US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/11/2025

OPDIV:

NIH

Name:

Historically Black Colleges and Universities (HBCU) tool

PIA Unique Identifier:

P-6278176-506881

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The Privacy Impact Assessment (PIA) that was originally submitted inadvertently listed the system as a Federal Information Security Management Act (FISMA) reportable system in question 3b. The PIA has been updated to reflect the correct FISMA status. No other changes were made.

Describe the purpose of the system.

The Historically Black Colleges and Universities (HBCU) tool allows those with access to see what grants and contracts are available through periodic data uploads from the National Institutes of Health (NIH) grants website (grants.nih.gov), NIH Research Portfolio Online Reporting Tools Expenditures and Results (RePORTER), System for Award Management (SAM) website (beta.sam.gov), and the Federal Procurement Data System (FPDS) website (FPDS.gov). The data uploaded from these sites reduces the user’s reporting effort by prepopulating about 75% of the data input fields. Consolidating the upcoming grants and contracts into this system decreases the burden on the HBCUs and businesses by giving them one site to access NIH funding opportunities. The

information entered by an HBCU or a business is viewable only by that HBCU or business and the NIH Small Business Program Office (SBPO) staff.

Describe the type of information the system will collect, maintain (store), or share.

Data collection includes the collection of the following personally identifiable information (PII): Name, email address, phone number, mailing address and log in credentials for external individuals that are stored in a system.

NIH users log in utilizing their Personal Identity Verification (PIV) card via NIH portal. This is done via the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network, assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

External users login utilizing their email address and encrypted password stored within the database.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The HBCU tool allows those with access to see what grants and contracts are available through periodic data uploads from the NIH grants website (grants.nih.gov), NIH RePORTER, SAM website (beta.sam.gov), and the FPDS website (FPDS.gov). The data uploaded from these sites reduces the user's reporting effort by prepopulating about 75% of the data input fields. Consolidating the upcoming grants and contracts into this system decreases the burden on the HBCUs and businesses by giving them one site to access NIH funding opportunities. The information entered by an HBCU or a business is viewable only by that HBCU or business and the NIH SBPO staff.

Data collection includes the collection of the following: Name, email address, phone number, mailing address and log in credentials for external individuals that are stored in a system.

NIH users log in utilizing their PIV card via NIH portal. This is done via the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network, assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

External users login utilizing their email address and encrypted password stored within the database.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Mailing Address
Phone Numbers
Log-in credentials

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

To allow those with access to see what grants and contracts are available through periodic data uploads from the NIH grants website, NIH RePORTER, SAM website, and the FPDS website. Users accessing the system will be shown specific features.

Describe the secondary uses for which the PII will be used.

n/a

Identify legal authorities governing information use and disclosure specific to the system and program.

42 USC 241

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Email
Government Sources
Within the OPDIV
Other HHS Operating Divisions
Other Federal Entities
Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable. HBCU does not solicit the public for information.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Currently, there is no agreement because the system has not been rolled out for use to other government entities. The feature has just been merely created for utilization in the near future.

Describe the procedures for accounting for disclosures.

n/a

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The application shows the "Terms and Conditions" banner that informs the user that personal information is collected.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no opt-out method for users since their email address and log-in credentials are needed for authentication purposes. Individuals do have the option to not submit an email and log-in credentials however, they will not have access to the system.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

If changes were to occur, an email will be sent to the users to mention the changes and either obtain their consent or let them opt out of the system.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

If the user has any concern that their data is inappropriately obtained, used, or disclosed, they have the option to use the "Contact Us" page to contact the Office of Acquisition and Logistics Management (OALM) Staff.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

PII data within HBCU Tool will be backed up every day to ensure the data availability and will be reviewed periodically to ensure the integrity of the data.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

HBCU Tool have role-based authorization to ensure least privilege access to the data in the system. An individual user’s access in terms of read/write/review within HBCU Tool is controlled by very strict role-based control.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Access to PII is assigned to personnel based upon current job responsibilities. For NIH users, a NIH IAM Systems account login is required to gain access to the stored PII data. For external users, specific login credentials are required to access the stored PII data.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

n/a

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Item Number 07-103: Information technology development project records. System development records.
Description: These records relate to the development of information technology (IT) systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving.
Disposition Instruction: Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.
Disposition Authority Agency (DAA): DAA-GRS-2013-0005-0007

Item Number 07-104: Information technology development project records.
Description: Special purpose computer programs and applications: Computer software programs or applications that are developed by the agency or under its direction solely to use or maintain a master file or database authorized for disposal in a General Records Schedule (GRS) item or a National Archives and Records Administration (NARA) approved records schedule.
Disposition Instruction: Delete when related master file or database has been deleted, but longer retention is authorized if required for business use.
Disposition Authority: DAA-GRS-2013-0005-0008

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access. The System is hosted at NIH Office of Information Technology (OIT) within a secure Windows environment and can only be accessed by Administrators with authentication information.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware. Technical controls such as firewall is in place to protect from unauthorized intrusions.

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Identify the publicly-available URL:

https://oamp.hbcu.od.nih.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null