Privacy Impact Assessment (PIA)

for the

Student Aid Internet Gateway

March 30, 2020

For PIA Certification Updates Only: This PIA was reviewed on **March 30, 2020** by **Alisa Anderson** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Alisa Anderson
Contact Email: Alisa.Anderson@ed.gov

System Owner

Name/Title: Reza Venegas/SAIG System Owner
Principal Office: Federal Student Aid

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

*Please complete this **Privacy Impact Assessment (PIA)** on 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, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Student Aid Internet Gateway (SAIG) is within the Federal Student Aid's IT infrastructure. The U.S. Department of Education sponsors the SAIG to promote the electronic exchange of Title IV information over the Internet by providing telecommunications support and "electronic mailboxes" for file delivery and administration of Title IV programs and their corresponding application systems. These application systems include Common Origination and Disbursement (COD), Central Processing System (CPS), Debt Management Collection System (DMCS), Financial Management System (FMS), National Student Loan Database System (NSLDS), and the HEAL Online Processing System (HOPS). The SAIG promotes the electronic exchange of Title IV information between higher education institutions, Federal Student Aid, Title IV application system contractors, state agencies, lenders, financial aid services and needs analysis services. SAIG is a "mailbox" and has no way or reason to read the mail. The SAIG is hosted at the Next Generation Data Center (NGDC).

Transaction Delivery Community Manager (TDCM) is a Student Aid Internet Gateway (SAIG) web-based application that allows users to manage their mailboxes and to view data transmission history to and from mailboxes.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

PII data is maintained for the creation of administrative accounts (referred to throughout as "accounts") to access the TDCM server software. The TDCM accounts are used to access the applications' transmission activities. The PII information sourced from and shared with the CPS/SAIG Help Desk for account verification.

1.3. Is this a new system, or one that is currently in operation?

[1] 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

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

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

Contractor

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

☐ N/A

Yes

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

Title IV of the Higher Education Act of 1965, as amended (HEA), 20 U.S.C. 1070et seq. The collection of Social Security numbers of users of this system is authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

☐ N/A

The records to create the TDCM administrative accounts are covered by the Student Aid Internet Gateway, Participation Management (SAIG, PM) System of Records Notice which was most recently published in full on March 1, 2018 at 83 FR 8855.

https://www.federalregister.gov/documents/2018/03/01/2018-04141/privacy-act-of-1974-system-of-records

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

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

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

General Records Schedule (GRS) 3.2, Item 031 System Access Records for systems requiring special accountability for access.
Disposition Instructions: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
DAA-GRS-2013-0006-0004.

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

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

Information for TDCM account users (Federal, contractor, FSA application system users) maintained within SAIG include full name, last 4 digits of SSN, user ID, phone number, and work email address.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

Individual user information is collected directly from the individual.

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

Individual user information is collected by completing the TDCM User ID request form either electronically or on paper and then emailing it to the applicable application system Information System Security Owner (ISSO) for approval.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

On a quarterly basis, TDCM accounts go through a recertification review. 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 programs application systems to review the current status of their users' accounts. As per FSA policy, any TDCM account who has not logged into the system within 90 days will have their access disabled. Any user who has not accessed their account in 180 days will have their access deactivated.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

The PII is used to create the TDCM account in order to manage the SAIG "mailbox". Additionally, the CPS/SAIG Help Desk uses the PII information to validate a user when contacted about being locked out of their TDCM account and requiring a password reset. The CPS/SAIG Help Desk Analyst validates the user by asking them to verify the last 4 digits of SSN.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

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

☑ N/A

Click here to enter text.

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.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

The last 4 digits of SSN are used by the CPS/SAIG Help Desk to validate a user when contacted about being locked out of their TDCM account and requiring a password reset. The Help Desk Analyst validates the user by asking them to verify the last 4 digits of SSN. The SSN 4 digits are not utilized by the SAIG Support Team.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

Other methods such as a Two-Factor Authentication (TFA) method or the use of a user selected four-digit PIN have been considered for alternatives but SSN remains the most reliable method for validating user identity at the moment.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

A Privacy Act Statement is provided on the TDCM User ID Request form. Public notice is also provided through the posting of this PIA and applicable SORN referenced in Question 2.2.1

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

Privacy Statement: Personal information, including the last 4 digits of the user's SSN, is collected solely for purposes of user account creation and validation. Personal information will be reviewed annually as part of the user account validation process. Personal information will also be used to confirm a user's identity when they call the CPS/SAIG Help Desk for technical support. 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. The Department of Education will not share your information with any outside party, other than what is permitted under the System of Records notice titled "Student Aid Internet Gateway, Participation Management System," which may be located here: https://www.federalregister.gov/documents/2018/03/01/2018-04141/privacy-act-of-1974-system-of-records.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The form clearly states which requested information is required. By signing and submitting the form, users are consenting to the collection and use of information. Existing users can opt out by submitting the TDCM User ID request form and selecting the disable user option.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

Click here to enter text.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

Click here to enter text.

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.6. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

TDCM admin users are able to view their account information once they log into the site. The data is read only.

As indicated in the SORN referenced in Question 2.2.1, users may also contract the system manager listed in the SORN to access their records.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

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

As indicated in the SORN referenced in Question 2.2.1, users may also contract the system manager listed in the SORN to correct inaccurate or erroneous information.

6.3. How does the project notify individuals about the procedures for correcting their information?

Directions for changing account information are located on the TDCM User IS request form that is completed for initial account creation. Additionally, because the records maintained in this system are covered by the SORN referenced in Question 2.2.1, the SORN and this PIA are considered a method of notification for how individuals can correct their information.

7. Safeguards

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

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

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/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 inactivated. 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 increase security.

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

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

Quarterly scanning is implemented, and the Risk Management Plan is assessed and reviewed annually. SAIG components being readied for production release are scanned using appropriate vulnerability assessment tools to ensure SAIG system security requirements are addressed and that the components are free from security vulnerabilities.

8. Auditing and Accountability

8.1. How does the system owner 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 in order to receive an Authority to Operate (ATO). Furthermore, the SAIG system makes sure that the National Institute of Standards and Technology (NIST) 800-53 controls are implemented. The NIST controls comprise of an 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 Life-cycle Management Methodology, which address security and privacy risks through the system's lifecycle.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

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

There is minimal privacy risk associated with this system because the information collected is considered business contact information with the exception of the last four digits of the SSN.

This does create a small risk and to mitigate the potential for exposed PII data, the last 4-digits of the the SSN are visible to only 25 people on the CPS/SAIG Help Desk. All staff on the CPS/SAIG Help Desk have a 5C clearance at minimum.

As mentioned in section 3.8.2, changing the enrollment process to collect a user selected 4-digit PIN, in place of the last 4-digits of the SSN, could also be considered in the future for a mitigation strategy.