Privacy Impact Assessment (PIA)

for the

FSA Partner Connect

December 14, 2020

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Corey Johnson / Information System Security Officer
Contact Email: corey.johnson@ed.ov

System Owner

Name/Title: Samuel Aba / Senior IT Manager
Principal Office: Samuel.Aba@ed.gov

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 FSA Partner Connect platform (Partner Connect) is a major application whose infrastructure is hosted on the FSA Cloud. Partner Connect is a unified digital website for school partners, financial institution partners, FSA staff, and contractors involved in the administration of Title IV financial aid for postsecondary education.

Partner Connect will serve as the foundational platform for FSA's partners, including more than 5,500 postsecondary institutions, as they navigate their participation in the Title IV student aid programs. FSA Partner Connect will feature—

- Knowledge Center – The Knowledge Center will replace the Information for Financial Aid Professionals (IFAP) website. The redesigned site will offer a new look and feel, streamline information, and improve search capabilities and feature an updated FSA Handbook that will be presented in a more user-friendly format, including both a digital version and a downloadable PDF version.
- Partner Dashboard – This feature will allow authenticated users to view a summary dashboard with snapshots of data related to their school or organization. The dashboard will include partner metrics, important communications, notifications, news, and high-level operational data tailored to users based on their role.
- Partner Search and Profile – This feature will allow authenticated users to easily search and view comprehensive and consolidated information from FSA systems for a school.
- Student, Parent, Borrower Accounts – This feature will provide authenticated users with a comprehensive and consolidated view of account information for students, parents, and/or borrowers. Authentication and role-based access are used to ensure that users have access only to information they are authorized to view.
- Partner Role Management – This feature will allow Account Administrators to easily manage access to Partner Connect for individuals within their organization. Once an individual user has been granted access, the user will be able to view and manage his or her access through the Account Access Management Center.

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

To enable Partner Connect functionality, Partner Connect obtains PII (via encrypted Application Programming Interface) sourced from other connected FSA systems for display to authenticated users (see explanation of Partner Dashboard above). The PII processed by the system includes information that has been collected by FSA for borrower identity verification, financial aid eligibility, or Title IV program participation eligibility. This information has been processed and maintained by other FSA back-end systems responsible for various Title IV functions throughout FSA. Specifically, information provided through Partner Connect is sourced from National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD), and Student Aid Internet Gateway Enrollment (SAIG) / Participation Management (PM). For more information on how records are handled from these respective systems, please refer to those individual PIAs and system of records notices, available at www.ed.gov/privacy.

The PII collected via Partner Connect enables access to privileged system data available in FSA back-end systems responsible for various Title IV functions throughout FSA. The PII collected in this system is used for the following purposes:

- To enable access and login to Partner Connect for FSA staff and contractors as well as partners, specifically: postsecondary institutions, third-party servicers, state agencies, accrediting agencies, software providers, guaranty agencies, federal loan servicers, Federal Family Education Loan (FFEL) Lenders, lender servicers, and private collection agencies (PCAs);
- To associate individual partner users with the appropriate partner organizations; detailed institutional information is provided to users with the appropriate system relationships; and
- To provide postsecondary institutions and FSA staff with the ability to view comprehensive account information for FSA customers (students, parents, or borrowers).

While Partner Connect collects PII to enable Partner Connect accounts, Partner Connect has established a service with FSA's existing Access and Identity Management System (AIMS) application for identity authentication and access services. For most partners

[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

(external users), the relationship with AIMS has already been established and the initial point of collection of PII is the SAIG Enrollment PM web site where partners enter – last name, first name, email, address, phone number, date of birth, and last four digits of Social Security number (SSN). The account information collected in PM is then passed to AIMS to generate a unique user ID in AIMS for user authentication and authorization to provide access to FSA applications. This is not a probabilistic match; all information submitted must match the AIMS ID information exactly in order to be authenticated. For most FSA staff or contractors (internal users), the relationship with AIMS has already been established and the collection of PII occurs by completing the FSA application security access form provided by the Application ISSO on behalf of the internal Department employee. If an account is not found, the user will receive either an email or be redirected to AIMS to obtain an account.

Partner Connect collects the minimal PII needed by AIMS – first name, last name, date of birth, and last four digits of the SSN to create Partner Connect accounts and integrate with AIMS ID to enable a consistent authentication experience for users. User credentials for Partner Connect accounts are stored in a linked database, maintained separately from the AIMS ID database. User information collected (as described above) as well as a 'user authentication' flag are stored indefinitely.

Once a Partner Connect account is established, users with appropriate permissions can view detailed institutional information or comprehensive account information for FSA customers to facilitate the administration of student aid. As stated previously, this data is sourced from other FSA back-end systems responsible for various Title IV functions and Partner Connect enables a consolidated view of information that is available in FSA systems today.

Please see 3.1 for the complete list of PII collected, used, maintained, or shared.

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

New System

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

New 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.

- The Higher Education Act of 1965 (HEA), as Amended, section 441 and 461 Title IV, section 401;
- Executive Order 13478—Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers
- 31 U.S.C 7701, Taxpayer Identifying Number

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.

☐ N/A

Student Aid Internet Gateway (SAIG), Participant Management System (18-11-10). March 1, 2018. 83 FR 8855.
https://www.federalregister.gov/documents/2018/03/01/2018-04141/privacy-act-of-1974-system-of-records

Common Origination and Disbursement System (18-11-02). August 16, 2019. 84 FR 41979-41987.
https://www.federalregister.gov/documents/2019/08/16/2019- 17615/privacy-act-of-1974-system-of-records

[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

National Student Loan Database System (18-11-06). September 9, 2018. 84 FR 47265-47271.
https://www.federalregister.gov/documents/2019/09/09/2019- 19354/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.

The records maintained or transmitted through Partner Connect follow the records disposition schedule for each back-end system. The applicable records schedules are as follows:

- ED Records Schedule No. 051 – National Student Loan Data System (DAA-0441-2017-0004) (ED 051). Records are destroyed 30 years after cutoff. Cutoff is annually when an applicable account is paid in full.
- ED Record Schedule No. 072 – FSA Application, Origination, and Disbursement Records (DAA-0441-2013-0002) (ED 072). This records schedule is being amended and pending approval by the NARA. Applicable records will be held indefinitely until the applicable NARA approved amendments are in effect.

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.

Partner Connect collects, uses, disseminates, or maintains each of the following:

General Information

- Full name
- Username
- Social Security number
- Taxpayer Identification Number
- Student loan account number
- Driver license number and issuing state
- Citizenship status
- Date of birth
- Contact information
- Home address;
- Home, work, alternate, and mobile telephone
- Email address

Household Information

- Family size, dependency status, marital status, spousal identifiers, estimated family contribution

Financial Information

- IRS Data for Income Based Repayments, (adjusted gross income, tax filing status and year, and exemptions), yearly income, credit report information

Employment Information

- Name, Employer Identification Number, address, phone number, website, begin and end date of employment

Loan/Grant Information

Dollar amount, payment milestones from origination through final payment
Promissory note information and eligibility information

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

Yes

Partner Connect collects the minimal PII needed by AIMS – first name, last name, date of birth, and last four digits of the SSN -- to create Partner Connect accounts and integrate with AIMS ID to enable a consistent authentication experience for users. This information is the minimum necessary to create the accounts and enable authentication.

Once accounts are established, users with appropriate permissions view detailed institutional information or comprehensive account information for FSA customers to facilitate the administration of student aid. The information is the minimum necessary to provide a consolidated view of the information that is available in the FSA systems listed above.

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

To enable accounts access and login to Partner Connect, individuals will provide their PII which will then be sent to AIMS to see if an account has been created. If an account is located, Partner Connect creates an account to match the AIMS account for that individual. If an account is not found, the user will receive either an email or be redirected to AIMS to obtain an account.

Once Partner Connect establishes a service with FSA's existing AIMS application for identity authentication and access services, the authenticated users with the appropriate permissions will be able to conduct specific searches and view the specified data that is processed and maintained by FSA back-end systems responsible for various Title IV functions throughout FSA.

These searches can result in the display of information regarding FSA customers (students, parents, borrowers) as well as Title IV institution specific information. This information is retrieved from the following FSA back-end systems using application programming interfaces (APIs):

- National Student Loan Data System (NSLDS)
- Common Origination and Disbursement (COD)
- Student Aid Internet Gateway (SAIG), Participant Management (PM) System

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

The PII collected via Partner Connect at fsapartners.ed.gov is provided directly from the individual or Title IV organizations when creating a Partner Connect account.

Postsecondary institutions and FSA staff users with the ability to access and view account information for FSA customers (students, parents, or borrowers) retrieve these records using one of the established PII data elements identified in 3.1. This information is retrieved from the listed FSA back-end systems (see question 3.3) using APIs.

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?

Data is collected directly from individuals, who are responsible for self-validating the correctness of the information. All information submitted must match the AIMS ID information exactly in order to be authenticated within Partner Connect. All other validation of records is the responsibility of the back-end system. Please consult the PIAs for the back-end systems to understand the validation process for the information maintained in those systems.

Use

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

PII is used for identification verification and throughout the student aid lifecycle and for Title IV aid administration purposes.

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

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.

Yes

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 SSN is the unique identifier for Title IV, HEA programs and is required by program participants and their trading partners to satisfy borrower identification, borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. The SSN is the required identifier for numerous business processes.

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

☑ N/A

The SSN is the unique identifier for Title IV, HEA programs and is required by program participants and their trading partners to satisfy borrower identification, borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. The SSN is first collected on the FAFSA and is the required identifier for numerous FSA business processes. The collection of SSNs of student, parent or borrower is required and authorized by 31 U.S.C. 7701 and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008). No alternatives currently exist for SSN collection.

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.

The information in each system that Partner Connect accesses is covered by a SORN, which provides notice to individuals. For FSA customers (students, parents, or borrowers), direct notice, prior to collection, is provided during the Free Application for Federal Student Aid (FAFSA) process at studentaid.ed.gov. for FSA customers (students, parents, or borrowers) A Privacy Act Statement is provided to users at the point of collection.

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

Please refer to the following systems' PIAs to obtain the most current and accurate notice information:

- COD PIA
- SAIG PIA
- NSLDS PIA
- AIMS PIA

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?

For external users, please refer to the PIAs listed in question 4.2 for what opportunities are available for users to consent to uses, decline to provide PII, or opt out.

Internal users may decline to have an account created on their behalf. However, access to Partner Connect and various FSA applications requires an account.

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

Authenticated users may view information available within Partner Connect but Partner Connect does not provide any of the data within the system to any external entities via email, data exchanges, etc.

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.

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.

[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.

5.9. 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?

All users have access to their account information through the Account Access management center built into FSA Partner Connect.

Borrowers may access their information as stated in the following systems' PIAs:

- COD PIA
- SAIG PIA
- NSLDS PIA
- AIMS PIA

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

Please refer to the following systems' PIAs to obtain the most current and accurate redress information:

- COD PIA
- SAIG PIA
- NSLDS PIA
- AIMS PIA

Internal users can modify and update demographic information in the Account Access management center built into Partner Connect.

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

Please refer to the following systems' PIAs to obtain the most current and accurate notice information:

- COD PIA
- SAIG PIA
- NSLDS PIA
- AIMS PIA

The system does not notify internal users on the procedures for correcting their information as there is an area within the system that allows for modifications.

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?

In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every FSA system must receive a signed Authorization to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security and privacy controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. The Partner Connect system is currently undergoing ATO activities and an ATO is scheduled to be received on March 26, 2021.

The security and privacy controls that are implemented for the system comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Access to the Partner Connect system is available only to users who have been authenticated to the Department of Education network using their Department-issued PIV and/or PIV-I card. Access to all privileged roles is controlled through processes that enforce formal requests and approvals for access on a need-to-know and least-privilege basis.

Additional examples of specific controls include multifactor authentication, encryption of data at rest and in transit, firewalls, Intrusion Prevention and Intrusion Detections Systems (IPS/IDS), event monitoring systems, penetration testing, system audits, user recertification, and threat management. Finally, all privileged users are provided a copy of the Rules of Behavior and are required to complete the annual Cybersecurity and Privacy Awareness training.

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.

Once this system becomes operational, the monitoring will begin to ensure the security and privacy controls work properly at safeguarding PII. Continuous monitoring,

scanning, and testing will commence once the Partner Connect enters the Ongoing Security Authorization (OSA) Program.

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 records are maintained in accordance with the provisions of the Federal Records Act, Departmental policies, and the Privacy Act, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system.

The system owner participates in all major security and privacy risk briefings, meets regularly with the information system security officer (ISSO), and participates in FSA's Lifecycle Management Methodology (LMM), which addresses security and privacy risks throughout the system's life cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as system of records notices, memorandum of understanding, interconnection security agreement, etc.

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?

The main privacy risks are the unauthorized access, use, or loss or control of the data which can result in identity theft or other forms of fraud. These risks are mitigated through various safeguards such as access controls, configuration management and anomaly detection, strict password rule and two-factor authentication capabilities, and continuous monitoring of intrusion detection and firewall alerts.