

Privacy Impact Assessment – ECA-PMOS

1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- (a) Date PIA was completed: December 15, 2014
- (b) Name of system: Educational and Cultural Affairs Program Management and Outreach System
- (c) System acronym: ECA-PMOS
- (d) IT Asset Baseline (ITAB) number: 2599
- (e) System description (Briefly describe scope, purpose, and major functions):

The ECA-PMOS is a business umbrella grouping of several systems with varying degrees of privacy information and record subjects. The systems support programs managed by the U.S. Department of State's Bureau of Educational and Cultural Affairs (ECA), in particular, those international education and training programs involved with exchange-of-persons between the United States and other countries. ECA-PMOS systems (also referenced as system components) are deployed in ECA, at posts, in private-sector organizations that are Department of State partners, and on the internet.

The ECA-PMOS facilitates electronic data transfer and collaboration among all of the partner organizations. It also allows users to track and manage the full life cycle of ECA programs in order to support ECA's public diplomacy goals. The program life cycle includes planning, solicitations, proposals, grants, funding, projects, itineraries, participants, results and outreach to exchange alumni.

ECA-PMOS includes the following systems (See Appendix A for additional applications not currently part of ECA PMOS 2599):

Academic Exchanges Information System II (ITAB # 4515) tracks grantees and their activities for Fulbright and several other academic programs such as Gilman, Humpries, Study of the US etc. It maintains information on participants, organizations and location (US or overseas), and supports inquiries and generates reports for management, Congress and the Public. The bulk of information is provided in one annual Data call from non-government cooperative organizations. Data is submitted by Cooperative Agencies electronically in batches for the Enterprise Monitor system to load into AEIS. AEIS II includes batch processing of grantees to DHS Student and Exchange Visitor Information System (SEVIS) application.

Alumni Archive (ITAB # 665) is a central repository for ECA Alumni data, housing information on alumni of the Exchange programs partially or fully funded by the ECA programs from 1970 forward. This consolidated data is used to:

Privacy Impact Assessment – ECA-PMOS

- Re-engage the alumni and offer them new program opportunities
- Determine updated contact information for alumni
- Determine the value of their exchange on the ECA program

The Alumni Archive application is used to:

- Identify and acquire new sources of Alumni archival records from the non-government organizations (NGO)
- Extract, transform, and load records into the central Alumni database
- Provide a web interface that allows all ECA staff, Posts, commissions, & designated authorities to easily update records and generate reports
- Provide an electronic mechanism for outside data sources to submit alumni records into the Alumni Archive database on a regular reporting basis.

Alumni Affairs Management System (ITAB # 5097) assists the Office of Alumni Affairs with managing, tracking, and reporting on alumni outreach activity, funding, and strategy success. Annually the Office of Alumni Affairs promotes a competition among U.S. Missions for funding of alumni-focused project proposals. The Alumni Affairs Management System collects information related to the annual project proposal competition, stores historical documents, captures the rank order of the proposals after panel, and record other relevant program management information. Additionally, the system provides data for program status reporting, including Mission-specific alumni programs and funding history, as well as country-specific alumni coordination profiles.

COINS (ITAB # 4247) provides an automated web-based enrollment system for the Department of State's Accident and Sickness Program for Exchanges (ASPE). The Department "self-insures" (provides medical benefits to) Participants enrolled in some of the Department's exchange programs. Authorized access is restricted both on OpenNet and the internet.

E-Teacher (ITAB # 5045) supports the E-Teacher Scholarship Program in its enrollment of teachers of English and teacher trainers from over 60 countries in on-line courses that explore five major areas of the academic specialty of Teaching English as a Foreign Language (TEFL). It supports the E-Teacher Program in nominee submission, review, approval and reporting. E-Teacher automates and secures the following functions:

- Allow Post users to create, update and submit nominees for review to the E-Teacher Program Management Office (PMO).
- Allow E-Teacher PMO staff to review nominees made by Relocation (RELOs) and Post users.
- Provide the capability to create and print reports via a web interface and generate nominee lists.
- Allow E-Teacher access for PMO staff, RELOs and Post users at anytime via the Department's OpenNet.

English Language Fellows (ITAB # 844) automates the Fellow program requests from posts and documents the review and selection of English Language Fellow programs. Posts submit proposals for a Fellow Program via the ELF system. The ELF officers in DC and the regional English language officers at Posts review the program proposals and select the best qualified programs. The system notifies the designated Grantee organization of the status of the programs. The Grantee organization logs into system and

Privacy Impact Assessment – ECA-PMOS

reviews the selected proposals in order to find candidates to fulfill the program requirements (latter is outside scope of this system.)

English Language Specialist (ITAB # 6634) The EL Spec application supports the ECA/A/L English Language Specialist Program, which sends U.S. experts in the field of Teaching English as a Foreign/Second Language (TEFL/TESL) to work on short-term projects that contribute to the host country's capacity to teach English and a Post's public diplomacy goals. The application allows the Regional English Language Officers (RELO), RELO Assistants, and Post users to initiate, update, submit, and track proposals for Specialists to perform English language projects via an online form. The application also supports the proposal review and approval process performed by the program office staff.

Eureka (ITAB # 1020) captures funding, participant, and organization information on all Citizen Exchanges projects. It tracks exchange projects, itineraries and participants, and enables the program office to generate ad hoc reports. Eureka collects data on participants and support services (such as entry of DS-2019 data) that are critical to the Citizen Exchanges Office. Office staff enters data on program projects. Participant data can also be entered directly -- as part of DHS' SEVIS database -- or captured from other sources such as health-insurance enrollments and direct transfers from grantee institutions.

Eureka Web (ITAB # 6086) is a web-based application initiated by ECA/PE/C. The purpose of the application is to create online visibility where Post personnel can create, store, modify, and submit proposals for current Citizen Exchanges programs. The submitted/accepted proposals can then be managed with the Eureka application.

Exchange Visitors Database-Enhanced EVDB-E (ITAB # 1017) was developed to support ECA's International Visitor Program that is administered by the Office of International Visitors. The emphasis of the IV Program is to increase the mutual understanding between nations through communication at the personal and professional levels. The Office develops and coordinates programs for individual visitors or groups of visitors to visit the United States. It tracks all IV projects and participants, program costs by project and participant and program itineraries. It supports visitor nomination, assignments to program agencies and collaboration with program agencies on project design and production of program books. The type of International Visitor Program being administered determines the way in which the various users interact with EVDB-E. A SEVIS module is also included in EVDB-E. Privileged users who are qualified as Responsible Officers (RO and Alternate Responsible Officers (ARO)) by the Department of Homeland Security (DHS) are provided with the capability to batch and transfer (via FTP) participant data to DHS's SEVIS database.

Executive Office Suite (ITAB # 1019) is a financial tracking and program management tool supporting users in the ECA Budget, Grants, and Program Management offices. It provides:

- Tracking and reporting of all budgetary and financial transactions - including detailed document tracking and audit trails.
- Workflow queues that monitor and assign work items and track all commitment types and funding transactions through completion.

Privacy Impact Assessment – ECA-PMOS

- Automated tracking of program versus operational plan, reprogramming limits, monitoring of funding and commitments by assigned project numbers, reimbursements, advice of allotments, earmarks, and representational funds.
- Full lifecycle initiation, funding, and management of ECA grants through PM, budget, and Grants offices with automatic assignment of users and activities tied to specific grant lifecycle phases.
- Integration with grants.gov.

ORDIV Website (ITAB # 5159) provides a central point-of-access for the Online Resource Directory and the IV Upcoming Projects.

Post EVDB Web (ITAB # 1021) provides the capability for Posts to create Contacts, Nominees and Projects for the International Visitors Program. The data is hosted in a central database repository, IMS. The goal of the IV Program is to increase the mutual understanding between nations through communication at the personal and professional levels. The IV Program Office develops and coordinates programs for individual visitors and groups to visit the United States. The Post EVDB Web application allows the Posts to nominate visitors to participate on these programs.

(f) Reason for performing PIA:

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): Not applicable – not a significant modification.

(h) Date of previous PIA (if applicable): April 23, 2010

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

There are three distinct levels of PII for systems within ECA-PMOS: (1) personally identifiable information about U.S. Citizens (non USG-employees); (2) contact information for USG employees; and (3) information from or about non U.S. persons.

The first level includes data on U. S. Citizens. Systems included in this level are listed in the table immediately below.

Privacy Impact Assessment – ECA-PMOS

Sub-system	PII data element
<p>Academic Exchanges Information System II (AEIS II)</p>	<p>Individual's Name (Last, First, Second Last, Middle Names; Suffix) Title Position/Occupation Type Gender Race Ethnicity Date of Birth Birth City Birth Country Citizenship Country (1st, 2nd, 3rd) Date of Naturalization Marital Status Spouse's Citizenship Country Home Street Address Home City Address Home Country Home State, Zip Code and Congressional District Home Email Address Home Phone Number Home Fax Number Home Cellular Number Visa Type SEVIS Number Home Institution Name Home Institution Country Host Street Address Host City Address Host Country Address Host State, Zip code and Congressional District Host Email Address Host Phone Number Host Fax Number Host Cellular Number Major Field of Study Specializations Program Start Date Program End Date</p>
<p>Alumni Archive</p>	<p>Individual's Name (Prefix; Last, First, Second Last, Middle Names; Suffix) Suffix</p>

Privacy Impact Assessment – ECA-PMOS

Sub-system	PII data element
	Sex / gender Date of Birth Deceased Status Disabled Status Country of Citizenship Second Citizenship Country Home Street Address Home City Address Home State, or Province and Country Address Home Congressional District Business Street Address Business City Address Business State, or Province and Country Address Business Country Address Preferred Address Home Phone Business Phone Mobile Phone Other Phone Preferred Phone Fax Number Email 1 Email 2 Preferred Email Business Name Field of Study
COINS	Individual's Name (Last, First, Second Last, Middle Names; Suffix) Gender Birth Date Phone Number Email Address Citizenship Home Street Address Home City Address Home State and Zip Code, or Province and Country Address Host Organization Host Organization Address Medical Notes (If any...) Accident and Sickness Program coverage inception

Privacy Impact Assessment – ECA-PMOS

Sub-system	PII data element
English Language Fellows (ELF)	Individual's Name Business Phone Business Email
English Language Specialist Program (EL Spec)	Individual's Name (Last, First) Title Business Email (i.e. Department of State email) Business Country (i.e. Post country) Business City (i.e. Post city)
Eureka	Individual's Name (Last, First, Middle Names; Suffix) Nickname Birth Date Birth Country Birth City Birth State Birth Province Citizenship Country Residence Country Naturalization Date Professional Title Organization Affiliations Passport Number Passport Expiration Sex Marital Status Disabled / Disabilities Home Street Address Home City Address Home State and Zip Code, or Province and Country Address Phone Email Visa Type Subject/Field of Study Language Capabilities (Reading, Writing, Speaking) Social Security Number Occupation Comments Travel Itineraries Expertise Types and Levels (1-5)

Privacy Impact Assessment – ECA-PMOS

Sub-system	PII data element
<p>Exchange Visitors Database – Enhanced (EVDB-E) and Post EVDB Web</p>	<p>Individual’s Name (Last, First, Middle Names; Suffix) Nickname Organization / Institution Name Business Street Address Business City Address Business State and Zip Code, or Province and Country Business Phone Business Email Gender Personal Web address Birth Date Birth Country Birth City Birth State Birth Province Citizenship Country Residence Country Professional Title Organization Affiliations (Past and Present) and Memberships Marital Status Home Street Address Home City Address Home State and Zip Code, or Province and Country Address Phone Email Visa Type (if J-1 Visa- SEVIS) or if B1 visa applies Subject/Field of Study (SEVIS) DS2019 Position (SEVIS) Language Capabilities (Reading, Writing, Speaking)- Expertise Types and Levels (1-5) Occupation Comments Travel Itineraries Past US and Foreign Travel Publications Educational Background Passport data MAY BE stored in free text fields if entered by the EVDB-E user, but it is not a dedicated field in the IMS database.</p>

Privacy Impact Assessment – ECA-PMOS

Sub-system	PII data element
Executive Office Suite - EOS	Individual's Name (Last, First, Second Last, Middle Names; Suffix) Familiar Name Phone Number Email Address Home Street Address Home City Address Home State, or Province and Country Address Organization (employer) Name Organization Address Organization Position Organization Contact Individual's Name
ORDIV	Similar to EVDB-E above: Individual's Name (Last, First, Middle Names; Suffix) Nickname Organization / Institution Name Business Street Address Business City Address Business State and Zip Code, or Province and Country Business Phone Business Email Gender Personal Web address Birth Date Birth Country Birth City Birth State Birth Province Citizenship Country Residence Country Professional Title Organization Affiliations (Past and Present) and Memberships Marital Status Home Street Address Home City Address Home State and Zip Code, or Province and Country Address Phone Email

Privacy Impact Assessment – ECA-PMOS

Sub-system	PII data element
	Language Capabilities (Reading, Writing, Speaking)- Expertise Types and Levels (1-5) Occupation Comments Travel Itineraries Past US and Foreign Travel Publications Educational Background

The second level of PII collected on U.S. citizens is **solely official contact information of U.S. federal employees**. The ECA-PMOS child systems that fall within this category are listed in the table immediately below. All except English Language Fellows and Federal Exchanges Data System contain PII on non-US citizens.

Sub-system	PII data element
Alumni Affairs Management System	Individual's Name Business Address Business Phone Number Business Email
English Language Fellows (ELF)	Individual's Name Business Phone Business Email
E-Teacher	Individual's Name Business Address Business Phone Number Business Email
Eureka Web	Individual's Name (Last, First, Middle Names; Suffix) Residence Country Professional Title Organization Affiliations Home Street Address Home City Address Home State and Zip Code, or Province and Country Address Phone Email Visa Type Subject/Field of Study Occupation Comments

Privacy Impact Assessment – ECA-PMOS

	Travel Itineraries Expertise Types and Levels (1-5)
--	--

The third level of PII is solely collected on non-U.S. citizens. The ECA-PMOS system that falls within this category is:

- Post EVDB Web

The PII has several sources, including individuals, depending on the Exchange Program. All involve either direct collection of information or use of data already collected by or for the U.S. Department of State.

- Data are provided by Public Diplomacy staff at the Embassy, after prior collection from the individuals.
- Data are collected from individuals by NGOs acting under contract to Department of State. NGOs then provide that data to Department of State.
- Data are entered directly by individuals into a form on a Department of State website.
- Data are copied from one of the component information systems to another component information system.

b. How is the information collected?

AAMS collects official contact information by entering the data online directly into the system or through uploaded .pdf reports.

AEIS II collects data as direct online input by Department of State ECA Academics Exchange Specialists or by email sent from Grantee Organizations managing the Exchange Program. There is no direct access into the system other than via the Department's intranet network.

Alumni Archive has data automatically loaded from other Department Academic Exchange systems (ie, EVDB-E, AEIS II, Eureka). Also Posts and Program Agencies (under contract with the Department) email or mail the information to the Alumni Archive system manager to upload into Alumni Archive. The information is sent upon request by the system manager or as a condition of the grant.

COINS collects ASPE enrollment information directly from Program Agencies who email the information or who manually enter the data online. The information is also collected automatically from other Department authorized systems. Exchanges Participants and Grantees do NOT access COINS directly.

English Language Fellows collects the Department employees' official contact information by entering the data online directly into the system. The Grantee Organization cannot update any data but it can view the data.

e-Teacher collects the participants' official contact information by entering the data online directly into the system.

The EL Spec application collects contact information on Post and Regional English Language Officer (RELO) users directly from each user via the web proposal form.

Privacy Impact Assessment – ECA-PMOS

Eureka collects information from Department Program staff via online manual input, automatically from other Department systems and automatically from the Department of Homeland Security's SEVIS system.

Eureka Web collects information via online manual entry by POST users.

EVDB–E collects business contact information of US Citizens who are contracted with Program Agencies / Grantee Organizations or employed by the Department of State via online manual input by the contacts themselves or by staff in the supporting Program office.

EOS collects information via manual online entry by Department of State's ECA Budget and Grants Offices.

ORDIV, eNPA/eCIV, and NPA-CIV Web collect data as direct input by the individuals in the respective organizations reported or by staff in those organizations.

Post EVDB Web collects data as direct online input by Department of State Foreign Service Officers, Locally Employed Staff, or USG. There is no direct access into the system other than via the Department's intranet network.

For ECA-PMOS systems covered in this document that collect contact information on the federal workforce, that contact data is either entered in the systems by the subjects themselves or is entered by Department of State staff supporting the respective program and office from the global address list.

c. Why is the information collected and maintained?

The information is collected and maintained to provide contracted Program Agencies or Grantee Organizations with sufficient data to contact and evaluate an Exchange nominee or participant, and to provide the public with contact information at Grantee organizations regarding programs of interest.

d. How will the information be checked for accuracy?

Information collected directly from the record subject is presumed to be accurate. The contact information about an individual is collected from Department of State records and interviews with the subject individual.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 1431 et seq. (Smith-Mundt);
- United States Information and Educational Exchange Act of 1948, as amended;
- 22 U.S.C. 2451-58 Fulbright-Hays Mutual Educational and Cultural Exchange Act of 1961, as amended;
- 22 U.S.C. 2651 a (Organization of the Department of State); and
- 22 U.S.C. 3921 (Management of the Foreign Service).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Information collected and maintained by ECA-PMOS systems is the minimum amount of information necessary to identify potential and awarded Grantees and Participants for

Privacy Impact Assessment – ECA-PMOS

Exchange Programs. Basic contact information is necessary to contact the subject individual or submitter if needed.

Because personally identifiable information (PII) is collected and maintained by ECA-PMOS, appropriate management, technical and operation security controls are in place to ensure the confidentiality and integrity of the data. Access is available only to authorized Department of State employees performing sanctioned duties. Users must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through Diplomatic Security. Access to computerized files is password-protected. The computerized files are available only on the Department of State intranet or on the internet but hosted internally at the Department of State or an authorized, contracted off-site hosting facility.

4. Uses of the Information

a. Describe all uses of the information. The information is used to:

- evaluate and award nominees / candidates of Department of State Exchange programs,
- process the Participant through the subject Exchange program,
- provide official contact information to the public for Exchange programs
- generate reports used by Department of State managers and staff in the management of an Exchange program
- allow Department of State and contacted Grantee organizations to contact current Exchange participants and alumni of Exchange programs
- fulfill requirements of the Department of Homeland Security.

There is no placement of Personally Identifiable Information on portable computers. Authorized system users who telecommute can only access the system through the Department of State's secure access using the Global OpenNet (GO) system with two-factor authentication where one of the factors is provided by a RSA soft/hard token with a use-once password.

b. What types of methods are used to analyze the data? What new information may be produced?

The data in ECA-PMOS are not used for analytical purposes. No new information may be produced, except high-level statistics for program reporting purposes sent to the White House and Congress as required or published on the Federal Exchanges Data System website.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

ECA-PMOS does not use commercial information, publically available information, or information from other Federal agency database when processing information on U.S. citizens.

d. Are contractors involved in the uses of the PII?

Privacy Impact Assessment – ECA-PMOS

Contractors are involved with the operational maintenance of the system. Contractors use the data in ECA-PMOS consistent with the statutory purposes, and do not produce any additional data. Privacy Act contract clauses are inserted in their contracts and other regulatory measures are addressed. Rules of Behavior have been established and training regarding the handling of PII under the Privacy Act of 1974, as amended.

Contractors are employed by the U.S. Department of State within the Bureau of Educational and Cultural Affairs as members of staff to support Bureau programs. All contractors, whether technical or direct program support, must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through Diplomatic Security.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Data collected and maintained by the ECA-PMOS is only used for purposes of managing the respective Exchange program, for fulfilling the program requirements and for ECA internal task assignments. The information is not analyzed or disseminated for any other purpose. ECA-PMOS does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions.

5. Retention

a. How long is information retained?

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration. For detailed descriptions of the appropriate record disposition schedules, see Domestic Records Disposition Schedules.

Application	Retention Schedules used					
AEIS	A-36-004-02	A-36-004-03				
AAMS	A-36-006-10	A-36-015-03				
Alumni Archive	A-36-015-03b	A-36-015-02				
COINS	?					
E-Teacher	A-36-006-08a	A-36-006-09a				
ELF	A-36-006-10	A-36-006-08a				
EI-Spec	A-36-006-10	A-36-006-08a				

Privacy Impact Assessment – ECA-PMOS

Eureka	A-36-016-09	A-36-016-09a	A-36-016-09b	A-36-016-09c	A-36-016-09d	A-36-016-09e
Eureka Web	A-36-016-09d	A-36-016-09b				
EVDB-E	A-36-018-01	A-36-018-01a	A-36-018-01b	A-36-018-01c	A-36-018-01d	
EOS	A-36-003-02	A-36-003-03	A-36-003-04	A-36-003-05a	A-36-003-06	
ORDIV	A-36-015-02	A-36-015-03				
Post EVDB Web	A-36-015-02	A-36-015-02				

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

If data are destroyed too soon, good information will be lost. Record retention is discussed and implemented to ensure necessary data is kept for the necessary length of time based on data owner requirements.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

For Participants on Programs where their Grant provides health benefits through the Department’s self-insured Accident and Sickness Program for Exchanges (ASPE), the Participant’s data are automatically fed into the COINS system. Where the automated data feed is not established, responsible Program offices can manually enroll their Program Participants into ASPE online. With the exception of the ASPE Administrators, staff managing a particular Program are restricted to access data on individuals participating in their particular Program. The Participants do not have access to COINS. The shared data consist of the Participant’s name, contact information (home and mailing addresses, email), gender, birth date, citizenship and ASPE coverage dates.

All ECA Exchange offices provide (electronic feeds or manual input) Participant bio, contact and Program data to the Exchanges Statistical Management System (ESMS) administered by the ECA Executive Office. ESMS aggregates the Participant data into high-level program data for reporting to Congress and the public. It does not report any individual’s information. ESMS does not store any Participant personal data fed into the system; it merely categorizes and summarizes the data to report at the Program level.

The Offices of Citizen Exchanges, International Visitors and Academic Exchanges provide Participant data to the Alumni Affairs office for inclusion in the Alumni Archive database. The data is available to authorized Department employees on the Department’s intranet and used to re-engage with alumni and maintain up-to-date records to facilitate public diplomacy outreach. Bureau staff access the database for statistical data on participants to be used in Congressional testimony or results reporting.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

All information is transmitted via automated electronic feeds or via manual online input.

Privacy Impact Assessment – ECA-PMOS

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

When shared within the Department, all information is still used in accordance with ECA-PMOS stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons.

All employees of the Department of State have undergone a thorough personnel security background investigation. Access to Department of State facilities is controlled by security guards, and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Privacy Data on non-US Citizens are sent to the SEVIS system at the Department of Homeland Security from the following systems: AEIS II, Eureka and EVDB-E. The Department of Homeland Security requires electronic submission of Visa and J1 Visa applications. This data are provided to Homeland Security by the ECA-PMOS system to aid that agency in processing these individuals at their point-of-entry into the U.S.

Data are also shared with Grantee organizations under the terms of their Grant. They are restricted to access data on individuals that are applicants, candidates or participants on their Program. Information is shared to confirm ASPE enrollments, re-engage alumni and abide by federal regulations involving visits by non-US citizens. Data are also shared to provide Program contact information.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Systems sending data to and from Homeland Security do so through a web service using HTTPS protocol that enforces encryption.

Grantee organizations are required to authenticate their credentials to access ECA-PMOS systems through a unique login ID and encrypted password. Each organization can only access data on participants enrolled in their respective grant programs.

There is no anonymous access to ECA-PMOS systems containing personal information outside the Department.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Risks to privacy are mitigated by limited access to and release of personal information on a need-to-know basis.

8. Notice

The system:

Privacy Impact Assessment – ECA-PMOS

- contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records.
(visit www.state.gov/m/a/ips/c25533.htm for list of all published systems):
[Educational and Cultural Exchange Program Records. STATE-08](#)
- does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

A Privacy Act Statement is available for those individuals that provide this information by form and notice. Additionally, the collection of information in ECA-PMOS is covered by the system of records notices State-08, Educational and Cultural Exchange Program Records.

b. Do individuals have the opportunity and/or right to decline to provide information?

The individual may decline to provide the required information; however, such actions may prevent them from participating in Exchanges programs.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Conditional consent is not applicable to the official purpose of ECA-PMOS.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notification is provided to the Public via System of Records Notices STATE-08, as well as through Privacy Act Statements on forms that are used in collection of PII in ECA-PMOS.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director, Office of Information Programs and Services; Department of State; SA-2; 515 22nd Street NW; Washington, DC 20522-6001. The individual must specify that he/she wishes the Cultural Property Advisory Committee Records to be checked. At a minimum, the individual should include: Name; date and place of birth; social security number; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record, and the approximate dates which give the individual cause to believe that the Office of International Information Programs has records pertaining to them.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Procedures are available for individuals to access or amend records they believe are incorrect. The notice is reasonable and adequate in relationship to the system's purpose and use.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The level of access and capabilities permitted is restricted by the role assigned to each individual user. Some users are granted read-only access if they have no need to update system records. The applications in ECA-PMOS utilize single sign-on through OpenNet for access. This ensures that users must be authenticated first to the Department's intranet before using the ECA-PMOS applications. The separation of roles with different access privileges is in accordance with NIST Special Publication 800-53 rev 3.

All authorized staff using the system must comply with the Department of State's general "appropriate use policy for information technology." Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years.

Access to ECA-PMOS is restricted to Department of State personnel, Grantee organizations under contractual terms of their Grant.

Department of State system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through Diplomatic Security.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of State systems and security. Contracts are reviewed upon renewal by management and contract personnel experts in such matters.

b. What privacy orientation or training for the system is provided authorized users?

Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security. This training includes information regarding handling personally identifiable information.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized usage. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

The certification and accreditation process independently verifies and validates the application system security controls. Administrative procedures, including independent

Privacy Impact Assessment – ECA-PMOS

security investigations of Department applicants and assignment of unique system access rights to individuals, limit access to the system.

There is little residual risk related to access, in particular because the system is available only on a Department of State intranet and there is minimal and controlled direct electronic transfer of data between ECA-PMOS and hosts accessible to external organizations or individuals.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risks to any information technology.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Information is transmitted via email quite frequently. A potential risk includes an email containing personally identifiable information inadvertently sent to an unauthorized recipient.

To mitigate this risk, Department of State staff receives training and notifications warning of phishing scams to obtain personal data.

12. Security

What is the security certification and accreditation (C&A) status of the system?

As a component system to the Educational and Cultural Affairs Program Management and Outreach System, ECA-PMOS was granted Full Accreditation at the Sensitive-But-Unclassified (SBU) level in October 2010. The authorization is valid for up to 36 months. This Accreditation expires on October 29, 2013. A new ATO is expected by May 2015.

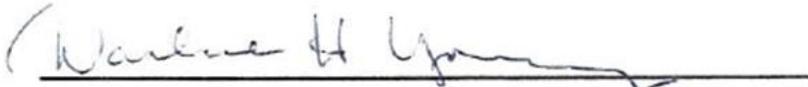
13. Certifying Officials' Signatures



System Owner – Antoinette Bowser



Program Manager – Bill Lawrence



Information System Security Officer – Darlene Young

Email the completed PIA in MSWord format to "PIA Team". Upon signing, please send this signature page to the same group email box in the form of a scanned PDF, or send as paper via interoffice mail to the Privacy Office "A/GIS/IPS/PRV".

TO BE COMPLETED BY THE PRIVACY OFFICE

Reviewer: Roxana Dufford Approver: 