Privacy Impact Assessment (PIA)

for the

Conferences Web Site (CWS)

Enter final date

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: Don Dorsey
Contact Email: Don.dorsey@ed.gov

System Owner

Name/Title: Debra Byrne
Principal Office: FSA / PPO Directorate

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 Federal Student Aid (FSA) Conferences Web Site (CWS) is an informational website that provides information to the public about FSA conferences. The CWS is made up of a series of webpages that provide information to the public and deliver video content regarding the annual FSA Training Conference. Individuals interested in FSA conferences can use this site to gain knowledge on upcoming events. The annual conference itself is generally held as an in-person conference; however, it has also been hosted virtually on a separate platform. CWS provides links to virtual sessions of the conference which will be hosted on an external hosting website. In addition, CWS also provides external links for attendees to register, book lodging, attain travel information, and download pertinent conference materials.

Individuals can register through a link on the CWS website that leads to Eleventh and Gather (E&G), a third-party application that manages registrations for the events.

Using the third-party application, the individuals may complete a registration form which will enable registered users to participate in a conference. The E&G registration system is a web-enabled application that exists within the CWS system boundary. E&G provides reports to FSA through encrypted email that include participant registration information such as name, email address, work address, phone number, agency name, company name, attendee type (e.g., Federal government employee, contractor, press), job title, and organization name. This information is collected and reviewed by FSA to track participant attendance and compile statistics about participants. Registration information is mainly stored within the E&G application, which utilizes Amazon Web Services.

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

CWS collects PII as demographic information on participants in the CWS. This PII is needed for tracking attendance and reporting on training attendance for statistical purposes.

[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

E&G collects PII in order to register individuals for conferences, and to organize and administer such events.

1.3. Is this a new, 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

The Privacy Safeguards Office reviewed the CWS PTA and system architecture and determined that there is PII maintained in the system and as such, warrants a PIA be completed.

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.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Sections 701 and 702 of the Public Health Service Act, as amended (42 U.S.C. 292 and 292a), which authorize the establishment of a Federal program of student loan insurance; Section 715 of the Public Health Service Act, as amended (42 U.S.C. 292n), which directs the Secretary to require institutions to provide information for each student who has a loan; Section 709 of the Public Health Service Act, as amended (42 U.S.C. 292h), which authorizes disclosure and publication of HEAL defaulters; and the Debt Collection Improvement Act (31 U.S.C. 3701 and 3711–3720E).

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 Student Aid Internet Gateway (SAIG), Participation Management System SORN covers CWS. Federal Registration Citation Number 83 FR 8855.

https://www.federalregister.gov/documents/2018/03/01/2018-04141/privacy-act-of-1974-system-of-records

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

Click here to enter text.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

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.

DISPOSITION INSTRUCTIONS:

[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

a. Record Copy of Department Sponsor Relating to Significant Conferences and Conventions

   Consists of records that meet one or more of the following criterion 1) were the subject of Congressional or White House interest, 2) came under intensive public scrutiny, or 3) resulted in significant changes to Departmental programs or national education policies.

   PERMANENT

   Cut off annually upon the end of conference or convention and transfer to a certified records center. Transfer nonelectronic records to the National Archives 10 years after cutoff. Transfer electronic records to the National Archives every 5 years, with any related documentation and external finding aids, as specified in 36 CFR 1228.270 or standards applicable at the time

b. Copies Relating to all Other Conferences or Conventions

   TEMPORARY

   Cut off after end of conference or convention. Destroy/delete 2 years after cutoff.

c. Records of All Other Attendees

   TEMPORARY Cut off after end of conference. Destroy/delete 2 years after cutoff or when no longer needed for reference, whichever is sooner.

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 registration system, operated by E&G, collects the information below:

Participant Contact Information

- First Name
- Last Name
- Email Address
- Work Address
- Phone Number
- Position Title
- Agency or Institution Name

E&G then shares this information with CWS to track participant attendance and compile statistics about participants.

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

Yes

The registration site collects only that information that is required to register and contact participants, and learn about their roles and affiliations. CWS collects only the information necessary to track attendance and compile statistics.

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

Registration information is collected from individuals from any type of institution, agency, contractor, company, or vendor, who wish to attend an event and register for the event on the E&G third-party website. FSA then collects this information from E&G

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

Information is collected directly from individuals when they register on the third party E&G website.

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?

There are no continuous checks to ensure that the CWS PII remains valid and accurate; however, registrants are expected to "self-validate" that they have entered data correctly. Manual checks are done on an ad-hoc basis.

Use

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

The PII collected is used to register individuals for conferences or other events. Attendance reports are generated for demographic purposes, statutory reporting of conference attendance, and to compile statistics.

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

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

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.

A privacy notice is posted to the FSA website. When users click the registration link that leads to the E&G registration system, a privacy notices is shown to the participants registering for conferences. This PIA also provides public notice. E&G also has a privacy policy which can be found here: https://www.prereg.net/privacy/EandGPrivacyPolicy.pdf.

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

https://fsaconferences.ed.gov/

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?

Registering for events is completely voluntary and initated at the request of the participants. There is an "Opt Out" feature for future email notifications when an attendee registers to participate in an event.

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

Click here to enter text.

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

☑ N/A

Click here to enter text.

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

Click here to enter text.

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

☑ N/A

Click here to enter text.

[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.

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

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?

If you wish to gain access to a record in this system, you must contact the system manager at the address listed above. You must provide necessary particulars such as your 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. Your request must meet the requirements of the Department's Privacy Act regulations at 34 CFR 5b.5, including proof of identity.

Additionally, individuals have the ability to access their PII through a user interface within E&G. Within their registration confirmation email, there is a link to take them to the E&G interface.

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

If you wish to determine whether a record exists about you in the system of records, you must contact the system manager at the address listed above. You must provide necessary particulars such as your 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. Your request must meet the requirements of the regulations in 34 CFR 5b.5, including proof of identity.

Additionally, CWS notifies users about the procedures for correcting their information through the registration confirmation email. Within that email, the user receives detailed instructions for updating their information.

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

CWS notifies users about the procedures for correcting their information through the registration confirmation email. Within that email, the user receives detailed instructions for updating 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 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

Low

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

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 Authorization to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. The CWS system received its ATO on August 7, 2020.,

FIMSA controls implemented comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Access to the CWS system is available only to users who have been authenticated to the Department network using their Department issued PIV card. Access to all privileged roles is controlled through processes that enforce formal requests and approvals for access on a need to know and least privilege basis.

Additional examples of specific controls include multifactor authentication, encryption of data at rest and in transit, firewalls, Intrusion Prevention and Intrusion Detections Systems (IPS/IDS), event monitoring systems, penetration testing, system audits, user recertification, and threat management. Finally, all privileged users are provided a copy of the Rules of Behavior and are required to complete the annual Cybersecurity and Privacy Awareness training.

The E&G registration site did not undergo security assessment as part of receiving an ATO, but plan to have that done in the future. In the interim, FSA staff are receiving regular security scan results of the vendor environment. These scans are used to analyze the system for vulnerabilities. The vendor is also obligated to notify the Department if and when system updates are made. Weekly meetings with E&G are also planned to discuss security threats to the system and identified incidents.

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.

Monitoring, testing, and evaluation are ongoing as FSA follows the Department's Lifecycle Management framework and takes part in the ATO process which includes a rigorous assessment of the security and privacy controls and potential plans of actions and milestones to remediate any identified deficiencies.. CWS is not enrolled in the FSA's Ongoing Security Authorization (OSA) program, but the NIST SP 800-53 security controls are continually assessed on a yearly basis. The system also follows the FSA Continuous Diagnosis Monitoring (CDM) program including asset compliance scans and vulnerability scans conducted weekly for each application in production and non-production environments. FSA Security Operation Center (SOC) team analyzes data and reports issues weekly to Information System Security Officer (ISSO) and the Information System Owner (ISO) for remediation. Other types of scans being conducted are scans to monitor, test, or evaluate central processing unit (CPU) patching, annual penetration testing, pre and post maintenance release activities. Annually, CWS Disaster Recovery Testing is required.

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 the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, ensuring Privacy Act records are maintained in accordance with the provisions of the Federal Records Act, Departmental policies, the Privacy Act, and the published SORN, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard 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, 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 organizations, such as memorandum of understanding, interconnection security agreement, etc, and was assessed as part of the CWS ATO.

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?

While some new privacy risks are possible due to the virtual conference environment (e.g., hacking, incorrect posting of nonpublic information to a public site), these risks are mitigated through administrative, technical, and operational security controls.

Examples of privacy risks associated with the CWS System and the E&G registration system is listed below:

- loss of PII data
- inadvertent or malicious compromise of the confidentiality and integrity of the individual's personal information
- Unauthorized access to or use of PII
- Mishandling or misuse of PII

The risks are mitigated by updating the security patches and software throughout a continuous monitoring process, limiting access to the CWS System to only those with a legitimate need-to-know purpose, and working closely with the security and privacy staff at the Department.

Risk to data maintained by the CWS system is mitigated by a comprehensive security program over the entire platform and its supporting business processes. A key component of the security program is the continuous monitoring effort which ensures that the security and privacy controls remain enforced over time and that new threats are assessed, and appropriate countermeasures implemented.

The risk of unauthorized access to PII is mitigated through an array of safeguards including: strict access controls, segregation of duties, physical access controls at the hosting facility, data encryption (both in flight and at rest), annual access certifications, and network and host-based intrusion detection systems.