Privacy Impact Assessment (PIA)
for the

Enterprise Business Management System (EBMS)

December 8, 2023

Point of Contact

Contact Person: Alan Asbury
Title: Information Systems Security Officer (ISSO)
Email: Alan.Asbury@ed.gov

System Owner

Name: Patrick Fedorowicz
Title: Information System Owner
Principal Office: Federal Student Aid

Submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

Please complete this ***Privacy Impact Assessment (PIA)****, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The Enterprise Business Management System (EBMS) is a configurable software development platform that supports the modernization of business processes across Federal Student Aid (FSA). EBMS is used to develop and deploy applications for FSA business automation. EBMS enables performance monitoring and continuous process improvement in addition to communication and collaboration across teams and processes supporting various FSA enterprise business functions.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

EBMS is a business management application portal hosted on the U.S. Department of Education's (Department's) Appian Government Cloud (EDAppian). The EBMS portal is a custom website which provides the FSA development team (contract staff) with a back-end development environment to configure the applications hosted within EBMS. Access to the applications is role-based and is managed through FSA's Access and Identity Management System (AIMS).

Within the EBMS development environment, users can "drag-and-drop" programming objects, allowing non-technical FSA users to contribute to design and development efforts for their respective application(s). EBMS allows information to be stored in many different formats.

Currently, the only application hosted by EBMS is the Correspondence Management System (CMS), which automates FSA strategic communications workflows for FSA's Chief Operating Officer (COO). This includes the intake and routing of documents for the FSA COO's review and approval, as well as inquiries submitted to FSA by external sources such as Congress. Information is received from these external sources (collectively referred to as "requestors") by email; FSA staff enter information pertaining to these requests and upload any related documentation into CMS. If FSA staff require additional information, they can email the requestor directly through the system. When the requestor responds to the email, the response is automatically stored in CMS. The application enables users to organize relevant information and prepare it for review, coordination, and approval or action where appropriate. Information processed in CMS may be included in responses to the original requestor.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☐ Database	☐ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

CMS (hosted within EBMS) contains internal FSA business information such as decision memos, informational documents, and inquiries from external media and internal Department components. Contact information from points of contact from external inquirers may also be collected and appended to the record of inquiry. EBMS collects PII to associate an individual with the request they submitted so status updates can be provided to the requestor, the requestor can be contacted for additional information if needed, and the individual can receive a response to their request.

In addition, PII is collected from Federal employees and contractors in order to administer the system.

1.5. Is the IT system operated by the agency or by a contractor?

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating

[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

the system.

The contractor performs operations and maintenance and provides development, modernization, and enhancement services for EBMS and CMS.

The contractor develops, tests, installs, and maintains the custom application(s) developed for FSA business users. Their responsibilities also include coordinating changes to cloud environments with Appian, the cloud service provider used by EBMS, and performing tests to ensure environments and applications are functioning correctly following any service changes. The contractor also provides system administration including creation and deletion of user accounts with the approval of the EBMS ISO, ISSO, and Product Owner.

□ N/A

1.7. If the IT system is operated by a contractor, does the contract and other acquisition-related documents include privacy requirements?

[✓ Yes]

□ N/A

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, contact your program attorney.

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

Title IV of the Higher Education Act of 1965, as amended (HEA) (20 U.S.C. 1070 et seq.).

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☐ Yes

☒ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

☑ N/A

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes**,** there is/are approved records retention schedule(s) for the information. List the schedule(s):

- ED 063, "General Correspondence," N1-441-08-013
- ED 062, "Significant Correspondence," N1-441-08-19
- ED 091, "Communications Records," N1-441-08-12
- General Records Schedule 3.1 item 050, "Data administration records."

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☐ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☐ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☐ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☐ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☐ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☐ Federal Student Aid Number

☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☐ Username/User ID	☐ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "specify below," describe the PII:
Correspondence received from the public may include other types of PII including SSN, date of birth, place of birth, home address, financial information, and medical information.

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Name, work phone number, and work email address

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Name, work phone number, and work email address

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

CMS collects contact information (name, email address, and phone number) from external media inquiries and other individual requestors. The system also maintains any information included within inquiries and related documents. Correspondence received from the public may include other types of PII including SSN, date of birth, place of birth, home address, financial information, and medical information.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

PII is collected directly from the individuals/entities (e.g., school administrators, parents, students, advocacy groups, and any other member of the public) who send in the correspondence.

PII is also collected from EBMS users for account creation.

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

System administrators manually enter information pertaining to user accounts into EBMS. EBMS users manually enter information related to requestors into CMS.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

Name is necessary to identify the source of an inquiry. Email address and phone number are necessary to obtain additional information from, or provide a response to, the requestor. Other PII may be necessary as part of FSA's response to a request in CMS.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☐ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

Individuals submitting information to the Department through inquiries are responsible for ensuring the accuracy of their own information. EBMS users entering information into CMS ensure that this information matches what is contained in the inquiries.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.7 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.7 is **YES,** what controls are in place to minimize the privacy 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.8 is **YES**, cite the authority for collecting or maintaining the SSNs.

□ N/A

Title IV of the Higher Education Act of 1965, as amended (HEA) (20 U.S.C. 1070 et seq.)

3.9.2. If the above answer to question 3.8 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

□ N/A

If an individual chooses to include an SSN in the communication, it will be retained on the document in the system. The SSN would not be entered or searchable as a separate data item, nor would the system indicate whether the SSN was included in the communication.

3.9.3. If the above answer to question 3.8 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

□ N/A

Submission of SSNs is completely voluntary as SSNs would only be collected incidentally as part of documents maintained on the system. There are no consequences for not providing an SSN as SSNs are not required for operation of any part of the system.

3.9.4. If the above answer to question 3.8 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

□ N/A

SSNs are not solicited from any individuals using or submitting information to EBMS. No alternatives were considered as SSNs may only be collected incidentally by this system.

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

Individuals or entities voluntarily provide information when they contact the Department. Notice of how their information is handled once submitted to the Department is provided through the publication of this PIA.

EBMS users are presented with a privacy notice when logging into the system through AIMS.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

N/A

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

Please refer to the AIMS PIA for the text of the AIMS privacy notice.

□ N/A

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Submission of inquiries to the Department is entirely voluntary. However, if an individual submits an inquiry, contact information including name, email address, and phone number must also be submitted to allow the Department to respond to their inquiry.

4.5. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practices, policies, or activities that affect the PII and the privacy risks to ensure that individuals are aware of and, where feasible, can consent to, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

No

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☑ N/A

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☑ N/A

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

No

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☑ N/A

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☑ N/A

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☑ N/A

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☑ N/A

Click here to select.

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

No

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☑ N/A

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☑ N/A

Click here to select.

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Information pertaining to to user accounts in EBMS can be accessed by users within the system. EBMS username is synchronized with the AIMS system and cannot be edited. Other basic user fields may be edited within the EBMS application via self-service. External requestors do not have access to information maintained in EBMS.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

EBMS users may edit information pertaining to their accounts within the system, with the exception of username which is linked to AIMS. Users must contact AIMS system administrators to correct this information. Individuals from the general public request changes to contact information through subsequent emails to FSA.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Information regarding accessing and correcting information pertaining to EBMS users is provided through the AIMS privacy notice. EBMS does not notify individuals from the general public for procedures for accessing information as these individuals cannot access EBMS. Corrections made to information maintained in EBMS pertaining to members of the general public are done in the same method as those individuals' original requests.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low
☒Moderate
☐High

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

All system users are vetted in accordance with FSA personnel security policies prior to obtaining access to EBMS. Users submit an access request form which is reviewed and approved by the user's supervisor, Contracting Officer's Representative (for contractor staff), ISO, and ISSO. Users review and acknowledge rules of behavior including privacy requirements as part of the user access request. Users are assigned to specific roles providing only the access and permissions needed to perform their assigned tasks in the system. Quarterly audits of accounts are performed to verify the need for continued access to EBMS. Individuals who no longer need access to EBMS are removed from the system.

Users are required to log in to EBMS through the AIMS which enforces two-factor authentication via a hardware token or through the Symantec VIP Access application. The Appian platform uses full disk encryption for all data stored in Appian.

Data at rest is protected for Appian Cloud environments at the disk level using industry standard algorithms at key lengths considered to be strong for that algorithm. Data in transit between the Appian Cloud database and the clients is encrypted using the Transport Layer Security (TLS) protocol.

8. Auditing and Accountability

8.1. How does the ISO assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner completes the Department's risk management framework process to receive an ATO. During the ATO process, the EBMS system owner ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, that the data are secured, 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 lifecycle.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

Continuous diagnostics and mitigation (CDM) scans are produced on a weekly basis to identify security and privacy vulnerabilities which are reviewed by the system owner, FSA Security Operations Center (SOC), Next Generation Data Center (NGDC) SOC, and ISSO. In the review, system owners are notified of any findings that require action.

EBMS also participates in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provide quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. EMBS has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

The system owner, in coordination with the ISSO and FSA Security Assessment Team (SAT), ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed and that all data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. EBMS will also participate in annual assessments and audits as required to ensure the effective safeguarding of PII.

8.3. What are the specific privacy risks associated with this program or IT system and how are those risks mitigated?

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

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.