Privacy Impact Assessment (PIA)

for the

Enterprise Business Collaboration (EBC)

January 10, 2020

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: Mike Murray/ISSO
Contact Email: mike.murray@ed.gov

System Owner

Name/Title: Sergio Perez
Principal Office: Federal Student Aid/Technology Office

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.

Enterprise Business Collaboration (EBC) provides the Department of Education (ED) with a platform where users (employees, contractors, external partners) can collaborate with each other using SharePoint, Project Server, Solutions Business Manager, and other end user productivity tools.

EBC includes both the Employee Enterprise Business Collaboration (EEBC) and the Partners Enterprise Business Collaboration (PEBC).

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

Section 117 of the Higher Education Act of 1965 (HEA), as amended, provides that institutions of higher education must file a disclosure report with the Secretary whenever an institution is: owned/controlled by a foreign source OR receives gifts or contracts whose value total $250K or more for all gifts and contracts received during the calendar year from an individual foreign source.

The PII (individual name and address) is being collected as responses to some of the questions on the Foreign Gifts and Contract Collection Solution (FGC) form as part of the larger Application to Participate in Federal Student Financial Aid Programs (eAPP). The purpose for providing this contact information is to provide the Department the ability to follow-up with the foreign entity contact in the event of an audit or investigation into the foreign gift reported by the institution of higher education completing the form.

[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

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.

For Foreign Gift Collection located in PEBC, Section 117 of the Higher Education Act of 1965 (HEA), as amended, provides that institutions of higher education must file a disclosure report with the Secretary whenever an institution is: owned/controlled by a foreign source OR receives gifts or contracts whose value total $250K or more for all gifts and contracts received during the calendar year from an individual foreign source.

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

Click here to enter text.

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's name or other personal identifier, all records are retrieved by OPEID which is associated with the institution of higher education completing the report.

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.

ED Schedule Locator No.: 074 Approved Date: 1/5/2011 Title: FSA Guaranty Agency, Financial & Education Institution Eligibility, Compliance, Monitoring and Oversight Records. NARA Disposition Authority: N1-441-09-15

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

[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

3.1. 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.

Domestic party legal name, domestic or foreign address, the entity which the foreign individual is associated with, and the value of the gift or contract given to the Title IV school.

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.)?

PII is provided on the FGC form which is completed by a designated individual at a Title IV school. Note that the PII provided on the form is not the PII of the individual completing the form.

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

PII is collected from Title IV schools through an electronic form.

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?

It is the responsibility of the Title IV school to ensure the validity and integrity of all PII provided as part of the FGC form. Data is further validated by the Department when an investigation or audit is requested. This occurs 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 non-sensitive PII is used as contact information in case the Department needs to contact a foreign source in the event of an audit or investigation into the foreign gift reported by the institution of higher education.

[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.

3.7. 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

3.8.1. 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.

Notice is not provided directly to the individual by the Department. It is the responsibility of the Title IV school to inform individuals that their information may be shared with the Department pursuant to Section 117 of the HEA.

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

Click here to enter text.

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?

There are no opportunities for individuals to consent to uses, decline to provide PII, or opt out. It is the responsibility of the Title IV school to communicate this with the individuals whose information is provided on the FGC form.

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.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

All information collected and listed in question 3.1 will be shared with assigned members from FSA Program Compliance, FSA Policy Liaison Office, and ED Office of General Counsel.

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

☐ N/A

PII is shared with assigned members from FSA Program Compliance, FSA Policy Liaison Office, and ED Office of General Counsel in order to conduct audits and investigations regarding the foreign gift information reported by the Title IV school

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

5.7. Is the sharing with the external entities authorized?

☑ N/A

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.

[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.

5.10. 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 an individual wishes to access their information they will need to reach out to the Title IV school responsible for reporting the information originally.

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

If an individual wishes to correct erroneous information they will need to reach out to the Title IV school responsible for reporting the information originally.

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

It is the responsibility of the Title IV school responsible for the reporting requirements to notify individuals procedures for correcting 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?

No

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?

Information contained within EBC is protected from unauthorized access by numerous security controls implemented within the application and Next Generation Data Center (NGDC) environment. EBC security controls are compliant with all Federal and Department of Education requirements for security in Federally-owned information systems and the data stored within those systems. The data is stored in an encrypted format in the SharePoint database, encrypted in motion, and stored separately from the rest of the information collected in the larger eAPP that do not contain PII.

All users with access to the information are authenticated through the FSA's Access and Identity Management System (AIMS) and approved for access by the system owner and ISSO of the PEBC. All users login with their username, agree to proper use of a government system, and provide a token number. SharePoint controls access through having their accounts added to the proper Active Directory group.

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 AIMS user accounts required to access the information is revalidated on a quarterly basis. Security scans occur weekly to ensure controls are in place and effectively

securing all data. Additional reviews of logs are audited when outliers are flagged per request.

Continuous monitoring occurs through the Department's Cybersecurity Risk Scorecard which provides a detailed view of the systems implementation of the required security and privacy controls and associated risk level of the implementation.

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 used in accordance with stated practices in this PIA by working closely with the Privacy office when there is a change in how the PII is managed in the EBC. via security authorization and assessment process and by participating in Federal Student Aid's lifecycle management methodology. The system owner is responsible for ensuring proper access to the PII maintained in the system by signing off on all access requests and ensuring all necessary security controls are implemented to sufficiently protect the PII. The system owner is involved in all security and privacy activities both internal and external.

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 FGC collects minimal information, but it contains enough to potentially infer additional information about a specific individual that is not collected by the Department. This could include information such as where someone works, what their interests are, and potentially their personal financial status. Although the collected information will be posted publicly to ED.gov, reducing the risk of unauthorized disclosure or unauthorized access to the PII, the system still ensures proper security controls are implemented to reduce these risks prior to posting.