

**Privacy Impact Assessment (PIA)**

for the

**Presidential Cybersecurity Education Award**

**October 1, 2019**

**For PIA Certification Updates Only:** This PIA was reviewed on October 1, 2019 by Jean Morrow certifying the information contained here is valid and up to date.

**Contact Point**

**Contact Person/Title:** Jean Morrow, Policy Advisor and STEM Lead

**Contact Email:** Jean.morrow@ed.gov

**System Owner**

**Name/Title:** Jean Morrow, Policy Advisor and STEM Lead

**Principal Office:** Office of Planning, Evaluation, and Policy Development (OPEPD)

**Please submit completed Privacy Impact Assessments to the Privacy Office at** [**privacysafeguards@ed.gov**](mailto: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.

The system will be called Presidential Cybersecurity Education Award (the PCEA). The purpose of the PCEA is to collect information from nominations to determine one elementary and one secondary educator awardees on an annual basis. The PCEA is being created to carry out the Executive Order 13870 signed by President Trump on May 2, 2019.

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

The information collected and maintained will be used to: (1) determine the eligibility of applicants and review and evaluate the nominations of candidates, including, but not limited to, assessing candidate eligibility, in order to select one elementary and one secondary educator to whom the Department will present, on an annual basis, the Presidential Cybersecurity Education Award; (2) develop and implement the Presidential Cybersecurity Education Award program’s annual recognition component; and, (3) carry out the responsibilities set forth in Section 3(c) of the authorizing Executive Order 13870.

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

Agency

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



Click here to select.

# 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.

Executive Order 13870, Executive Order on America’s Cybersecurity Workforce

<https://www.govinfo.gov/content/pkg/FR-2019-05-09/pdf/2019-09750.pdf>

**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?   
       
     Yes  
     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.



To be provided at a future date. SORN currently pending review for publication in the Federal Register.

* + 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.



Click here to enter text.

**Records Management**

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

All records are retained and disposed of in accordance with Department Records Schedule 102: Recognition Programs Files (N1-441-09-6), Items (d) and (e). The Department will transfer official recognition program records, such as final publications awards, photographs, and videos, to the National Archives and Records Administration annually upon the close of the program awards cycle. Background recognition program records, namely, records received as part of the application or nomination process, may be destroyed four (4) years after cut off, which occurs annually upon the close of the program awards cycle.

* 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.

The collection includes but is not limited to nominated educator’s full name, level of education taught, name, city, state, or district of school or facility taught at, and work email and phone number, a narrative statement that details demonstrated superior educator accomplishment without respect to research, scholarship, or technology development, academic achievement by the educator’s students, and a letter of reference including the reference’s name and email address to validate accomplishments. In the event an individual is nominating an educator on their behalf, the nominator’s name and email will be collected.

More information on the specific qualifications for nominations can be found in the Executive Order (<https://www.govinfo.gov/content/pkg/FR-2019-05-09/pdf/2019-09750.pdf>)

* 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 information collected on the nominations is provided directly by the applicant him or herself or by the individual nominating them.

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

Nominations are collected electronically via email.

* 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 PII is validated throughout the nomination review process. Without correct contact information provided, the award cannot be given. The letter of reference will be used to validate and verify the accomplishments of the educator nominated.

**Use**

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

This PII is requested in order to carry out the authorizing Executive Order 13870.

Nominations are reviewed by Department staff to help determine the awardee of one elementary and one secondary award.

* 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 SSNs 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.

Notice will be made via the SORN still to be published in the Federal Register, the posting of this PIA, and through a Privacy Act Statement on the nomination instructions.

* 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 Statement: The Department’s authority to ask for this information is Executive Order 13870 issued on May 2, 2019. The information provided is voluntary. The main purpose for the information is to make awards. Should nominations not provide the information requested, nominations may be deemed ineligible. The routine use disclosures which may be made of the information will be published in a SORN in the Federal Register. The Department will be able to disclose information from this SORN for certain enumerated purposes to specific users without the nominees’ or awardees’ prior written consent pursuant to such routine use disclosures. The routine use disclosures are expected to include disclosures to references listed in applications and nominations in order to permit the Department to determine that applicants and nominees meet the criteria for the Presidential Cybersecurity Education Award, to the general public to announce the awardees, to the media to announce the awardees and to respond to inquiries about them, to government officials to notify them of the awardees in their States or districts, to assist with preparing congratulatory letters, certificates, or other honors, or to schedule events and office visits, to state and local education official to inform them of awardees in their states, districts, or schools, to White House or other Federal agencies for speechwriting and briefings of officials who will be addressing the awardees at events or to obtain needed security clearances at such events, to individuals and entities, such as vendors, in preparation for the awards ceremony or related educational and celebratory activities, to the Department’s contractors as needed to carry out any function of the Department, to members of Congress in response to an inquiry made at the nominee’s or awardee’s written request, to the Department of Justice to obtain advice, to the Department of Justice, parties, counsel, representatives, witnesses, courts, or other adjudicative authorities as relevant and necessary to administrative or judicial litigation, to appropriate parties and entities to respond to a breach of data, to researchers to carry out research on the purposes and functions of the system of records, to law enforcement officials if information in the system of records on its face or in connection with other information indicates that there has been a violation of statute, regulation, or order, and to the Department of Justice or the Office of Management and Budget if the Department concludes that disclosure is desirable or necessary in determining whether particular records are required to be disclosed under the Freedom of Information Act or the Privacy Act.

* 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 information provided by either self-nominations or nominators themselves is completely voluntary. Nominations should be submitted to [CyberAwards@ed.gov](mailto:CyberAwards@ed.gov). Once a nomination is submitted, a generated email response from the Department will be sent to confirm receipt to the person who submitted the nomination. Therefore, educators who are nominated by someone else will not be notified unless they are selected for the Presidential Cybersecurity Education Award. At that point they provide consent for continued and future use of their information.

* 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.  
       
     Yes
  2. What PII will be shared and with whom?  
     

Copies of each individual’s completed nomination package (containing PII) will be provided to internal U.S. Department of Education staff only in order to select the awardees. Reviewers will be Department employees with expertise in cybersecurity or cybersecurity-related education. Staff will maintain strict confidentiality when reviewing nominations and notify the Awards Coordinator should any conflicts of interest arise. The reviewers will then provide their recommendation for one elementary and one secondary educator award awardee to the Secretary of Education and the Office of the Secretary.

Information will also be shared with the Department’s Office of Communications and Outreach to disclose information about awardees to external entities.

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

The purpose for sharing with Department staff is to review nominations to help determine the awardees of one elementary and one secondary award and then disseminate the awardee’s names to interested entities described below.

**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.  
       
     Yes
  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**.   
     

The Department will obtain prior written consent from the awardees prior to disclosing their information to The White House or the National Science Foundation. However, the Department expects to publish routine uses to permit the Department to disclose information about the awardees without their consent in order to promote the selection and recognition of the recipients of the Presidential Cybersecurity Education Award, including to: the general public to announce the awardees; members of the media to publicize the awardees and respond to Press inquiries about them; national, state, or local government officials or their staff for the purposes of notifying them of awardees in their States or districts, and to assist with preparing congratulatory letters, certificates, and other honors or scheduling events or office visits, as applicable; State and Local Education Officials to notify them of awardees in their states, districts, or schools; White House and Federal agencies for any speechwriting or briefings for officials addressing the awardees or guests at recognition events, or to obtain needed security clearances at such events; individuals and entities, such as area vendors, in preparation for and in connection with the awards ceremony and related educational and celebratory activities; and to references in order to verify the accomplishments of the educator.

Also see the Privacy Act Statement in 4.2 for more details.

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

The Department may disclose records in order to promote the selection and recognition of the awardees of the Presidential Cybersecurity Education Award and the visibility of the awards.

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

Yes

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

Yes

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

Information will be shared with external entities via email and public press releases.

* 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?  
     

No

* 1. Does the project place limitation on re-disclosure?  
       
     No

# Redress

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

If self-nominators or nominators wish to gain access to their information, they may contact the Awards Coordinator at [CyberAwards@ed.gov](mailto:CyberAwards@ed.gov).

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

To correct inaccurate or erroneous information, an individual may contact the Awards Coordinator at [CyberAwards@ed.gov](mailto:CyberAwards@ed.gov). The individual must provide their name and any other identifying information requested by the Awards Coordinator as well as identify the information needing to be corrected.

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

Through the publication of the SORN and the PIA, individuals are informed that they should reach out to the Awards Coordinator at [CyberAwards@ed.gov](mailto:CyberAwards@ed.gov) in order to correct their information. These procedures can also be obtained by inquiring directly with the [CyberAwards@ed.gov](mailto:CyberAwards@ed.gov) email as well.

# 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?  
       
     No
  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?**  
     Click here to select.
  3. What administrative, technical, and physical safeguards are in place to protect the information?

All records are maintained in a password protected Excel document and in an email inbox which only the Award Coordinator and two additional employees have access to.

All physical access to the Department of Education site where records are maintained and the sites of the Department of Education’s staff and contractors with access to the system is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.

The computer systems employed by the Department and its contractors offer a high degree of security against tampering and circumvention. These security systems limit data access to Department and contract personnel on a “need to know” basis and control individual users’ ability to access and alter records within the system.

* 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?

No

* 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 Awards Coordinator in charge of the information will ensure to lock the computer when away from desk as well as continue to abide by Department security controls to properly safeguard the PII.

# 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 the Awards Coordinator and those the Coordinator has trained will have approved access to the information (i.e. the nomination Department reviewers). This PIA was conducted in the early stages of the formation of the award program and privacy was built into the process at every step of the way.

* 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 is minimal because the information provided is for the purpose of sharing with others to celebrate educators’ accomplishments. There is a risk that the completed nominations could be accessed by an unauthorized user, but that risk is mitigated by only giving three employees access to the nominations. Those same three employees will have access to the email address where nominations are sent to. Additionally, the excel sheet will be password protected and only accessible by the three employees.

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)