Privacy Impact Assessment (PIA)

for the

Forms Automation Platform

November 6, 2023

Point of Contact

Contact Person: Stephanie Valentine
Title: Information System Owner
Email: stephanie.valentine@ed.gov

System Owner

Name: Stephanie Valentine
Title: Information System Owner
Principal Office: Office of Planning, Evaluation and Policy Development (OPEPD)

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

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The Forms Automation Platform (FAP) will provide forms automation services for Office of Management and Budget (OMB)approved information collections and other public-facing forms. These forms will be compliant with the 21st Century Integrated Digital Experience Act (21st Century IDEA), OMB Memorandum M-22-10 (M-22-10), "Improving Access to Public Benefits Programs Through the Paperwork Reduction Act," Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. §794(d)) (Section 508), and other relevant laws and policies.

FAP will support the Strategic Collections and Clearance team within the Office of the Chief Data Officer (OCDO) Governance and Strategy Division (GSD) in the Office of Policy, Evaluation and Policy Development (OPEPD) at the U.S. Department of Education (Department) by providing a platform that enables:

- collection of data
- validation of submissions
- correction of form submissions and related documents as appropriate
- reporting based on collected data to monitor program performance
- collection of performance metrics
- dissemination of data for public-facing forms and information collections in compliance with the 21st Century IDEA and the M-22-10

FAP will include forms for the following Department programs:

a) Presidential Scholars Program (PSP) – a national recognition program established to recognize and honor some of the nation's most distinguished graduating high school seniors.

b) Recognizing Inspiring School Employees (RISE) – a national award program recognizing and promoting the commitment and excellence exhibited by full or part-time school employees who provide exemplary service to students in pre-kindergarten through high school.

c) School Ambassadors Fellows (SAF) – a national program to enable outstanding teachers, administrators, and other school leaders, such as school counselors, psychologists, social workers, and librarians to bring their school and classroom expertise to the Department and to expand their knowledge of the national dialogue about education.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

FAP provides a toolset that will allow the Department's program offices to design and deploy forms for use by the public. The system will be accessed through a web browser. All forms will require public users to use Login.gov to submit information. Federal employees and contractors using the system internally will authenticate their identity through the Education Identity, Credential and Access Management (ED ICAM) system. The system will store completed digital forms and other related documents.

Some forms will have workflow components that automate business processes supporting the review of forms submitted (e.g., multilevel review process, approval processes, communication with form submitters) that will aid in helping Department employees and contractors analyze data, be responsive to requests for services, and make business decisions based on the data received. The data collected from forms will be maintained for reporting, analysis, and performance monitoring. ED ICAM will be integrated with the FAP system for internal user authentication. The application will be hosted on an Appian GovCloud.

FAP is accessed by the public through applications designed on the Appian platform. The public will access automated forms developed in response to OMB approved information collections for RISE, PSP, and SAF. Individuals who access these collections through FAP include nominees and nominators for awards, members of review panels, and system administrators. RISE, PSP, and SAF each have their own databases, applications, and websites within the FAP boundary that provide users with the ability to submit nominations for each program as well as for reviewers to review and rank applications.

Eligible nominators or candidates, depending on the program, will receive an email alerting them to the opportunity to submit a nomination or application for each of

these recognition programs. Emails are sent to potential PSP candidates meeting program requirements using contact information obtained from the College Board and ACT, Inc. PSP candidates may also be nominated by Chief State School Officers and partner organizations. Partner organizations vary from year to year depending on which ones can participate, but they are: Junior Science and Humanities Symposia (JSHS), National Association for Urban Debate Leagues (NAUDL), Posse Foundation, QuestBridge, and Regeneron Science Talent Search (RSTS). Once a student is nominated by a Chief State School Officer or partner organization, they are sent the same email as those nominated based on information obtained from the College Board and ACT, Inc.

Emails are sent to State officials who nominate candidates for RISE. SAF applicants self-nominate and will register using a static link posted on a program website. Opportunities to apply will also be publicized on Department websites maintained for each program. Nominators, candidates, and other individuals supplying documentation in support of a candidate will receive an email with a token to nominate, apply, or submit information through FAP.

Nominators and candidates will be directed to the site for the relevant application to create a Login.gov account (if one does not already exist) prior to logging in to submit nominations, applications, or supporting information.

Once the forms are completed, data submitted through the application are stored in a logically separated area for each application within the FAP boundary where they are reviewed by panelists for each program. A printable version of the application and any files that are uploaded by the applicant can be viewed and printed for the applicant's recordkeeping purposes. Any documents submitted as part of the application process will be reviewed as well.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

The types of information collected by the system include data from OMB approved information collections and forms developed by program offices for completion by the public.

PSP: The purpose of the PII collected is to conduct a recognition program to recognize and honor some of the nation's most distinguished graduating high school seniors. PII about students, principals, teachers, and parents (if the students are under 18) is collected as part of the nomination process.

RISE: The purpose of the PII collected is to conduct a process to recognize and promote the commitment and excellence exhibited by full- or part-time school employees who provide exemplary service to students in pre-kindergarten through high school. PII about nominees and principals or superintendents of nominees' schools or districts is collected as part of the nomination process.

SAF: The purpose of the PII collected is to conduct a process to enable outstanding teachers, administrators, and other school leaders, such as school counselors, psychologists, social workers, and librarians to bring their school and classroom expertise to the Department and to expand their knowledge of the national dialogue about education. PII about applicants is collected as part of the nomination process.

1.5. Is the IT system operated by the agency or by a contractor?

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

The contractor manages the instance of the platform, designs and deploys forms, and provides support to users in the use of forms.

[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

☐ N/A

1.7. If the IT system is operated by a contractor, does the contract and other acquisition-related documents include privacy requirements?

Yes

☐ N/A

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, contact your program attorney.

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

PSP: The program was established by Executive Order 11155 (1964), amended by Executive Order 12158 (1979) and Executive Order 13697 (2015).

RISE: The program was established by was established by the Recognizing Achievement in Classified School Employees Act (20 U.S.C. § 6301).

SAF: The Intergovernmental Personnel Act (IPA) mobility program regulations (5 CFR part 334), revised effective May 29, 1997, allow Federal agencies to facilitate cooperation between the Federal government and the non-Federal entity through the temporary assignment of skilled personnel to the SAF program to incorporate practicing education professionals' unique approaches to solving educational problems and developing and identifying support for effectively implementing Federal policies and programs.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

A SORN is under development for the Department's recognition programs that will include PSP, RISE, and SAF.

A SORN is currently in place for PSP: Presidential Scholar Program Files and Application (18-06-03), 70 FR 61436. When the new FAP SORN is approved, the PSP SORN will be rescinded.

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

For PSP and RISE, GRS 102: Recognition Programs Files is the currently approved records retention schedule.

SAF does not have a records retention schedule, but there is a plan to establish a schedule (see below). In the future, PSP, RISE, and SAF will all be covered under a new records retention schedule, DAA-0441-2022-0001-0006. The new proposed schedule has been submitted to NARA and is pending approval. Until the new schedule is approved, PSP and RISE records will follow the retention schedule listed above and SAF records will be held permanently.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☐ Date of Birth	☒ Gender or Sex
☒ City, State, or County of Birth	☒ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☒ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☒ Educational Background/Records	☒ Group/ Organization Membership	☒ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☒ Race/Ethnicity	☐ Religion

Identification Numbers

☐ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☒ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☐ Other (Specify below)

If you have been directed to "specify below," describe the PII:

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Email address, username, and password

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Email address, username, and password

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

Respondents may include students, families, K-12 school teachers, administrators, school principals, employees, graduating high school seniors, Chief State School officers, and program reviewers.

The types of information collected include PII about the nominators and nominees:

- For SAF applicants: name, school name, school address, school phone number, school type, current job role, a description of job role if "other" was selected in the application, email address, telephone number, username, and password.
- SAF applicants are asked to provide information that showcases their achievements and experiences and demonstrates their record as outstanding educators across the following categories: (A) Educational publications; (B) Presenting and leading professional learning; (C) Honors and Recognition; (D) Continuing learning and advanced educator credentials; (E) Involvement in educational policy discussions and decision-making. SAF applicants are required to secure three professional recommendations from individuals, one of which must be a current supervisor, who can

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

provide insight into their experiences and quality as educators.

- For PSP students: name, permanent address, gender, phone number, age (to determine whether the applicant is over 18), email address, high school name, high school address, high school phone number, standardized test scores, first-choice college, information about extracurricular activities, work experience, community activities, special talents and awards, school transcripts, and responses to short answer questions and one essay topic. Username, password, and a consent election to be directly contacted by the press are also collected.
- For PSP students' parents: email address and digital signature. Parents must sign students' applications if students are under 18.
- For PSP teachers: name, title, email address, school subject area, school name, school address, username, and password.
- For PSP principals: name, email address, username, and password.
- For RISE, from nominators including State governors' office representatives: name, position, email address, and phone number. Username and password are also collected.
- For RISE, regarding nominees and principals or superintendents of nominees' schools or districts: name, position, email address, and phone number.
- State officials are asked to describe how RISE nominees demonstrate excellence through the following categories: (A) Work performance; (B) School and community involvement; (C) Leadership and commitment; (D) Local support (from co-workers, school administrators, community members, etc., who speak to the nominee's exemplary work); (E) Enhancement of classified school employees' image in the community and schools; and (F) Any other areas the State deems exceptional and pertinent to the RISE Award.
- For PSP, RISE, and SAF, the Department's may collect other information includes education history for nominees, descriptive data about the worthiness of nominees for recognition, nominee rankings, and nominee resumes.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

Information is collected from Department employees and contractors who review applications and administer the system.

PSP: Information is collected from individual students, parents of students under the age of 18, school staff, Federal employees and contractors, Chief State School officers, other recognition program partner organizations and testing agencies. Each partner organization nominates students in the same way, contributing the same information as described below.

The information needed in order to invite PSP candidates to apply includes student name, student home mailing address, student gender, student email address, high school name, high school mailing address, high school College Board code (CEEB code), and art discipline and GPA (for arts candidates). The nomination information is collected from the Chief State School Officers and the partner organizations through FAP. The nominator creates a profile in the portal and adds the nomination information.

RISE: Information is collected from nominating officials from State education agencies and gubernatorial staff about nominees.

SAF: Information is collected from individual applicants (teachers, administrators, and other school staff, such as school counselors, psychologists, social workers, and librarians).

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

PSP: PII is collected electronically through the FAP web-based application. PSP obtains email addresses of potential candidates through an annual data draw from ACT, Inc and The College Board. Only students who have agreed to release their information to interested third parties during the ACT/SAT registration process are included. Nominations are also obtained through Chief State School Officers and the partner organizations listed above. Students who did not release their information during the ACT/SAT registration process are able to contact the FAP help desk via email to find out if they have the eligible scores for the current program year.

RISE: PII is collected electronically from states through the FAP web-based application. The Department obtains the email addresses for State educational agency and gubernatorial staff by searching online or contacting the gubernatorial offices.

SAF: PII is collected electronically from fellows who self-nominate through the FAP web-based application.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the

PII elements that are indicated in Question 3.1, please describe why the information is necessary.

PSP: Data submitted is used to carry out the Executive Orders by implementing PSP on a yearly cycle and by selecting PSP semifinalists and finalists by reviewing candidates' submitted applications. Data such as name/email address/phone number are required to contact applicants. GPA/short answer questions and narrative statements are required to effectively evaluate applicant suitability. Gender is collected as Executive Order 11155 requires that "one boy and one girl shall be chosen as Presidential Scholars."

RISE: Data submitted allows state officials to submit individual nominations of classified school employees electronically and reviewers internal to the Department and from external organizations such as the National Education Association (NEA), National Association of Secondary School Principals (NASSP), and National Association of Elementary School Principals (NAESP) to review these nominations online. Data such as name/email address/phone number are required to contact nominators; educational background information of nominees such as narrative responses are required to effectively evaluate applicant suitability for the program.

SAF: Data submitted allows individual educators (teachers, administrators, and other school staff, such as school counselors, psychologists, social workers, and librarians) to self-nominate by submitting an application form electronically. Data such as name/email address/phone number are required to contact applicants; educational background information of applicants such as narrative responses and recommendations are required to effectively evaluate applicant suitability for the fellowship.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

PSP: Data submitted for PSP by the Chief State School Officers, partner organizations, and testing agencies are reviewed and either confirmed or corrected by the individual students completing their applications. Candidates are responsible for verifying the

accuracy of their own information. Data submitted by school nominators are reviewed and confirmed by the school principal through the submission of a verification form.

RISE: Nominators are responsible for verifying the accuracy of the data entered on the application.

SAF: Each SAF applicant is responsible for verifying the accuracy of the data they enter on the electronic application.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

No

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

No

3.9.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

☑ N/A

3.10.2. If the above answer to question 3.10 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☑ N/A

If the above answer to question 3.10 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☑ N/A

If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☑ N/A

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

FAP provides notices to individuals through a Privacy Act Statement posted on the website for candidates who apply online. Candidates are invited to apply to PSP, RISE, and SAF but they are not required to apply. If a candidate chooses to apply to the program, the notice clarifies that the collection of PII is necessary to be considered for the award. Users are notified that registration and submission of PII is necessary because applications cannot be submitted anonymously. For PSP, each candidate selects for himself/herself whether they are willing or unwilling to be contacted by the press if the press makes an inquiry to them.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

No

N/A: FAP does not maintain a website not hosted on the ed.gov domain.

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do

not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

The Privacy Act Statement for each program can be found at the following URLs:

https://forms.ed.gov/suite/sites/presidential-scholars-program
https://forms.ed.gov/suite/sites/school-ambassador-fellowship
https://forms.ed.gov/suite/sites/recognizing-inspiring-school-employees

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Participation in PSP, RISE, and SAF is voluntary; however, if candidates choose to submit applications, PII is necessary for registration and applications. If an individual no longer wants to be considered for a program, they could contact the help desk and their information can be deleted. .

4.5. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practices, policies, or activities that affect the PII and the privacy risks to ensure that individuals are aware of and, where feasible, can consent to, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☐ N/A

PSP: All of the information submitted, including contact information and educational background information, is shared with the Review Committee, which are Federal contractors. Winners' city, state, school, and contact information will be shared with the

Department's Office of the Secretary, the Office of Communications and Outreach, the Office of Legislation and Congressional Affairs, and Federal contractors.

RISE: Only the individual's name is shared with the Office of the Secretary.

SAF: All of the information submitted, including contact information and educational background information, is shared with internal and external reviewers. The name of the selected individuals, their email address, and their state is shared with the Office of Elementary and Secondary Education's Executive Office.

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☐ N/A

PSP: The Review Committee receives the information for the review of applications. The Secretary sends each Scholar a personalized letter. The Department's Office of Communications and Outreach coordinates media requests for the Scholars and the legislative offices manage Congressional inquiries for recognizing Scholars. Information is shared with federal contractors for the production of program recognition materials and the U.S. Presidential Scholars Yearbook.

RISE: The information is shared with the Department's Office of the Secretary to make the final selection of the honoree.

SAF: Information is shared with reviewers to verify eligible candidates, provide technical assistance, and conduct the annual selection of Scholars. Information is shared with the Office of Elementary and Secondary Education's Executive Office to initiate processes related to establishing the Intergovernmental Personnel Agreement (IPA) for the successful applicants. The SAF program also makes an internal announcement to Department officials, including the names, roles, and information about the schools of the successful applicants once their IPA is approved.

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

PSP: Winners' city, state, school, and contact information will be shared with the entities below. The Presidential Scholars Foundation (PSP's alumni association) receives email addresses if the Scholar provides permission. Congressional legislative offices receive mailing addresses upon request and occasionally phone numbers if a senator or representative wants to call and congratulate the student. Before any disclosure of contact information, the Scholar will provide consent for this in the application.
Routine programmatic disclosures include the following:

- The Commission on Presidential Scholars
- The general public through announcements of the PSP candidates, semifinalists, and finalists
- The general public through the annual U.S. Presidential Scholars Yearbook
- National, state, and local media to publicize the Scholars and respond to press inquiries about them
- Federal, state, and local officials in Scholars' states or districts
- White House and federal agencies for briefings or speeches

RISE: Application information is shared with both internal and external reviewers. Once applications are selected, the name, school name, and state will be shared with state education agencies and governor's offices. The state may share the winner and finalists with local media. The Department publishes the names, roles, and information about the schools of the successful applicants on the ed.gov website once their IPA is approved.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

PSP: The purpose for sharing information is to perform the following functions:

- Announce the program's candidates, semifinalists, and finalists to the general public
- Produce program recognition materials, including medallions and the annual U.S. Presidential Scholars Yearbook
- Host in-state recognition ceremonies for semifinalists and finalists
- Arrange national recognition events, including Scholar accommodations, transportation, and other services
- Inform national, state, and local media so that they may publicize Scholars and the program

- Provide information to the White House and federal agencies for briefings, speeches, or to obtain security clearances for recognition events
- Notify federal, state, and local officials of candidates, semifinalists and Scholars in their states or districts and assist with the recognition of these individuals
- Notify state and local education officials to notify them of candidates, semifinalists, and Scholars in their states, districts or schools

RISE: The purpose of sharing information with reviewers is for scoring applications. The purpose of sharing with states and the media is to recognize the award for inspiring school employees that have provided exemplary service to the schools and communities they serve.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

PSP: The program was established by Executive Order 11155 (1964), amended by Executive Order 12158 (1979) and Executive Order 13697 (2015).

RISE: The program was established by was established by the Recognizing Achievement in Classified School Employees Act (20 U.S.C. § 6301).

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

If PII is sent to external entities (e.g., Congressional offices), it is sent either via email in zip file with encryption that is password protected or placed in a private folder on the Department's external SharePoint site, which is restricted to specific users.

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☐ N/A

No

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Users can access their own information within the system. Procedures are provided through user guides on the FAP website as well as through email communications.

If an individual wishes to gain access to a record in this system, that individual may contact the system manager at the address listed in the Recognition Programs SORN. The request must provide necessary particulars including name, address, telephone number, and any other identifying information requested by the Department to distinguish between individuals with the same name. The request must meet the requirements of regulations at 34 C.F.R. 5b. 5.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

Users may correct or amend inaccurate information within the system until an application is finalized. Once an application is submitted, users may the FAP help desk to correct or amend inaccurate information.

If an individual wishes to contest the content of a record regarding that individual, the individual must contact the system manager at the address listed in the Recognition Programs SORN. Requests must contain the individual's name, address, and telephone number. The request must meet the requirements of the regulations at 34 C.F.R. 5b. 7.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Instructions are provided via a system-generated email at the start of the application process.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

No – System currently under development

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

The system employs a full suite of administrative, technical, and physical safeguards to protect information based on Federal requirements pursuant to National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 (SP 800-53) and best practices. The system has been evaluated against the SP 800-53 moderate profile with FedRAMP cloud enhancements. Safeguards include password-based and

two-factor authentication, role-based access control, data encryption, and physical data center security for candidates, contractors, and Federal employees.

Security protocols for this system meet all required security standards. Physical access to the Department site where this system is maintained is controlled and monitored by security personnel who check each individual entering the building for their employee or visitor badge.

The system limits access to users on a "need to know" basis and controls users' ability to access and alter records within the system. Access to various parts of the system is restricted based on user role and level of authorization.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every Department system must receive a signed Authorization to Operate (ATO) from a designated Department official. The ATO process includes a rigorous assessment of security and privacy controls, plans of actions and milestones (POA&Ms) to remediate any identified deficiencies, and a continuous monitoring program.

8. Auditing and Accountability

8.1. How does the ISO assess and ensure that the PII is used in accordance with stated practices in this PIA?

FAP, RISE, and PSP administrators ensure that PII is used in accordance with the stated practices in this PIA through several methods. The first method is by completing the Department Risk Management Framework process to receive an Authorization to Operate (ATO). When going through the ATO process, the system owner establishes monitoring processes to ensure that information is used in accordance with approved practices. The second method is by ensuring that Department staff and contractors, systems, and processes comply with NIST 800-53 controls for a Moderate application which include administrative, technical, and physical controls.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

Security and privacy controls are monitored through incident reports, vulnerability reports, and annual reviews of controls and documentation.

Once the system has obtained an ATO, FAP will enter Ongoing Security Authorization (OSA) program, which requires monitoring of controls through assessments on a quarterly basis over a three-year cycle. As FAP is a moderate system, it will be

evaluated against NIST 800-53 Rev. 5 baseline and privacy controls. Controls are assessed quarterly. Any corrections needed to controls will be addressed through POA&Ms.

8.3. What are the specific privacy risks associated with this program or IT system and how are those risks mitigated?

The main privacy risks associated with FAP 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 identity theft, or embarrassment. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

PSP: The primary risk is associated is the unintentional disclosure of applicant narratives, short answer responses, grade point average and standardized test score data. The associated impact of disclosures of applicant narratives short answer responses, and other applicant information is high as many students write about personal experiences.

A secondary risk is the unintentional disclosure of applicant name and contact information. The associated impact is low, because applicants are unlikely to be embarrassed by disclosure of being nominated for a prestigious program. If unintentionally disclosed the program, the PSP program office will contact the individual and the Department Privacy Program to mitigate the risk associated with the disclosure.

RISE: The primary privacy risk is the unintentional disclosure of applicant contact information. The applicant's name and information about their nomination is already public on the state websites. The associated likelihood of contact information being disclosed is low, because of the limited number of individuals with exposure to applications. If unintentionally disclosed, the RISE program office will contact the individual and the Department Privacy Program to mitigate the risk associated with the disclosure.

SAF: The primary privacy risk is the unintentional disclosure of applicant name and contact information. If unintentionally disclosed, the SAF program office will contact the individual and the Department Privacy Program to mitigate the risk associated with the disclosure.

Department staff and contractors, systems, and processes comply with NIST 800-53 controls for a Moderate application which include administrative, technical, and physical

controls. These controls are in place to ensure integrity, availability, accuracy, and relevancy of the data and to mitigate privacy risks.