loans/grants)
- FTI (information received from the IRS)

Once FPS has processed the FAFSA information received from an applicant and received information from NSLDS, a copy of all of these data is sent to FTI Module (FTIM), where FTI will be appended to the ISIR, and FTIM will transmit the ISIR to FTI-SAIG in compressed format. The compressed ISIR will be retrieved by all institutions of higher education (IHEs) (hereafter referred to as Title IV institutions) that the student lists on the FAFSA, along with any State agencies associated with the schools or State of legal residence to determine student's eligibility for State aid, and if students have submitted a FAFSA.

The primary function of FTI-SAIG, as a store-and-forward managed file transfer solution, is to route inbound files to the appropriate mailbox, where they can be received as needed by Title IV institutions. FTI-SAIG will be hosted within the FTI Infrastructure (FTII) general support system (GSS) to meet the security requirements of IRS Publication 1075.

Central to SAIG and FTI-SAIG, TDNgine (TDN), a commercial off-the-shelf (COTS) product, is an open architecture gateway solution that manages the mailbox structure for sending, storing, retrieving, and archiving Title IV data. TDN has been enhanced to support IRS Publication 1075, ensuring IRS-mandated safeguards are in place. Through TDN, FTI-SAIG is store-and-forward only; Title IV institutions are not permitted to manipulate, view, or edit information within FTI-SAIG. The data files remain on the FTI-SAIG for a default period of 90 days; after 90 days, files are purged from the system.

The following software tools are available for interaction with the FTI-SAIG system:

- TDClient is a COTS application that runs on the end user's computer or server and is used to transmit FTI securely over the Internet to TDN. TDClient performs functions such as compression, decompression, and other security functions necessary to interoperate over the Internet through a command line interface (CLI). The CLI gives Title IV application systems a way to integrate access to the FTI-SAIG system into their existing systems. TDClient is one of only two methods that can be used to communicate with TDN, with EDconnect being the

[2] Results from exchanging information with the Social Security Administration, U.S. Department of Veterans Affairs, U.S. Department of Homeland Security, and U.S. Department of Justice. The results from these exchanges are used in determining a student's eligibility.
[3] If a student is not determined to be eligible the rejects are the reasons/issues a student needs to correct to become eligible.
[4] These are indicators schools use to assist in reviewing and packaging a student's financial aid packet. For example, Pell Grant Flag indicates if the student is eligible for a Pell Grant.

other. Prior to accessing FTI-SAIG, end users need to obtain credentials through the Participation Management (PM) registration process. After successfully registering, TDClient initiates multifactor authentication (MFA) sessions with TDN using the following credentials:

  - FSA user ID (provided by the PM system)
  - FSA password
  - FTI mailbox (provided by the PM system)
  - User-specific certificate

- EDconnect is a custom FSA application that runs on the end user's computer or server and is used to transmit FTI securely over the Internet to TDN. To connect to TDN, EDconnect is built using the TDClient application programming interface (API). Use of the API permits EDconnect to performs functions such as compression, decompression, and other security functions necessary to interoperate over the Internet through a graphical user interface (GUI); through the GUI, the application allows users without technical expertise access to their mailbox. EDconnect is one of only two methods that can be used to communicate with TDN, with TDClient being the other; from the perspective of TDN, there is no difference between the two communication methods. Prior to accessing FTI-SAIG, end users need to obtain credentials through the PM registration process. EDconnect users are authenticated using the Access and Identity Management System (AIMS) to secure access to the web application. TDCM provides the following information to AIMS to aid in authentication though an application-specific webservice:
  - FSA user ID (provided by the PM system)
  - FSA password
  - FTI mailbox (provided by the PM system)
  - One-time passcode (OTP)
  - User-specific certificate
- TDCM application is a web-based COTS application that allows FTI mailbox owners (e.g., individual users at Title IV institutions and FSA system users) to view the transaction metadata for transmissions to/from their mailbox. TDCM provides a s process for managing user authentication certificates. The certificates are used by TDClient and EDconnect to provide MFA authentication, which ensures that data are transferred securely and that only authorized users can access the FTI-SAIG environment. Prior to the expiration of the user authentication certificate (certificates expire yearly), the user will receive an email announcing the imminent expiration; no FTI will be used in the certificate announcement.

The following systems transmit data to FTI SAIG:

- The FPS is responsible for determining financial aid eligibility and notify the applicant and IHEs the results of the determination. The FAFSA gives applicants the option of having the IRS provide FTI for their application, as opposed to having the applicant enter the FTI themselves. When a user consents to the IRS directly providing FTI for their application, FPS will generate an ISIR for each Title IV institution that does not yet include the FTI . The FTI will be added to the ISIR in the FTIM.
- The FTIM is responsible for supplying FTI to the ISIR for subsequent transmission to authorized Title IV institutions. FTIM will receive ISIRs from their mailbox and add FTI. After successful insertion of FTI into the ISIR, FTIM will transmit the ISIR to the FTI-SAIG mailbox of each of the appropriate Title IV institutions.
- The PM system establishes mailboxes in the FTI-SAIG. FTI-SAIG maintains an interface with the PM system to process changes for SAIG user enrollment. This interface enables FTI-SAIG to retrieve the participant files containing the newly assigned mailboxes and participant information for new enrollment accounts, updated participant information for existing accounts, or deleted participants for inactive accounts. These files are transmitted to the FTI-SAIG PM specific mailbox for respective Title IV institutions to then access and download.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☐ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[5] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

PII is collected to create TDCM administrative accounts to access the FTI-SAIG environment. Administrators access, view, and monitor mailbox transmission activities. In the event an administrator has been locked out of their TDCM account or otherwise requires a password reset, they can contact the Central Processing System (CPS)/SAIG

[5] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

Help Desk (managed by CPS PM). PII is shared with the CPS/SAIG Help Desk to verify the identities of administrative account users that contact the Help Desk for customer support.

In addition, FPS will use the FTI-SAIG system to transmit ISIR files with FTI to the appropriate Title IV institutions for the purpose of administering Title IV programs. The ISIR files will be stored in a compressed format while in FTI-SAIG.

1.5. Is the IT system operated by the agency or by a contractor?

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

FTI-SAIG contractor (Groundwell) is responsible for:

- Maintenance of FTI-SAIG specific applications (TDN and TDCM);
- Installation/configuration/maintenance of applications in the development and test environments; and
- Continuing operations in all environments, but only has read-only access in stage and production environments, where the FTII contractor would have to perform the necessary tasks.

FTII contractor (Peraton) is responsible for:

- Maintenance of all infrastructure components (servers, database, network); and
- Installation/configuration/maintenance of applications in the stage and production environments.

☐ N/A

1.7. If the IT system is operated by a contractor, does the contract and other acquisition-related documents include privacy requirements?

Yes

☐ N/A

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, contact your program attorney.

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

Collection of information related to postsecondary Federal student aid is authorized by Title IV of the Higher Education Act of 1965, as amended (HEA) (20 U.S.C. § 1070 et seq.).

The Fostering Undergraduate Talent by Unlocking Resources for Education (FUTURE) Act (P.L. 116- 91) amends Section 6103 of the IRC and allows the IRS to provide certain tax return information to the Department for the purposes of administering Federal student aid programs authorized under Title IV of the HEA.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, titled "Aid Awareness and Application Processing," 18-11-21, 88 FR 39233, was published in the Federal Register on June 15, 2023.

The SORN, titled "FUTURE Act System (FAS)," 18-11-23, 88 FR 42220, was published in the Federal Register on June 29, 2023.

Records Management

If you do not know your records schedule, consult with your records liaison, or send an email to RMHelp@ed.gov

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

The Department will maintain FTI that the Department receives from the IRS pursuant to section 6103(l)(13)(A) of the IRC for the purpose of determining eligibility for, or repayment obligations under, IDR plans under title IV of the HEA with respect to loans under part D of title IV of the HEA, in accordance with ED Records Schedule 072, "FSA Application, Origination, and Disbursement Records" (DAA–0441–2013–0002)(ED 072); ED Records Schedule 075, "FSA Loan Servicing, Consolidation, and Collections Records" (DAA–N1–441–09–016) (ED 075); and ED Records Schedule 051, "FSA National Student Loan Data System (NSLDS)" (DAA–0441–2017–0004) (ED 051). The Department has proposed amendments to ED 072, ED 051, and ED 075 for NARA's consideration and will not destroy records covered by these records schedules until such amendments are in effect, as applicable.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

2.5. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

☒ Yes
☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☐ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☐ Home Address

☐ Personal Phone Number	☒ Work Phone Number	☐ Personal Email Address
☒ Work Email Address	☐ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☒ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☐ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☒ Other ID That Can Be Traced to Individual		

(Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☐ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "Specify below," describe the PII:
In addition to the PII elements selected above, Four-digit security PIN is also collected. This PII elements above do not represent information contained in the ISIR, as it is compressed while in transit through the FTI-SAIG.

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:
For TDCM administrators, the FTI-SAIG collects from the user requesting access: Full name, four-digit security PIN, user ID, work phone number, and work email address.

☒ Federal Contractors

Specify types of information collected from Federal contractors:
For TDCM administrators, the FTI-SAIG collects from the user requesting access: Full name, four-digit security PIN, user ID, work phone number, and work email address.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State, and local government employees), and the types of information collected from each:[6]

TDCM administrators, the FTI-SAIG collects from the user requesting access: Full name, four-digit security PIN, current user ID, work phone number, and work email address.

As previously specified, FTI-SAIG only collects information on users requesting TDCM Administrator access. The information not maintained in FTI-SAIG but, rather, maintained in other systems includes:

- Mailbox users (Title IV institutions): information associated with their FTI-SAIG mailbox account is collected by the PM system, which is assessed as part of the SAIG PIA.

- ISIRs: FPS/FTIM are the sources for the information in ISIRs. The ISIR files will contain applicant PII, but that information is not accessible by FTI-SAIG, since the ISIR is compressed and encrypted. That information is assessed as part of the FPS and FTIM systems.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

TDCM Administrator information is collected directly from the individual via the TDCM User ID Request form. The TDCM User ID Request form is emailed from the prospective TDCM Administrator to the applicable application system Information System Security Owner (ISSO) to process user accounts. PII is shared with the CPS/SAIG Help Desk to verify the identities of administrative account users that contact the Help Desk for customer support.

PII is also contained in the compressed ISIR files transmitted from FTIM via the FTI-SAIG. Once a FAFSA has been processed, an ISIR is created that contains data provided by the applicant and all contributors on the FAFSA. Once FPS has processed the record

[6] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

and received information from NSLDS, a copy is sent to FTIM, where FTI will be appended to the ISIR and transmit it to FTI-SAIG in compressed format.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, webpage, database)?

TDCM Administrator information is collected from the individual by completing the TDCM User ID Request form, acquiring the appropriate signatures, and then emailing it to the applicable application system ISSO for signature approval. The form is then sent to the FTI-ISSO for final approval before being forwarded to FTI-SAIG for processing.

FTI-SAIG only collects information on users requesting TDCM Administrator access. FTI-SAIG processes ISIRs, where the information is obtained from other source systems for the following purposes:

- Mailbox users (Title IV institutions): information associated with their FTI-SAIG mailbox account is collected by the PM system and not maintained in FTI-SAIG.

- ISIRs: FPS/FTIM are the sources for the ISIR information. The ISIR files will contain applicant PII, but is not accessible by FTI-SAIG, since the ISIR is compressed.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

The information collected provides the minimum amount required to identify the user requesting TDCM Administrator access and is collected from the user via the TDCM User ID Request form. For each submission, the form and its contents are verified by the applicable system's ISSO and the FTI-SAIG ISSO to ensure that only the PII identified in 3.1 is entered.

PII maintained in ISIRs is collected and maintained by other FSA source systems. The PII is in a compressed format when being transported from FTI-SAIG to Title IV institution and is not accessible in FTI-SAIG.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

TDCM Administrator accounts go through a recertification review on a quarterly basis. This review is specifically meant to identify users who have left an organization, no longer need access to TDCM, or updated their names or contact information. Additionally, this is an opportunity for Title IV institutions to review the status of their users' accounts. Per FSA policy, any TDCM account who has not logged into the system within 90 days will have their account disabled. Any user who has not accessed their account in 180 days will have their account deactivated.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

No

3.9.1. If the above answer to question 3.9 is **YES**, cite the authority for collecting or maintaining the SSNs.

☑ N/A

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☑ N/A

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☑ N/A

3.9.4. If the above answer to question 3.9 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☑ N/A

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

A Privacy Act Statement is provided on the TDCM User ID Request form. Notice is also provided in the SORN referenced in question 2.3.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

No

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

FTI-SAIG Privacy Notice

Authorities: Title IV of the Higher Education Act of 1965, as amended (HEA) (20 U.S.C. 1070 *et seq.*); section 141(f) of the HEA (20 U.S.C. 1018(f)), and 6103(1)(13) and p(4) of the IRC and IRS Publication 1075 Tax Security Guidelines for Federal, State, and Local Agencies.

Purpose: Collection of personally identifiable information (PII) (Full Name, Four-Digit Security PIN, Current User ID, Phone Number and Work Email Address) is required for the purpose of creating and managing a user's account in the FTI-SAIG system. The PII will be reviewed quarterly as part of the user account validation process. The PII will also be used to confirm a user's identity when they call the CPS/SAIG Help Desk for technical support.

Disclosures: The U.S. Department of Education can potentially share user information with third parties under what is permitted in the "ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES" section of the System of Records notice titled "FUTURE Act System (FAS) (18–11–23)."

Consequences of Failure to Provide information: If the user chooses not to provide the requested personal information (Full Name, Four-Digit Security PIN, Current User ID, Phone Number and Work Email Address), they will not be able to obtain a user account. Should the user determine that they no longer want their personal information maintained in the Department of Education's Federal Student Aid records, they may opt-out at any time by submitting a new TDCM request form to have their account deactivated.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

All information on the TDCM User ID Request form is required information. If the required information is not provided, the request will be rejected; rejection can be done by either the applicable application system ISSO or the FTI-ISSO. Existing users disable their account out by submitting the TDCM User ID Request form and selecting the "Disable User" option.

4.5. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practices, policies, or activities that affect the PII and the privacy risks to ensure that individuals are aware of and, where feasible, can consent to, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

No

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☑ N/A

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☑ N/A

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

No

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

PII from the TDCM User ID Request form is not shared with any external entity.

PII, contained within the FTI-ISIR files, is transmitted in a compressed format from FTIM via the FTI-SAIG to authorized Title IV institutions. FTIM supplies FTI to the ISIR for subsequent transmission to authorized Title IV institutions.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

FTI-ISIR files are sent to authorized Title IV institutions in order to process Federal student aid applications.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

The HEA allows for sharing of information to Title IV institutions for processing Federal student aid applications.

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

Within the FTI-SAIG, PII (contained within the FTI-ISIRs) is routed to the appropriate mailbox, where they can be received as needed by Title IV institutions. The FTI-SAIG includes FIPS 140-3 encryption for data at rest and TLS v1.3 end-to-end encryption during transport.

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with

the external entities?

☐ N/A

Yes

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

Once the ISIRs are received by the designated Title IV institution, the information is not allowed to be redisclosed, unless explicit permission is provided by the Department.

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

TDCM Administrative users can view, but not edit, their account information from the TDCM website.

As indicated in the FUTURE Act SORN Record Access Procedures, users may also contact the system manager listed in the SORN to access their records.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

Since the data viewed in the TDCM account is read-only, any updates to an existing user requires the user to submit a new TDCM User ID Request form and go through the approval process of getting the necessary ISSO signatures.

As indicated in the FUTURE Act SORN Record Access Procedures, users may also contact the system manager listed in the SORN to amend their records.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Instructions for changing account information are located on the TDCM User ID Request form that is completed for initial account creation. In addition, information contained in

the SORN referenced above provides the procedures for accessing and correcting information maintained in the system.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

No – System currently under development

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

TDCM user account passwords are disabled automatically after 90 days of inactivity. After 180 days of inactivity the accounts are deactivated on the system. Temporary accounts are removed after 30 days and emergency accounts after 7 days. The temporary and emergency accounts are created for auditing teams to run security scans and conduct manual testing with the TDCM application. The request for access follows the standard FSA/FTI-SAIG access procedures. Since audits can be ad-hoc and potentially time-sensitive, an emergency account request would expedite the process for the access. Once the scans and testing have been completed, the access is deactivated. SAIG employs access control policies (e.g., identity-based, role-based, rule-based) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or user processes) and objects (e.g.,

devices, files, records, processes, programs, domains). Access enforcement mechanisms are used at the application level to increase security.

FTI-SAIG uses proprietary software which provides integrity controls along with controls inherited from the FTII. It has built-in compression and encryption. Antivirus software is run automatically, and virus definition updates are regularly applied. Intrusion detection software is used to monitor the servers and uses a collection of one-way hash functions to detect file and system changes.

8. Auditing and Accountability

8.1. How does the ISO assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA by completing the Department of Education Risk Management Framework process to receive an ATO. Furthermore, FTI-SAIG ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 controls are implemented. The NIST controls are comprised of administrative, technical, and physical controls to ensure that information is used in accordance with approved practices. The system owner also participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology, which address security and privacy risks through the system's lifecycle.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

FTI-SAIG is required to obtain and maintain an ATO. This process includes a tri-annual independent assessment of all required security and privacy controls and produces Plans of Actions and Milestones (POA&Ms) to ensure any deficiencies are remediated. FTI-SAIG will also participate in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security and privacy controls are in place and working properly. FTI-SAIG has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities. Following each patch release an additional scan is conducted to ensure continuing operations. Additional activities include conducting regular self-assessments, contingency plan testing, and participating in tabletop exercises.

Privileged access user logs are produced by the FTII and provides them to the FTI-SAIG ISSO and FSA Security Operations Center (SOC) on a quarterly basis to ensure proper

monitoring of all privileged users accounts and that information and systems are not compromised by unauthorized access.

Additionally, FTI-SAIG administrators analyze and correlate audit records across its servers, databases, filesystems, and reports to the FSA SOC to make them aware of any suspicious events.

FTI-SAIG administrator monitors TDN and TDCM logs daily for suspicious activities. FTI-SAIG administrators have the capability to perform ad-hoc audits pulling data as evidence for findings or reporting purposes. FSA periodically conducts ad-hoc audits or requests an audit in the event of an incident reported at which time FTI-SAIG Support follows its Incident Response Plan (IRP). Report findings are sent to Information System Owners (ISO), ISSOs and FSA SOC personnel.

8.3. What are the specific privacy risks associated with this program or IT system and how are those risks mitigated?

Privacy risks associated with FTI SAIG include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII, and credentials are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.