



Privacy Impact Assessment (PIA)
for the

Accreditation and State Liaison (ASL) System

April 14, 2020

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

Contact Point

Contact Person/Title: Amy Wilson
Contact Email: amy.wilson@ed.gov

System Owner

Name/Title: Amy Wilson
Principal Office: Office of Postsecondary Education (OPE)

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.

OPE-ASL is a Moderate impact application with a front-end website that enables accrediting agencies and foreign medical schools, desiring to be recognized by the Secretary of Education to identify, categorize and submit their petition narratives and supporting documentation electronically. Accrediting agencies are private educational entities that are recognized through the regulatory process.'

https://www2.ed.gov/admins/finaid/accred/accreditation_pg11.html#Part602-Secretary'sRecognition.

An application for recognition consists of a narrative addressing the agency's compliance with each of the subparts of the criteria for recognition and evidence of the agency's compliance with each of the criteria for recognition by appending supporting documentation.

The system also allows for collection of information for the Foreign Veterinary standards that foreign countries use to accredit medical schools in those countries to determine whether those standards are comparable to the standards used to accredit veterinary schools in the United States. The system also houses information regarding the federal degree granting process.

The website stores documents created by various agencies and countries for review by the National Advisory Committee on Institutional Quality and Integrity (NACIQI) and the National Committee on Foreign Medical Education and Accreditation (NCFMEA). Large quantities of printed material from meetings held by these organizations are kept for historical purposes and are occasionally referenced for research or Freedom of Information Act (FOIA) purposes. Storing these documents is done electronically to save physical space as well as enable ASL staff to efficiently retrieve documents.

1.2. Describe the purpose for which the personally identifiable information (PII)¹ is collected,

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

used, maintained or shared.

The PII in the system is being collected to have contact information for the account being created for the accrediting agencies and foreign medical schools that includes accrediting agency name, name of contact, work email, work phone. The entity provides this information along with a narrative for review to obtain recognition by the Secretary of Education.

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?

New PIA

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 legal authority to collect and use this data is derived from Title IV of the Higher Education Act of 1965, as amended (Pub. Law 102-325, Section 34 CFR 602 and 603). In accordance with this authority, the Department receives and maintains personal information in the ASL programs cited in 1.1.

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](#)

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?

No

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

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

The information is not retrieved by an individual identifier, the information is not maintained in a system of records. The information that is in the system is based on the name of the accrediting agency or the name of the country applying for recognition. There are points of contact for the agencies, only using names and email addresses

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.

The records disposition schedule is ED 189: Accreditation Case Files
Disposition: Records on successful applications are destroyed 11 years after termination of the accreditation process, or after completion of audit related activities or litigation, whichever is later.

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>

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

Yes

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 accrediting agency records include personally identifiable information such as agency name, work address, contact name, work phone and work email address.

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

Yes

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

The sources of PII collected are the accrediting agencies or the foreign government that act on behalf of the foreign medical school. OPE works with accrediting agencies or countries that apply for the process. Each agency or group must provide a contact for ASL.

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

ASL collects the PII directly from the electronic participant application. The accreditation group must have prior had contact with the agency or group. They must submit details prior to account creation. This information is maintained in the backend database. The data is only available to the submitter and to the ASL system admin.

- 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?

Accreditation Group Staff verify information from the application on first request of accreditation. There is a review done by a committee to ensure that Agency groups understand our regulations and that they are expected to vet the groups. After completing that process, an ASL account is established for the Agency.

Use

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

The information is used for communication with the agency regarding their request for accreditation.

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

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.

No

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.

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

N/A

[Click here to enter text.](#)

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

N/A

[Click here to enter text.](#)

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.

ASL is currently working on a Privacy Notice to be given prior to the collection of PII.

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

The text of the notice is currently being drafted and will be provided on the website once completed. <https://opeweb.ed.gov/e-Recognition>

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?

We require information from the agency, but they don't wish to provide an individual information they can. Additionally, if they decline to provide this information about the agency, we would not be able to follow our processes and they wouldn't be recognized.

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

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.](#)

5.8. 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

[Click here to enter text.](#)

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

[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?

The individual has access to the system and can access their information. The users log in and are restricted to editing their own information. This is an agency account that includes point of contact information. The POC information may be edited.

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

The individuals have access to the ASL system and can edit/update their information. They are notified when they contact the Committee for processing. They are then assigned a staff member and will be reminded during their interactions with an analyst.

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

Users are notified verbally and are asked to make their own updates in the system. The users are notified when they contact the Committee for processing. They are then assigned a staff member and will be reminded during their interactions with an analyst. The users are informed at the start of the process when contacting the Department, and during any resubmissions. Accrediting agencies must reapply for recognition every 5 years.

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 Authority 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?

Access to the application is only available to registered users who have been authorized to have valid credentials (user ID and password) that are authenticated by the system. OPE has about 30 staff/committee members who sign into the system with ASL credentials. There are 64 recognized accrediting agencies and about 20 countries that can sign in. The application compares user provided credentials with stored credentials. Credentials that match are required to authenticate the user and the system grants access. The user must use a suitable browser using HTTPS with TLS for a secure web connection. This protects all data in motion. An OPE staff member must approve access requests from educational institutions to add, delete or change application users. An OPE staff member must approve access requests for system administrators, application administrators, and system developers. OPE provides a system administrator with an

email to add, delete or change internal system and application users. New users are provided a secure password that must be changed on the first login.

ED staff (OPE's employees and contractors) must have and maintain the proper security clearance level to access the system and information collected. ED staff are required to complete the Department's mandatory Cybersecurity and Privacy Awareness courses.

- 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.

The following tasks are performed to safeguard the ASL information:

Monthly vulnerability scans performed

Annual contingency plan test performed

Annual self-assessments conducted

Annual security assessments performed by the ED Security Authorization Team

Annual Authorization To Operate (ATO) signed by designated ED Authorizing Official

Follows the Department's Life Cycle Management framework

Annual updates to system security documents and information

Annual mandatory training for Cybersecurity and Privacy Act for employees and contractors.

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 ASL web application and the underlying infrastructure provide audit trails of user activity that can support forensic analysis in the event of a data breach or loss. The ASL system provides mechanisms that enforce role-based access for both the web application and the underlying computer systems. Without having an approved role, institution users (external users) are only granted minimal application privileges. External users are not

given any type of system privileges. There are no actions that can be taken by an anonymous person as registered user accounts are required for access. The general public is not granted any means of access.

The system provides role-based access for individuals so that they are only provided with information that is relevant for them. The Information System Owner (ISO) and Information System Security Officer (ISSO) are involved in PIA process with the privacy office. The system maintains a current ATO and engages in the security assessment processes as required.

Direct access to the database is not provided to any ASL users or OPE staff. The database admin is the only member of ED staff (employees and contractors) who can access the database within the AWS GovCloud. Only properly vetted and approved ED staff are given any elevated system or application privileges. OPE maintains a listing of authorized users that is reviewed on a quarterly basis. OPE follows the ED personnel security policy OM: 3-104 for terminations.

Only ED staff that directly support data collection or data analysis are allowed access to the data. ED staff must have appropriate security clearances and they also sign confidentiality and non-disclosure agreements to protect against unauthorized disclosure of confidential information. All staff must have appropriate security clearances and be specifically approved before accessing ASL data. ED staff are required to complete annual mandatory security awareness and privacy act training.

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 privacy risk associated with this system is unauthorized access to an account. The ASL system employs role-based access and each system role provides varying levels of access. External users, such as agencies and country representatives, are only granted minimal roles to reduce exposure to the PII contents. The system design prevents one agency or country from viewing or accessing any information from another agency or country. All login and logout events (including attempted logins) are recorded in the application's event logs.

The system maintains two auditing reports that track authorized access to user accounts. These are the login and activity reports. The login report gives details about every access to the system. The activity report tracks all system changes made by authorized users. Records of users are audited on a quarterly basis by the ISO and ISSO to ensure that users are accurate. ASL follows the OCIO policy, PR.AC 6: *User Account Recertification*. The system admin may be directed to immediately remove any individuals who must no longer be granted access (i.e., in the event of an employee termination). In the event there is a POC change at an agency, the ASL staff will notify the system admin who will then remove that person from the system access (within 24 hours of notification). The user accounts will have the passwords changed and the accounts are then disabled. After 90 days, those accounts are then deleted.

ASL complies with the Department's Security Assessment and Authorization (SA&A) policy. The SA&A is updated on an annual basis to ensure that the information system has adequate security commensurate with its level of risk. There are security assessment testing and security impact analyses that are comprehensive evaluations of the technical and non-technical security features of the information system. There are other safeguards (e.g., physical, personnel, procedural and environmental) that establish the extent that the system's design and implementation meet the set of OCIO specified security requirements. The ATO granted using the formal ED process that includes signatures by the Authorizing Official, ISO, and ISSO. The ATO demonstrates that the information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.