Privacy Impact Assessment (PIA)
for the

National Assessment of Educational Progress (NAEP)
August 11, 2023

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

Contact Point

Contact Person/Title: Bobbi Woods/Information System Owner
Contact Email: roberta.woods@ed.gov

System Owner

Name/Title: Bobbi Woods/Information System Owner
Principal Office: Institute of Education Sciences

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.

The National Assessment of Educational Progress (NAEP) system is used to prepare for, collect, process, and store information for the NAEP program.

The NAEP Program

NAEP is a program that is overseen and administered by the National Center for Education Statistics (NCES), an office within the U.S. Department of Education's (Department) Institute of Education Sciences (IES). The National Assessment Governing Board (NAGB), an independent body appointed by the Secretary of Education, sets NAEP policy. The NAEP program provides important information to the Department and the public about student achievement and learning experiences in various subjects.

As described below, NAEP assesses a sample of students across the country to be representative of all students in the United States. Students who are selected for the assessment represent the Nation's geographic, racial, ethnic, and socioeconomic diversity. Each student's participation is critical for providing an accurate and complete picture of student achievement and ensuring that policymakers, researchers, and educators have reliable data to inform educational improvements.

How exactly do students and schools participate in NAEP?

- The NAEP assessment is administered to students on-site, and in school during regular school hours. Students spend between 90 and 120 minutes taking the assessment, which is an examination on one subject, such as reading or math. Students also complete a survey questionnaire which includes general demographic questions. All student assessment and survey results are anonymous and non-identifiable. NAEP representatives bring all necessary materials, including tablets or laptops for digitally-based assessments, to the schools on assessment day. Allowable

accommodations are provided as necessary for students with disabilities and/or English learners.
- NAEP survey questionnaires are administered to teachers and schools through a web application and can be filled out anywhere remotely.
- All responses to NAEP assessments and survey questionnaires are private and are publicly reported as aggregates only, as authorized by Congress.

What other data are collected during a NAEP assessment?

NCES conducts three types of survey questionnaires as part of NAEP to help provide context for assessment results. Students, teachers, and school officials may skip any question by leaving a response blank.

- Student questionnaires provide information regarding opportunities to learn in and outside of the classroom, educational experiences, and a variety of other topics, including socioeconomic status and technology use.
- Teachers who are responsible for the subject of the administered assessment complete questionnaires that gather information on teacher training and instructional practices.
- School questionnaires, usually completed by the principal or assistant principal, gather information on school policies and characteristics.

The NAEP System

The NAEP system consists of the following applications:

- The NextGen assessment applications production environment is a web application used to collect NAEP assessment data. The environment is used to configure the assessment and provide accessibility options for the NAEP assessments and questionnaires, as well as making them available on NAEP-provided tablets and laptops. This application uses Databricks within Amazon Web Services (AWS) to process data and provide warehousing capabilities to the student response data lake. DataBricks is used for collaboration purposes and centralized data analysis by Department employees, Department contractors, and special users (subject matter experts who serve on a NAEP Program Committee or NAGB Board members).
- NAEP Access Portal—Built on Microsoft SharePoint, the portal is a collaboration tool for NAEP users, which includes State and District

coordinators,[1] Department employees, Department contractors, and special users. This portal contains several applications:

1. Integrated Management System (IMS)—This is NAEP's primary document repository/library and contractor workspace, which contains meeting minutes, agendas, and assessment design documents and items. IMS is built on SharePoint.
2. NAEP Network—This SharePoint application is a collaborative tool built within the portal used by State/District coordinators to communicate and document their daily activities.
3. Content management system (CMS)—The CMS, a SharePoint application, allows for webpages to be reviewed and then deployed/published on public sites. The CMS allows reviewers (Department employees, Department contractors, and special users) to collaborate, review, and edit the information before it is approved by the NAEP Webmaster and then finally by the IES Webmaster before going on the web. The NAEP public websites are hosted in the IES Data Center:
    - https://nces.ed.gov/nationsreportcard/—the website that explains the "business" of NAEP, an overview of how the NAEP Program operates, and
    - https://www.nationsreportcard.gov/—*The Nation's Report Card*, which reports data/results from the NAEP assessment given to students.
4. Assessment observation coordination and scheduling—This custom-built web application was developed for internal use by government staff and contractors to see where NAEP assessments were being given so that one could schedule a time to "observe" an assessment. Currently, due to COVID-19, this tool is not in use.
5. Report tracking management—This custom-built web application was developed to track the data reports being published by the NAEP program and their status in the review process.
6. Public communication management—This commercial off-the-shelf web application tracks inquiries that come via email from the public about the NAEP program, along with government responses so that the government does not have to "reinvent the wheel" for repeat questions. Public site users ask questions via a form on the NAEP website which is then routed to the correct individual. This helps inform what information gets posted on the public website and/or

[1] State and District Coordinators are State and District employees contracted to the Department for assistance with the NAEP program.

what information needs to be better explained. This form only collects a user's email address for a response.

7. NAEPq and early response data access for teacher and school participants—When the NAEP program goes to a school, teachers and school administrators may fill out a questionnaire called NAEPq. To log into the NAEPq application, schools and teachers use login information that is stored in the National Center for Education Statistics Longitudinal Data Collection System (NCESLS) system and provided to them. This includes a custom URL and password.

   As an incentive, they are offered early access to response data. The data are collected via the NAEPq custom application where sampled schools/teachers are given a unique URL, NAEP ID, and password. As an incentive to participate, participants are allowed to "opt-in" to view "preliminary" response aggregate data. For example, a user can see how many schools responded that they use laptops in their classrooms. By default, participants provide no PII through the NAEPq questionnaire; however, if participants "opt-in" to view response data, they provide first name and last initial, as well as work email address, to which NAEP sends the NAEP ID and password.
8. NAEP Help Desk—NAEP has a "Help Desk" that users may contact via email if they have issues with their access to the system.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] is collected, used, maintained, or shared.

NAEP collects contact information from a variety of audiences for the described purposes below:

- Contact information is collected from school administrators and teachers of sampled schools for the purpose of contacting those individuals regarding the NAEP Online Teacher and School Questionnaires (NAEPq).
- Contact information is collected from Department employees, Department contractors, and special users (subject matter experts who serve on a NAEP Program Committee or NAGB Board members) to be used for authorization of access to NAEP applications.
- Contact information is collected from State/District coordinators to facilitate communication through the NAEP Network.

[2] 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

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

New Department guidance on how to apply the definition of PII required that a PIA be completed for the system. NAEP collects and maintains the names and work contact information (as outlined in question 3.1) of school administrators and teachers, State/District coordinators, Department employees, Department contractors, and special users, as defined in question 1.2. This information is collected for communicating with external participants and allowing access to the system for Department employees, Department contractors, and special users.

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.

The legal authority that permits the NAEP program is the National Assessment of Educational Progress Authorization Act (Pub. L. 107-279 Title III, section 303).

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?

Yes

Records are retrievable by assessment year, subject area, age, or grade at the school.

2.2.1. If the above answer is **YES,** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).[3] Please provide the SORN name, number, Federal Register citation, and link, or indicate that a SORN is in progress.

☐ N/A

The SORN, titled "National Center for Education Statistics National Assessment of Educational Progress," 18-13-03, 64 FR 30184, was published in the Federal Register on June 4, 1999.

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

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.

IES is waiting on the 21st Century Information Retention Policy Framework to be approved and implemented. Until that framework is implemented, the records will not be destroyed until NARA approves said schedule.

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] 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

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 NAEP system hosts the NAEPq application, which receives PII (first name, last name, email address, and unique identifier (alphanumeric randomized set of digits. NOTE: the same person would have a different unique identifier across different NAEP assessment years)) of survey participants (school administrators and teachers) from the NCESLS system. Survey participants accessing preliminary survey results also have a password maintained on the system. All other survey information is not identifiable.
- The IMS SharePoint application includes a program contacts directory for Department employees, Department contractors, and special users that includes: name, organization, title, work/business phone number, work/business email address, and work/business address.
- The NAEP Network collects the following contact information from State/District coordinators: name, work/business address, work/business email address, work/business phone number, and State/District with which the user is associated, and optional emergency contact information (name, phone number) when registering for workshops/meetings to be used in case of an emergency.
- For Department employees, Department contractors, and special users, NAEP system maintains name, work/business email address, and organization.

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 NAEP to meet the requirements of the NAEP program. First name, last name, and work email addresses collected from school administrators and teachers of sampled schools are necessary for contacting those individuals regarding the NAEP Online Teacher and School Questionnaires (NAEPq), which are provided through NCESLS. A unique identifier is generated within NCESLS, and associated with an individual for a specific NAEP assessment year. This identifier is shared with the NAEP system.

First name, last name, organization, title, work/business phone number, work/business email address, and work/business address collected from Department employees, Department contractors, and special users (subject matter experts who serve on a NAEP Program Committee or NAGB Board members) are necessary for access to NAEP applications.

First name, last name, work/business address, work/business email address, work/business phone number, and State/District with which the State/District user is associated, and optional emergency contact information (name, phone number) collected from State/District coordinators facilitate communication through the NAEP Network. In addition, State coordinators need access to each other for collaboration purposes, as part of their duties.

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

1. The NAEP System collects PII from all system users (State/District coordinators, Department employees, Department contractors, and special users) to support the program. Specifically, these are stored in these 3 elements:
    a. NAEP Active Directory (Department employees, Department contractors, and special users)
    b. NAEP Network (State/District coordinators)
    c. IMS Contacts List (Department employees, Department contractors, and special users).
2. In addition, the NCES Longitudinal Studies (NCESLS) system provides the NAEP system with school and teacher information for NAEPq. This PII is collected by NCESLS during the pre-assessment phase from participating NAEP schools.

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

1. NAEP Active Directory and IMS Contacts List – Department employees, Department contractors, and special users who need access to the NAEP system will contact the NAEP help desk to initiate the account creation process. An email is sent to individuals requesting the relevant information to create an account. Providing information for the IMS Contacts List is voluntary.
2. NAEP Network – The NAEP State/District coordinators receive a welcome email and provide their contact information (name, phone number, and email address) in their responses.
3. NAEPq – PII (first name, last name, and email address) from NCESLS for questionnaire respondents is collected via a web application within NCESLS. The NCESLS system shares the PII (first name, last name, and email address) and a system-generated password through a secure system-to-system application program interface (API) with NAEPq.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

1. NAEP Active Directory – There is an annual audit of users within the Active Directory. A designated staff member for each organization (e.g., Department employees and contractors, and special users) is sent a list of users to review and validate.
2. IMS Contact List – Each individual's current information is emailed to them every other month for their review and they are requested to update if necessary.
3. NAEP Network – This information is provided by and validated by the user, and they are prompted to update their information every six months.
4. NAEPq – This information is verified within the NCESLS system.

Use

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

1. NAEP Network/NAEP Active Directory/IMS Contact List – Contact information is used to facilitate collaboration on the NAEP program. This contact information is provided to enable access to this collaboration website. The information posted on the collaboration website is only accessible to users who are logged in to the system and is not accessible to the general public.
2. NAEPq
   a. PII is used to facilitate the collection of survey data.
   b. A unique URL is sent via email for login and to support password recovery for the NAEPq survey questionnaire tool through NCESLS.

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

[4] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

It is the Department's Policy that, 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

3.8.2. 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.

NAEP Active Directory, IMS Contact List, and NAEP Network – Notice of PII collection and use is shared with the welcome email sent to all new users.

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

Authority: The legal authority that permits the NAEP program is the National Assessment of Educational Progress Authorization Act (Pub. L. 107-279 Title III, section 303).

Purpose: We ask for your name, organization, title, work/business phone number, work/business email address, and work/business address to provide access to the NAEP system and network. To aid in collaboration, we publish your first name, last name, and email address within the IMS Contacts list that is only available to NAEP System users. This list is available at

https://www.naepims.org/sites/ims/Lists/Contacts/All%20contacts%20by%20Last%20Name.aspx. If you would not like your information listed please just inform us. You may also include additional attributes such as your work phone number etc. at your request. Optionally for users of the NAEP Network, the information you provide to the NAEP State Service Center (NSSC) is stored in the Contact List within that application.

Disclosure: Your name, organization, and contact information will be shared with other members of the NAEP network to allow for collaboration among members. Although the Department does not otherwise anticipate further disclosing the information provided, it may also be disclosed as indicated in the Routine Uses described in the System of Records Notice: "National Center for Education Statistics National Assessment of Educational Progress" (18-13-03).

Failure to provide the requested information may result in not gaining access to the NAEP system.

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?

1. NAEP Active Directory – Users must supply basic information (full name and email address) to receive access.
2. IMS Contact List/NAEP Network – The welcome letter offers individuals the opportunity to opt out/decline by contacting the NAEP Help Desk via email. In addition, every other month the individuals on the IMS Contact List receive a reminder of the information the system has on file for them, as well as means to update that information if necessary.

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

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

☑ N/A

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.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

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

☑ N/A

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

[5] 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.

5.10. 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?

1. NAEP Active Directory – Any NAEP system users can request their information via emailing the NAEP Helpdesk at any time.
2. IMS Contact Lists – The IMS/NAEP Network Contact Lists are available for NAEP system users to view/edit their information through the private website at any time.
3. NAEPq – NAEPq provides the ability for questionnaire respondents to access their information via logging into the application.

Alternatively, if an individual wishes to gain access to a record in this system of records, they can contact the system manager and provide their name. The request must meet the requirements of the regulations at 34 CFR 5b.5, including proof of identity.

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

1. NAEP Active Directory and IMS Contact List – Any NAEP system users can request updates to their information via emailing the helpdesk at any time.
2. NAEPq – Initial information is validated in the NCESLS system. If something changes, the participant may inform the assessment coordinator via email to update.

Alternatively, if an individual wishes to contest information contained in this system of records, they should contact the system manager. They should specify the particular record they are seeking to amend, whether a deletion, an addition, or a substitution is being sought and the reason(s) for the requested change(s). The request should meet the requirements of the regulations at 34 CFR 5b.7.

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

1. NAEP Active Directory – The welcome letter offers details on how to update information.
2. IMS Contact List – The welcome letter offers details on how to update information and periodic emails are sent for users to review/update their information as necessary.
3. NAEP Network – The welcome letter offers details on how to update information.
4. NAEPq – Notification procedures can be found in the National Center for Education Statistics Longitudinal Data Collection System (NCESLS) PIA.

Alternatively, procedures for accessing and amending record(s) are also outlined in the system of records entitled "National Center for Education Statistics National Assessment of Educational Progress," (18-13-03).

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?

The Department establishes policies that mandate all PII be properly stored and secured and conduct quarterly workshops with system owners to discuss policy changes.

PII in NAEP is secured by implementing National Institute of Standards and Technology (NIST) Special Publication 800-53 compliant security controls (compiled in a system

security plan (SSP)) including strong encryption, secure passwords, two-factor authentication (2FA), requiring data in transit TLS encryption, using secure encrypted wireless and virtual private networks (VPNs), and requiring that data at rest be encrypted. All decommissioned media is properly sanitized before disposal. NAEP is monitored continuously by security vulnerability scanners (Rapid7 Nexpose and Tenable Nessus) to detect intrusions and prevent data breaches. In addition, NAEP is continuously patched to ensure it has the latest security updates.

Physical safeguards: All PII collected by NAEP is stored in the AWS cloud. Only authorized employees have physical access to AWS cloud servers in AWS data centers.

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 Department and the Office of the Chief Information Officer (OCIO) publish policies that mandate all PII be properly stored and secured and conduct quarterly workshops with system owners to discuss policy changes.

PII in NAEP is secured by implementing NIST Special Publication 800-53 compliant security controls (compiled in an SSP) including strong encryption, secure passwords, 2FA, requiring data in transit TLS encryption, using secure encrypted wireless and VPNs, and requiring that data at rest be encrypted. All decommissioned media is properly sanitized before disposal. NAEP is monitored continuously by security vulnerability scanners (Rapid7 Nexpose and Tenable Nessus) to detect intrusions and prevent data breaches. In addition, NAEP is continuously patched to ensure it has the latest security updates.

In addition, all PII collected by NAEP is stored in the AWS cloud. Only Amazon-authorized employees have physical access to AWS cloud servers in AWS data centers.

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 Program to complete both PTA and PIA forms and ensure both are accurate and updated as required. The system owner also completes the Department Risk Management Framework process and participates in the Department's Ongoing Security Authorization (OSA) program to maintain an ATO. Under this process, an independent assessor assesses a variety of controls each quarter to ensure the system and the data residing within are appropriately secured and protected. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. These methods along with regular communication with NAEP users ensure that the information is used within the stated practices outlined in this PIA.

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 the NAEP website include the exposure of PII that in this case includes business contact information that could be used to perpetrate targeted phishing emails or embarrass the user. Other privacy risks can involve the user credentials, that if harvested by a threat actor, can be used to perform unauthorized access, commit fraud, or other computer crimes that are potentially hazardous to both individuals and organizations. Examples of 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 performed;
- Annual contingency plan test performed;
- Annual self-assessments conducted and/or annual security assessments performed by the Department Security Authorization Team;
- Annual updates to system security documents;

- Annual mandatory Cybersecurity and Privacy Training for employees and contractors
- Monthly Continuous Monitoring is in place with vulnerability scans hardware/software inventories, and configuration management database updates are posted to the Cyber Security and Management (CSAM) system;
- In addition, the NAEP system participates in the Department's OSA program which evaluates many of the above items at a higher frequency.