Privacy Impact Assessment (PIA) for the
Person Authentication Service (PAS)

Oct 3, 2017

This PIA was approved on Oct 3, 2017 and reviewed on Sep 27, 2017 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: David W. Petersen
Contact Email: David.Petersen@ed.gov

System Owner

Name/Title: Ganesh Reddy
Program Office: Federal Student Aid (FSA)

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.

All text responses are limited to 2,000 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 N/A Describe the system including the system name, system acronym, and a brief description of the major functions.

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

- Free Application for Federal Student Aid (FAFSA)
- Studentaid.gov (ISE)
- StudentLoans.gov (SL)
- TEACH Grant Agreement to Serve (ATS)
- Federal Student Aid Information Center (FSAIC)
- National Student Loan Data System (NSLDS) Student Access
- Health and Human Services (HHS)
- Enterprise Complaint Service (ECS)
- Access and Identity Management System (AIMS)

PAS contains records about former, current, and prospective students and parents who apply for an Education account User ID and password or PAS credentials, and also those persons who previously had an Education Personal Identification Number (PIN). (The PIN system is replaced by PAS.)

1.2 N/A Describe the purpose for which the personally identifiable information (PII) 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 nonrepudiation 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.

1.3 N/A Is this a new system, or one that is currently in operation?

Currently Operating System
1.4 N/A Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

| Updated PIA | Original Publication Date: 01/09/2015 |

1.5 N/A Is the system operated by the agency or by a contractor?

Contractor

2. Legal Authorities and Other Requirements

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

2.1 N/A What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?


---

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.

2.2 N/A Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer YES or NO.

   Yes

2.2.1 N/A If the above answer is YES this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN name and number, or indicate that a SORN is in progress.

PAS has its own System of Records notice: SORN # 18-11-12, "Person Authentication Service," which was published in the Federal Register on March 20, 2015.

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 N/A Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

No, the system is waiting for final approval of the draft NARA schedule.

2.4 N/A Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer YES or NO.

   Yes

3. Characterization and Use of Information

Collection

3.1 N/A List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

PAS collects: first name, middle name, last name, email address, date of birth, Social Security number (SSN), cell phone number, and a security challenge questions and corresponding answers.

3.2 N/A Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer YES or NO.

   Yes

3.3 N/A What are the sources of information 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 user ID.

---

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/ons/Documents/SORN-Process.pdf
3.4 □ N/A  How is the information collected from stated sources (paper form, web page, database, etc.)?

The information is collected on the online registration website.

3.5 □ N/A  How is this information validated or confirmed?³

The information provided is confirmed by matching the SSN with the Social Security Administration.

Use

3.6 □ N/A  Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

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 nonrepudiation 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 □ N/A  Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

3.7.1 □ N/A  If the above answer is YES, what controls are in place to minimize the risk and protect the data?

3.8 □ N/A  Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 □ N/A  If the above answer is YES, please explain.

³ Examples include form filling, account verification, etc.
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  □ N/A Does the system collect Social Security Numbers? Please answer YES or NO.

Yes
3.9.1 □ N/A If the above answer is YES, explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

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 nonrepudiation 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.

3.10 □ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

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 □ N/A How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

A privacy policy is provided on the PAS enrollment website. There is also a link to view the Departmental privacy policy. A Privacy Act notice was posted on the PAS registration page. Additionally, all the FSA applications that PAS provides access to also have Privacy Act notices posted.

4.2 □ N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

https://studentaid.ed.gov/sa/privacy
https://www2.ed.gov/notices/privacy/index.html

4.3 □ N/A What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

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

5. Information Sharing

Internal

5.1 □ N/A Will information be shared internally with other ED organizations? Please answer YES or NO. If the answer is NO, please skip to Question 5.4.

Yes
5.2 □ N/A What information will be shared and with whom?

PA&S shares Name, DOB and SSN with the following Department of Education business units:
- Customer Experience
- Business Operations
- Ombudsman Group
- Technology Office

5.3 □ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The purpose as described in section 1.2.

External

5.4 □ N/A Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer YES or NO. If the answer is NO, please skip to Question 5.8.

Yes

5.5 □ N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

SSNs are shared with SSA.

5.6 □ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The purpose as described in section 1.2.

5.7 □ N/A How is the information shared and used by the external entity?

SSA uses the information sent by PAS to match the SSN with the user’s identity.

5.8 □ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer YES or NO.

Yes
5.9 □ N/A Does the project place limitation on re-disclosure? Please answer YES or NO.

Yes
6. Redress

6.1 □ N/A  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.

6.2 □ N/A  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 into their account.

6.3 □ N/A  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 the site on how to change their information.

7. Safeguards

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

7.1 □ N/A  Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer YES or NO.

| Yes |

7.2 □ N/A  What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

End users register for their own accounts and have access to their own information. PAS administrative users (developers, engineers, HelpDesk CSR, administrators, application users and project management personnel), have their own user names and passwords. PAS utilizes a role-based access controls which separates user roles and functions to protect privacy between other users. Also role-based access restricts access to the PII based on a need to know basis. A system matrix is used to define role and their associated responsibilities/capabilities. Additionally, Privileged Users have to accept the Privacy Act Acknowledgement online every time they login to PAS through AIMS using their FSA ID and password.

7.3 □ N/A  What administrative, technical, and physical safeguards are in place to protect the information?

---

*If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.*
FISMA controls implemented by PAS comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, data minimization and retention (DM), data quality and integrity (DI), Transparency (TR), 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.

7.4 □ N/A Is an Authority to Operate (ATO) required? Please answer YES or NO.

Yes

7.5 □ N/A Is the system able to provide account of any disclosures made? Please answer YES or NO.

Yes
7.6 □ N/A  Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 □ N/A  Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 □ N/A  Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

8. Auditing and Accountability

8.1 □ N/A  How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

FISMA controls implemented by PAS comprise a combination of management, operational, and technical controls. The following privacy controls are tested for implementation and control effectiveness as part of the department’s continuous monitoring program:

- Authority and Purpose (AP)
- Accountability
- Audit
- Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM),
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

8.2 □ N/A  What are the privacy risks associated with this system and how are those risks mitigated?
The risks are intentional/unintentional disclosure, theft, and or modification of borrower/parent PII data while in transit and at rest. The risks are mitigated through the implementation of the following controls:

- **Transparent data encryption is used to protect data at rest**
- **All websites and services provided by this system are available only through a secure connection (HTTPS)**
- **Interface with SSA (upon enrollment) through CPS to verify data (SSN) integrity**
- **Strong password requirements for end users**
- **Multifactor authentication requirements for all support personnel**
- **Endpoint security such as patch management and data loss prevention (DLP)**
- **Monitoring and Response**
  - Auditing, logging, and alerts of selected indicators of compromise and or threshold triggers (e.g. invalid log attempts, attempts to change a password from specific IP’s)
  - Security Information Event Management (SIEM)
- **Secure Remote VPN access for all privileged support users**
- **Web Application Firewalls to protect, detect, monitor, alert, or block attacks such as SQL injection and cross-site scripting**
- **Privileged account security/logging/auditing to reduce the risk of misused privileged insider attacks**
- **Automated vulnerability scanning**
  - Perimeter firewall
  - Perimeter IPS/IDS
- **Risk Assessments**
  - Continuous security control testing the FSA OSA program