



Privacy Impact Assessment

For
Person Authentication Service (PAS)

Date:
January 9, 2015

Point of Contact and Author:

Hanan Abu Lebdeh

Hanan.Abulebdeh@ed.gov

System Owner:

Ganesh Reddy

Ganesh.Reddy@ed.gov

Office of Federal Student Aid
U.S. Department of Education



1. System Information.

Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions. Indicate whether the system is new or existing and whether or not the PIA is new or being updated from a previous version; specify whether the system is “agency” or “contractor.”

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

- Free Application for Federal Student Aid (FAFSA)
- StudentLoans.gov
- TEACH Grant Agreement to Serve (ATS)
- Federal Student Aid Information Center (FSAIC)
- National Student Loan Data System (NSLDS) Student Access
- Direct Consolidation Loans
- Student Authentication Network (STAN)

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 being replaced by PAS.)

2. Legal Authority.

Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The Higher Education Act of 1965, as amended, 20 U.S.C. 1092b.

3. Characterization of the Information.

What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

PAS collects the following information at the online registration website: 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. This information is collected from the student or parent.

4. Why is the information collected?

How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

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.



Privacy risks are mitigated through multiple security and program reviews, the implementation of required Federal security and privacy controls, and a continuous monitoring program (see section 11 for more detail).

5. Social Security Number (SSN).

If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

SSN use is the only identifier accepted by the Social Security Administration (SSA). PAS is collecting the SSNs to verify, identify and check with the HHS, IRS, DHS and SSA.

6. Uses of the Information.

What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

- A. Information is used for authenticating users to public-facing FSA applications/websites, and to provide the identification and authentication information required by those applications and websites. This use varies according to the specific application. [PAS has the capability to provide applications with the profile data in a user's account described in #3. FSA will need to provide information regarding how it may be used by individual applications]. Data is collected directly from system users for their own accounts. The only data from external sources is to validate SSN with the Social Security Administration as described in #5.
- B. Data will be analyzed through secure identification and access management systems with strictly managed security policies. Data will also follow the Lightweight Directory Access Protocol (LDAP) to further support the security of the identification and authentication process.

7. Internal Sharing and Disclosure.

With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

PAS has no interfaces to other systems for the purposes of information sharing so this sharing would occur as the result of business processes outside of PAS.

8. External Sharing and Disclosure.

With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

PAS send SSNs to the SSA for the purpose describes in question #5; this information sharing with the SSA is in accordance with a signed computer matching agreement.



9. Notice.

Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

A Privacy Act notice will be posted on the PAS registration. Additionally, all the FSA applications that PAS provides access to also have Privacy Act notices posted.

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.

10. Web Addresses.

List the web addresses (known or planned) that have a Privacy Notice.

- Free Application for Federal Student Aid (FAFSA)
- StudentLoans.gov
- TEACH Grant Agreement to Serve (ATS)
- Federal Student Aid Information Center (FSAIC)
- National Student Loan Data System (NSLDS) Student Access
- Direct Consolidation Loans
- Student Authentication Network (STAN)

11. Security.

What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

In accordance with the Federal Information Security Management Act of 2002 (FISMA), PAS must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of action and milestones to remediate any identified deficiencies, and a continuous monitoring program. PAS is targeted to receive its ATO on Aug 5, 2014.

FISMA controls implemented by each PCA 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, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

PAS complies with the following Federal laws, standards, and guidelines:

- Federal Information Security Management Act of 2002
- Privacy Act of 1974
- E-Government Act of 2002
- Federal Information Processing Standards Publications (FIPS PUBS) on IT Security
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002
- NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, May 2010



- NIST SP 800-35, Guide to Information Technology Security Services, October 2003
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- NIST SP 800-40, Procedures for Handling Security Patches, November 2005
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, September 2009
- NIST SP 800-42, Guidelines on Network Security Testing, October 2003
- NIST SP 800-44, Guidelines on Security Public Web Servers, September 2007
- NIST SP 800-45, Guidelines on Electronic Mail Security, February 2007
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002
- NIST SP 800-50, Building an Information Technology Security Awareness Program, October 2003
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems, August 2009
- NIST SP 800-55, Performance Measurements Guide for Information Security, July 2008
- NIST SP 800-58, Security Considerations for Voice Over IP Systems, January 2005
- NIST SP 800-60, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-60, Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-61, Computer Security Incident Handling Guide, March 2008
- NIST SP 800-64 Security Considerations in the Systems Development Life Cycle, October 2008
- NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process. January 2005
- NIST SP 800-70, National Checklist Program for IT Products: Guidelines for Checklists Users and Developers, February 2011
- NIST SP 800-77, Guide to IPsec VPNs, December 2005
- NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide, April 2010
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling, November 2005
- NIST SP 800-88, Guidelines for Media Sanitization, September 2006
- NIST SP 800-92, Guide to Computer Security Log Management, September 2006
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007
- NIST SP 800-95, Guide to Secure Web Services, August 2007
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007
- NIST SP 800-113, Guide to SSL VPNs, July 2008
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, April 2010
- NIST SP 800-123, Guide to General Server Security, July 2008 and
- NIST SP 800-124, Guidelines on Cell Phone and PDA Security, October 2008



Department of Education Policies:

- Department of Education Handbook for Information Technology Security
- Department of Education Handbook for Information Technology Security General Support
- System and Major Application Inventory Procedures
- Department of Education Handbook for Certification and Accreditation Procedures
- Department of Education Handbook for Information Technology Security Configuration Management Procedures
- Department of Education Handbook for Information Technology Security Contingency Planning Procedures
- Department of Education Information Technology Security Test and Evaluation Plan Guide
- Department of Education Incident Handling Program Overview
- Department of Education Handbook for Information Technology Security Incident Handling Procedures
- Department of Education Information Technology Security Training and Awareness Program Plan.

12. Privacy Act System of Records.

Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

A system of records notice has been drafted and is under review.

13. Records Retention and Disposition.

Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

PAS maintains and disposes of its records in accordance with the following records retention schedule:

Schedule locator number: 083

Approved date: 05/03/2010

Title: Personal Identification Number (PIN) Registration System

Principal office: Federal Student Aid (FSA)

NARA Disposition Authority: N1-441-09-26.