

**Privacy Impact Assessment (PIA)**

for the

**Access and Identity Management System (AIMS)**

**Sep. 5, 19**

**For PIA Certification Updates Only:** This PIA was reviewed on September 5, 2019 by Yolanda Hutcherson 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: Yolanda Hutcherson / AIMS System Owner / Infrastructure Operations**

**Principal Office: Federal Student Aid (FSA)**

**Please submit completed Privacy Impact Assessments to the Privacy Office at** [**privacysafeguards@ed.gov**](mailto: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.***

# Introduction

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

The Access and Identity Management System (AIMS) application provides identity authentication and access services for FSA users. AIMS users are comprised of internal and external users. Internal users are FSA employees. External users are FSA partners and FSA support contractors. FSA partners includes Destination Point Administrators (DPAs) at Title IV institutions, Private Collection Agency (PCA) staff, and Not-for-Profit and Title IV Additional servicers. The AIMS application is comprised of tools and technologies that ensure secure access of systems across the enterprise. In particular, the AIMS application provides tools, technologies, and protocols for identity and access management. AIMS provides consistent access control, authorization, and auditing across the entire FSA enterprise.

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

The PII is collected in order to generate a unique user ID in AIMS for user authentication and authorization to provide access to FSA applications. The following FSA applications are authenticated by AIMS:

Central Processing System – FAA Access (CPS FAA)

Common Origination and Disbursement (COD)

Digital Communication Tool (DCT)

Enterprise Data Warehouse and Analytics (EDWA) Cognos

Enterprise Business Collaboration (EEBC) – Performance Award Tracking system (includes HSP, FIMS, SBM)

Electronic Cohort Default Rate Appeals (eCDR)

Enterprise Service Bus (ESB) message Status Inquiry Tool (MSIT)

Experimental Sites Data Collection Instrument (XSITES)

eZ-Audit Datamart (MicroStrategy)

Federal Feedback system (Formerly – enterprise Complaint System (ECS) – CEMS (Servicers)

Financial Partners Datamart (MicroStrategy)

FSA Information Center (FSAIC) Oracle RightNow Cloud Solution (ORCS) CRM

HEAL Online Processing System (HOPS)

Integrated Student Experience (ISE) Admin Site

Student Aid Internet Gateway (SAIG) EDconnect – client software

Integrated partner management (IPM) Document Management

National Student Loan Data System (NSLDS FAP and NSLDS Training)

NetScaler VPN Appliance

Ombudsman Case Tracking System / Gainful Employment customer service/Borrower Defense (OCTS/GECS/BD))

Student Aid Internet Gateway Enrollment (SAIG) / Participation management (PM)

Student Aid Internet Gateway Enrollment Customer Service Site (PM CS)

Student Aid Internet Gateway Help Desk Customer relationship management (CRM)

Partner Enterprise Business Collaboration (PEBC) - SharePoint

PAS Administration / CSR Tool

Teamsite FSA (EITI)

* 1. Is this a new system, or one that is currently in operation?  
     Currently Operating System
  2. Is this PIA new, or is it updating a previous version?  
     Updated PIA
  3. Is the system operated by the agency or by a contractor?

Contractor

* + 1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

Yes

# Legal Authorities and Other Requirements *If you are unsure of your legal authority, please contact your program attorney.*

* 1. Whatspecific 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**

* 1. 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  
     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]](#footnote-2) Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.



Student Aid Internet Gateway (SAIG), Participation Management System (83 FR 8855) Date: March 01, 2018.

* + 1. 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.



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**](mailto:RMHelp@ed.gov)

* 1. 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 Record Schedule GRS 3.2 item 031

Disposition: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Disposition Authority: DAA-GRS2013-00060004

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

# Characterization and Use of Information

**Collection**

* 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.

The elements of Personal Identifiable Information (PII) maintained by the AIMS system are Username, First Name, Last Name, Date of Birth, and last four digits of the Social Security number.

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

Yes

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

For external users, the first point of collection is SAIG enrollment (PM) web site <https://fsawebenroll.ed.gov/PMenroll/index.jsp> where external users enter name, email, address, phone number, date of birth, and last four digits of the Social Security number. The account information is passed to AIMS to establish AIMS ID.

For internal users, the first point of collection is the FSA application security access form provided by the Application ISSO on behalf of the internal Department employee.

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

For external users, the PII is collected from SAIG Enrollment (PM) website and stored in a database. The information is passed to AIMS for processing AIMS ID.

For internal users, the application security access forms are received electronically via scanned images. The scanned images are digitally signed, approved and retained on department’s OneDrive for audit purposes. In the rare instance when we do receive the AIMS paper access request form, the access request forms are converted to scanned images and the AIMS paper access request are shredded immediately.

* 1. How is the PII validated or confirmed to ensure the integrity of the information collected?[[3]](#footnote-3) Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

For external customers that enroll via SAIG Enrollment (PM), PM validates account information via the Central Processing System (CPS) match with Social Security Administration (SSA).

For internal customers, no PII data is collected. Validation of account information is cross checked by AIMS ISSO within the Department’s Security Manager, which provides account information for all ED staff and contractors that require background investigations and clearances.

**Use**

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

This information is collected in order to generate a unique user ID in AIMS for user authentication and authorization to provide access to FSA applications leveraging AIMS.

* 1. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?   
       
     No  
     1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?



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.*

* 1. 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

* + 1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.



For AIMS account creation, AIMS uses only the last four digits of an SSN in order to verify a unique identity that is created when the user registers for an account. Due to the fact the primary registration point for the external customers (Participation Management) uses SSN, date of birth, and the user's name to uniquely identify a user, there was no alternative to the collection and use of the SSN. SSNs are never sent from AIMS to other FSA or ED systems.

* + 1. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.



Last name and first name were considered but were not selected because the application needed a unique identifier.

# Notice

* 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.

For external users, the SAIG Participation Management SORN, which includes AIMS, provides individuals information about the collection of PII prior to the collection and enrollment. SAIG Enrollment (PM) web site is the first point of entry collection, so SAIG Enrollment (PM) web site provides the Privacy notice.

For internal users, direct notice is not provided to individuals because request forms are filled out on behalf of the employee by the application’s ISSO and is often required to support specific job duties or functions. If internal users public notice through this PIA is provided.

* 1. 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.



For external users, SAIG Enrollment (PM) web site is the first point of entry collection. The notice is provided by SAIG Enrollment (PM) web site.

<https://fsawebenroll.ed.gov/PMEnroll/index.jsp>

For internal users, there is no direct notice but rather public notice in the form of this PIA.

* 1. 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, applying for access to FSA applications, the external user must consent to uses of their PII data as outlined in the SAIG Enrollment (PM) SORN. If a user wants to opt out of PM, the primary destination point administrator from that specific institution will need to request PM to disable the account. PM sends feed to AIMS indicating account is disabled.

Internal users may decline to have an account created on their behalf however access to AIMs and various FSA applications is often dependent on job duties so there is limited flexibility in consenting to various uses.

* 1. 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

# Information Sharing and Disclosures

**Internal**

* 1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.  
       
     No
  2. What PII will be shared and with whom?



Click here to enter text.

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



Click here to enter text.

**External**

* 1. 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
  2. What PII will be shared and with whom? List programmatic disclosures only.[[4]](#footnote-4)   
     **Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.



Click here to enter text.

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



Click here to enter text.

* 1. Is the sharing with the external entities authorized?



Click here to select.

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



Click here to select.

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



Click here to enter text.

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



Click here to select.

* 1. Does the project place limitation on re-disclosure?  
       
     Click here to select.



# Redress

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

For external users, the Primary Destination Point Administrator (PDPA) can view and modify account information for DPAs assigned to the PDPA’s Title IV institution after login. For internal users, individuals cannot access their account information. In order to update account information, internal users must contact the Application ISSO or AIMS ISSO to have the updates made to the internal user’s profile. Procedures for allowing external individuals to access their own information are explained in the System of Records notice listed in question 2.2.1

For internal users, they can request to view their information via the AIMS ISSO.

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

For external users, the Primary Destination Point Administrator (PDPA) can modify and update demographic information for DPAs assigned to the PDPA’s Title IV institution after login. For internal users, individuals cannot update their account information. In order to update account information, internal users must contact the Application ISSO or AIMS ISSO to have the updates made to the internal user’s profile. Procedures for allowing external individuals to access their own information are explained in the System of Records notice listed in question 2.2.1.

For internal users, they can contact AIMS ISSO to coordinate updates to the user’s profile.

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

The System of Records notice listed in question 2.2.1 explains the procedures for correcting external customer information.

For external customers, PDPAs are instructed to contact the system manager listed in the SAIG, Participation Management SORN and provide their name, user ID, and any other identifying information to distinguish between individuals of the same name. For internal customers, AIMS ISSO updates AIMS account information for individuals upon request from individual.

For internal customers, upon initial request for AIMS access, the access form indicates changes to demographic or access requires an updated AIMS access form.

# Safeguards *If you are unsure which safeguards will apply, please consult with your* [*ISSO*](https://share.ed.gov/teams/OCIO/IA/SEA/SEA_Collab/SitePages/ED%20ISSOs.aspx)*.*

* 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

* 1. Is an Authority to Operate (ATO) required?  
       
     Yes
  2. Under [NIST FIPS Pub. 199](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf), what is the security categorization of the system: **Low, Moderate, or High?**  
     Moderate



* 1. What administrative, technical, and physical safeguards are in place to protect the information?

FSA information is governed by the concepts of least privilege and separation of duties. All system access is granted by predefined roles and privileges, and all FSA system users must undergo a Federal background security clearance process. AIMS uses multi-factor authentication including username/password, one-time password (OTP) via hard or soft VIP token.

* 1. 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

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

Yes

* 1. 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 weeklyfor each application in production and non-production environments. FSA SOC team analyzes data and reports issues weekly to AIMS ISSO and System Owner for remediation. AIMS logs are also forwarded to Splunk team for analysis with Splunk tool. In addition, user logs are monitored on a monthly basis by the ISSO.

# Auditing and Accountability

* 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.

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

Yes

* 1. 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 AIMS system. All users of this system of record is given unique user identification and is 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.

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](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf) [↑](#footnote-ref-1)
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> [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
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. [↑](#footnote-ref-4)