Privacy Impact Assessment (PIA)

for the

Higher Education Programs Institutional Services: Information Technology (HEPIS)

January 29, 2021

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

Contact Point

Contact Person/Title: Beverly Baker
Contact Email: Beverly.Baker@ed.gov

System Owner

Name/Title: Beverly Baker
Principal Office: Office of Postsecondary Education (OPE)

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

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

Higher Education Programs Institutional Services Information Technology (HEPIS) is used to determine eligibility for new Title III/Title V discretionary grants; to collect interim, annual, and final performance reports for Title III/Title V and Title VII (FIPSE) grants; to collect endowment performance reports; and to calculate Formula grant distributions.

The HEPIS reporting website is built in Linux (operating system), Apache (web server software), MySQL (database software) and PHP (programming language), a common technology configuration collectively known as "LAMP-stack." Users access the HEPIS website in order to complete Annual Performance Reports by entering data into fields on online data entry forms. The website is hosted in a FedRAMP-certified Amazon Web Services (AWS) GovCloud environment. There are no direct connections into or out of the system (i.e., this system does not have an API, or an Application Programming Interface, that allows it to link directly to another system's database; nor does this system take advantage of any other systems' API to pull data programmatically from another system without direct human involvement), although there are regular exports and imports to/from the G5 system performed via a combination of manual steps on a regular basis (i.e., once a year someone accesses G5, searches for a list of new grants in this system's programs, exports it to an Excel spreadsheet, and then manually imports that spreadsheet into the HEPIS system).

Title III programs support improvements in educational quality, management, and financial stability at qualifying postsecondary institutions. Funding is focused on institutions that enroll large proportions of minority and financially disadvantaged students with low per-student expenditures. From its inception, one of the primary missions of the Title III programs has been to support the nation's Historically Black Colleges and Universities (HBCUs). The Title III programs have been expanded to support American Indian Tribally Controlled Colleges and Universities and Alaska Native and Native Hawaiian Serving Institutions, as well as other minority-serving institutions. The Title III programs also include the Minority Science and Engineering Improvement Program.

The Title V programs strengthen institutions serving Hispanic and other low-income students. The Title V programs, as well as the Title III programs, provide financial assistance to help institutions solve problems that threaten their ability to survive, to improve their management and fiscal operations, and to build endowments.

Title VII, Fund for the Improvement of Postsecondary Education (FIPSE), supports the implementation of innovative educational reform ideas, evaluates how well they work, and shares findings with the larger education community.

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

PII is collected for two reasons: (a) to provision user accounts in the system, and (b) to record contact information on the performance reports.

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

This is a new PIA for a currently operating system because the previous determination that the system did not contain PII has been changed.

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

[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

Yes

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The information is collected under the legal authority of The Higher Education Act of 1965, as amended, Title III, Title V, and Title VII, which offer grants for the purposes of strengthening higher education institutions and expanding educational opportunities for students.

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

Information is retrieved by the grant's PR Number, which is a unique identifier assigned to every grant. This identifier contains the CFDA Code, which identifies the Program under which the grant was awarded, along with a six-digit number that tracks back to the original grant application. There is nothing in the PR Number that directly identifies the institution, or any individuals associated with the institution.

[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

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

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

The records disposition schedule is ED 254: Grant Administration and Management Files. Disposition: Temporary. Destroy/Delete five (5) years after final action is taken on file, but longer retention is authorized if required for business use. The records schedule number is N 1-441-11-00.

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 PII collected for establishing and maintaining user accounts for federal employees and contractors, grantees in Title III/Title V/Title VII programs, and staff members at institutions consist of: first name, last name, email address, office phone (optional) and cell phone (optional).

The PII collected for submission of performance reports consists of: work contact information about grantee project directors, certifying officials, and additional contacts. The PII elements collected are: first name, last name, email address, office mailing address, and office phone.

"Additional Contacts" do not exist on every grant. Some grantees have more resources and larger departments where the Project Director may have assistants who perform direct data entry into the system. Other grantees have smaller departments where the Project Director does all the data entry themselves. Either way, the Project Director, Certifying Official, and Additional Contact are all employed by the grantee institution

and are authorized to access the HEPIS system for the purpose of performance reporting.

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

Yes

The system collects only name and work contact information, which is needed to provision accounts, and to contact those who use the system.

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

Data are either imported from the G5 system or submitted by the grantee.

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

Data from G5 are manually exported from that system into a spreadsheet and then imported into the HEPIS system.

Data submitted by the grantee are entered into the system on a data entry form on a secure 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?

Data imported from G5 are tested prior to import to ensure they conform to expected formatting where possible. There is no way to check the accuracy of the data entered into G5 by the G5 users, but formatting checks can catch certain errors for example in telephone numbers and email addresses.

Data entered by grantees are validated programmatically to ensure they conform to expected formatting where possible. There is no way to check the accuracy of data entered onto the reports by grantees, but Program Officers are able to catch errors during their reviews of the reports for substantive progress on the grant's objectives.

[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.

Use

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

Name and contact information are used to provision accounts so staff, grantees, and other users may access the system to submit information and manage the program. It is also used so that Program Officers know how to contact key personnel on the grant: Project Director, Certifying Official, and any Additional Contacts (additional data entry persons), if applicable.

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.

The HEPIS website does not currently have a link to a Privacy Policy, but one will be added as a link from the home page. The HEPIS Privacy Policy will be modeled on the ed.gov Privacy Policy, which is found here: www2.ed.gov/notices/privacy/index.html.

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?

Use of the HEPIS website is required to meet reporting requirements necessary to receive grant funding.

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.

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

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

Click here to 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?

Grantees can log into the HEPIS system and access their accounts.

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

Prior to submission grantees may make as many edits to their reports as they like. Once a report is submitted it is locked to prevent further editing. To make changes after submission, grantees must contact their Program Officer or the Help Desk and request that their report be unsubmitted.

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

Grantees are notified how to correct information via the online User Guide and via onscreen guidance during the report submission process.

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?

HEPIS is hosted outside of the Department's network on a FedRAMP-certified Cloud Service Provider (CSP) – AWS GovCloud. AWS enforces security controls over the physical facility where the system is located in adherence with FedRAMP standards. Authentication to the server is permitted only over secure, encrypted connections. HEPIS has an ATO in place and is in compliance with all NIST standards related to security and encrypted connections. A firewall is in place which allows only specific trusted connections to access the data.

Passwords must adhere to strict password requirements, they expire in 90 days, and they cannot reuse any of the previous five passwords.

Two-factor authentication (TFA) is required via a second device that can receive either an SMS text message, a voice phone call, or a smartphone app push notification. Users must configure at least one default TFA method but may configure one of each type for a maximum of three per account. Users may select only one TFA method during each login attempt.

User accounts are locked after three unsuccessful username/password combination attempts, or after three unsuccessful TFA attempts. Locked accounts can only be unlocked manually by an ED user or a System Administrator. Users are logged off the website after 30 minutes of inactivity but will receive a pop-up warning 30 seconds before they are logged off.

User data are saved to the database automatically every time they exit one field and enter another, or manually every time they click a Save button.

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 System Administrator runs Nessus security scans on a monthly basis to ensure system integrity. HEPIS is enrolled in the Department's monthly WebInspect scanning program. Event log monitoring is performed on a daily basis. System alerts have been implemented to notify administrators whenever there is unusually high utilization of resources, or unexpected peaks in traffic. System and software patches are tested as they are released and applied once they are verified.

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 works with the Department's Privacy Office to conduct a Privacy Impact Assessment and to ensure that it's accurate and updated as required. The system owner also completes the ED Risk Management Framework process to secure an ATO. The system owner also works with the contractor to ensure the system is being used appropriately and in accordance with the practices detailed in this document.

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?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats, and to mitigate the risks to the data. Once key risk to the data is unauthorized access, use, or disclosure of PII pertaining to the users. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud. The risks are mitigated by the above-mentioned controls and safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. In order to mitigate this risk the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual security assessments for ATO renewal

Additional privacy risks are mitigated as the system collects the minimum necessary PII to achieve the purpose. Additionally, the information collected is considered to be fairly low risk, as it is only name and work contact information and does not include any elements that have been identified as sensitive.