

**Privacy Impact Assessment (PIA)**

for the

**Graduate Assistance in Areas of National Need (GAANN)**

**May. 14, 19**

**For PIA Certification Updates Only:** This PIA was reviewed on March 14, 2019 by Rebecca Ell certifying the information contained here is valid and up to date.

**Contact Point**

**Contact Person/Title: Daveta Brown**

**Contact Email: Daveta.Brown@ed.gov**

**System Owner**

**Name/Title:** **Rebecca Ell**

**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.***

# Introduction

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

GAANN is a Web-based data management application that supports the collection and processing of performance data required by the Office of Postsecondary Education. This system is used to provide performance data about the GAANN Fellowship Program for the Department of Education’s (Department) use in responding to the requirements of the Government Performance and Results Act. In addition, information obtained from the system of records may also be used for the general purpose of administering the GAANN Fellowship Program.

The Program Performance Plan (APR/FPR) describes the goals and intended outcomes of the Department's programs and initiatives. Annual targets and strategies, along with measures for monitoring progress, are published in performance plans prior to each fiscal year. The plans also include actual performance data showing whether targets were met in previous years.

The GAANN program is a program that awards fellowships through academic institutions of higher education. Both the Annual Performance Report (APR) and the Final Performance Report (FPR) collect individual student records provided by the grantee institution.

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

This system captures long and short-term performance data that monitor the funds allocated to recipient institutions, tracks the time-to-degree completion, and graduation rates of GAANN fellows. System data includes individual student data, financial data, graduation rate data, and employment data of all GAANN fellows.

This system contains records on individuals who apply for fellowships and receive admission to a GAANN project.

This system contains information including the individual’s name, gender, ethnicity, field of study, source of student’s GAANN Fellowship (federal or institutional matching), amount of stipend per year of student’s GAANN Fellowship, amount of institutional contribution to tuition per year of student’s GAANN Fellowship, amount of support the student received after the GAANN Fellowship (optional), year and term the student entered institution’s graduate program, current education status, current employment status, cost of attendance, tuition and fees (if included in financial need) and expected family contribution. It also collects project director information such as name, department, email, phone, and address information.

* 1. Is this a new system, or one that is currently in operation?
	Currently Operating System
	2. Is this PIA new, or is it updating a previous version?
	Updated PIA
	3. Is the system operated by the agency or by a contractor?

Contractor

* + 1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

No

# Legal Authorities and Other Requirements*If you are unsure of your legal authority, please contact your program attorney.*

* 1. Whatspecific 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 authority of Title VII, Part A, Subpart 2, Section 711 of the Higher Education Act of 1965, as amended; the program regulations in 34 CFR 648; and the Education Department General Administrative Regulations (EDGAR) in 34 CFR 74.51. Further, the performance report form lends itself to the collection of quantifiable data needed to respond to the requirements of the Government Performance and Results Act (GPRA). Grantees are required to provide the data requested in order to obtain or retain grant funding according to 20 U.S.C. 1135, 34 CFR Section 648.66.

**SORN**

* 1. 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

		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]](#footnote-2) Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.



Click here to enter text.

* + 1. 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.
		

A system of record notice is not needed because the information collected is not retrieved by any personal identifiers. Therefore, a system of record as defined by the Privacy Act is not being created and the reporting requirements of OMB Circular A-130 do not apply.

**Records Management**

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

* 1. 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: Records on successful applications are destroyed five years after final payment from the Department to the institution, or after completion of audit related activities or litigation, whichever is later.

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

	Yes

# Characterization and Use of Information

**Collection**

* 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.

This system contains information including the fellow’s name, gender, ethnicity, race, institution, department, field of study, source of student’s GAANN Fellowship, amount of stipend per year of student’s GAANN Fellowship, amount of institutional contribution to tuition per year of student’s GAANN Fellowship, amount of support the student received after the GAANN Fellowship (optional), year and term the student entered institution’s graduate program, current education status, current employment status, cost of attendance, tuition and fees (if they were included in determination) and estimated family contribution. It also collects project director information such as name, department, email, phone, and address information.

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

Yes

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

The GAANN program collects the student information directly from a participant's educational institution and not from the student.

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

The information is collected on-line via a website and moved to a database. Information contained in this system is obtained from the institutions that the fellows attend. Grantees enter annual and final performance report information in the GAANN system. Information is provided to the program officer by the grant director at the educational institution and not by the students.

* 1. How is the PII validated or confirmed to ensure the integrity of the information collected?[[3]](#footnote-3) Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The project director and certifying official of each institution must certify the accuracy and completeness of all information in the report. Information is collected by the institution and that is gathered directly from the students ensuring accuracy.

**Use**

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

The Department uses APR and FPR data to: (1) evaluate program accomplishments; (2) demonstrate program effectiveness, and (3) aid in compliance monitoring. Collecting performance report data on an annual basis provides the Department with the ability to assess each grantee's progress in meeting the program' s goals and objectives and to determine compliance with the statute and program regulations. APR and FPR data have also been instrumental in determining whether grantees are entitled to continuation of funding by analyzing financial data submitted by grantees.

* 1. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

	No

		1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?
		

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.*

* 1. 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

* + 1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.
		

Click here to enter text.

* + 1. Specify any alternatives considered in the collection of SNNs and why the alternatives were not selected.
		

Click here to enter text.

# Notice

* 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 system is a database for grantee institutions to input performance data. The website posts a Privacy Act notice before access is granted.

* 1. 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.
	

Privacy Act Notice is posted on the home page https://opeweb.ed.gov/gaann and cites the Privacy Act of 1974 (5 USC section 552a).

-----------------------------

Authority - Collection of this information is required under the Education Department General Administrative Regulations (EDGAR) volume 75.590, 75.720, and 75.730-732 and under 2 CFR 200.328 (Monitoring and reporting program performance).

Purpose - The primary purpose of the information collected is for use in the performance monitoring of the Department of Education’s (the Department's) GAANN program.

Routine Uses - The information you provide will ordinarily not be disclosed outside of the Department and as otherwise allowed by 20 U.S.C. 1135C (1993) Title 20. Education § 1135c.

Participation - Further funding or other benefits may be withheld under this program unless all required reports are completed and filed as mandated under the U.S. Code of Federal Regulations.

* 1. 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?

 The project directors are the individuals who collect and report data and, while the information is voluntary, it may result in non-funding if not reported.

* 1. 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

# Information Sharing and Disclosures

**Internal**

* 1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

	No
	2. What PII will be shared and with whom?
	

Click here to enter text.

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

Click here to enter text.

**External**

* 1. 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
	2. What PII will be shared and with whom? List programmatic disclosures only.[[4]](#footnote-4)
	**Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.
	

Click here to enter text.

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

Click here to enter text.

* 1. Is the sharing with the external entities authorized?
	

Click here to select.

* 1. Is the system able to provide and retain an account of any disclosures made and make it available upon request?
	

Click here to select.

* 1. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?
	

Click here to enter text.

* 1. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?
	

Click here to select.

* 1. Does the project place limitation on re-disclosure?
	
	Click here to select.

# Redress

* 1. What are the procedures that allow individuals to access their own information?

Fellows wishing to access their own information must contact their institution. Only institutions (the grant's project director) update information in the GAANN system. The fellows do not contact the Department or have access to their information in the GAANN system.

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

The institution is the organization that collects and provides the information to the Department. The fellow can make a formal request to correct information via the educational institution.

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

It is the responsibility of the institution to ensure data is correct. Fellows must go through their educational institution to make a request for correction of the records.

# Safeguards*If you are unsure which safeguards will apply, please consult with your* [*ISSO*](https://share.ed.gov/teams/OCIO/IA/SEA/SEA_Collab/SitePages/ED%20ISSOs.aspx)*.*

* 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

* 1. Is an Authority to Operate (ATO) required?

	Yes
	2. Under [NIST FIPS Pub. 199](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf), what is the security categorization of the system: **Low, Moderate, or High?**
	Moderate
	3. What administrative, technical, and physical safeguards are in place to protect the information?

Due to the Federal Information Security Management Act of 2002 (FISMA), GAANN must receive a signed Authority to Operate (ATO). The ATO process includes a rigorous assessment of security controls, a plan of action and milestones (PO&AMs) to remediate any identified deficiencies, and a continuous monitoring program. FISMA controls implemented by GAANN comprise of 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 environment protection, planning, personnel security, risk assessment, system and service acquisition, system and communications protection, system and information integrity, and program management.

* 1. 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

* 1. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

* 1. 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 following tasks are performed to safeguard the GAANN information:

* Monthly vulnerability scans performed
* Annual contingency plan test performed
* Annual self-assessments conducted; and/or Annual security assessments performed by the ED Security Authorization Team
* Ongoing - Follow the Department's Life Cycle Management framework
* Annual updates to system security documents
* Annual mandatory Cybersecurity and Privacy Act Training for employees and contractors
* Monthly Continuous Monitoring is in place with vulnerability scans (RA-05), HW/SW inventories (CM-08), and configuration management database updates (CM-06) are posted to CSAM.

System and Data hosting are provided by the Amazon Web Service (AWS) as a Federal Risk and Authorization Management Program (FedRAMP) certified cloud.

# Auditing and Accountability

* 1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

Only contractor staff that supports the data collection or data analysis and a small number of Department staff are allowed access to the data. Contractor staff have appropriate security clearances and also sign confidentiality and non-disclosure agreements to protect against unauthorized disclosure of confidential information. OPE employees who access the data have appropriate security clearances. Contractors and Departmental employees are required to complete annual mandatory security awareness and privacy act training.

* 1. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

* 1. What are the privacy risks associated with this system and how are those risks mitigated?

The privacy risk associated with the system is the exposure of performance-based data submitted by grantees containing confidential student-based information. The data reside in a secured facility in a secured server behind a Department approved firewall system that continuously monitors for intrusion and unauthorized access. The IT contractor security staff is notified of Windows security updates and view server security status reports and applies updates as needed and uses anti-virus software on all servers and workstations.

The data collection site requires grantees to log in with a Department issued login ID and password. All screens and data transfers are encrypted and transmitted using hypertext transfer protocols (HTTPS). The IT contractor transfers the data to the analysis contractor via a secured file transfer protocol (FTP) site. As with the IT contractor, the data analysis contractor's security program is compliant with federal government regulation and National Institute of Standards and Technology (NIST) standards.

Only contractor staff that supports the data collection or data analysis and Department staff are allowed access to the data. Contractor staff has appropriate security clearances and also signs confidentiality and non-disclosure agreements to protect against unauthorized disclosure of confidential information.

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](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf) [↑](#footnote-ref-1)
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> [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
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. [↑](#footnote-ref-4)