Privacy Impact Assessment

For
Access and Identity Management System (AIMS)

Date:
July 25, 2016

Point of Contact:
Hanan AbuLebdeh (202) 377-4678, Hanan.Abulebdeh@ed.gov

System Owner:
Ganesh Reddy, (202) 377-3557, ganesh.reddy@ed.gov

Author:
Hanan AbuLebdeh

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

   Access and Identity Management System (AIMS) provides a framework to enforce and assist user access management, controls, and security related services for Federal Student Aid systems and Department of Education systems. The architecture includes access management tools, identity management tools, enterprise policy repositories, enterprise user repositories, two-factor authentication and other related security components.

   The core COTS product for AIMS includes; IBM Security Access Manager (SAM), IBM Tivoli Identity Manager (TIM), Federated Identity Manager (FIM), and custom-developed code that is designed to provide a standardized set of enterprise security services and controls for FSA's web applications

   Components or functions supported by AIMS include:
   - **Authentication and Authorization –** Using Security Access Manager to enable consistent Authentication, Authorization, & Accountability
   - **Customer User Interface (AIMS CUI)** - A custom-developed application to allow users to self-register for user accounts and approvers (DPAs or SSOs) to approve and manage users. There is also the ability for users to edit their profile.
   - **AIMS Reusable Common Services (RCS)** - A set of web services functions to facilitate interactions between applications and AIMS for user provisioning, account modification, authorization checks, and to retrieve user data.
   - **Two-Factor Authentication (TFA)** - TFA is a service to integrate with Symantec's Validation and ID Protection Service (VIP) services to provide a second form of authentication to validate a user's access. The user is required to enter their one-time passcode generated from a physical or soft token.
   - **Federation authentication -** A framework to provide web and federated single sign-on using known protocols (i.e. SAML, Liberty).
   - **Department of Education PIV (Personal Identification Verification) –** The framework in providing single sign-on using PIV credentials.

   The AIMS solution supports over 70,000 Power Users (Users who have access to other users' PII) (Partners, Employees, Contractors) and secures critical web systems at Federal Student Aid.

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?

   The elements of Personal Identifiable Information (PII) are collected and maintained by the system are Username, First Name, Last Name, Date of Birth, and the Last 4 digits of SSN. This information is derived from the users of the following applications: eCB, eCDRA, FSA Acquisitions, MicroStrategy, TeamSite, Experimental Sites, and Participation Management. The information is

collected from the website when a user registers as DPA, FAA, or through a PM feed and/or Active Directory feed. The information is not used to link or cross-reference any multiple databases.

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 information is collected in order to generate a unique user ID in AIMS for user authentication and authorization to provide access to those applications. This information is used to ensure that users do not get duplicate accounts created when they register for multiple systems or via multiple sources.

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.

   Only the last four digits of an SSN are collected in order to verify a unique identity that is created when the user registers for an account. Due to the fact that the primary registration point for the partner users (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. The last 4 digits of the SSN are never sent from AIMS to other FSA or ED systems.

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.

   AIMS provides a common security infrastructure for multiple Federal Student Aid web applications; AIMS uses the information for user account and ID creation for authentication and authorization.

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?

   Data exchanges between AIMS and other IT systems:

   The last 4 digits of SSN are never sent from AIMS to other FSA or ED systems.

   The eCB system uses user account information for users authenticated and authorized by Security Architecture. This information includes: username, first name, last name, date of birth (MMDD), ecbid (combination of OPEID and access right per year), access groups, and sessionID. AIMS does not share the user's full date of birth with the eCB system (the year is omitted).

   No other AIMS-protected systems receive any privacy-related data from AIMS.

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?

AIMS does not share privacy information with external systems.

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?

The AIMS system provides a link to the Department's Privacy and Security Policy Notices (http://www.ed.gov/notices/privacy/index.html and http://www.ed.gov/notices/security/index.html) located at the bottom of the pages.

10. **Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.**
https://cbfisap.ed.gov/ecb/CBSWebApp/servlet/CBServlet?Login.x=30&Login.y=10
https://cbfisap.ed.gov/enrole/SAphaseIVWeb/ecb/confirmIdentity.jsp?url=cbfisap.ed.gov
https://cbfisap.ed.gov/dpaadmin/SAphaseIVWeb/ecb/displayPendingRequests.do?url=cbfisap.ed.gov
https://ecdrappeals.ed.gov/ecdra/eCDRAppeals/viewCurrentCases.htm
https://ecdrappeals.ed.gov/enrole/SAphaseIVWeb/eAppeals/confirmIdentity.jsp?url=ecdrappeals.ed.gov
https://ecdrappeals.ed.gov/dpaadmin/SAphaseIVWeb/eAppeals/displayPendingRequests.do?url=ecdrappeals.ed.gov
https://sa.ed.gov/enrole/SAphaseIVWeb/jsp/selectApplications.jsp
https://experimentalsites.ed.gov/exp/ExSitesWebApp/Controller
https://fsateamsite.ed.gov/
https://faaaccess.ed.gov/FOTWWebApp/FaaAccessServlet
https://fsawebenroll.ed.gov/PMEnroll/index2.jsp
https://sa.ed.gov/enrole/SAWeb/forgotPwd.jsp
https://sa.ed.gov/enrole/SAWeb/changePwd.jsp
https://sa.ed.gov/enrole/SAWeb/forgotUserID.jsp
https://sa.ed.gov/profile/SAphaseIVWeb/jsp/editMyAccount.jsp
https://www.nsldsfap.ed.gov/nslds_FAP/
https://www.nsldstraining.ed.gov/nslds_FAP/
https://faaisir.ed.gov
https://itacsfsawebenroll.ed.gov
https://eaiweb.ed.gov/msit/MSIT/index.jsp
https://microstrategy.ed.gov/mstr
https://fp-mart.ed.gov/mstr/
https://sa.ed.gov/cas/CASWeb/pages/Authentication.faces
https://partners.ed.gov/fsa
https://sa.ed.gov/enrole/FsaicRegWar/
https://sa.ed.gov/enrole/SAWeb/selfmenu.jsp
https://sa.ed.gov/tfa/aimstfa/app/selfservice.jsp
https://sa.ed.gov/cas/CASWeb/pages/TFA/fytoken/fytmenu.faces
https://sa.ed.gov/sso/AIMSSecurityDashboard
https://sa.ed.gov/helpdesk/AIMSHelpdesk/index.htm

https://sa.ed.gov/helpdesk/cpshlpdsk/main.jsp
https://sa.ed.gov/profile/AimsUserMgtWar/manageUsers.htm
https://cbfisap.ed.gov/profile/LDAPUtils/index.jsp
https://cbfisap.ed.gov/helpdesk/LDAPUtils/index.jsp
https://aims.ed.gov/cas/CASWeb/pages/Authentication.faces
https://aims.ed.gov/cas/CASWeb/Essoauth
https://fsadatacase.ed.gov
https://ipm.ed.gov
https://fsavdc.ed.gov
https://www.g5.gov

The following external application leverages AIMS authentication. The user's are redirected to https://sa.ed.gov/cas/CASWeb/pages/Authentication.faces for login.

Salesforce URL: https://fsaocts.my.salesforce.com
Office 365 URL: https://cpssaig.crm9.dynamics.com/main.aspx
HP ORCS URL: https://studentaidhelp.ed.gov/app/account/launch_page

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?

    The information is stored in the IBM Directory Server (LDAP); the BMC Portal monitoring tool is used to monitor the AIMS servers, audit data are logged and derived in IBM Security Access Manager (SAM) and IBM Tivoli Identity Manager (TIM). The WebSEAL component of Security Access Manager is used for authentication. AIMS Security Authorization was completed in early 2014 and AIMS has been granted the ATO in 4/7/2014. After that date; AIMS is enrolled in the Ongoing Security Authorization program.

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?

    The registration process currently follows the PM registration processes and is encapsulated by the PM SORN notice: Student Aid Internet Gateway (SAIG), Participation Management System (75 FR 74, 20346-50) Date: April 19, 2010.

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:

    ED 273 - FSA Access and Identity Management System (AIMS) is the retention and disposition schedule, and was approved by NARA and published in January 2016.