



Privacy Impact Assessment (PIA)
for the

National Assessment Governing Board (NAGB) Website

(NAGBWEB)

May 10, 2023

For PIA Certification Updates Only: This PIA was reviewed on **5/10/2023** by **Munira Mwalimu** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Munira Mwalimu/Information System Security Officer
Contact Email: Munira.Mwalimu@ed.gov

System Owner

Name/Title: Elizabeth Schneider/Information System Owner
Principal Office: National Assessment Governing Board (NAGB)

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

May 10, 2023

*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.

The National Assessment Governing Board Website (NAGBWEB) is a website (www.nagb.gov) for the National Assessment Governing Board (NAGB). The NAGB was created by Congress in 1988 as an independent, nonpartisan Board to set policy for the National Assessment of Educational Progress (NAEP). In overseeing NAEP, the NAGB identifies subjects to be tested, determines the content and achievement levels for each assessment, approves all test questions, and takes steps to improve the reporting of results. The NAGB is responsible for communicating NAEP results to a wide range of audiences; outreach and dissemination strategies take place via NAGBWEB. Governing Board members represent a range of backgrounds. Membership must, by law, include two State governors, who may not be members of the same political party, and two State legislators, who must also belong to different parties. The other members are selected on a nonpartisan basis. Board members represent different parts of society, such as representatives for institutions of education (K-12), state and local education agencies, education industry subject matter experts, businesses, and general public representatives (i.e., parents of current students).

NAGBWEB is a public-facing website that includes secure content, including advance meetings and new member orientation meeting materials for NAGB members. In addition, the website maintains information about current and former Board members of the NAGB. NAGB members are categorized as “special government employees,” but are not employees of the U.S. Department of Education (Department). The website hosts a secure application submission portal for a nationwide public campaign that solicits applications for Board vacancies. The annual campaign conducted via the website seeks voluntary applications for open NAGB positions.

The NAGBWEB also maintains two restricted websites for the nominations and ratings processes:

- Nominations Portal -- Information is collected from the candidates via the secure portal. Before submitting an application, candidates are required to create an account to log in to the portal to submit an application. Once authorized for

access, candidates can submit their application for Board membership. The collected information as part of the application includes name, title, organizational affiliation, organizational and/or home mailing address (in the instance where the candidate is a parent, this would be the home address), phone number, email address, gender, and ethnicity.

- Member/Ratings Portal – Rating officials (comprised of NAGB members) are required to create an account to log in to the portal to review and rate submitted applications. Applications submitted are then reviewed by the NAGB’s Nominations Committee, consisting of existing NAGB members. A final list of recommended nominees is sent from the NAGB Nominations Committee to the Secretary of Education, who makes the final selection of new NAGB members. Each member reviews approximately 10 applications.

The NAGB reaches out through the website and social media (i.e., Facebook, LinkedIn, and Twitter) to encourage members of the public to submit applications for open positions on the NAGB. Categories for vacancies include:

- general public representatives (which includes parents)
- fourth, eighth, and twelfth-grade teachers
- elementary and secondary school principals
- chief State school officers
- testing and measurement experts
- curriculum experts
- State legislators
- nonpublic school administrators
- local and State school Board members
- local school superintendents
- business representatives

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

PII is collected to allow individuals to apply for NAGB vacancies in various open categories of membership. This information is necessary to meet the requirements stated in Public Law 107-279, Education Sciences Reform Act of 2002, including “The Secretary and [NAGB] shall ensure at all times that the membership of [NAGB] reflects

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](#)

regional, racial, gender, and cultural balance and diversity.”

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?

Updated PIA

This PIA is being updated as part of a regular biennial review.

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.

NAGBWEB is authorized by Public Law 107-279, Education Sciences Reform Act of 2002, allowing NAGB to conduct an annual nominations campaign to solicit applicants for Board membership in various categories.

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

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 based on the position/category to be filled. Information is not retrieved by name or other personal identifier.

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 the General Record Schedule (GRS) 6.2, Federal Advisory Committee Records; official records are maintained for up to 15 years or upon the termination of the committee, whichever is sooner.

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.

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>

For NAGB applicants: name, title, organizational affiliation, organizational mailing address, phone number, email address, gender, ethnicity, username, and password. In addition to the information collected, the applicant will submit a resume, personal statement, letter of commitment, and up to three letters of support.

For NAGB application reviewers: name, email address, username, and password are required to access submitted applications.

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

Yes

The PII collected and maintained is the minimum amount required by NAGBWEB. The minimum amount collected is to allow for access, communication with applicants, review applications and select Board members, and is necessary to meet the requirements stated in PL 107-279, including “The Secretary and [NAGB] shall ensure at all times that the membership of [NAGB] reflects regional, racial, gender, and cultural balance and diversity.” PII collected and maintained about reviewers is the minimum necessary to allow for providing access to the Ratings portal to review applications that are submitted.

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

PII is collected from applicants for vacant NAGB positions. In addition, PII is collected from application reviewers to allow access to the system for reviewing submitted applications.

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

Information is collected via application forms submitted via a secure portal from applicants interested in applying for vacancies. I

Information is collected via the Ratings Portal from Board members for access to the environment for review of submitted applications.

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?

Applicants are responsible for ensuring that information on their applications is accurate.

Use

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

Information collected is used to review and screen applicants for potential appointments to NAGB membership.

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

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

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.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

N/A

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 about the collection of PII is posted on the NAGB website.

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

PRIVACY NOTICE (DRAFT)

The National Assessment Governing Board (Governing Board) is committed to maintaining the integrity and privacy of personal information collected via our website at www.nagb.gov. This privacy notice (“notice”) describes our information collection and dissemination practices in connection with your application for serving as a Governing Board member and for members of the Governing Board in their review of applications for Governing Board membership. We encourage you to review this notice to understand how we use your data.

By using this website, you are agreeing to the terms and conditions of this notice. Please review the entire notice and feel free to contact us using the contact information below if you have any questions. By using the website, you are agreeing to the collection, use, and disclosure of your information in accordance with the notice.

COLLECTION OF INFORMATION

We collect information you voluntarily provide in connection with applications for Governing Board vacancies. Information we collect relates to your contact and demographic information -- your full name, address, email, phone number, gender, race, and ethnicity. We collect your gender, race, and ethnicity information because we are required by law to assure membership of the Assessment Board reflects regional, racial, gender, and cultural balance and diversity. [Public Law 107-279](#). To protect your information, we require that you set up a username and password to log onto the website.

USE OF INFORMATION

We use the information we collect via the website to prepare and review candidate application packages for vacancies on the Governing Board, and submit the finalists to the Office of the Secretary for review and appointment in accordance with the requirements of [Section 302, Public Law 107-279](#).

CONTACT INFORMATION

If you have any questions about this notice or our practices, please contact us at the National Assessment Governing Board, 800 North Capitol Street N.W., Suite 825, Washington DC 20002, or via email at nagbqueries@ed.gov.

- 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?

All applications for NAGB membership are voluntary; however, all information collected through the application is mandatory to be considered for membership.

- 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

Once applications are reviewed by Board members, information is submitted to the Office of the Secretary for the final selection of NAGB Board members for the upcoming year.

- 5.2. What PII will be shared and with whom?

N/A

NAGB applicant's name, title, organizational affiliation, organizational mailing address, phone number, email address, gender, ethnicity, resume, personal statement, letter of commitment, and up to three letters of support are submitted to the Office of the Secretary for final selection.

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

N/A

Once applications are reviewed by Board members, information is submitted to the Office of the Secretary for the final selection of NAGB Board members for the upcoming year.

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.

Yes

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

The publicly available NAGB website provides the name and titles of current and former NAGB Board members. For current members, the website also provides current work position, Board term, Board category, representative board activities, and educational background.

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

N/A

The purpose of posting the Board member information is for oversight and transparency regarding who makes up the Board and their responsibility within the Board.

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.

5.7. Is the sharing with the external entities authorized?

N/A

Yes

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

N/A

No

Since information is made public through the NAGB website, the Department is not able to account for any disclosures of the publicly available information.

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

N/A

Information is shared through the NAGB website.

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

No

5.11. Does the project place limitation on re-disclosure?

N/A

No

6. Redress

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

Applicants: Once an application has been submitted, applicants may not access their information.

Reviewers: Reviewers have an opportunity to access their information through the Ratings portal.

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

Applicants: If an applicant believes their application contains inaccurate information, they can contact nagbnominations@ed.gov to correct the errors.

Reviewers: If a reviewer believes their information is not accurate, they can correct it through the Ratings portal.

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

Individuals are notified about procedures to correct their information through the NAGB website.

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?

NAGBWEB is hosted on the AWS Government cloud computing platform. Access to the system is limited to authorized Department users and NAGB members responsible for reviewing incoming applications. Authorized personnel includes Department employees and special government employees. The system limits data access to users on a “need to know” basis and controls individual users’ ability to access or alter records

within the system. Department employees are also required to complete security and privacy awareness training on an annual basis.

The NAGBWEB Information System Owner (ISO) is responsible for daily operational oversight and management of the system's security and privacy controls and ensuring to the greatest possible extent that the data are properly managed and that all access to the data has been granted in a secure and auditable manner. The NAGBWEB ISO is responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the Department's Office of the Chief Information Officer (OCIO), the Student Privacy Policy Office (SPPO), and the appropriate Department officials in accordance with Federal policy and established Department procedures.

- 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 required scans/tests on a monthly and annual basis as required. Security and system documentation is updated as required. Monitoring and auditing of all event logs are performed on a regular basis. Patches are checked for on a periodic basis and tested and applied to the server weekly, depending on necessity.

When going through the ATO/Ongoing Security Authorization (OSA) process, the system owner establishes monitoring processes to ensure the information is used in accordance with the approved practices. During the OSA process, smaller subsets of security controls are tested every quarter.

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 ISO ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, NAGBWEB makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of 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, and 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 and meets regularly with the Information System Security Officer (ISSO).

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?

Privacy risks associated with NAGBWEB 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 embarrassment or loss of credentials that are used to gain access to other resources. 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 and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.