

**Privacy Impact Assessment (PIA)**

for the

**National Center for Education Statistics (NCES) Applications at RTI**

**May. 16, 19**

**For PIA Certification Updates Only:** This PIA was reviewed on May 16, 2019 by Tracy Hunt-White certifying the information contained here is valid and up to date.

**Contact Point**

**Contact Person/Title: Gail Mulligan, Longitudinal Surveys Branch Chief**

**Contact Email: Gail.Mulligan@ed.gov**

**System Owner**

**Name/Title:** **Tracy Hunt-White**

**Principal Office: Institute of Education Sciences (IES)**

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

*Please complete this* ***Privacy Impact Assessment (PIA)*** *on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*

***If a question does not apply to your system, please answer with N/A.***

# Introduction

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

The NCES Applications at RTI is an existing, operational Major Application that includes IES projects, performed by RTI International (RTI), that require Federal Information Processing Standards (FIPS) moderate security (e.g., National Postsecondary Student Aid Study (NPSAS), High School Longitudinal Study (HSLS), Baccalaureate and Beyond Longitudinal Study (B&B), Beginning Postsecondary Students Longitudinal Study (BPS), National Longitudinal Transition Study (NLTS), High School and Beyond (HSB), and Middle Grades Longitudinal Study (MGLS)). The NCES Applications at RTI, which provide a secure workspace appropriate for NIST Moderate-impact level data, are used for managing PII received from NCES and other external sources during the execution of RTI’s contracts. Data collected by NCES are processed and analyzed in this workspace. RTI delivers to NCES data that contain no direct identifiers and are perturbed for disclosure avoidance to ensure that no individual respondent can be identified in a data file with certainty. The NCES Applications at RTI are part of RTI's FIPS Moderate Network General Support System (GSS; formerly the Enhanced Security Network (ESN)) and can only be accessed via Citrix, running entirely within the Moderate Network.

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

Direct identifiers are needed to sample institutions and students, to collect information from institutions and students, and to conduct records matching that allows for the collection of information about study members from administrative records. The use of direct identifiers is minimized to the fullest extent possible and are keep secure within the ESN. No direct identifiers are included in any data files made available for research. In addition, the data are perturbed to ensure that no individual respondent can be identified in a data file with certainty, sensitive variables are included only in restricted data files that researchers must apply for and for which there are penalties for misuse, and data released to the general public are coarsened.

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

Contractor

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

Yes

# 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.

Title 20 – EDUCATION, CHAPTER 76 - Education Research, Statistics, Evaluation, Information, and Dissemination, Subchapter I – Education Sciences Reform Act of 2002. The National Postsecondary Student Aid Study (NPSAS) is also covered by the Higher Education Opportunity Act of 2008 [HEOA 2008, 20 U.S.C. §1015(a)(k)].

**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.



The NCES SORN, entitled the “National Center for Education Statistics (NCES) Longitudinal and Cross-sectional Studies’’ (18-13-01), was published in the Federal Register on November 14, 2018 https://www.govinfo.gov/content/pkg/FR-2018-11-14/pdf/2018-24847.pdf.

* + 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**

* 1. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

The Department shall submit a retention and disposition schedule that covers the records contained in this system to the National Archives and Records Administration (NARA) for review. The records will not be destroyed until such time as NARA approves said schedule.

* 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.

PII that is maintained and used in the NCES Applications at RTI includes items such as: name, physical addresses, phone number(s), SSNs, dates of birth, email addresses, financial information, schools attended, educational information, employment information, parent(s) name(s), and parent(s) addresses. NCES maintains the website (surveys.nces.ed.gov) that is used to collect the information from institutions and individuals; however, the NCES Applications at RTI are not used to directly collect respondent data. SSNs are used for administrative record linkages but are never disclosed.

* 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.)?

Data are collected from educational institutions and individuals.

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

NCES maintains the website (surveys.nces.ed.gov) that is used to collect the information from institutions and individuals.

* 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?

NCES maintains the web site (surveys.nces.ed.gov) that is used to collect the information from institutions and individuals. The NCES Applications at RTI are not used to directly collect respondent data. For individuals, there are edit checks built into the survey instrument. For institutions, there are edit checks built in their data collection instrument. Once data are collected and reviewed, the data provider may be contact to address questions about the data. In addition, the data undergo extensive quality checks before being released or official statistics are produced.

**Use**

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

Data are delivered to NCES in accordance with contract requirements. RTI maintains project data for use in the conduct of these studies longitudinally (e.g., to be able to follow study respondents as they complete high school and transition to the work force or postsecondary education or to follow study respondents as they transition from the completion of a baccalaureate program into the work force or additional higher education). De-identified data, which contain no direct identifiers and are perturbed for disclosure avoidance to ensure that no individual respondent can be identified in a data file with certainty, are delivered to NCES to build NCES data tools and generate tables and reports on various topics. The data tools and reports are publicly available to data users. In addition, a restricted-use micro-level data file (which contains no direct identifiers and is perturbed for disclosure avoidance to ensure that no individual respondent can be identified in a data file with certainty) is made available to researchers who obtain a restricted-use license. At no time are direct identifiers available to data users. For an example of the data products available, go to nces.ed.gov/surveys/npsas.

* 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.

Yes

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

Social Security Numbers are collected with OMB concurrence for the express purpose of record linkage with Department records systems and in some cases for sample surveys, state or local student records. In the case of longitudinal studies, the SSN may also be used for tracking study respondents as they change schools and/or geographic locations over the course of the study (e.g., to be able to follow study respondents as they complete high school and transition to the work force or postsecondary education or to follow study respondents as they transition from the completion of a baccalaureate program into the work force or additional higher education). NCES keeps abreast of studies that focus on the use of names for such linkages and follow-up studies, but the return rate on matches based only on name is substantially lower than that obtained using SSN. SSNs are never disclosed.

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

NCES keeps abreast of studies that focus on the use of names for administrative record linkages and follow-up studies, but the return rate on matches based only on name is substantially lower than that obtained through the use of SSN.

# 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.

Notices of NCES’s intent to conduct data collection, along with all questions that will be asked of respondents, are published in the Federal Register with a public comment period.

When respondent data are collected by applications at NCES (surveys.nces.ed.gov), respondents are assured of the confidential nature of the data collection and are asked to provide informed consent prior to the start of data collection. The informed consent statement is built into the data collection instrument. It is one of the initial screens that respondents encounter before answering questions. Respondents must give their consent before being asked the first question. On the data collection website, the Paperwork Reduction Act statement and OMB clearance number are provided, as well as information on NCES's legal authorization to collect these data.

* 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.
	

Below is an example of the text included on the data collection websitefor one of the NCES studies (e.g., https://surveys.nces.ed.gov/bb/confidentiality.aspx):

NCES is authorized to conduct B&B:08/18 by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543) and to collect students’ education records from education agencies or institutions for the purposes of evaluating federally supported education programs under the Family Educational Rights and Privacy Act (FERPA, 34 CFR §§ 99.31(a)(3)(iii) and 99.35). The data are being collected for NCES by RTI International, a U.S.-based nonprofit research organization. All of the information you provide may be used only for statistical purposes and may not be disclosed, or used, in identifiable form for any other purpose except as required by law (20 U.S.C. §9573 and 6 U.S.C. §151). According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this voluntary information collection is 1850-0729. The time required to complete this information collection is estimated to average approximately 35 minutes per response, including the time to review instructions, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate, suggestions for improving this survey, or any comments or concerns regarding the status of your individual submission of this survey, please write directly to: The 2008/18 Baccalaureate and Beyond Longitudinal Study (B&B:08/18), National Center for Education Statistics, Potomac Center Plaza, 550 12th St., SW, 4th floor, Washington, DC 20202. OMB Clearance No: 1850-0729. Expiration Date: 04/30/2021.

* 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?

Individuals may decline to participate in the study, and they may opt out of a study at any time after providing initial consent by contacting NCES and/or the data collection contractor.

* 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?
	

 RTI performs records matching with the Department's Federal Student Aid office - the National Student Loan Data System (NSLDS) and the Central Processing System (CPS) to add value to the data collection and to minimize respondent burden. Records matching are conducted using SSNs, last name, and date of birth. These data are transmitted from the ESN to FSA using a Secure Sockets Layer (SSL) encrypted website provided by FSA.

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

Data are delivered to NCES in accordance with contract requirements. Records matching is performed with the Department’s Federal Student Aid system to obtain CPS data on demographic characteristics about respondents, including their dependency status and expected family contribution; and to obtain NSLDS data on amount and types of federal aid received.

**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**.
	

External data sources (e.g., LexisNexis, NCOA) are sometimes utilized for the purpose of locating sample members. Record matching for the purposes of adding value to the data collection and minimizing respondent burden is also done with other sources of data such as the National Student Clearinghouse, providers of admissions test data, and institutional student records. Specifically, these sources are used to provide information on students' enrollment history and degree completion, college admission test scores such at the ACT and SAT, and information on the attendance status, credit hours, majors, and state and institution financial aid. In addition, matching is conducted with the Veterans Benefits Administration in order to accurately identify veterans and obtain information on their educational benefits. RTI International provides these data sources with some information about sample members for the purpose of receiving more information on those sample members. This information may include SSN, which is solely used for record linkage and is never disclosed. These external data sources are not allowed to retain any data sent by RTI on the sample members. In addition, these external data sources cannot identify the specific study for which the matching was conducted. There are approved sharing agreements in place to conduct matching with external data sources. In addition, all individuals involved in the matching process must sign an Affidavit of Nondisclosure or adhere to another type of legally enforceable confidentiality agreement.

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

Records matching with these sources is conducted to obtain information on students' enrollment history and degree completion, college admissions test scores, and information on the attendance status, credit hours, majors, state and institutional financial aid, and veterans' educational benefits.

* 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.)?
	

IES has a secure data transfer system, which uses SSL technology, allowing the transfer of encrypted data over the Internet. The IES File Transfer System is used for all administrative data sources that do not have their own secure file transfers systems. All data transfers will be encrypted.

* 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?
	

Yes

* 1. Does the project place limitation on re-disclosure?
	
	Yes

# Redress

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

Individuals may access their record by following the instructions in the SORN. Specifically, they must contact the SORN system manager and provide the required information, including proof of identity.

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

Individuals may correct their record by following the instructions in the SORN. Specifically, they must contact the SORN system manager and provide the required information, including proof of identity.

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

The NCES SORN, entitled the “National Center for Education Statistics (NCES) Longitudinal and Cross-sectional Studies’’ (18-13-01), was published in the Federal Register on November 14, 2018 https://www.govinfo.gov/content/pkg/FR-2018-11-14/pdf/2018-24847.pdf.

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

* 1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

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

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

All end user connections are considered remote and occur through a Juniper SSL/VPN appliance so that all network traffic is encrypted using FIPS 140-2 compliant SSL certificates. SSL also provides data integrity checks. All traffic to and from the Moderate network that the NCES Apps at RTI resides on is encrypted via the SSL/VPN. An AES256 encrypted tunnel is utilized when a VPN tunnel is initiated. RTI’s primary data center is on the RTP main campus while the secondary data center is at TierPoint located in Raleigh, NC. Entrance into the Ragland computer rooms is controlled by automatically locking doors that are continuously monitored by RTI Corporate Security. Corporate Security Officers regularly patrol the data centers. Entrance to the facilities is controlled by two-factor authentication (badge access and 4-digit PIN that only the user knows). TierPoint security staff monitors real-time physical alarms and surveillance equipment. All visitors are vetted against a predefined authorized contact list and must provide government issued ID during visitor sign in process. Security guard monitor facilities 24/7/365 and review visitor log at time of access The Ragland data center is protected by uninterruptible power supplies capable of sustaining data center operations until emergency backup generators come online. Generators are maintained and periodically load-tested by RTI’s facilities staff and are stocked with multiple days’ worth of fuel at all times. All TierPoint data center equipment is supported by UPS systems with a minimum of fifteen (15) minutes of backup capacity. Generators are set to be online and providing backup power within thirty (30) seconds of a power interruption.

* 1. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

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

Yes

* 1. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

As part of the Authority to Operate (ATO) the NCES Apps at RTI, the SSP lists monitoring, testing and evaluation controls for the system. Such activities include the following. Monitoring servers for various service failures, events that exceed resource limitations, and other adverse events. Logs are sent to the SIEM device (as defined in AU-6), they are configured to store audit logs locally if the SIEM device is unavailable. RTI’s Information Technology Services (ITS) Governance, Security and Compliance (GSC) department performs continuous monitoring on ITS security controls using a variety of methods. The methods include items such Self assessments to ensure compliance with FISMA are performed as described in control CA-2. Information is correlated from a variety of sources including, but not limited to, the following: SharePoint, ServiceNow, and Nessus. These sources are managed and evaluated by RTI’s ITS GSC staff. ITS utilizes firewalls with IPS/IDS functionality at key network boundaries within the network to monitor (and in some cases block) malicious or unwanted traffic. The Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) signature database is updated weekly to ensure the latest signatures are available and applied when required. RTI maintains Business Continuity Plans and Emergency Response documents with testing of the Information Technology Contingency Plan and Disaster Recovery Plan (C/DRP) occurring annually.

# 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?

The system owner ensures that the information is maintained and used in accordance with stated practices in this PIA. An annual security assessment is conducted. In addition, every three years all the security controls are assessed for the system to maintain its Authority to Operate. The Department’s, contractor’s, and subcontractors’ employees who “maintain” (collect, maintain, use, or disseminate) data in this system must comply with the requirements of the Privacy Act and the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573), which provides criminal penalties for violations. Access to individually identifying data is strictly controlled. Staff with access to the system are required to complete annual security awareness training. In addition, they are required to have background clearance at the 5c level or higher. The system owner ensures that data calls are addressed and that updated security requirements are met and supported with documentation.

* 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?

There are privacy risks associated with any system that uses or maintains PII. Mitigation of those risks at a system level includes following NIST Guidelines for Moderate-impact systems and maintaining our Authority to Operate (ATO). At the project level the use of direct identifiers is minimized to the fullest extent possible. All direct identifiers are removed from each data file, data are coarsened, sensitive variables are removed from public releases, and the data are perturbed to ensure that no individually respondent can be identified in a data file with certainty.

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)