Privacy Impact Assessment (PIA)
for the

Person Authentication Services (PAS)
February 3, 2020

For PIA Certification Updates Only: This PIA was reviewed on **February 3, 2020** by **John Hsu** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: John Hsu / Information System Security Officer
Contact Email: John.Hsu@ED.GOV

System Owner

Name/Title: Robert Anderson / PAS System Owner
Principal Office: Federal Student Aid (FSA)

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.

Person Authentication Service (PAS) is used to generate authentication and log-on credentials for those individuals wishing to access the following student financial assistance systems to obtain information about their personal records:

- Free Application for Federal Student Aid (FAFSA)
- StudentAid.gov (Digital Customer Care)
- Borrower Defense (BD)
- Federal Student Aid Information Center (FSAIC)
- National Student Loan Data System (NSLDS) Student Access
- Health and Education Loan System (HEAL) Online Processing System (HOPS)
- Customer Engagement Management System (CEMS)
- Federal Student Aid Information Center (FSAIC) call center IVRU

PAS contains records about former, current and prospective students and parents who apply for an account User ID and password or PAS credentials.

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

The data collected by PAS is required to uniquely identify and authenticate users of various FSA information systems, which helps establish the level of trust, security, and non-repudiation required for FSA to safely advance its mission. This identification and authentication are also required to help ensure that a non-authorized person does not fraudulently conduct business on a legitimate user's behalf, or view data they are unauthorized to view.

[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

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

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.

The Higher Education Act of 1965, as amended, 20 U.S.C. 1092b, and Executive Order 9397 (November 22, 1943), 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

PAS has its own System of Records notice: SORN # 18-11-12, "Person Authentication Service, 80 FR 14981, Friday, March 20, 2015. https://www.federalregister.gov/documents/2015/03/20/2015-06503/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.

ED Record Schedule 0278

NARA Disposition: DAA-0441-2016-0001

Disposition: Temporary, depending on record type, destroy 5 years after annual cutoff or Destroy 75 year(s) after date of enumeration, or when no longer needed for Agency business, whichever is sooner.

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.

PAS collects the following information at the online registration website: first name, middle initial, last name, email address, date of birth, Social Security number (SSN), mailing address, mobile phone number, and security challenge questions and corresponding answers.

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.)?

This information is collected directly from the student or parent via the website when creating an FSA ID.

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

For users, the PII is collected from the FSAID.ED.GOV website (and StudentAid.gov beginning in FY20).

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?

The information provided is confirmed by matching the SSN with records maintained by the Social Security Administration as detailed in the Computer Matching Agreement - Match #1051 titled Social Security Numbers and Citizenship Status. Additional data validation is done to ensure form filling accuracy. Confirm fields are used to make users enter commonly misspelled information twice to reduce error. Additionally, form field validation such as character length and valid character restrictions are used to ensure the integrity of the information. These checks occur each time when a user creates an account or updates their account information.

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 data collected by PAS is required to uniquely identify and authenticate non-privileged users of various FSA information systems, which helps establish the level of trust, security, and non-repudiation required for FSA to safely advance its mission. This identification and authentication is also required to help ensure that a non-authorized person does not fraudulently conduct business on a legitimate user's behalf, or view data they are unauthorized to view.

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.

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

SSNs are required to provide matching with the Social Security Administration for identity verification purposes.

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 programs and its use is required by private and Federal program participants and their business partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. There is no alternative to the SSN for this use.

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 policy is linked on the FSA ID website. Additionally, all the FSA applications that PAS provides access to also have Privacy Act notices posted.

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

https://fsaid.ed.gov links to https://studentaid.gov/notices/privacy

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?

Provision of PAS information is voluntary; however, failure to provide the requested information will result in FSA not allowing access to those systems that require PAS login credentials.

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.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

PAS shares PII data with the following ED offices:

- Office of Inspector General (OIG) – PAS sends a monthly feed of PAS system data.
- Enterprise Data Warehouse & Analytics (EDWA) PAS sends a monthly feed of PAS system data.

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

☐ N/A

OIG requires PAS data to investigate fraudulent activities and perform analysis to prevent potential criminal activities. EDWA/COGNOS requires PAS data for business intelligence analysis and reporting purposes.

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.

Yes

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

User provided first names, middle initials, last names, date of birth, and Social Security Numbers are shared with the Social Security Administration for matching against their records to provide identity verification.

All PAS collected account information is available to be shared with the trusted systems listed in Section 1.1 of this document. These systems may use PAS information for disclosures to: Guaranty agencies, educational and financial institutions, Federal Loan Servicers, Federal Perkins Loan Servicers, and their authorized representatives; Federal, State, or local agencies and their authorized representative; private parties such as

[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.

relatives, business and personal associates, and present and former employers; creditors; consumer reporting agencies; adjudicative bodies; and the individual whom the records identify as the endorser or the party obligated to repay debt.

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

☐ N/A

PAS shares user provided first names, middle initials, last names, date of birth, and Social Security Numbers with the Social Security Administration for the purposes of identity verification matching. This is used to associate the PAS account to the identity of a real person, verified against an independent and authoritative source of trusted data.

All PAS information shared with PAS trusted systems stated in Question 1.1 may be used for the purposes defined in the PAS SORN # 18-11-12, "Person Authentication Service, 80 FR 14981, Friday, March 20, 2015.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

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

☐ N/A

Yes

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

☐ N/A

PII is shared with the external entities identified in Question 1.1 using encrypted lines of backend communication. PII shared with the Social Security Administration for identity verification matching is according to the Computer Matching Agreement - Match #1051 titled Social Security Numbers and Citizenship Status.

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

Yes

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

☐ N/A

Yes

6. Redress

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

Upon user registration, users are prompted to create their user IDs as well as their passwords and challenge questions. Users can access/modify their information at any time through this login. Users may also access their information by calling the Federal Student Aid help desk.

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

Users can access/modify their information at any time by logging in after selecting the designated manage account tab (or via Settings on StudentAid.gov). Users may call the help desk to correct information or start the account recovery process.

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

There is a link on the website to edit their FSAID. There are instructions on FSA websites on how to change their information. Individuals are also notified of the procedures for collecting their information through the posting of this PIA and the publication of the SORN listed in question 2.2.1.

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?

Transparent data encryption is used to protect data at rest. All websites and services provided by this system are available only through a secure HTTPS connection. An interface with SSA exists through the Central Processing System (CPS) to verify user data integrity. Multifactor authentication is required for all system support personnel. Endpoint security includes patch management and data loss prevention (DLP). Auditing, logging, monitoring, and response/alerts of selected indicators of compromise exist with threshold triggers. This system utilizes one-way hashing encryption for account passwords and challenge question answers. Web Application Firewalls protect, detect, monitor, alert, or block attacks such as Structure Query Language (SQL) injection and cross-site scripting. Physical safeguards exist for the system's physical host at the FSA Next Generation Data Center (NGDC). All building access is controlled and monitored by security personnel who check individuals entering the building for their employee or visitor badge.

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.

The system follows the FSA Continuous Diagnosis Monitoring (CDM) program including asset compliance scans and vulnerability scans conducted weekly for each application in production and non-production environments. FSA Security Operation

Center (SOC) team analyzes data and reports issues weekly to PAS ISSO and System Owner for remediation. PAS logs are also analyzed for outlier behavior. In addition, user logs are monitored on a monthly basis by the ISSO.

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 participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology, which addresses security and privacy risks throughout 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?

Privacy risks of unauthorized disclosure of PII are mitigated by limiting access and implementing controls to the PAS system. All users of this system of record are given unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy. Transparent data encryption is used to protect data at rest, and all websites and services provided by this system are available only through a secure connection and using DHS mandated protocols (TLS 1.2). Secure remote VPN access for all privileged support users with multifactor authentication is a requirement for all support personnel. Web application Firewalls (WAF) are in place to protect, detect, monitor, alert, or block attacks such as SQL injection and cross-site scripting. Periodic background investigations are conducted for internal staff members. ISSOs conduct periodic reviews to ensure access levels are adequate for each individual. Privileged account security, logging, and auditing controls are in place to reduce the risk of misused privileged insider attack.