Privacy Impact Assessment (PIA)

for the

National Center for Education Statistics Longitudinal Data Collection System (NCESLS)

Enter final date

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

Contact Point

Contact Person/Title: Gail Mulligan
Contact Email: Gail.Mulligan@ed.gov

System Owner

Name/Title: Gail Mulligan, Longitudinal Surveys Branch Chief
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.

1. Introduction

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

The National Center for Education Statistics (NCES) Longitudinal Studies Data Collection System, referred to as NCESLS, stores, processes, and transmits all information related to several NCES data collections for which Westat is the contractor, including respondent and/or survey data, staff and agency contact information, study data and reports, and other electronic and hardcopy information. The system consists of several applications, public-facing websites, web servers, database servers, and other storage and network components. The data collections for which NCESLS is used include the National Assessment of Educational Progress (NAEP), the Program for International Student Assessment (PISA), the Teaching and Learning International Survey (TALIS), the Trends in International Mathematics and Science Study (TIMMS), the International Computer and Information Literacy Study (ICILS), the International Early Learning Study (IELS), and the Early Childhood Longitudinal Study, Kindergarten Class (ECLS-K).

NAEP is mandated by Congress to assess the educational achievement of U.S. students and monitor changes in those achievements. In this study, students are assessed on what they know and can do in various subject areas. These assessments are conducted periodically in Mathematics, Reading, Science, Writing, Arts, Civics, Economics, Geography, U.S. History, and Technology and Engineering Literacy.

PISA is an international assessment of 15-year-old students that measures how well students apply their knowledge and skills in reading, mathematics, and science to problems set in real-life contexts. Conducted every 3 years since 2000, PISA 2022 will include students from more than 80 countries and education systems around the world, including the United States. PISA is coordinated by the Organization for Economic Cooperation and Development (OECD) and managed in the United States by NCES.

TALIS is a study about teachers, teaching, and learning environments. First conducted in 2008 and conducted every 5 years, its main objective is to provide international indicators that will help countries develop well-informed education policy. TALIS offers teachers and principals the opportunity to provide their perspectives on education in the United States.

TIMSS is an international assessment and research project designed to measure trends in mathematics and science achievement at the fourth- and eighth-grade levels, as well as school and teacher practices related to instruction. Since 1995, TIMSS has been administered every 4 years. TIMSS 2019, the seventh study in the series, will involve students from more than 60 countries, including the United States.

ICILS is an international assessment and research project designed to measure trends in computer and information literacy at the eighth-grade level, as well as school and teacher practices related to instruction. ICILS provides a unique opportunity to compare U.S. student skills and experience using technology with that of their peers in other nations, and to provide data on factors that may influence student computer and information literacy skills. ICILS was first administered internationally in 2013, and ICILS 2018, the second study in the series, involved students from about 20 countries.

IELS is an assessment of five-year-olds on assorted literacy and problem solving skills. Supplemental on-line questionnaires are completed by school teachers and parents to gather contextual data about child participants. This innovative study fills important gaps in the international comparisons of education systems and helps countries to better understand how their early education and care systems prepare children for primary school.

The ECLS-K will follow students from the kindergarten class of 2023-24 through their elementary school years. The students will be assessed at several time points to measure their knowledge and skills in reading and mathematics at a given point in time as well to measure growth over time. Information about their background and educational experiences will be collected from their parents, teachers, and principals using web surveys.

PIRLS is an international school-based assessment of the reading knowledge and skills of fourth-graders. PIRLS has been conducted every 5 years since 2001, with more than 60 countries including the United States planning to participate in PIRLS 2021. PIRLS is coordinated by the International Association for the Evaluation of Educational Achievement (IEA) and managed in the United States by NCES.

PIAAC is a multicycle international program to assess adult skills and competencies. PIAAC data collection has occurred in 2012, 2014, and 2017 and work is underway for the Cycle Field Test in 2021 and Main Study in 2022.

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

This system is used to fulfill NCES's statutory mandate to collect, report, analyze, and disseminate statistical data on the condition and progress of education in the United States and other nations at the early childhood, preschool, elementary, secondary, postsecondary, and adult levels. These data must be timely, objective, and non-ideological; free of political influence and bias; and relevant and useful to practitioners, researchers, policymakers, and the public. PII is collected for statistical sampling. Many of the studies have complex sample designs that employ differential sampling based on student characteristics. Information on these characteristics must be obtained from educational institutions. PII is also needed in order to send informational and consent materials to sampled students' parents. Some studies include multiple respondents associated with sample students, such as parents and teachers. Those associated respondents must be identified so that they can be asked to complete surveys. In addition, for some studies, locating information (child/student and parent names, home address, and home telephone number) must be collected in order to track students and their families over time so that they can be contacted for follow-up data collections. Without this information, retaining sampled students and contacting respondents at each data collection round would be extremely difficult.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

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

Contractor

[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

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

Yes

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

NCES is authorized by law to collect and use these data under the Education Sciences Reform Act of 2002 (20 U.S. Code Section 9543): "The Statistics Center shall collect, report, analyze, and disseminate statistical data related to education in the United States and in other nations, including — (7) conducting longitudinal and special data collections necessary to report on the condition and progress of education."

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

□ N/A

National Center for Education Statistics (NCES) Longitudinal and Cross-sectional Studies (18-13-01), November 14, 2018. 83 FR 56831-56834. https://www.federalregister.gov/documents/2018/11/14/2018-24847/privacy-act-of-1974-system-of-records-national-center-for-education-statistics-nces-longitudinal-and

National Center for Education Statistics National Assessment of Educational Progress (18-13-03), June 4, 1999. 64 FR-30160-30191.

[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

https://www.federalregister.gov/documents/1999/06/04/99-12656/privacy-act-of-1974-systems-of-records

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

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

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

The Department will 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.

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

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The NCESLS collects information such as child/student name, parent name, home address, home telephone number, date of birth, and school name. General financial information, such as household income and receipt of welfare benefits, as well as medical information, such as whether a child has a disability, are also collected within this system.

This system also contains responses from students, their parents or legal guardians, teachers, administrators, service providers, and other adults to data collection instruments. The specific information collected varies by study but includes information such as background and demographic data, functional measures (reports of children's functioning in cognitive, social, emotional, and physical domains), family characteristics, education and/or employment experiences, finances, aspirations, plans, and attitudes. Cognitive assessment scores, administrative records, and high school transcripts are also appended to some records. The appended administrative records contain data such as attendance, program participation, and other information.

The records for service providers, schools/institutions, and local educational agencies contain information such as numbers and characteristics of students, teaching staff, and administrators; data on facilities, programs, services, and finances; and information related to student enrollment, persistence, completion, and performance. The records related to teachers and administrators contain data on topics such as certifications, training, experience, staff evaluations, salary, benefits, and attitudes and opinions related to various aspects of education and operations.

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

Yes.

Before every data collection, the data collection instrumentation and protocols are fully reviewed by multiple groups to assure that the information collected is needed to meet the requirements for a given study. In the study development stage, NCES staff, contractor staff from at least two different contractors, and external experts all provide input on the information to be collected. These reviews include consideration of whether the collection of identifying information is necessary; if so, NCES and contractor staff must agree on the most secure way to collect the least amount of information needed. This can vary by study for which the NCESLS system is used. For example, student name and a small set of student-level characteristics, such as disability and English proficiency classification, are needed for sample purposes for NAEP, but because parent consent is not required and there is no parent survey, no parent contact information is collected. In contrast, for a longitudinal study such as the ECLS-K, more detailed student information and parent contact information are needed for purposes of obtaining consent to participate, asking parents to complete surveys, and following students over time.

Once instrumentation is finalized in the development stage, it is submitted to the Office of Management and Budget (OMB) for both public review and OMB review and approval. The OMB clearance requests include justifications for the information collected, with some studies such as the ECLS-K tying each item to a specific research question the study is intended to address. At an overall level, the PII collected must be needed for contacting purposes, consent purposes, or sampling purposes, or it must be considered an item of relevance for analyses of student educational experiences and outcomes.

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

Information in the records comes from responses to surveys that are completed by individuals selected for each study and assessment instruments completed by the children/students selected for each study. The respondent groups vary by study but include children/students, parents/guardians, and school staff (i.e., teachers, school administrators, support staff). Information may also come from administrative records maintained by K-12 schools and school districts, as well as from some third parties, such as state and Federal agencies.

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

Data are collected using various methods: hard-copy surveys, web surveys, telephone surveys, and in-person direct assessments and personal interviews. In the process of providing student roster information for the purposes of sampling, school or field staff may also consult administrative records. The system does not collect or store the administrative records themselves.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

For individuals, there are edit checks built into the survey instruments.

[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.

For institutions, there are edit checks built in their data collection instrument. Quality checks are conducted by statisticians and other trained process staff on the student roster information that is provided by schools.

Data are thoroughly cleaned and reviewed after data collection. Edits are performed when errors are identified and the correct information can be confirmed. For example, if information has been scanned incorrectly from a hard-copy survey, the database can be edited to include the correct information.

Use

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

PII is collected for serval purposes: statistical sampling, to communicate with selected individuals about study activities, to obtain consent from parents/guardians for sampled students to participate, and to track students and their families over time so that they can be contacted for follow-up data collections. How PII is used and for how long it is maintained vary by study. For cross-sectional studies that occur once, the PII is used by sampling statisticians to select a sample with the necessary characteristics to be representative of the population of interest and to contact selected individuals at the beginning of a collection. The PII is maintained until a data file is approved for release to researchers, at which point it is destroyed.

For longitudinal studies with multiple rounds of data collection, the PII also is used by sampling statisticians to select a sample with the necessary characteristics to be representative of the population of interest and to contact selected individuals at the beginning of a collection. The PII is also used to maintain contact with study participants over the course of the study. The frequency of contact varies by study but typically happens at least once per year when participants are contacted and asked to provide updated contact information. Contacts happen more often in years with data collections. Because of the need to contact participants throughout the life of a study, PII are maintained until the very end of a longitudinal study, after final data are released. This can be as long as 10 years.

For all studies, PII is always stored separately from responses that are provided or collected in surveys and other data collection instruments.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

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.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

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

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

The specific studies for which NCESLS collects and stores data are covered by two SORNs associated with the National Center for Education Statistics:
National Center for Education Statistics (NCES) Longitudinal and Cross-sectional Studies (18-13-01), November 14, 2018. 83 FR 56831-56834.
https://www.federalregister.gov/documents/2018/11/14/2018-24847/privacy-act-of-

1974-system-of-records-national-center-for-education-statistics-nces-longitudinal-and

National Center for Education Statistics National Assessment of Educational Progress (18-13-03), June 4, 1999. 64 FR-30160-30191. https://www.federalregister.gov/documents/1999/06/04/99-12656/privacy-act-of-1974-systems-of-records

All data collections must be approved by the Office of Management and Budget, which requires a 60-day public comment period during which the details of each study, including the information collected, are provided publicly in the Federal Register. In the OMB clearance packages it is noted that confidentiality and data security protection procedures have been put in place to ensure that study staff comply with all privacy requirements, including the Privacy Act.

In addition, consent materials provided to schools and parents, as well as all data collection instruments for adults and older students, include information on NCES's legal authorization to collect these data, and assurance of the confidential nature of the data collection.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

Here is an example of the text of the notice for one of the NCES studies:

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 1850-0928. The time required to complete this information collection is estimated to average 270 minutes for schools that do not submit student sample information or 390 minutes for schools that submit student sample information manually, plus an additional 10 minutes for each student identified as SD or ELL, including the time to review instructions, search existing data resources, 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 collection, or any comments or concerns regarding the status of your individual submission, please write to: National Assessment of Educational Progress (NAEP), National Center for Education Statistics (NCES), Potomac Center Plaza, 550 12th St., SW, 4th floor, Washington, DC 20202.

OMB No. 1850-0928 APPROVAL EXPIRES 9/30/2021

National Center for Education Statistics (NCES) is authorized to conduct NAEP by the National Assessment of Educational Progress Authorization Act (20 U.S.C. §9622) 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).

All of the information provided by participants 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). By law, every NCES employee as well as every NCES agent, such as contractors and NAEP coordinators, has taken an oath and is subject to a jail term of up to 5 years, a fine of $250,000, or both if he or she willfully discloses ANY identifiable information about students. Electronic submission of each student's information will be monitored for viruses, malware, and other threats by Federal employees and contractors in accordance with the Cybersecurity Enhancement Act of 2015. The collected information will be combined across respondents to produce statistical reports.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Individuals may decline to participate in a NCES study. They may opt out by contacting NCES or the data collection contractor. They may also decide not to provide any type of response to a solicitation for information. In addition, if an individual does choose to participate in a study, he or she is also free to decline to answer any question at any time.

It should be noted that Per the *No Child Left Behind Act of 2001*, the *Every Student Succeeds Act of 2015*, and the *Education Sciences Reform Act of 2002, Public Law 107-279 Title III, section 303,* Congress requires all states to participate in the NAEP reading and mathematics assessments at the fourth and eighth grades every two years as a condition for receiving Title I funding. States that do not wish to receive such funding need not participate. State participation in NAEP assessments for all other subjects and grades is completely voluntary. In addition, while states and school districts must allow NAEP data collection to occur in their schools to receive Title I funding, participation is still completely voluntary for individual students.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

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

☑ N/A

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

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

☑ N/A

Click here to enter text.

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

☑ N/A

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

☑ N/A

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

☑ N/A

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

☑ N/A

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

If an individual wishes to determine whether a record exists in this system or to gain access to their information in the system, the individual may contact the system manager. The request process is described in the system of records notice. Requests must meet the requirements in the Department's regulations at 34 CFR 5b.5, including proof of identity.

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

If an individual wishes to contest the content of a record in the system of records, the individual may contact the system manager. The request must meet the requirements of the Department's regulations at 34 CFR 5b.7, including proof of identity.

It should be noted, however, that data are not maintained or released in a format that associates their information with their name, and the data are not used for evaluative or compliance purposes. Therefore, errors in the data have no negative impact on any specific individual.

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

The procedures are specified in the NCES SORN, entitled the "National Center for Education Statistics (NCES) Longitudinal and Cross-sectional Studies'' (18-13-01)

In addition, all studies have NCES contacts who are identified publicly on the NCES website. An individual can obtain such information by contacting NCES staff.

7. Safeguards

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

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

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

□ N/A

Moderate

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

Department staff at the NCES who are assigned to the studies for which the NCESLS system collects and maintains data have all passed a public trust background clearance at a level 5c or higher. In addition, all staff sign an affidavit of nondisclosure when they begin employment at NCES. NCES staff are not given access to the NCESLS system, which is maintained by the contractor, Westat, in a manner that allows them to make changes to the system or access PII. For example, while NCES staff may access a component of the system to test data collection instruments, they would not make changes to the system itself. Any changes that may be needed after testing would be made by Westat staff. Furthermore, while NCES staff are given access to lists of sampled institutions upon request, they are not given access to PII at the individual or respondent level as a routine procedure. In rare instances when NCES staff become aware of PII such as respondent names or location of residence, it is typically as a result of self-disclosure when sampled individuals contact NCES staff directly or when staff are conducting quality control visits during data collection in schools. NCES staff never have access to directly identifying PII in conjunction with survey responses or administrative record data that are collected and maintained in the NCESLS system.

All Westat personnel having access to system components or data are explicitly authorized for such access, and are either assigned to the project or are members of Westat's systems staff. Staff with authorized access to the system all have at minimum a Public Trust 5c level of clearance and a business need for access to the system. Access to system information is controlled by creating/removing accounts and access groups, assigning rights to accounts and access groups, assigning accounts to access groups, granting access through physical access controls, and granting permission for access, transport, or storage of information. Physical access controls are implemented in several ways, including guards stationed at the entry to visitor parking lots on Westat's campus, controlled entry to buildings using an ID-swipe system, and receptionists stationed in locations that allow access by the public. Staff accessing connected system assets from Wesnet or the enclave environments do so from their individually assigned workstations, from servers, or from project assets. Users who have successfully logged in are subject to the policies and procedures established by Westat, including access control and rights assignments for hosted systems. Authorized users who have successfully logged into Wesnet or the FISMA High Enclave (FHE; an isolated area of the Westat network, used for projects with FISMA High requirements) are therefore considered to have successfully logged into the hosted system for the purposes of connecting to those system assets that derive credentials from Wesnet or the FHE (i.e., Active Directory) for identification and authentication. Westat staff remotely connect to Wesnet via Citrix Virtual Private Network (VPN) connections to their local workstations. All individuals having access to system components or data are authorized for such access. These include but are not limited to agency staff, external respondents/participants, project staff, and Westat systems staff supporting project assets. Role based access control (RBAC) is used for providing access to system information and is controlled by creating/removing accounts and access groups (e.g. field staff, data collection managers), assigning rights to accounts and access groups, assigning accounts to access groups, granting access through physical access controls, and granting permission for access, transport, or storage of information. Using RBAC, users are able to access only the information in the system for which they have a business need.

Access to secure computer systems is password protected. All server and network data storage areas are protected by access privileges, which are assigned by the appropriate system administrator. Login passwords are encrypted and stored only in their encrypted form in protected files on each system. A non-displaying or non-printing feature prevents the password from appearing on the computer screen during the login process. The system automatically limits the number of unsuccessful attempts to log in, after which the account is disabled and must be reset by the system administrator. To ensure the confidentiality of passwords, users are required to change their network passwords every 60 days. Passwords must be of a minimum length, must meet certain character and numeric usage rules, and cannot be reused. Accounts that have not been used for 90 days are automatically disabled and deleted within 1 week upon notifying relevant managers.

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

Yes

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

Yes

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

NCESLS is monitored, tested, and evaluated in accordance with National Institute of Standards and Technology (NIST) guidelines for moderate-impact systems. In order to receive official authorization to operate (ATO), documents such as a system security plan (SSP) are developed and approved during a detailed assessment by the Department's Office of the Chief Information Officer. The SSP details 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. Westat performs vulnerability scans weekly on servers to identify possible vulnerabilities. Results are made available to the appropriate systems technical administrators and managers who are required to respond with information on any corrective actions taken. As a further measure, Westat periodically monitors traffic between each internally defined network security zone (i.e., internal sub-networks whose traffic is mediated by the firewall). This activity recognizes the pattern of common types of suspicious traffic that may indicate attempts by an internal or external user to access a specific computer for which the user is not authorized.

Server and workstation operating systems are updated with applicable security patches as they are made available by the vendors. Systems support staff subscribe to several nationally recognized security alert services to keep informed about current and emerging security issues and product vulnerabilities. Procedures are in place for staff to respond to early warnings about security threats whether during or outside regular business hours. Westat's response protocol includes immediate action to gather information, protect systems, inform users, and take any new protective measures, such as applying newly released security software updates.

Intrusion detection software running on our firewalls detects and blocks outside users who are identified as attempting to gain unauthorized access to our network. Intrusion detection signature patterns are automatically updated regularly by the firewall application vendor to keep pace with the latest techniques used to break into networks. Westat also employs a breach detection and notification system that provides extensive detection techniques, monitoring of all network activity, custom sandbox analysis, and correlated threat intelligence that can detect and analyze malware, command and control (C&C) communications, and evasive attacker activities that are invisible to standard security defenses. In addition, Westat maintains Business Continuity Plans and Emergency Response documents with testing of the Information Technology Contingency Plan and Disaster Recovery Plan occurring annually.

8. Auditing and Accountability

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

The system owner 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 ATO. The Department’s, contractor’s, and subcontractors’ employees who collect, maintain, use, or disseminate data in this system must comply with applicable 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 PII 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.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

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

The main risk associated with this system is the potential for unauthorized individuals gaining access to PII of respondents. This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data and mitigate privacy risks. Mitigation of those risks at a system level includes selecting, implementing, assessing, and monitoring a full range of security and privacy controls, pursuant to NIST guidelines for moderate-impact systems.

Access to PII is limited to staff who work on the study and need the PII to complete study tasks. All such staff must sign an affidavit of nondisclosure. Per the *Education Sciences Reform Act of 2002* (20 USC 9573) these staff, as well as anyone who accesses NCES data, are subject to penalties if they willfully disclose respondent information or uses the data for other than statistical purposes.[5]

Study respondents are never identified in data files released for research purposes. This is true for both NCES restricted-use files, which are available only to researchers through license with NCES, and public-use files, which NCES makes freely available without restrictions.

At the project level, the use of direct identifiers is minimized to the fullest extent possible. Direct identifiers, when needed, are used during actual data collection for sampling, consent, and contacting purposes. Within the NCESLS system, any directly identifying information is stored separately from data collected in the assessments and surveys. The collected data are processed within the NCESLS system with an interim ID number that is randomly generated. Another (different) randomly generated ID number is used as a case-level identifier in the micro-level data files developed for research purposes. Thus, direct identifiers are never associated with collected data in compiled

[5] See 20 USC 9573(c)(2) and 20 USC 9573(d)(6) for more detail on the confidentiality requirements and penalties.

data files. Only someone who has access to a cross-walk between the direct identifiers and the interim or final IDs would be able to tie the collected/released data back to a specific individual. Only a small set of data collection contractor staff have access to this crosswalk.

All data included in data files intended for research use, both restricted use and public use, undergo a disclosure risk analysis and are subject to data perturbation techniques that must be reviewed and approved by the Institute of Education Sciences' Disclosure Review Board. All data are subject to swapping to ensure that no individual respondent can be identified in a data file. Further, sensitive variables are removed from public-use files and other data are coarsened. No data can be approved for release without the issuance of a "Safe-to-release" memo by the IES DRB chair. This memo confirms that the data files have undergone all steps necessary to assure that no potentially identifying information as been include in the files.

It should be noted that some restricted-use files, such as those for the ECLS-K, include an NCES school identifier, which identifies the school attended by a study respondent. The purpose of providing this identifier is to allow for linkages to NCES school universe data files that include school characteristics data. Because information is collected from school administrators in the ECLS-K, there is potential for a data user to identify the administrator if they are able to determine who the administrator was at the time of data collection. However, as noted above, researchers are only allowed access to the restricted data through a license with NCES. In order to qualify for a license, researchers must have a legitimate research question that can only be answered with restricted-use data, must meet requirements to assure the security of the data, and must sign a notarized agreement that they will abide by the license requirements or face penalties for misuse of the data, which would include intentional identification of a study participant. All applications for a restricted-use license are reviewed and approved by the IES DRB chair or NCES Chief Statistician

A data use agreement, pasted below, also must be agreed to by researchers accessing public-use data.

Under law, public use data collected and distributed by the National Center for Education Statistics (NCES) may be used only for statistical purposes. Any effort to determine the identity of any reported case by public-use data users is prohibited by law. Violations are subject to Class E felony charges of a fine up to $250,000 and/or a prison term up to 5 years.

NCES does all it can to assure that the identity of data subjects cannot be disclosed. All direct identifiers, as well as any characteristics that might lead to identification, are omitted or modified in the dataset to protect the true characteristics of individual cases. Any intentional identification or disclosure of a person or institution violates the assurances of confidentiality given to the providers of the information. Therefore, users shall:

- Use the data in any dataset for statistical purposes only.
- Make no use of the identity of any person or institution discovered inadvertently, and advise NCES of any such discovery.
- Not link any dataset with individually identifiable data from other NCES or non-NCES datasets.

To proceed you must signify your agreement to comply with the above-stated statutorily based requirements. This window will close and you can now download the file.