Privacy Impact Assessment (PIA)
for the

Access and Identity Management System (AIMS)
June 1, 2023

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Jordan Hughes / Information System Security Officer
Contact Email: Jordan.Hughes@ed.gov

System Owner

Name/Title: Yolanda Hutcherson / Information System Owner
Principal Office: Federal Student Aid

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.

The Access and Identity Management System (AIMS) is a U.S. Department of Education (Department) system that authorizes internal Department and external users to access Federal Student Aid (FSA) applications. AIMS provides identity authentication and access services for FSA applications, allowing users to be easily identified, authenticated, and managed. AIMS provides access to web applications' URLs for users to access specific FSA application systems. AIMS also provides users' credentials including AIMS Identification (ID) and password to log in to FSA applications.

Users cannot access AIMS-protected FSA applications without first logging into AIMS. Internal users are Department employees and contractors. External users are FSA partners including Destination Point Administrators (DPAs) (i.e., financial aid office members or servicers managing Higher Education Act of 1965 (HEA) Title IV (Title IV) programs on behalf of an institution of higher education to receive Title IV funds) and staff of Not-for-Profit, guaranty agencies, and State and local education agencies.

There are two processes for users to gain an AIMS ID for access to FSA application systems.

Internal Department Users

For internal Department users, the FSA application security access form is submitted by the user requesting AIMS ID or the user's supervisor to the respective Information System Security Officer (ISSO) for the AIMS-protected FSA application for which the user requests access. After supervisor and ISSO approval, the AIMS ID is generated for the requesting user.

External Users

External users enroll by completing a web application on the Student Aid Internet Gateway (SAIG) Participation Management (PM) website. SAIG PM passes customer data to AIMS after the SAIG Enrollment application has been processed. User information, including name, last four digits of Social Security number (SSN), and date of birth, is passed to AIMS to establish a unique AIMS ID and/or identify the FSA

application systems to which the user has access. AIMS uses the SSN coupled with name and email address to determine whether the user has an existing AIMS ID, whether the user is a new user, or whether the user has the same name as an existing user. This process helps prevent the creation of duplicate AIMS IDs for one individual or assigning access to an incorrect individual.

Once an AIMS ID has been established, internal Department and external users can request access to additional FSA systems. These requests are vetted by the ISSO of the FSA application system for which access has been requested.

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

PII is collected to generate a unique user ID in AIMS to provide access to FSA applications. The following FSA applications are authenticated by AIMS (* denotes applications that are only accessible by internal Department users):

- Amazon Web Services (AWS) Console / NextGen Data Center (NGDC)
- Box.com
- Common Origination and Disbursement (COD)
- Central Processing System (CPS)*
- Digital and Customer Care (DCC) Customer Care Platform (CCP)*
- Enterprise Business Management System (EBMS)*
- Electronic Cohort Default Rate Appeals (eCDR Appeals)
- Enterprise Data Management and Analytics Platform Services (EDMAPS)*
- Financial Management System (FMS)*
- FSA Citrix Web Two Factor Authentication (TFA)*
- HEAL Online Processing System (HOPS)
- Integrated Technical Architecture (ITA)*
- Message Status Inquiry Tool (MSIT)*
- Microsoft Dynamics 365 (GDIT CRM Solution)*
- NetScaler Virtual Private Network (VPN) Appliance*
- NextGen Data Center (NGDC) CyberArk*
- National Student Loan Data System (NSLDS) / Financial Aid Professionals (NSLDSFAP)
- NSLDS / Training Site (NSLDS Training)
- Partner Enterprise Business Collaboration (PEBC)
- Person Authentication Service Admin Application (PAS Admin)*
- Partner Participation Oversight Portal (PPO) / FSA Partner Connect

[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

- SAIG EDConnect Desktop Client
- Student Aid Information Gateway (SAIG) Participation Management (PM) Enrollment

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

The PIA is being reviewed as part of the biennial review process.

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. 1070, 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.

☐ N/A

The SORN, titled "Student Aid Internet Gateway (SAIG), Participation Management System," 18-11-10, 83 FR 8855, was published in the Federal Register on March 1, 2018.

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

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.

General Record Schedule (GRS) 3.2 item 031, "System access records."

Disposition: Temporary. Destroy when 7 years 6 months after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Disposition Authority: Disposition Authority: N1-GRS-07-3, item 13a1 & N1-GRS-07-3, item 13a2.

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

Yes

[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

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.

The elements of PII maintained by AIMS are full name, date of birth, work email address, work address, work phone number, signature (digital or wet), last four digits of the SSN, username (AIMS ID), and password.

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

Yes

AIMS collects only the minimum amount of PII required to establish a new AIMS account and to add or remove services to an existing AIMS account in order to access FSA systems. The PII collected ensures duplicate AIMS accounts are not generated for individuals with existing accounts who have had name changes to first or last name or change in email address. The PII collected also prevents AIMS from assigning two different individuals with same name the same AIMS ID. When two individuals have the same name, the partial SSN is used to determine that these are two different people. If individuals do not provide the required PII, it would prevent the individuals' access to FSA systems.

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

For external users, PII is collected through the FSA SAIG PM website from which account information is passed to AIMS to establish an AIMS ID.

For internal Department users, PII is collected through the FSA application security access form submitted by the application ISSO, AIMS ISSO, or the requestor's supervisor.

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 external users, PII is collected from the SAIG PM website through webforms and passed via daily nightly batches from SAIG PM to AIMS for processing and establishing AIMS IDs.

For internal Department users, the security access forms are received via email with the encrypted access form as an attachment. The access forms are processed for establishing AIMS IDs for internal Department users. The access forms are digitally signed, approved by AIMS ISSO, and retained on the Department's OneDrive for audit purposes. In the rare instance when AIMS paper access request forms are received, the access request forms are scanned, and the paper forms are shredded immediately.

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?

For external users, the SAIG Enrollment agreement is completed and signed by the Chancellor, President, or Chief Executive Officer (CEO) attesting that the information provided is true and designating a Primary Destination Point Administrator (PDPA) and DPA. These individuals administer the Title IV programs on behalf of the institution and require access to AIMS to gain access to FSA application systems. The signer of the SAIG Enrollment agreement is responsible for validating PII information submitted to SAIG PM for accessing FSA application systems.

For internal Department users, account information is individually manually verified by the AIMS ISSO within the Department's Security Management system, PerSec, which provides security clearance information for all Department employees and contractors that require background investigations and clearances. To gain access to AIMS, internal Department users must have a Public Trust (Tier 4) preliminary clearance.

Use

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

PII is collected to generate a unique user ID in AIMS. AIMS authorizes users to access FSA applications. Users cannot access AIMS-protected FSA applications without first logging into AIMS.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

[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.

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

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

For external users, AIMS uses the last four digits of an SSN to verify that the customer does not already have established AIMS ID or whether there is another customer with the same name. This process ensures that a duplicate ID will not be created for individuals with the same name.

For internal Department users, account information is verified by the AIMS ISSO within PerSec, which provides security clearance information for all Department employees and contractors that require background investigations and clearances. As part of this process, the PII (to include SSNs) for these individuals are stored in PerSec, which is used for identity validation in order to ultimately obtain an AIMS ID.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

Full name was considered as an alternative; however, SSNs were selected as they are the only identifiers that could reliably ensure duplicate accounts were not assigned to the same individual.

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 Act Statement is located on the SAIG PM enrollment form. For internal Department and external users, the SAIG PM SORN, which covers AIMS, provides information about the collection of PII during the enrollment process.

Direct notice is provided to individuals during the login process after AIMS authentication, but prior to allowing access to requested FSA application system, where the Privacy Act Statement and Rules of Behavior (ROB) are displayed.

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

Privacy Act Statement

We use the information that you provide on this application to enroll your organization and its users for services with Federal Student Aid systems.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM AND DISCLOSURE OF SOCIAL SECURITY NUMBERS:

Title IV of the Higher Education Act of 1965, as amended (HEA); 20 U.S.C. 1070 et seq.: Section 31 U.S.C. 7701: and Executive Order 9397 (November 23, 1943), as amended by Executive Order 13478 (November 18, 2008) authorize the collection of Social Security numbers of users of this system. The Social Security number is voluntary in order to identify individuals for Federal purposes, but you will not be provided with access to or use of the system if you do not provide a Social Security number.

PURPOSE(S):

The information in this system entitled “Student Aid Internet Gateway (SAIG), Participation Management System” (18-11-10) is maintained for the purposes of: (1) Processing stored data from the SAIG Enrollment Forms (Web and paper versions); (2) maintaining the SAIG Enrollment Web site (titled https://fsawebenroll.ed.gov); (3) managing the assignment of individual electronic SAIG mailbox numbers, known as

‘‘TG numbers’’; (4) authorizing users of the CPS, NSLDS, Common Origination and Disbursement (COD) System, Financial Management System (FMS), Enterprise Complaint System (ECS) (now known as Customer Engagement Management System [CEMS]), and the Access and Identity Management System (AIMS); and (5) or other Federal agencies' systems for the purposes of administering the HEA programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:
The Department may disclose information contained in a record in this system of records under the routine uses listed in the system of records notice, which was published on March 1, 2018 (83 Fed. Reg. 8855-8859) (https://www.federalregister.gov/documents/2018/03/01/2018-04141/privacy-act-of-1974-system-of-records) without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected.

These disclosures may be made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act of 1974, as amended (Privacy Act), under a computer matching agreement.
(1) Program Disclosures. The Department may disclose records maintained in the SAIG, Participation Management System, to other Federal agencies' systems for the purpose of allowing authorized users who are eligible to participate in the electronic exchange of data with the Department to transmit files to and from the following databases and access the Department's websites online for the purposes of administering or assisting in administering programs authorized under Title IV of the HEA:
(a) COD System;
(b) CPS;
(c) NSLDS;
(d) FMS;
(e) ECS/CEMS;
(f) FSA Partner Connect;
(g) AIMS; and
(h) Other Federal agencies' systems for the purposes of administering the HEA programs.

The Department will only disclose records from this system to other Federal agencies' systems for purposes of administering or assisting in administering programs authorized under Title IV of the HEA and only after the Department has approved in writing a request from other Federal agencies' systems to access these records.
(2) Freedom of Information Act (FOIA) Advice or Privacy Act Disclosure. The Department may disclose records to the Department of Justice (DOJ) or the Office of

Management and Budget (OMB) if the Department seeks advice regarding whether records maintained in the system of records are required to be disclosed under the FOIA or the Privacy Act.

(3) Disclosure to the DOJ. The Department may disclose records to the DOJ to the extent necessary for obtaining DOJ advice on any matter relevant to an audit, inspection, or other inquiry related to the programs covered by this system.

(4) Contract Disclosure. If the Department contracts with an entity to perform any function that requires disclosing records to the contractor's employees, the Department may disclose the records to those employees. As part of such a contract, the Department shall require the contractor to protect the security and confidentiality of the records in the system.

(5) Litigation and Alternative Dispute Resolution (ADR) Disclosures.

(a) Introduction. In the event that one of the following parties is involved in judicial or administrative litigation or ADR, or has an interest in judicial or administrative litigation or ADR, the Department may disclose certain records to the parties described in paragraphs (b), (c), and (d) of this routine use under the conditions specified in those paragraphs:

i. The Department, or any of its components;

ii. Any Department employee in his or her official capacity;

iii. Any Department employee in his or her individual capacity where the DOJ agrees to or has been requested to provide or arrange for representation of the employee;

iv. Any Department employee in his or her individual capacity where the Department has agreed to represent the employee;

v. The United States where the Department determines that the litigation is likely to affect the Department or any of its components.

(b) Disclosure to DOJ. If the Department determines that disclosure of certain records to the DOJ is relevant and necessary to judicial or administrative litigation or ADR, and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to the DOJ.

(c) Adjudicative Disclosures. If the Department determines that disclosure of certain records to an adjudicative body before which the Department is authorized to appear or to a person or entity designated by the Department or otherwise empowered to resolve or mediate disputes, is relevant and necessary to the judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to the adjudicative body, person, or entity.

(d) Parties, Counsel, Representatives, and Witnesses. If the Department determines that disclosure of certain counsel, representative, or witness is relevant and necessary to the judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to the party, counsel, representative, or witness.

(6) Research Disclosure. The Department may disclose records to a researcher if the official serving or acting as the Chief Operating Officer of Federal Student Aid determines that the individual or organization to which the disclosure would be made is qualified to carry out specific research related to functions or purposes of this system of records. The official may disclose records from this system of records to that researcher solely for the purpose of carrying out that research related to the functions or purposes of this system of records. The researched to agree to maintain safeguards to protect the security and confidentiality of the disclosed records.

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?

External users applying for access to FSA applications must consent to uses of their PII as outlined in the SAIG PM Enrollment agreement. If the user does not consent, they are not authorized to enroll in SAIG PM or have an AIMS ID assigned.

If a user wants to opt out of AIMS, the primary destination point administrator from the user's specific organization requests SAIG PM to disable the user's AIMS account.

If any individual (internal Department or external user) declines to provide requested PII, the individual will not be granted access to AIMS or any FSA application systems.

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.

No

5.2. What PII will be shared and with whom?

☑ N/A

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

☑ N/A

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.

No

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

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

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

☑ N/A

Click here to select.

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

☑ N/A

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

[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.

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

If an individual wishes to gain access to a record in this system, they must contact the system manager at the address listed for the system of records entitled "Student Aid internet Gateway (SAIG), Participation Management System" (18-11-10). They must provide necessary particulars such as name, user ID, date of birth, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. The request must meet the requirements of the Department's Privacy Act regulations at 34 CFR 5b.5, including proof of identity.

Internal Department users can also gain access to their information by requesting a copy of account information from the AIMS ISSO or application ISSO. The internal user will be provided a copy of their information. The internal Department user can also contact AIMSSupport@ed.gov for assistance.

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

If an individual wishes to contest or change the content of a record about themselves in the system of records, they must contact the system manager listed for the system of records entitled "Student Aid internet Gateway (SAIG), Participation Management System" (18-11-10). They must provide necessary particulars such as name, user ID, date of birth, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. Requests to amend a record must meet the requirements of the Department's Privacy Act regulations at 34 CFR 5b.7.

Internal Department users can gain access to their information by requesting a copy of account information from the AIMS ISSO or application ISSO. The internal user will be provided a copy of their information. The internal Department user can also contact AIMSSupport@ed.gov for assistance.

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

The procedures for accessing and amending record(s) for external users are outlined in the system of records entitled "Student Aid internet Gateway (SAIG), Participation Management System" (18-11-10).

For internal Department users completing the access form, their supervisor directs the user to AIMSSupport@ed.gov or the AIMS ISSO if they need to make any corrections to their information.

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 Authorization 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?

FSA information systems follow the concepts of least privilege and separation of duties. All system access is granted by predefined roles and privileges, and all FSA system users that have access to system databases and other information resources must undergo a Federal background security clearance process. AIMS uses multi-factor authentication to authenticate users for access to FSA applications where users enter username/password and one-time password (OTP).

In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every FSA

system must receive a signed ATO from a designated FSA official. The ATO process includes an assessment of security and privacy controls, plans of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program.

Physical safeguards include the staffing of security guards 24 hours a day, seven days a week, to perform random checks on the physical security of the record storage areas. All sensitive data are encrypted in transit and at rest, access to records is strictly limited to those staff members trained in accordance with the Privacy Act and Automatic Data Processing (ADP) security procedures.

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.

AIMS is required to obtain and maintain an ATO. This process includes a tri-annual independent assessment of all required security and privacy controls producing Plans of Actions and Milestones (POA&Ms) to ensure any deficiencies are remediated. AIMS also participates in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security controls are in place and working properly. AIMS has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

AIMS participates in the FSA Continuous Diagnosis Monitoring (CDM) program including asset compliance and vulnerability scans conducted weekly for each application in production and non-production environments. The FSA Security Operations Center (FSA SOC) team analyzes data and reports issues weekly to the AIMS ISSO and System Owner for remediation. AIMS logs are also forwarded to the FSA SOC, for analysis for fraudulent patterns of behavior or inappropriate access. In addition, user logs are monitored monthly 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 ensures that the information is maintained and used in accordance with the stated practices in this PIA. The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, AIMS makes sure that the applicable National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices. The System Owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. 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 (LMM), which addresses security and privacy risks throughout the system's life cycle. Additionally, the System Owner regularly reviews signed agreements that govern data use between FSA systems, such as memoranda of understanding.

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?

The main privacy risks associated with AIMS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

These risks are mitigated by granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, masking SSNs, and encrypting data in transmission.

Risks are also mitigated by updating security patches per the patch scheduling and updating devices' operating software.

As referenced above, patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.

An additional risk to privacy is the possibility of insider threats. This risk is mitigated by ISSOs conducting 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.