MEMORANDUM

UNITED STATES DEPARTMENT OF EDUCATION
Institute of Education Sciences
National Center for Education Statistics

September 30, 2021

TO: Peggy Carr, Ph.D.
NCES, Commissioner

FROM: Marilyn M. Seastrom, Ph.D.
NCES, Chief Statistician

SUBJECT: 2020 Report to OMB on the NCES Implementation of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) in 2020

Background

As an OMB recognized statistical agency or unit, NCES is required per OMB CIPSEA Guidelines (CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.)) to report annually on (1) the use of the CIPSEA pledge, including an affirmation that the agency has followed the procedures established in the OMB CIPSEA Guidance and (2) the use of agents as allowed under CIPSEA. NCES is also required to identify any data or information it collects for nonstatistical purposes (as authorized by law). In particular, statistical agencies are instructed to explain the confidentiality provisions for all information not protected under CIPSEA, including any limitations on the confidentiality provisions.

Summary of Report

To satisfy these requirements, NCES surveys are identified as requiring confidentiality pledges if covered by CIPSEA; as requiring data protection pledges if covered by the Education Sciences Reform Act (ESRA), as amended by the U.S.A. Patriot Act; and as not requiring a pledge of confidentiality in the case of administrative data. CIPSEA confidentiality pledges are included in Appendix A and ESRA data protection pledges are included in Appendix B. Our confidentiality and data protection procedures used to safeguard confidential information are described in the body of the report. The report also includes a description of the NCES use of various categories of CIPSEA agents and a discussion of the contractual and licensing procedures that are used to authorize these agents. Relevant language for data collection contracts is provided in Appendices C and D and relevant documents used to allow qualified researchers to access confidential or protected data off-site are included as Appendices E through H. NCES reports the employment of 4,978 contractor agents during calendar year 2020. An additional 1,573 Bureau of the Census staff worked on NCES data collections bringing the total number to 6,551. At the end of the 2020 calendar year, NCES also had 3,803 qualified researchers who were approved on NCES data licenses to access restricted-use data.

NCES Report to OMB on the use of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) and Agents

Reporting Requirements Section 1

Confidentiality and Data Protection Pledges

REPORTING REQUIREMENT: Report of the use of the CIPSEA pledge. "Any Federal agency acquiring data under CIPSEA Subtitle A shall report to OMB on an annual basis on those collections it has conducted under CIPSEA and affirm that the agency has followed the procedures in this guidance to ensure the confidentiality of the information is protected." (excerpted from OMB Guidance on the Implementation of CIPSEA).

In 2020, NCES collected the following surveys under CIPSEA Subtitle A; please see Appendix A for the confidentiality pledges used for each data collection and details:

- National Assessment of Educational Progress (NAEP)
  NAEP 2021 eNAEP Pretesting and Usability Study
  (OMB No. 1850-0803)

In 2020 NCES collected the following surveys under the Education Sciences Reform Act (ESRA) of 2002; please see Appendix B for the data protection pledges used for each data collection:

- Baccalaureate and Beyond Longitudinal Study (B&B) B&B:16/20 Full-Scale Study Panel Maintenance
  (OMB No. 1850-0926)
- Baccalaureate and Beyond Longitudinal Survey (B&B:16/20) Full-Scale Study
  (OMB No. 1850-0803)
- Beginning Postsecondary Students Longitudinal Study (BPS) 2020/22 Beginning Postsecondary Students Longitudinal Study (BPS:20/22) Cognitive and Usability Testing Update
  (OMB No. 1850-0803)
- Civil Rights Data Collection (CRDC) CRDC Burden Research Study
  (OMB No. 1850-0803)
- Current Population Survey (CPS) 2020 CPS School Enrollment Cognitive Testing
  (OMB No. 1850-0803)
- Early Childhood Longitudinal Study (ECLS) ECLS-K:2023 Preschool Field Test
  (OMB No. 1850-0750)
- ECLS-K:2023 Kindergarten-First Grade Field Test Instruments Usability Testing
  (OMB No. 1850-0803)
- Early Childhood Longitudinal Study (ECLS) ECLS-K:2023 Focus Groups with School Administrators, Teachers, and Parents
  (OMB No. 1850-0803)
- Fast Response Survey System (FRSS) FRSS 110: Use of Educational Technology for Instruction in Public Schools
  (OMB No. 1850-0733)

- High School and Beyond Longitudinal Study 2020 (HS&B:20)
  - High School and Beyond 2020 (HS&B:20) Base Year Field Test
  - Base Year Full Scale Study

  (OMB No. 1850-0944)
- High School and Beyond (HS&B)
  - HS&B:22 Base-Year Field Test
  - HS&B:22 Base-Year Full-Scale Study

  (OMB No. 1850-0944)
- High School and Beyond (HS&B)
  - HS&B:20 Cognitive and Usability Testing Round 2

  (OMB No. 1850-0803)
- Middle Grades Longitudinal Study of 2017-18 (MGLS:2017)
  - MGLS:2017Main Study First Follow-up (MS2) – Tracking and Recruitment
  - MGLS:2017 Operational Field Test Second Follow-up (OFT3) – Tracking and Recruitment

  (OMB No. 1850-0911)
- National Assessment of Educational Progress (NAEP)
  - NAEP 2020 Pilot DBA for 2021 Mathematics, Grades 4 and 8
  - NAEP 2020 Pilot DBA for 2021 Writing, Grades 4, 8, and 12
  - NAEP 2020 Pilot DBA for 2022 U.S. History, Civics, and Geography, Grade 8
  - NAEP 2020 Pilot DBA for 2022 U.S. History, Civics, Geography, and Economics, Grade 12
  - NAEP 2020 Pilot DBA for 2022 TEL, Grades 8 and 12
  - NAEP 2021

  (OMB No. 1850-0928)
- National Assessment of Educational Progress (NAEP)
  - NAEP 2020 Operational national PBA Long-Term Trend (LTT)

  (OMB No. 1850-0928)
- National Assessment of Educational Progress (NAEP)
  - 2023 NAEP Family Structure Study

  (OMB No. 1850-0803)
- National Assessment of Educational Progress (NAEP)
  - NAEP Survey Assessments Innovation Lab (SAIL) Test Assembly Experimental Study

  (OMB No. 1850-0803)
- National Assessment of Educational Progress (NAEP)
  - NAEP 2021 COVID-19 Educational Experiences Student, Teacher, and School Administrator Pretesting

  (OMB No. 1850-0803)
- National Assessment of Educational Progress (NAEP)
  - NAEP Engagement Augmentation Study

  (OMB No. 1850-0803)

- National Household Education Surveys (NHES)
  2022 NHES English and Spanish Cognitive Interviews
  (OMB No. 1850-0803)
- National Household Education Surveys (NHES)
  2022 NHES Web Usability Testing
  (OMB No. 1850-0803)
- National Postsecondary Student Aid Study (NPSAS)
  NPSAS:20 Institution Collection
  (OMB No. 1850-0666)
- National Postsecondary Student Aid Study (NPSAS)
  NPSAS:20
  (OMB No. 1850-0666)
- National Teacher and Principal Survey (NTPS)
  NTPS 2020–21 Preliminary Activities
  (OMB No. 1850-0598)
- National Teacher and Principal Survey (NTPS)
  NTPS 2020–21
  (OMB No. 1850-0598)
- National Teacher and Principal Survey (NTPS)
  NTPS 2020–21 Cognitive Interviews
  (OMB No. 1850-0803)
- National Teacher and Principal Survey (NTPS)
  NTPS 2020–21 Teacher and Principal Follow Up Survey Cognitive Testing
  (OMB No. 1850-0803)
- National Teacher and Principal Survey (NTPS)
  NTPS 2020–21 Testing Questions on the Teacher Questionnaire on Sexual Orientation and Gender Identity (SOGI), and Branding Changes
  (OMB No. 1850-0803)
- Progress in International Reading Literacy Study (PIRLS)
  PIRLS 2021 Field Test Recruitment
  (OMB No. 1850-0645)
- Progress in International Reading Literacy Study (PIRLS)
  PIRLS 2021 Main Study Recruitment and Field Test
  (OMB No. 1850-0645)
- Progress in International Reading Literacy Study (PIRLS)
  PIRLS 2021 Main Study Data Collection
  (OMB No. 1850-0645)
- Progress in International Reading Literacy Study (PIRLS)
  PIRLS 2021 Field Test Pretest
  (OMB No. 1850-0803)

- Program for International Student Assessment (PISA)
  PISA 2021 Main Study Recruitment and Field Test
  (OMB No. 1850-0755)
- Program for International Student Assessment (PISA)
  PISA 2021 Field Test Pretest
  (OMB No. 1850-0803)
- School Survey on Crime and Safety (SSOCS)
  SSOCS 2020
  (OMB No. 1850-0761)
- School Survey on Crime and Safety
  SSOCS:2020 Recruitment Materials
  (OMB No. 1850-0761)
- School Survey on Crime and Safety
  SSOCS Incident Count Check Cognitive Interviews
  (OMB No. 1850-0803)
- Trends in International Mathematics and Science Study (TIMSS)
  TIMSS 2023 Cognitive Interviews
  (OMB No. 1850-0803)

NCES collected four sets of administrative universe/census data with no pledge of confidentiality or data protection. In the case of the postsecondary data collection, the Office of Postsecondary Education uses some data elements for regulatory purposes. Some data elements from the elementary and secondary data are used by Program Offices in the Department of Education for monitoring purposes. In all three cases, directory information on the school name location, enrollment, and student characteristics is made available in online school locator tools.

- Common Core of Data (CCD) annually
- Private School Survey (PSS) 2019-20
- Integrated Postsecondary Education Data System (IPEDS) annually
- EDFacts Data Collection annually

Safeguarding Confidential Information.
REPORTING REQUIREMENT: Physical and Information Systems Security—only persons authorized are permitted access to confidential information stored in information systems.

NCES confidential data are stored electronically on Institute of Education Sciences (IES) servers that are hosted in the GovCloud Region of Amazon Web Services (AWS). The computer systems used by NCES received an Authority to Operate (ATO) through the Federal Government's Security Authorization process based on FISMA security controls. Under the Education Sciences Reform Act of 2002 (ESRA), NCES is a component of IES and is covered by the confidentiality provisions that are included in ESRA (U.S. Code Title 20, Chapter 76, section 9573). NCES has a data security program in place to assist NCES staff and their contractors in the implementation of data protections. The Institute for Education Sciences Disclosure Review Board (IES DRB) Chair and one of the six board members are in the NCES Data Security Program, and work along with one data security officer, six data security technicians and .54 FTE of disclosure risk review analyst to provide access to confidential data within NCES, process the license agreements with our researcher agents, provide

for the review all NCES products and the work of researcher agents for potential disclosures prior to release, and initiate and review the Public Trust applications submitted by contractor agents for their Public Trust positions.

The Education Sciences Reform Act of 2002 (ESRA 2002) (U.S. Code, Title 20, Chapter 76, Section 9573) requires that all individually identifiable information about students, their families, and their schools shall remain confidential. To this end, this law requires that no person may:

a. Use any individually identifiable information furnished under the provisions of this section of the law for any purpose other than statistical purposes for which it is supplied, except in the case of terrorism;

b. Make any publication whereby the data furnished by any particular person under this section can be identified; or

c. Permit anyone other than the individuals authorized by the Commissioner to examine the individual reports.

Employees, including temporary employees, or other persons who have sworn to observe the limitations imposed by this law, who knowingly publish or communicate any individually identifiable information will be subject to fines of up to $250,000, or up to 5 years in prison, or both (Class E felony).

NCES 2012 Statistical Standards include requirements that are consistent with the procedures specified in the OMB CIPSEA Guidance to ensure that the confidentiality of information is protected. Specifically, in the initial planning for a survey, staff are instructed to take the confidentiality and privacy provisions of the Privacy Act, the Education Sciences Reform Act of 2002 (ESRA), the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) transferred to Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.), the Protection of Pupils Rights Act (PPRA), and the Family Educational Rights and Privacy Act (FERPA) into account in designing any studies that will collect individually identifiable data. When developing a formal survey design, staff members are required to include plans for preserving the confidentiality of individually identifiable data during data collection and analysis and for an analysis of disclosure risk control. Disclosure risk control plans are submitted to the IES Disclosure Review Board for review and approval. Approved plans are implemented to protect the data and the data are reviewed prior to release to ensure the protections had the intended impact.

REPORTING REQUIREMENT: Confidentiality Training—all employees are certified annually.

All NCES staff members are required by the U.S. Department of Education to participate in annual training on cybersecurity and data confidentiality. In addition, the NCES standard on maintaining confidentiality requires all staff to be cognizant of the confidentiality requirements of the law and to monitor the confidentiality of individually identifiable information in their daily activities and in the release of information. This standard includes a discussion of the relevant laws—the Privacy Act of 1974, as amended; CIPSEA Act of 2002 transferred to Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Education Sciences Reform Act of 2002; and the U.S.A. Patriot Act of 2001. In addition to specifying requirements for NCES and contractor staff in the collection and handling of individually identifiable data, procedures required to protect individually identifiable data in both public- and restricted-use releases are described, and the role of the IES Disclosure Review

Board in the release process is established. Note: in 2018, Congress enacted the Foundations of Evidence-Based Policymaking Act. As it relates to Confidential Information Protection, this 2018 Act transferred the Confidential Information (and Statistical Efficiency) Act (CIPSEA) from the 2002 E-Government Act to the Foundations of Evidence-Based Policymaking Act of 2018 and codified CIPSEA in a new subchapter III, of chapter 35 of title 44, United States Code. The Class E felony penalties for any willful disclosure of confidential information are unchanged.

REPORTING REQUIREMENT: Record Keeping—the agency has records that identify all individuals authorized to access confidential information.

NCES Program staff members assigned to a specific data collection are granted access to those data as a condition of employment. NCES staff members needing access to confidential data other than those they are responsible for collecting must request copies from the NCES Data Security Program and sign for copies of the restricted use versions of the data in order to access the data.

REPORTING REQUIREMENT: Review of Information Prior to Dissemination—the agency has in place a process to review information prior to dissemination to ensure confidential information is not disclosed.

Microdata files:
All NCES data files that include information collected under a CIPSEA confidentiality pledge or an ESRA data protection pledge undergo data perturbations following a plan proposed by program staff that is reviewed and approved by the IES DRB. The perturbed data are also reviewed and approved by the IES DRB before the data can be recommended for release as a restricted use data file. Public use data files, when available, are prepared from the approved restricted use files. In each case, a disclosure avoidance plan is proposed by program staff, reviewed and approved by the IES DRB, and implemented by program staff. The resulting data file is reviewed and approved by the IES DRB before the data can be recommended for release as a public use or restricted use data file.

Tabulations, presentations, and reports:
All NCES tabulations and reports prepared by staff and contractors using restricted use data are reviewed for potential disclosures prior to release. Similarly, all research agents are required to submit reports or presentations to the NCES Data Security Program for review for potential disclosures prior to sharing the information with anyone who is not an authorized user of the data.

Reporting Requirements Section 2

Use of the Agents Provision in CIPSEA.
"Statistical agencies and units are authorized under Subtitle A of CIPSEA to designate agents, who may perform exclusively statistical activities, including data collection, and who are bound to the same legal requirements as agency employees for maintaining the confidentiality of the information. Statistical agencies or units that choose to designate agents shall report to OMB on an annual basis on the number of agents designated; the kinds of statistical activities performed by agents, *e.g.*, data collection, analysis, etc.; the different types of arrangements for access to confidential information (if applicable), *e.g.*, on-site at the statistical agency, through an agency-controlled research data center, or off-site licensing agreement; and the kind of written agreement that is required for each type of access." (excerpted from OMB Guidance on the Implementation of CIPSEA).

REPORTING REQUIREMENT: The Use of Contractor Agents—report the number of contractor employees designated as agents, separately by their reason for access.
NCES has four categories of agents. The first includes contractor staff tasked with the day-to-day responsibilities for data collection and management; design and planning, processing, documentation, and analysis; and IT support. Each contract employee with any access to individually identifiable data is required to sign an affidavit of nondisclosure as is required by the Department of Education to apply for and receive approval to serve in a moderate risk Public Trust position, or alternatively, to provide evidence of an existing approval to hold a moderate Public Trust position. The applications for Public Trust positions are now processed through the Defense Counterintelligence and Security Agency (DCSA) e-QIP system (this function was previously under the Office of Personnel Management) and adjudicated by the Department of Education's Security Office.

In 2020, NCES used 4,978 contractor agents. The contractor agents engage in all aspects of data collection and analysis; of the set of 4,332 contractor agents, 3,275 were involved in data collection and management for NAEP and 1,057 were involved in data collection and management for B&B, ECLS, EDfacts, FRSS, HS&B, HSLS, MGLS, NHES, NPSAS, NTPS, PIRLS, PISA, SSOCS, and TIMSS. Another 404 contractor agents worked on design and planning, processing, documentation, and analysis (174 on NAEP and 230 on the other data collections), and 242 contractor agents provided IT support for NCES data collections (177 on NAEP and 65 on the other data collections). Note that some NCES data collections are conducted by the Census Bureau on behalf of NCES (including the PSS, NTPS and NHES). Thus, Census employees work on these data collections, but do not contribute to the pool of NCES contractor agents. The Census Bureau manages their own staff Public Trust Positions processed through the e-QIP system. The total count of Census Bureau staff involved in these collections is 1,573 with 1,482 conducting data collection activities, 49 conducting data processing activities and 42 provide IT support.

REPORTING REQUIREMENT: The Use of Researcher Agents—report the number of researchers the agency has designated as agents, separately by where they accessed the data—off-site at the researcher's institution or organization.
The second category of NCES agents includes the NCES restricted-use data licensees who are qualified researchers who use NCES confidential data off-site in secure facilities at their institutions and organizations. During 2020, NCES was supporting 1,249 restricted-use data licenses with a total of 3,803 RUF licensed researcher agents using RUF data. (Each RUF license can include up to 7 licensed users.) There is an average of 3 licensed agents per RUF license in the reporting year. The majority of the researcher agents are in colleges and universities. A smaller number of the researcher agents are employed by research organizations and professional associations.

REPORTING REQUIREMENT: The Use of Federal or State Agencies—report the number of different agencies and the total number of Federal and State agency employees designated as agents.
The third category of NCES agents includes the Federal and State employees who enter into a Memoranda of Understanding (MOU) to access NCES restricted use data. NCES entered a Memoranda of Understanding with 35 Federal agencies or state agencies to support their use of restricted use data at the agencies' sites. (Note these agents were previously reported with the researcher agents, and thus are part of the 3,803 agents reported for the calendar year 2020).

REPORTING REQUIREMENT: The Use of Researcher Agents—report the number of researchers the agency has designated as agents, separately by where they accessed the data—off-site at an agency-controlled site.
NCES no longer supports use of researcher agents accessing data off-site at an agency-controlled site. Starting in 2012, NCES undertook efforts to create online data set training for researchers needing to learn and develop the skills to use NCES complex sample survey data, in general for their research goals, and for analyzing specific NCES surveys. All the data used in for the distance learning training modules are public-use data.

All public use data released by NCES are required to include a warning and consent form acknowledging that under law, data collected and distributed by NCES may be used only for statistical purposes and that no attempts may be made to use the data to identify individual respondents.

Requirements and Guidelines when Designating CIPSEA Agents

REPORTING REQUIREMENT: Contract and Written Agreements—all contracts and agreements include the appropriate provisions in the Appendix of the CIPSEA Implementation Guidance.
For contractor agents, the NCES standard on developing a Request for Proposals (RFP) for surveys requires the NCES Contracting Officer's Representative (COR) to prepare the required clearances and approvals consistent with the Department's relevant management directives. This includes the public notification process that is required under the Paperwork Reduction Act. The NCES Security Program has also written boilerplate language for inclusion in each data collection contract that specifies the data protection requirements and procedures for handling individually identifiable information (Appendix D).

The legal documents that bind the contracting firm, its representatives and staff to the terms of the Education Science Reform Act and/or the Confidential Information Protection and Statistical Efficiency Act and other relevant laws are included in the formal contract document that is executed between the Department of Education's Contracting Officer and the Contractor's representative; in addition, each staff member who will have any access to individually identifiable information during the normal course of their responsibilities on the contract is required to sign and have notarized a legally binding affidavit of nondisclosure committing them to the terms of the relevant confidentiality laws (please see Appendix D for information included in the contract and Appendix E for a copy of the Affidavit of Nondisclosure. As stated above, these contractor employees are also required under the contract to be approved to hold Public Trust positions). In the case of researcher agents, under the authorities previously granted the NCES Commissioner and now the IES Director, to employ the services of nongovernmental staff in fulfilling the agency's mission, NCES has issued restricted-use data licenses to qualified researchers since the early 1990's. To obtain a data license, an interested researcher must submit a formal request that explains why the public use data (if available) are not sufficient for their research needs, describes the research objectives and questions, variables to use, statistical analysis they want to conduct with the data, the audience to be served by the research, and specifies the time period for which they are requesting the data. The researcher is also required to submit a license document that is signed by the researcher and by a senior official from the

researcher's institution (the senior official must have the authority to legally bind the institution), a data security plan signed by the researcher, senior official and the designated security system officer, and signed and notarized affidavits of nondisclosure for each authorized user for the license (from 1 to 7).

The license and the affidavits of nondisclosure commit the researcher, the institution, and the authorized users to the confidentiality terms of the Education Sciences Reform Act, and to consent to participate in unannounced onsite security inspections to ensure compliance with the terms of the license and the submitted data security plan. The licensee also agrees to maintain a set of files that includes all related license documents. The researcher must submit an advance copy of any presentation or publication that uses the restricted data to the Data Security Program prior to release or publication for a disclosure review (every effort is made to conduct these reviews within 4 business days of receipt). Note, a key to data protection is the protection of unrounded unweighted sample size counts, thus all unweighted sample size numbers must be rounded to the nearest ten (nearest 50 for ECLS-B) prior to any dissemination to anyone not authorized to see the specific data.

The formal request application is in Appendix F, the license document is in Appendix G, and a copy of the security plan is in Appendix H. Note the procedures used in the Memorandum of Understanding that is used to provide access to NCES restricted use data to Federal employees in agencies outside of IES and to employees in State agencies mirror those included in the researcher license.

REPORTING REQUIREMENT: Physical and Information Systems Security—the number of off-site facilities that were inspected during the calendar year.
Researcher agents submit a data security plan that they agree to adhere to for the physical and electronic protection of NCES restricted use data. Consistent with the terms of the license (or MOU), researcher agents are subject to site inspections to ensure compliance with the terms of the license, including the data security plan. NCES contracts with an independent security firm that employs individuals with civilian or military law enforcement or related training to conduct security investigations. During calendar year 2020 there were 202 NCES licensees inspected. Insofar as many NCES licenses are issued for periods of 5 years, this number ensures that there is a high probability that each licensee will be inspected at least one time during the life of their data license or MOU with NCES.

REPORTING REQUIREMENT: Confidentiality Training—all agents are certified annually.
All contractor agents participate in confidentiality training and certification for each NCES data collection cycle. Since NCES data collection cycles are less than 12 months in duration, this training is equivalent to annual certification. In those cases where a contractor agent finishes one data collection and starts on a second data collection very soon, the training occurs more frequently than the annual requirement.

Researcher agents working off-site at their institutions or organizations are responsible for knowing and understanding the contents of the NCES Restricted Use Data Manual and the specific terms of their own license (or MOU), including their security plans. Researcher agents are also responsible for participating in online licensee security training and for maintaining an active license folder that includes their online licensee security training certificates and updates all correspondence with the

NCES Data Security Program to add or remove authorized users and to add or remove restricted use data files. The researcher agent is also responsible for ensuring that each authorized user on their license (or MOU) knows and understands the contents of the NCES restricted use data manual, the license documents, including the security plan, and any related materials. In 2006 and 2007, NCES converted the license application process from a pen and paper operation to an online system, requiring that only the license documents requiring signatures be transmitted in hard copy. As an additional step, in 2013, NCES updated the e-mail addresses for existing licensees, and continues to use this contact information to send licensees messages reminding them of the terms of their NCES restricted use data license.

REPORTING REQUIREMENT: Record Keeping—the agency has records that identify all agents with access to confidential information.
For contractor agents, each NCES contracting officer representative (COR) is responsible for maintaining a list of all contractor agents with signed and notarized affidavits of nondisclosure and for ensuring that they either hold or have access to the individual affidavits. NCES also maintains a database of all contractor agents who require approval to hold moderate- or high-risk Public Trust positions.

For researcher agents, the license documents include personally identifiable information on the licensee, and thus comprise a Federal system of records. Each researcher agent's summary record is maintained in a manipulable electronic data base. The original license documents and signed and notarized affidavits of nondisclosure are transferred to an electronic pdf file and are available online to the NCES Data Security staff. The original records are housed off site in a secure facility maintained by the NCES contracted security inspection firm. NCES maintains a database of all licensees and related authorized users.

In 2018, Congress enacted the Foundations of Evidence-Based Policymaking Act. As it relates to Confidential Information Protection, this 2018 Act transferred the Confidential Information (and Statistical Efficiency) Act (CIPSEA) from the 2002 E-Government Act to the Foundations of Evidence-Based Policymaking Act of 2018 and codified CIPSEA in a new subchapter III, of chapter 35 of title 44, United States Code. The Class E felony penalties for any willful disclosure of confidential information are unchanged.

Appendix A

Examples of Confidentiality Pledges for Data Collected Under CIPSEA (i.e., the Confidential Information Protection and Statistical Efficiency Act of 2018 (Title III, Public Law 115-435))

National Assessment of Educational Progress (NAEP)
NAEP 2021 eNAEP Pretesting and Usability Study
OMB No. 1850-0803

Taken from "Volume I-2021 eNAEP Pretesting Usability Study" with package date 04/28/2020:

> 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). The information [you/your child/each student - as applicable] provide[s] will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of the Foundations of Evidence-Based Policymaking Act of 2018, Title III, Part B, Confidential Information Protection and other applicable Federal laws, [your/your child's/each student's - as applicable] responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. 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 [you/your child/any student - as applicable]. Electronic submission of [your/your child's/each student's - as applicable] 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.

Appendix B

Examples of Data Protection Pledges for Data Collected Under ESRA (i.e., the Education Sciences Reform Act of 2002 (20 U.S.C. §9573))

Baccalaureate and Beyond Longitudinal Study (B&B)
B&B:16/20 Full-Scale Study Panel Maintenance
OMB No. 1850-0926

Taken from "Appendix C BB 2016-2020 FS Panel Maintenance Materials.docx" with package date 07/19/2019:

NCES is authorized to conduct B&B:16/17 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.

Baccalaureate and Beyond Longitudinal Study (B&B)
B&B:16/20 Full-Scale Study
OMB No. 1850-0926

Taken from Section A10 of Part A with package date 08/04/2020:

NCES is authorized to conduct the 2016/20 Baccalaureate and Beyond Longitudinal Study (B&B:16/20) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543) and to collect students' education records from educational agencies or institutions for the purpose 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).

Beginning Postsecondary Students Longitudinal Study (BPS)
2020/22 Beginning Postsecondary Students Longitudinal Study (BPS:20/22) Cognitive and Usability Testing Update
OMB No. 1850-0803

Taken from "Volume I BPS20-22 Cognitive Usability Testing" with package date 04/17/2020:

EurekaFacts, LLC and RTI International are carrying out this research for the National Center for Education Statistics (NCES), part of the U.S. Department of Education. NCES is authorized to conduct this study by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). 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).

Civil Rights Data Collection (CRDC)
CRDC Burden Research Study
OMB No. 1850-0803

Taken from "Appendix Recruitment Screener Questionnaire and Interview Protocol" with package date 11/06/2020:

Your participation is voluntary and 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).

Current Population Survey (CPS)
2020 CPS School Enrollment Cognitive Testing
OMB No. 1850-0803

Taken from "Att 1 CPS 2020 Cognitive Testing Communication Materials" with package date 05/21/2020:

Your participation is voluntary and 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). Your name will not be attached to the answers you provide.

Early Childhood Longitudinal Study (ECLS)
ECLS-K:2023 Preschool Field Test
OMB No. 1850-0750

Taken from Section A10 of Part A with package date 07/15/2020:

NCES is authorized to conduct the Early Childhood Longitudinal Study, Kindergarten Class of 2022-23 (ECLS-K:2023) 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 Westat, a U.S.-based research organization. All of the information [*respondent type*] 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). [The collected information will be combined across respondents to produce statistical reports.]

Early Childhood Longitudinal Study (ECLS)

Early Childhood Longitudinal Study (ECLS)
ECLS-K:2023 Kindergarten-First Grade Field Test Instruments Usability Testing
OMB No. 1850-0803

Taken from "Volume 1 ECLS-K2023 K-1 FT Instruments Usability" with package date 01/11/2021:

The National Center for Education Statistics (NCES) is authorized to conduct the Early Childhood Longitudinal Study (ECLS) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). The data are being collected for NCES by Westat, a U.S.-based 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).

Early Childhood Longitudinal Study (ECLS)
ECLS-K:2023 Focus Groups with School Administrators, Teachers, and Parents
OMB No. 1850-0803

Taken from "Volume 1 ECLS-K2023 FG with Admin Teachers Parents" with package date 03/26/2020:

The National Center for Education Statistics (NCES) is authorized to conduct the Early Childhood Longitudinal Study (ECLS) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). The data are being collected for NCES by Westat, a U.S.-based 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).

Fast Response Survey System (FRSS)
FRSS 110: Use of Educational Technology for Instruction in Public Schools
OMB No. 1850-0733

Taken from "Vol 1 FRSS 110 Instructional Technology Use" with package date 10/28/19:

NCES is authorized to conduct this study by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). While participation in this survey is voluntary, your cooperation is critical to make the results of this survey comprehensive, accurate, and timely. 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).

High School and Beyond (HS&B)
HS&B:20 Base-Year Field Test
HS&B:20 Base-Year Full-Scale Study
OMB No. 1850-0944

Taken from Section A10 of Part A with package date 04/22/2020:

NCES is authorized to conduct the High School and Beyond 2020 (HS&B:20) 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 [respondent type] 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). The collected information will be combined across respondents to produce statistical reports.

High School and Beyond (HS&B)
HS&B:22 Base-Year Field Test
HS&B:22 Base-Year Full-Scale Study
OMB No. 1850-0944

Taken from Section A10 of Part A with package date 11/23/2020:

NCES is authorized to conduct the High School and Beyond 2020 (HS&B:20) 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 [respondent type] 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). The collected information will be combined across respondents to produce statistical reports.

High School and Beyond (HS&B)
HS&B:20 Cognitive and Usability Testing Round 2
OMB No. 1850-0803

Taken from "Volume 1 HS&B 2020 Cog Labs Round 2.docx" with package date 09/09/2019:

EurekaFacts, LLC is carrying out this research for the National Center for Education Statistics (NCES), part of the U.S. Department of Education. NCES is authorized to conduct this study by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). 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).

Middle Grades Longitudinal Study of 2017–18 (MGLS:2017)
MGLS:2017 Main Study First Follow-up (MS2) – Tracking and Recruitment
MGLS:2017 Main Study First Follow-up (MS2)
OMB No. 1850-0911

Taken from Section A10 of Part A with package date 5/22/2020:

NCES is authorized to conduct MGLS:2017 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/ you and your child/respondents/schools/ schools and students} provide/ provided by schools, staff, students, and parents] 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). The collected information will be combined across respondents to produce statistical reports.

National Assessment of Educational Progress (NAEP)
NAEP 2020
NAEP 2020 Pilot DBA for 2021 Mathematics, Grades 4 and 8
NAEP 2020 Pilot DBA for 2021 Writing, Grades 4, 8, and 12
NAEP 2020 Pilot DBA for 2022 U.S. History, Civics, and Geography, Grade 8
NAEP 2020 Pilot DBA for 2022 U.S. History, Civics, Geography, and Economics, Grade 12
NAEP 2020 Pilot DBA for 2022 TEL, Grades 8 and 12
NAEP 2021
OMB No. 1850-0928

Taken from Section A10 of Part A with package date 02/20/2019:

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 participants. Electronic submission of participant'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.

National Assessment of Educational Progress (NAEP)
NAEP 2020 Operational national PBA Long-Term Trend (LTT)
OMB No. 1850-0928

Taken from Section A10 of Part A with package date 08/29/2019:

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 participants. Electronic submission of participant'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.

National Assessment of Educational Progress (NAEP)
2023 NAEP Family Structure Study
OMB No. 1850-0803

Taken from "Family Structure Volume I" with package date 12/09/2020:

The study will not retain any personally identifiable information. Prior to the start of the study, students will be notified that their participation is voluntary. As part of the study, students will be notified that the information they 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).

National Assessment of Educational Progress (NAEP)
NAEP Survey Assessments Innovation Lab (SAIL) Test Assembly Experimental Study
OMB No. 1850-0803

Taken from "Volume I NAEP SAIL Test Assembly" with package date 09/11/2020:

The study will not retain any personally identifiable information. Prior to the start of the study, students will be notified that their participation is voluntary. As part of the study, students will be notified that the information they 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).

National Assessment of Educational Progress (NAEP)
NAEP 2021 COVID-19 Educational Experiences Student, Teacher, and School Administrator Pretesting
OMB No. 1850-0803

Taken from "Volume I NAEP 2021 COVID19 SQ Pretesting" with package date 6/12/2020:

The study will not retain any personally identifiable information. Prior to the start of the study, students will be notified that their participation is voluntary. As part of the study, students will be notified that the information they 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).

National Assessment of Educational Progress (NAEP)
NAEP Engagement Augmentation Study
OMB No. 1850-0803

Taken from "Appendix NAEP Engagement Study Recruitment and Comms materials" with package date 12/07/2020:

The 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). 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 participants. Electronic submission of participant'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.

National Household Education Surveys (NHES)
2022 NHES English and Spanish Cognitive Interviews
OMB No. 1850-0803

Taken from "Attachment 1 NHES 2022 PFI ECPP Cog Labs Communication Materials and Consent" with package date 05/07/2020:

NCES is authorized to conduct this study by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C., § 9543). This cognitive interview has been approved by the Office of Management and Budget (OMB# 1850-0803). All 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).

National Household Education Surveys (NHES)
2022 NHES Web Usability Testing
OMB No. 1850-0803

Taken from "Att 1 NHES 2022 Usability Testing Communication Materials" with package date 04/21/2020:

You have volunteered to take part in a usability test of the National Household and Education Survey (NHES). The Census Bureau is administering the NHES usability testing on behalf of the National Center of Education Statistics (NCES), within the U.S. Department of Education. NCES is authorized to conduct this study by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C., § 9543).

National Postsecondary Student Aid Study (NPSAS)
NPSAS:20 Institution Collection
OMB No. 1850-0666

Taken from Section A10 of Part A with package date 9/18/2019:

NCES is authorized to conduct the 2019–20 National Postsecondary Student Aid Study (NPSAS:20) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543) and the Higher Education Opportunity Act of 2008 (HEOA 2008, 20 U.S.C. §1015). 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).

The Family Educational Rights and Privacy Act of 1974 (FERPA, 20 U.S.C. §1232g) allows for the release of institution record information to the Secretary of Education or her agent without prior consent of survey members (34 CFR §§ 99.31(a)(3)(iii) and 99.35).

National Postsecondary Student Aid Study (NPSAS)
NPSAS:20
OMB No. 1850-0666

Taken from Section A10 of Part A with package date 11/18/2020:

NCES is authorized to conduct the 2019–20 National Postsecondary Student Aid Study (NPSAS:20) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543) and the Higher Education Opportunity Act of 2008 (HEOA 2008, 20 U.S.C. §1015). 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).

The Family Educational Rights and Privacy Act of 1974 (FERPA, 20 U.S.C. §1232g) allows for the release of institution record information to the Secretary of Education or her agent without prior consent of survey members (34 CFR §§ 99.31(a)(3)(iii) and 99.35).

National Teacher and Principal Survey (NTPS)
NTPS 2020–21 Preliminary Activities
OMB No. 1850-0598

Taken from Section A10 of Part A with package date 11/12/2019:

The National Center for Education Statistics (NCES), within the U.S. Department of Education, conducts NTPS as authorized by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). 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).

National Teacher and Principal Survey (NTPS)
NTPS 2020–21
OMB No. 1850-0598

Taken from Section A10 of Part A with package date 06/15/2020:

The National Center for Education Statistics (NCES), within the U.S. Department of Education, conducts NTPS as authorized by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543). 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).

National Teacher and Principal Survey (NTPS)
2020-2021 NTPS Cognitive Interviews
OMB No. 1850-0803

Taken from "Attachment 1-4 - NTPS 2020-2021 Cognitive Interviews Recruitment & Screeners" with package date 11/29/2019:

Your participation is voluntary and 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). Your name will not be attached to the answers you provide.

National Teacher and Principal Survey (NTPS)
2020-21 NTPS 2020–21 Teacher and Principal Follow Up Survey Cognitive Testing
OMB No. 1850-0803

Taken from "Attachment 1 Communication Materials Screener Consent-OMB_11.18.20 (clean)" with package date 11/19/2020:

The U.S. Census Bureau is required by law to protect your information. We are conducting this voluntary survey on behalf of the National Center for Education Statistics under the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C., § 9543). 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).

National Teacher and Principal Survey (NTPS)
NTPS 2020–21 Testing Questions on the Teacher Questionnaire on Sexual Orientation and Gender Identity (SOGI), and Branding Changes
OMB No. 1850-0803

Taken from "NTPS 0803 v.277 Volume I 11.3" with package date 11/13/2020:

The National Center for Education Statistics (NCES), within the U.S. Department of Education, conducts NTPS as authorized by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543).
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).

Progress in International Reading Literacy Study (PIRLS)
PIRLS 2021 Field Test Recruitment
OMB No. 1850-0645

Taken from Section A.10 of Part A with a package date of 9/30/2019:

The National Center for Education Statistics (NCES) is authorized to conduct this study under the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543), and to collect students' education records from educational agencies or institutions for the purpose 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 [you provide/ provided by school staff and students] 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). In the United States, PIRLS is conducted by NCES, part of the U.S. Department of Education, and the data are being collected by Westat. The U.S. Office of Management and Budget has approved the data collection under OMB # 1850-0645.

Progress in International Reading Literacy Study (PIRLS)
PIRLS 2021 Main Study Recruitment and Field Test
OMB No. 1850-0645

Taken from Section A.10 of Part A with a package date of 10/16/2019:

The National Center for Education Statistics (NCES) is authorized to conduct this study under the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543), and to collect students' education records from educational agencies or institutions for the purpose 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 [you provide/ provided by school staff and students] 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). In the United States, PIRLS is conducted by NCES, part of the U.S. Department of Education, and the data are being collected by Westat. The U.S. Office of Management and Budget has approved the data collection under OMB # 1850-0645.

Progress in International Reading Literacy Study (PIRLS)
PIRLS 2021 Main Study Data Collection
OMB No. 1850-0645

Taken from Section A.10 of Part A with a package date of 11/19/2020:

The National Center for Education Statistics (NCES) is authorized to conduct this study under the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543), and to collect students' education records from educational agencies or institutions for the purpose 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 [you provide/ provided by school staff and students] 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). In the United States, PIRLS is conducted by NCES, part of the U.S. Department of Education, and the data are being collected by Westat. The U.S. Office of Management and Budget has approved the data collection under OMB # 1850-0645.

Progress in International Reading Literacy Study (PIRLS)
PIRLS 2021 Field Test Pretest
OMB No. 1850-0803

Taken from "Appendices PIRLS 2021 FT Pretest.docx" with package date 10/31/2019:

The National Center for Education Statistics (NCES) is authorized to conduct this study under the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543), and to collect students' education records from educational agencies or institutions for the purpose 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 school staff and students 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). In the United States, PIRLS is conducted by NCES, part of the U.S. Department of Education, and the data are being collected by Westat. The U.S. Office of Management and Budget has approved the data collection under OMB # 1850-0803.

Program for International Student Assessment (PISA)
PISA 2021 Main Study Recruitment and Field Test
OMB No. 1850-0755

Taken from Section A.10 of Part A with a package date of 12/23/2019:

The National Center for Education Statistics (NCES) is authorized to conduct the Program for International Student Assessment (PISA) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543), and to collect students' education records from educational agencies or institutions for the purpose 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 Westat, a U.S.-based 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).

Program for International Student Assessment (PISA)
PISA 2021 Field Test Pretest

OMB No. 1850-0803

Taken from "Appendices PISA 2021 FT Pretest.docx" with package date 11/19/2019:

The National Center for Education Statistics (NCES) is authorized to conduct the Program for International Student Assessment (PISA) by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543), and to collect students' education records from educational agencies or institutions for the purpose 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 Westat, a U.S.-based 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).

School Survey on Crime and Safety (SSOCS)
SSOCS 2020
OMB No. 1850-0761

Taken from Section A.10 of Part A with a package date of 06/09/2020:

The National Center for Education Statistics (NCES), within the U.S. Department of Education, conducts SSOCS as authorized by the Education Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543).
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).

School Survey of Crime and Safety (SSOCS)
SSOCS Incident Count Check Cognitive Interviews
OMB No. 1850-0803

Taken from "Volume 1 SSOCS-CRDC Incident Count Cognitive Interviews.docx" with package date 02/04/2020:

All 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).

Trends in International Mathematics and Science Study (TIMSS)
TIMSS 2023 Cognitive Interviews
OMB No. 1850-0803

Taken from "Appendix TIMSS 2023 Cog Labs_OMB updated" with package date 10/15/2020:

The National Center for Education Statistics (NCES), within the U.S. Department of Education, conducts TIMSS in the United Status as authorized by the Education Sciences Reform Act of 2002

(ESRA 2002, 20 U.S.C. §9543). 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).

Appendix C

Excerpted from Checklist of SOW Requirements for Data Collection and Processing Contracts

This checklist serves as a guide to ensure all necessary contract language is included in data collection and processing contracts. A page number is given for each item and provides the location of the general boilerplate language. Check to ensure your contract has these requirements:

✓	Contract Language Requirement	Page
	Overview of IES Confidentiality Statute	
	Data Security Plan	
	Adherence to NCES Statistical Standards	
	Quality Control Measures	
	Contractor Employee Security Screening	
	Requirement of Affidavit of Nondisclosure	
	Security and Confidentiality Training for Contractor Staff	
	Information Collection Request (ICR) Requirement	

There are other special contract requirements with specific language. The contracting office usually provides the language for these other requirements. Check to ensure that the following special contract requirements will be included in your contract:

- ✓ Department Security Requirements (307-13)
- ✓ Privacy Act Notification (52.224-1)
- ✓ Compliance with Privacy Act (52.224-2)
- ✓ Privacy or Security Safeguards (52.239-1)
- ✓ Rights in Data - Special Works (52.227-17)

Appendix D

Data Confidentiality, Data Security Plan, and Affidavit of Nondisclosure, and Contractor Employee Security Screening Requirements

Standard Contract Language – Section B

B.1 Confidentiality of Individuals and Institutions

NCES assures participating individuals and institutions that any data collected conforms to the IES standards for protecting the privacy of individuals as required by 20 U.S.C., § 9573:

> ". . . all collection, maintenance, use, and wide dissemination of data by the Institute, including each office, board, committee, and Center of the Institute, shall conform with the requirements of section 552A of Title 5, United States Code [which protects the confidentiality rights of individual respondents with regard to the data collected, reported, and published under this title]." (20 U.S.C., § 9573)

Under the Education Sciences Reform Act of 2002 (ESRA 2002), all individually identifiable information about students, their families, and their schools shall remain confidential. To this end, this law requires that no person may:

- Use any individually identifiable information furnished under the provisions of this section for any purpose other than statistical purposes for which it is supplied, except in the case of terrorism;
- Make any publication whereby the data furnished by any particular person under this section can be identified; or
- Permit anyone other than the individuals authorized by the Commissioner to examine individual reports.

Further, individually identifiable information is immune from legal process, and shall not, without the consent of the individual concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding, except in the case of terrorism. Employees, including temporary employees, or other persons who have sworn to observe the limitations imposed by this law, who knowingly publish or communicate any individually identifiable information will be subject to fines of up to $250,000 or up to 5 years in prison, or both (Class E felony).

B.2 Information Collection Request (ICR)

All respondents asked to participate in data collection initiatives shall be informed of the following:

- NCES enabling legislation which authorizes the information collection,
- purposes for which the information is needed,
- uses that may be made of the information,
- that data will not be reported in a way to reveal individual responses,

- participation is voluntary, and
- no adverse action will result if the requested information is not provided.

Survey respondents, if they so request, must be given access to their records and be permitted to amend their responses.

B.3 Protection and Security of Data

The confidentiality of individually identifiable information contained in project documents, data, and other information supplied by the National Center for Education Statistics, U.S. Department of Education (NCES/ED) or information acquired in the course of performance under this contract where the information was furnished under the provisions of 20 U.S.C., § 9573 is a material aspect of the contract and must be maintained, secured, and protected from disclosure as provided in 20 U.S.C., § 9573. The Privacy Act of 1974 (5 U.S.C. 552a) also applies.

The contractor shall enforce strict procedures for assuring confidentiality. These procedures shall apply to all phases of the project and should include but not be limited to: information used to locate study respondents, data collection in the field, coding and editing phases of data prior to machine processing, safeguarding response documents, and maintenance of any respondent follow-up information. Contractor shall physically separate the identifying data required for any follow-up from data required for research purposes.

The contractor shall be familiar with and comply with:

1) The Privacy Act of 1974 (5 U.S.C. 552a),
2) Confidential Information Protection and Statistical Efficiency Act (CIPSEA), Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.)
3) Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g; 34 CFR Part 99),
4) The Freedom of Information Act (5 U.S.C. 552),
5) The Education Sciences Reform Act of 2002 (20 U.S.C., § 9573),
6) No Child Left Behind Act (20 U.S.C. 70),
7) USA Patriot Act of 2001 (P.L. 107-56),
8) Office of Management and Budget (OMB) Federal Statistical Confidentiality Order of 1997,
9) OMB Guidance of 7/12/2006 on the Reporting of Incidents Involving Personally Identifiable Information (M-06-19), http://www.whitehouse.gov/OMB/memoranda/fy2006/mo6-19.pdf ,
10) OMB Guidance of 5/22/2006 on Safeguarding Personally Identifiable Information (M- 06-15) http://www/whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf,
11) Federal Information Security Modernization Act (FISMA) of 2014 (P.L. 107-347, Title III),
12) Any new legislation that impacts the data collection through this contract.

The contractor shall maintain the confidentiality of all documents, data, and other information

supplied by NCES/ED or acquired in the course of performance of this contract, except for any documents or other information specifically designated as non-confidential by NCES/ED. The contractor shall take such measures as are necessary to maintain the required security and protection of confidential information (see section Data Security Plan). The contractor shall be prepared to develop compliance procedures in cooperation with the COR concurrently with the development of the study design.

B.4 Data Security Plan

B.4a Definition of Personally Identifiable Information and Direct Identifiers

The term "personally identifiable information" (hereinafter PII) means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. The term "direct identifier" denotes any single datum that alone is deemed sufficient to yield a high risk of disclosure if released, such as social security numbers, full names, or biometric records.

B.4b Development of Data Security Plan

The contractor shall present a detailed security plan that expands upon what was presented in the proposal to the COR for approval. In order to ensure the anonymity of individual respondents, the contractor must draft and execute this plan in compliance with all relevant laws, regulations, and policies governing the security of data, particularly PII. These include (but are not limited to):

1) 20 U.S.C., § 9573 of the Education Sciences Reform Act of 2002, which states:
   (a) IN GENERAL - All collection, maintenance, use, and wide dissemination of data by the Institute, including each office, board, committee, and center of the Institute, shall conform with the requirements of section 552a of title 5, United States Code, the confidentiality standards of subsection (c) of this section, and sections 444 and 445 of the General Education Provisions Act (20 U.S.C. 1232g, 1232h).
   (b) STUDENT INFORMATION - The Director shall ensure that all individually identifiable information about students, their academic achievements, their families, and information with respect to individual schools, shall remain confidential in accordance with section 552a of title 5, United States Code, the confidentiality standards of subsection (c) of this section, and sections 444 and 445 of the General Education Provisions Act (20 U.S.C. 1232g, 1232h);
2) The Privacy Act of 1974 (5 U.S.C. 552a);
3) The E-Government Act of 2002 (P.L. 107-347);
4) The Foundations of Evidence-Based Policymaking Act of 2018 (P.L. 115-435);
5) The relevant sections of Title 34 of the Code of Federal Regulations entitled "Protection of Human Subjects" (34 CFR 97);
6) The U. S. Department of Education OCIO-1 Handbook for Information Assurance Security Policy (January 2009);

7) Office of Management and Budget Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost of Security in Agency Information Technology Investments";
8) OMB Guidance of 7/12/2006 on the Reporting of Incidents Involving Personally Identifiable Information (M-06-19).

The data security plan will, at a minimum, cover the following issues: the transfer/transport of PII, maintenance, storage, and use of direct identifiers, replacement of direct identifiers with internal codes, security of master survey files, security and confidentiality training for contractor staff, and reporting of data security breaches. Hence, the data security plan shall be written to place particular emphasis on the following aspects of confidentiality and security:

B.4c Guidelines for Transfer of PII

As a general principle, the physical and/or electronic transfer of PII (particularly direct identifiers) shall be limited to the extent practicable. This limitation includes both internal transfers (e.g., transfer of information between agents of the contractor, including subcontractors and/or field workers) and external transfers (e.g., transfers between the contractor and the agency, or between the contractor and another government agency or private entity assisting in data collection).

When it is necessary for the contractor to transfer PII, such transfer must occur in a manner that maximizes the security of information. The data security plan must describe the likely modes of data transfer and establish the most secure procedures practicable. The most secure method of transferring sensitive information is not necessarily the most efficient or convenient one.

- The preferred means of transferring PII (and particularly direct identifiers) is electronic transfer with 128-bit secure sockets layer (SSL) encryption.
- If electronic PII is transferred via physical media (e.g., a CD-ROM or DVD-ROM is created and sent via courier service or mail), all files on the media shall be encrypted (FIPS 140-2 standard) with a strong password (e.g., a random string of letters and numbers) and this password shall be sent separately from the data. In addition, no obvious external markings or information identifying the media as containing PII shall be written, stamped, or otherwise inscribed on the media or its packing material.
- If paper records or files must be transferred, then the contractor and its agents should hand carry these documents for delivery. Shipping or mailing these kinds of documents should be avoided. The contractor should clearly state in their data security plan if this requirement cannot be met. The data security plan should describe all transfers of paper records or files and how they will be secured. If these documents must be shipped/mailed, the contractor and its agents should avoid transferring multiple direct identifiers in the same shipment. For example, a mailing containing the names, addresses, and social security numbers of subjects is less secure than two mailings: one shipment with the names and addresses and a second shipment with the social security numbers and no additional information. Alternatively, a partial mailing of data could be followed up with a telephone call (for smaller amounts of PII) which provides the remainder of the data verbally. Any shipment sent must have a tracking number. As above, no obvious external markings or information identifying the mailing as containing PII shall be written, stamped, or otherwise inscribed on the packing material.

B.4d Maintenance, Storage, and Use of Direct Identifiers

Under no circumstances may the contractor release PII to unauthorized individuals. In addition, direct identifiers must be maintained in files which are physically separate from other research data, and which are accessible only to sworn agency and contractor personnel. Individual direct identifiers used during the course of the project shall be associated with data only for statistical purposes such as data gathering, matching new data with old, establishing sample composition, authenticating data collections, editing data based on callbacks, or obtaining missing information.

As a general principal, the number of personnel with access to PII (and particularly direct identifiers) shall be restricted to the smallest number as possible.

B.4e Replacement of Direct Identifiers with Internal Codes

Although direct identifying information is often required in the data collection process, to the extent practicable the contractor shall use internally generated identifying codes to track subjects in data files. Whenever possible, the transfer and storage of files containing multiple direct identifiers should be avoided. If the transfer of direct identifiers is required for statistical purposes such as data matching, the minimum number of direct identifiers needed for successful matching shall be used.

B.4f Security of Master Survey Files

The contractor shall maintain security on the complete set (and deliverable backups) of all master survey files and documentation.

B.4g Compliance with Department of Education IT Security Policy

The contractor, and all sub-contractors, shall comply with the Department of Education's IT security policy requirements, and other applicable procedures and guidance. The contractor, and all sub-contractors, shall develop and implement management, operational and technical security controls to assure required levels of protection for information systems. The contractor, and all sub-contractors, shall further comply with all applicable Federal IT security requirements including, but not limited to, the Federal Information Security Modernization Act (FISMA) of 2014, Office of Management and Budget (OMB) Circular A-130, Homeland Security Presidential Directives (HSPD), including HSPD-12, Personal Identity Verification (PIV) Enablement and Integration, and single sign-on, the most recent National Institute of Standards and Technology (NIST) special publications, standards and guidance, and the Federal Risk and Authorization Management Program (FedRAMP) requirements and guidance.

These security requirements include, but are not limited to, the successful Security Assessment and Authorization (SA&A) of the system (includes commercially owned and operated systems managed by the commercial vendor and its sub-contractors, supporting Department programs, contracts, and projects); obtaining a full Authority to Operate (ATO) before being granted operational status; performance of annual self-assessments of security controls; annual Contingency Plan testing; performance of periodic vulnerability scans; updating all information system security documentation as changes occur; and other continuous monitoring activities, which may include, mapping, penetration and other intrusive scanning. Full and unfettered access for any of the Department's third-party Managed Security Services Provider (MSSP) or Cyber-operations prevention testers, or vulnerability scanners, or auditors must be granted to access all computers and networks used for this system. Additionally, when there is a significant change to the system's security posture, the system

(Federal and commercial prime- and sub- contractors included) must have a new SA&A, with all required activities to obtain a new ATO, signed by the Authorizing Official (AO).

System security controls shall be designed and implemented consistent with the current, finalized version of the NIST SP 800-53, 'Recommended Security Controls for Federal Information Systems and Organizations.' All NIST SP 800-53 controls must be tested / assessed no less than every 3 years, according to federal and Department policy. The risk impact level of the system will be determined via the completion of the Department's inventory form and shall meet the accurate depiction of security categorization as outlined in Federal Information Publishing Standards (FIPS) 199, 'Standards for Security Categorization of Federal Information and Information Systems.'

System security documentation shall be developed to record and support the implementation of the security controls for the system. This documentation shall be maintained for the life of the system. The contractor, and all sub-contractors, shall review and update the system security documentation at least annually and after significant changes to the system, to ensure the relevance and accurate depiction of the implemented system controls and to reflect changes to the system and its environment of operation. Security documentation must be developed in accordance with the NIST 800 series and Department of Education policy and guidance.

The contractor, and all sub-contractors, shall allow Department employees (or Department designated third party contractors) access to the hosting facility to conduct SA&A activities to include control reviews in accordance with the current, finalized version of the NIST SP 800-53, and the current, finalized version of the NIST SP 800-53A. The contractor, and all sub-contractors, shall be available for interviews and demonstrations of security control compliance to support the SA process and continuous monitoring of system security. In addition, if the system is rated as 'Moderate' or 'High' for FIPS 199 risk impact, vulnerability scanning and penetration testing shall be performed on the hosting facility and application as part of the SA&A process. Appropriate access agreements will be reviewed and signed before any scanning or testing occurs.

Identified deficiencies between required security controls within the current, finalized version of the NIST SP 800-53 and the contractor's, and all sub-contractor's implementation, as documented in the Risk Assessment Report, System Security Plan (SSP) and Security Assessment Report (SAR), shall be tracked for mitigation through the development of a Plan of Action and Milestones (POA&M) in accordance with Department policy. Depending on the severity of the deficiencies, the Department may require remediation before an ATO is issued.

The contactor shall provide cybersecurity strategies, infrastructure hosting environments, and solutions that comply with the requirements of the Federal Information Security Modernization Act (FISMA), Department cybersecurity policy guidance, and guidance contained in the NIST Special Publications series such as NIST Special Publication 800-53 and other NIST Special Publications. The contractor shall provide solutions that support the Department's efforts to implement and maintain effective protection activities such as reducing the attack surface and complexity of IT infrastructure; minimizing the use of administrative privileges; utilizing strong authentication credentials; safeguarding data at rest and in-transit; training personnel; ensuring repeatable processes and procedures; adopting innovative and modern technology; ensuring strict domain separation of critical/sensitive information and information systems; implementing network segmentation

architectures to better protect and isolate the Department's high value assets and most sensitive information and data; and ensuring a current inventory of hardware and software components. The contractor shall include actions and initiatives to implement the NIST Cybersecurity Framework that emphasizes and measures capabilities to "Identify, Protect, Detect, Respond, and Recover," and ensure that all applicable Service Level Agreements (SLA)s are adhered to, complied with, and satisfied.

The contractor shall ensure that:

1. Their IT product/system is monitored during all hours of operations using entrusted detective/preventive systems;
2. Their IT product/system has current antiviral products installed and operational;
3. Their IT product/system is scanned on a reoccurring basis;
4. Vulnerabilities are remediated in a timely manner on their IT product/system; and
5. Access/view for cyber security situational awareness on their IT product/system is made available to the Department CIRC (cyber incident response capability).
6. All applicable Service Level Agreements (SLA)s are adhered to, complied with, and satisfied.

For IPv6, the contractor shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are:

- An IPv6 capable system that meets the IPv6 base requirements defined by the USGv6 Profile (http://www.antd.nist.gov/usgv6/profile.html).
- Systems being developed, procured, or acquired shall maintain interoperability with IPv4 systems/capabilities.
- Systems shall implement IPv4/IPv6 dual-stack and shall also be built to determine which protocol layer to use depending on the destination host it is attempting to communicate with or establish a socket with. If either protocol is possible, systems shall employ IPv6.

The contractor shall provide IPv6 technical support for system development, implementation, and management.

In accord with OMB Memorandums M-17-06, and M-15-13, and M-08-23, and with the NIST SP 800-44, all Federal websites and web services must be accessible through a secure connection (HTTPS only, with HSTS), and e-mail applications must have SMTP enabled. The use of HTTPS is encouraged on intranets, but not explicitly required. In accord with OMB Memorandum M-08-23, in order to ensure Domain Name System Security (DNSSEC), it is recommended that all federal websites be hosted on a *.gov location. In accord with OMB Memorandum M-17-06, each agency must use only an approved .gov or .mil domain for its official public-facing websites. The requirement to use only approved government domains does not apply in circumstances where the agency is a user or a customer of a third-party website or service that resides on a non-governmental domain. If a cloud solution will be used, then an ED-issued, FedRAMP-Compliant ATO is a Federal and a Departmental requirement, and it is recommended that one be obtained. Only FedRAMP-approved cloud solutions can be used. The contractor must implement controls to ensure that all

publicly accessible, externally hosted Department websites and web services only provide service through a secure connection, (such as the Hypertext Transfer Protocol Secure (HTTPS)).

B.4h Security of PII and Reporting of Data Security Breaches

If there is a suspected or known breach/disclosure of PII due to lost, theft, intercepted transfer, or other, the contractor must ensure that this breach is reported to the agency as soon as the contractor has knowledge of it. Per Office of Management and Budget Memorandum M-17-12, Federal agencies have a requirement to report breaches of PII security to the United States Computer Emergency Response Team (US-CERT)." The (PO) must notify the department within 30 minutes of discovering the incident (and the agency should not distinguish between suspected or confirmed breaches). The data security plan must be written to reflect this requirement, and the contractor must provide sufficient notification and documentation of the suspected loss, as it is understood at the time of notification to the agency for this requirement to be met. Follow-up reports of the final status of loss events will also be prepared by the contractor within a reasonable period of time as advised by the COR.

- The contractor shall cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.

- The contractor and subcontractors (at any tier) shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies and to comply with any agency-specific policies for protecting PII, with required security measures implemented for both office equipment as well as instruments/devices used in the field for data collection;

- The contractor shall complete regular Department training for contractors and subcontractors (at any tier) on how to identify and report a breach;

- The contractor and subcontractors (at any tier) shall report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;

- The contractor and subcontractors (at any tier) shall maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;

- The contractor shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Federal and Department PII Breach Response policies (such as OMB-M-17-12), the Department's breach response plan, and to assist with responding to a breach;

- The contractor shall identify roles and responsibilities, in accordance with Federal and Department PII Breach Response policies (such as OMB-M-17-12), and the agency's breach response plan; and,

- The contractor shall be aware that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

B.4i Websites

For requirements involving web applications, web servers, and web services, the contractor shall follow the policies, principles, standards, and guidelines on information security and privacy, in accordance with FISMA, and implement security and privacy requirements as set forth in OMB Circular A-130 and National Institute of Standards and Technology (NIST) Special Publication 800-44, Guidelines on Securing Public Web Servers.

The public expects Federal Government websites to be secure and their interactions with those websites to be private. The contractor shall comply with requirements specified in OMB Memorandum M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services, that requires that all publicly accessible Federal websites and web services only provide service through a secure connection (HTTPS with HSTS).

The contractor shall use only an approved .gov or .mil domain for official public-facing websites. The requirement to use only approved government domains does not apply in circumstances where the Department is a user or a customer of a third-party website or service that resides on a non-governmental domain. Department use of third-party websites and applications must comply with all relevant privacy protection requirements and a careful analysis of privacy implications as specified in OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites.

With respect to web Security, in accord with BOD-18-01, all publicly accessible Federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS); SSLv2 and SSLv3 are disabled on web servers, and DES and RC4 ciphers are disabled on web servers; and must provide a list to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains.

If an official public-facing website will be developed, modified, or maintained, then, in accord with OMB Memorandum M-17-06, each agency must use only an approved .gov or .mil domain for its official public-facing websites. The requirement to use only approved government domains does not apply in circumstances where the agency is a user or a customer of a third-party website or service that resides on a non-governmental domain.

All applicable web hosting for Information dissemination websites shall follow ACS OCIO 3-110 - Department Web Consolidation (https://connected.ed.gov/Documents/Department_Web_Consolidation.pdf).

A ".gov" hostname (typically hostname.ed.gov) is required for all government funded websites under OMB Memorandum M-05-04 (http://www.usa.gov/webcontent/regs_bestpractices/omb_policies/domains.shtml).

B.4j Freedom of Information Act (FOIA) Requests

If the contractor receives a FOIA request for any data under this contract, then the contractor will immediately refer this request to the COR. NCES will process all FOIA requests related to this contract.

B.4k Implementation of Data Security Plan

The contractor shall conform to the agreed-upon approved data security plan, in all activities, and shall strictly enforce all procedures for ensuring confidentiality. These procedures will apply to all phases of the project, including (but not limited to):

1) Data collection in the field;
2) The transfer or transport of PII in any format, including paper records and electronic data files;
3) Coding and editing phases of data prior to machine processing; and,
4) Safeguarding and storage of master data files and response/collection documents and electronic files.

To monitor compliance with the data security plan during data collection period, the contractor shall submit monthly timelines and data receipt reports that identify (1) the percent of cases transmitted within the target time; (2) the percent of cases received within the target time (paper); and (3) any outliers (e.g.: missing transmissions) and their causes with recommendations for solutions to be implemented in the next reporting period.

B.4l Security and Confidentiality Training

During the course of work on the tasks in this contract, contractor employees will be collecting, storing, editing, and otherwise handling data that are confidential. Given the restrictions on the use and handling of confidential information, all contractor employees with access to confidential information related to this contract shall be required to participate in NCES approved security and confidentiality training.

B.4m Affidavit of Nondisclosure

Any contractor employee needing access to confidential information under this contract shall first sign an Affidavit of Nondisclosure. Before any contractor employee starts work on the contract and has access to confidential information, a signed Affidavit of Nondisclosure must be completed. As new staff start and require access to confidential information or as staff who originally did not require such access subsequently need it, an Affidavit of Nondisclosure shall be executed for them on the first working day of the assignment. The contractor shall indicate the position in the organization of the person signing the Affidavit of Nondisclosure, and the person's functional relationship to this project in a memorandum provided to the COR.

The contractor shall execute these Affidavits of Nondisclosure and the contractor shall maintain the originals at its office. The contractor shall make Acrobat pdf copies of new Affidavits as they are completed. Throughout the life of the contract, the memorandum and Affidavits of Nondisclosure for new project staff, as well as interviewers and other short-term personnel, will be submitted on a schedule designated by the COR or, at a minimum, three times a year. The contractor shall be able to produce the original hard copies of the Affidavits within a few hours' notice from the COR. The NCES data security officer can provide blank copies of the Affidavits upon request.

B.4n Contractor Employee Security Screening Requirements for Public Trust positions

The Department has established policy on personnel security screening for all contractor and subcontractor employees and their field staff. The relevant Departmental Directive is OM:5-101. It was last updated in July 2010 and can be found at: http://www2.ed.gov/policy/gen/leg/foia/acsom5101.pdf. The contractor must comply with the personnel security-screening requirements in OM:5-101 throughout the life of the contract.

All contractor and subcontractor employees must undergo personnel security screening if they will be employed for thirty (30) days or more.

The type of screening and the timing of the screening will depend upon the nature of the contractor position, the type of data the contractor employee will have access to, or the type of Departmental information technology (IT) system they will access. Personnel security screenings will be commensurate with the risk and magnitude of harm the individual could cause to the Department or the public. A position risk level will be assigned to each contractor employee position, before a solicitation is released, consistent with the descriptions in Appendix I of OM:5-101. Hence, each contractor employee working on this contract must be assigned a position risk level. Depending on the risk level assigned to each person's position, a follow-up background investigation by the Office of Personnel Management (OPM) may occur.

The contractor must identify one of their employees as a security liaison for this process. This Contractor Security Liaison coordinates the distribution, collection, and dissemination of various forms required in this process. They answer general questions from their employees on completing the security screening process. And they are the first point of contact for contractor employees in using the OPM's Internet based security screening portal called e-QIP (http://www.opm.gov/e-qip/). The contractor is also responsible for ensuring that all subcontractors follow these personnel security screening procedures.

NCES requires each contractor employee to have or apply for a clearance for the security level designated for the position held on a contract.

Contractor employees who have undergone appropriate personnel security screening for another Federal agency will be required to submit proof of that personnel security screening for validation. For these employees, the contractor or subcontractor must follow these required steps:

1. The contractor must submit a letter for each employee with a pre-existing investigation through the IES Clearance Application Manager (ICAM) on the Company letterhead. The letter must list the full name of the employee, the agency that cleared the employee, the level of the investigation, and the date of the investigation. This letter must be transmitted to the NCES Security Team through ICAM within two (2) business days of starting work on an NCES contract.
2. The NCES Security Team reviews the letter to ensure that the required information is provided and either returns it to the contractor for completion or releases it to the Department of Education Chief of Personnel Security. The contractor must resubmit the letter to the NCES Security Team within 7 business days or the contractor employee must be removed from the contract.

3. The NCES Security Team will notify the contractor or subcontractor if the pre-existing investigation was identified and ruled to be acceptable by the Department of Education Chief of Personnel Security.
4. Those employees whose pre-existing investigations are not verified and approved must follow the process outlined next to apply for a security clearance.

For contractor employees who have not undergone appropriate personnel security screening for another Federal agency, all contractors must comply with the Principal Office (PO) Executive Office or Computer Security Officer's pre-processing requirements for personnel security screening and granting access privileges. **No contractor employees are permitted unsupervised access to unclassified sensitive information (i.e., personally identifiable information), direct access to respondents who are minors, or Department of Education IT systems until they have submitted applicable security screening documents.**

For each contractor employee in a moderate risk level position the completed security screening documents must be accepted by the NCES Security Team and submitted to the Department of Education Chief of Personnel Security within 14 days of the date the contractor employee starts working on the contract. In order to meet this Departmental requirement, steps 1 through 7 must be completed within 14 days of the date the contractor employee starts working on the contract. **To meet this 14-day deadline and the interim deadlines specified below, it is strongly recommended that the contractor request the account initiation three (3) weeks before the contractor employee starts contract work and encourage each contractor employee to complete all required security screening forms before starting contract work.**

Contractor employees in High Risk IT (6C) Level positions require preliminary personnel security screenings before they are given access to unclassified sensitive information or Department of Education IT systems (see page 7 of OM:5-101 for more details).

The security screening of contractor and subcontractor employees not holding Department of Education recognized security screening credentials must follow these required steps:

1. The contractor must provide the COR with an electronic listing of all employees on a specific contract, with the risk level associated with the position held by each employee as specified in the contract solicitation. The COR will review the electronic listing for completeness and approve. The listing will not be approved if it is found to be incomplete.

2. The Department of Education participates in the DCSA e-QIP system to facilitate the security screening process for contractor employees. NCES will initiate an e-QIP account for each contractor employee. **It is advisable to request the account initiation three (3) weeks before the contractor employee starts contract work.** For the initiation of these accounts, the Contractor Security Liaison must use the COR-approved list of employees and the risk levels assigned to the employees' positions to submit the following information using ICAM:

    a. For each contractor employee provide: Social Security Number, Full Name, Date of Birth, Place of Birth, Citizenship, risk level, Position Title, e-Mail Address, and phone number.

ICAM will send an e-mail notification of the transmission to the NCES Security Team. The NCES security staff will use this list to establish the contactor employee e-QIP accounts. The COR will work with the contractor to establish access to the NCES secure server at the outset of the contract.

b. Once NCES sets up the e-QIP accounts for contract employees, ICAM will send an email to the Contractor Security Liaison stating that the employee has an active account on the e-QIP system. The COR is copied on this email notification.

c. The Contractor Security Liaison must notify their employees of this active account. A computer with Internet access and web browsing software is required for the contractor employee to access their e--QIP account. Each employee must log into their personal account in e-QIP, enter the requested information, finish the application process and print, sign, and date the e-QIP signature pages.

3. The Contractor Security Liaison must work with each contractor employee to submit a completed set of security screening forms as provided by the COR and NCES Security Team, including for example:

   a. The signed and dated e-QIP signature pages,

   b. The Declaration of Federal Employment (OF-306 - only required for low risk positions),

   c. The Fair Credit Release Form,

   d. Current Cyber Security Certificate,

   e. Contractor Suitability Processing Request Form (CSPR),

   f. Position Designation Record (PDR).
      1) The contractor employee shall complete only those items in section 4 of the CSPR form (name, date of birth, place of birth, citizenship, position title, physical ED work location, social security number, e-mail address, and work phone number).
      2) The contractor shall complete section 5-11 using the assigned security clearance for each employee's position.
      3) The PDR is completed by the COR and provided to the Contractor Security Liaison for submission with the rest of the security screening forms.

   g. Two sets of fingerprints on separate copies of form FD-258,
      1) The Contractor Security Liaison shall help arrange fingerprinting for each contractor and subcontractor employee. Fingerprinting can usually be done at a local police station. (Electronic fingerprints are only acceptable if they are completed at LBJ or UCP at this time.)

4. Each contractor must ensure that the forms are complete, and that all contractor employee required security screening forms are transmitted into ICAM within two (2) business days of an employee starting work on an NCES contract.

   a. The Contractor Security Liaison must collate the forms in each security screening package by employee and transmit a complete set of security screening documents for each employee into

ICAM, and send the fingerprint cards to the NCES Security Team via courier (e.g., Federal Express) using a tracking number with signature required,

b. The NCES Security Team will not accept security screening packages that are not collated by employee (i.e., all forms noted in point 3 above will be bundled by employee). The NCES Security Team will review all security screening documents for each contractor employee for completeness, returning any incomplete security screening documents to the Contractor Security Liaison for completion in ICAM. The contractor must resubmit the completed security screening documents in ICAM within 7 business days or the contractor employee must be removed from the contract. **No contractor employees are permitted unsupervised access to unclassified sensitive information (personally identifiable information), direct access to respondents who are minors, or Department of Education IT systems until they have resubmitted applicable screening documents.**

5. The Contractor Security Liaison will submit the completed packages of security screening documents to the NCES Security Team in ICAM and send the fingerprint cards to the NCES Security Team via courier (e.g., Federal Express) using a tracking number with signature required for processing.

6. The NCES Security Team reviews each package of security screening documents and electronic information submission to ensure everything required has been provided and either rejects the package, sending it back to the submitter for completion/correction or releases it depending on the level of the risk position. Applications for low and moderate risk positions are released to an NCES Federal employee for review and release to OPM/DCSA. Applications for High Risk positions are released to the Department of Education Chief of Personnel Security for review and release to OPM/DCSA. In the event that a package is rejected at this stage, the contractor must resubmit the corrected forms to the NCES Security Team in ICAM or have the contractor employee correct the e-QIP submission, within two business days. As soon as the updated e-QIP submission is completed **the Contractor Security Liaison must resubmit in ICAM, which automatically notifies the NCES Security Team**.

7. The contractor employee application for each individual in a moderate risk level position must be submitted to the NCES Federal employee within 14 days of the date the contractor employee starts working on the contract. Contractor employees in High Risk IT (6C) Level positions require preliminary personnel security screenings before they are given access to unclassified sensitive information or Department of Education IT systems.

8. After a package of security screening documents is transmitted to the Department of Education Chief of Personnel Security, Office of Finance and Operations (OFO) security staff conducts a further review and either rejects the package of security screening documents for a high risk Public Trust position, sending it back to the submitter for completion/correction or releases it to OPM/DCSA. After a package if security screening documents for a low or moderate position is transmitted to an NCES Federal employee, the application undergoes a further review and is sent back to the submitter for completion/correction or is released to OPM/DCSA.

9. OPM/DCSA then assigns an investigator to conduct the type of investigation indicated by the department (this is tied to the level of access to PII that the applicant will have).

10. The Chief of Personnel Security will request the expansion of background investigations to obtain additional information to the extent necessary to make personnel acceptability or suitability determinations**.** These determinations will be made using criteria established by the OPM/DCSA for the purpose of determining suitability for employment in the Federal competitive service, as described in 5 CFR 731.202, and other OPM/DCSA guidance as applicable. The Chief of Personnel Security determines whether a contractor employee is acceptable for the position from a personnel security standpoint.

11. When the OPM/DCSA investigation is complete, the case is form is sent to the Department of Education's Office of Finance and Operations for processing.

12. On a monthly basis, the NCES Security Team pulls a report of contractor employees who are scheduled at DCSA from ICAM. Each NCES Security Representative confirms in e-QIP if the cases for their division have been completed. If a case is completed by DCSA, the representative notifies OFO the case is available for suitability determination.

13. The Chief of Personnel Security will inform the NCES Security Team when he or she determines that a contractor employee is not acceptable to render service(s) or, if appropriate, to otherwise perform under a contract. The NCES Security Team notifies the COR who must inform the Contracting Office and the contractor (i.e., employing firm) of this ruling. The contractor will notify the contractor employee. A final determination cannot be appealed.

14. At any time during the life of the contract a contractor or subcontractor employee (including any field staff) discontinues work on the contract or leaves the employment of the contractor, the contractor shall notify the COR and NCES Security Team within two days of the date that the employee is no longer working on the contract or within one business day if removed for cause. The contractor shall provide the reason why the employee is no longer working on the contract.

15. Each contractor is responsible for the protection of sensitive or Privacy Act-protected information from unauthorized use or misuse by its employees, subcontractors, or temporary workers, and for preventing access to others, who are not authorized and have no need to know such information.

16. The contractor shall submit monthly information to the COR indicating which employees were billed to the contract that include the e-QIP number of the person being billed. The COR will reject payments to employees without an e-QIP number. For employees with pre-existing investigations from other contracts, this shall be noted on the monthly payment form.

The contractor shall verify with the COR that the security screening processes have not changed by the time the contract is active.

Appendix E

Affidavit of Nondisclosure

_____ _____
(Job Title) (Date Assigned to work with NCES Data)

_____
(Organization, State or Local Agency)

_____ _____
(Organization or Agency Address) (NCES Database or File Containing Individually Identifiable Information*)

I, _____, do solemnly swear (or affirm) that when given access to the subject NCES database or file, I will not -

(i) use or reveal any individually identifiable information furnished, acquired, retrieved or assembled by me or others, under the provisions of Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279) and Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.) for any purpose other than statistical purposes specified in the NCES survey, project or contract;

(ii) make any disclosure or publication whereby a sample unit or survey respondent (including students and schools) could be identified or the data furnished by or related to any particular person or NAEP school under these sections could be identified; or

(iii) permit anyone other than the individuals authorized by the Commissioner of the National Center for Education Statistics to examine the individual reports.

_____
(Signature)

[The penalty for unlawful disclosure is a fine of not more than $250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both. The word "swear" should be stricken out when a person elects to affirm the affidavit rather than to swear to it.]

City/County of _____ Commonwealth/State of _____
Sworn to and subscribed before me this _____ day of
_____, 20_____. Witness my hand and official Seal.

_____ My commission expires_____
(Notary Public/Seal)

Appendix F

Formal Request for Restricted-use Data License

Formal Request:
(1) Title of survey(s).
(2) Description of the statistical research project for which the restricted-use data are needed. Explanation of why the restricted-use data are needed (e.g., instead of the public data version). A description of the sector(s) of the community that will be served by the research to be conducted,
(3) Name and title of the Senior Official.
(4) Name and title of the Principal Project Officer(s).
(5) Name and title of the Systems Security Official.
(6) Names and titles of the professional/technical staff.
(7) Estimated loan period (not to exceed five years).

Appendix G

LICENSE FOR THE USE OF INDIVIDUALLY IDENTIFIABLE INFORMATION PROTECTED UNDER THE EDUCATION SCIENCES REFORM ACT OF 2002 AND PROTECTED, AS APPLICABLE, UNDER THE FOUNDATIONS OF EVIDENCE-BASED POLICYMAKING ACT OF 2018 44 U.S.C., CHAPTER 35, SUBCHAPTER III, Part B, Section 3572 CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY ACT, THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT, AND THE PRIVACY ACT OF 1974

WHEREAS, the Institute of Education Sciences (IES) of the United States Department of Education has collected and maintains individually identifiable information, the confidentiality of which is protected by section 183 of the Education Sciences Reform Act of 2002 (ESRA) (PL 107-279) (20 U.S.C. 9573), and, as applicable, by the Privacy Act of 1974 (5 U.S.C. 552a); the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g); and Confidential Information Protection and Statistical Efficiency Act (CIPSEA), Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); and

WHEREAS, IES wishes to make the data available for statistical, research, or evaluation purposes to requestors qualified and capable of research and analysis consistent with the statistical, research, or evaluation purposes for which the data were provided or are maintained, but only if the data are used and protected in accordance with the terms and conditions stated in this license (License), upon receipt of such assurance of qualification and capability, it is hereby agreed between.

_____,
(Insert the name of the agency or organization to be licensed)

hereinafter referred to as the "Licensee", and IES that:

I. INFORMATION SUBJECT TO THIS AGREEMENT

A. All data containing individually identifiable information about students, their families, and their schools maintained by IES under section 183 of the Education Sciences Reform Act of 2002, that are provided to the Licensee and all information derived from those data, and all data resulting from merges, matches, or other uses of the data provided by IES with other data are subject to this License and are referred to in this License as subject data.

B. Subject data under this License may be in the form of CD-ROMs, electronic data, hard copy, etc. The Licensee may only use the subject data in a manner

and to a purpose consistent with:

1. The statistical, research, or evaluation purpose for which the data are maintained. All subject data that include individually identifiable information are protected under the Privacy Act, ESRA, and/or CIPSEA and may be used only for statistical, research, or evaluation purposes consistent with purposes for which the data were collected and /or are maintained (Licensee's description of the research and analysis which is planned is attached and made a part of this License - Attachment No. 1.);

2. Subject data that includes personally identifiable information from students' education records are protected under FERPA and may only be used for the evaluation of Federally-supported education programs or for conducting studies, for, or on behalf of, educational agencies or institutions to improve instruction. (Licensee's description of the evaluation or study which is planned is attached and made a part of this License - Attachment No. 1.);

3. The limitations imposed under the provisions of this License; and

4. Section 183 of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573); and, as applicable, CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Privacy Act of 1974 (5 U.S.C. 552a); and the Family Educational Rights Protection Act (20 U.S.C. 1232g) which are attached to and made a part of this License (Attachment No. 2.)

II. INDIVIDUALS WHO MAY HAVE ACCESS TO SUBJECT DATA

A. There are four categories of individuals that the Licensee may authorize to have access to subject data. The four categories of individuals are as follows:

1. The Principal Project Officer (PPO) is the most senior officer in charge of the day-to-day operations involving the use of subject data and is responsible for liaison with IES.

2. Professional/Technical staff (P/T) conduct the research for which this License was issued.

3. Support staff includes secretaries, typists, computer technicians, messengers, etc. Licensee may disclose subject data to support staff who come in contact with the subject data in course of their duties only to the extent necessary to support the research under this License.

4. The System Security Officer (SSO) is responsible for maintaining the day-to-day security of the licensed data, including the implementation, maintenance, and periodic update of the Security Plan to protect the

data in strict compliance with statutory and regulatory requirements.

B. Licensee may disclose subject data to only to only seven (7) staff, including the PPO, SSO, P/TS, and support staff, unless IES provides written authorization for a larger number of P/TS.

III. LIMITATIONS ON DISCLOSURE

A. Licensee shall not use or disclose subject data for any administrative purposes nor may the subject data be applied in any manner to change the status, condition, or public perception of any individual regarding whom subject data is maintained. (Note: Federal Law pre-empts any State law that might require the reporting or dissemination of these data for any purpose other than the statistical, research, and evaluation purposes for which they were collected and/or are maintained.)

B. Licensee shall not disclose subject data or other information containing, or derived from, subject data at fine levels of geography, such as school district, institution, or school, to anyone other than IES employees working in the course of their employment or individuals for whom access is authorized under this License agreement. Licensee may make disclosures of subject data to individuals other than those specified in this License only if those individuals have executed an Affidavit of Nondisclosure and the Licensee has obtained advance written approval from the IES Data Security Office.

C. Licensee shall not make any publication or other release of subject data listing information regarding individuals or specific educational institutions even if the individual respondent identifiers have been removed.

D. Licensee may publish the results, analysis, or other information developed as a result of any research based on subject data made available under this License only in summary or statistical form so that the identity of individuals or specific educational institutions contained in the subject data is not revealed.

IV. ADMINISTRATIVE REQUIREMENTS

A. The research conducted under this License and the disclosure of subject data needed for that research must be consistent with the statistical, research, or evaluation purpose for which the data were supplied. The subject data may not be used to identify individuals or specific educational institutions for recontacting unless Licensee has obtained advance written approval from the IES Data Security Office.

B. Execution of Affidavits of Nondisclosure.

1. Licensee shall provide a copy of this agreement, together with the Security Plan (Attachment No. 3) to the SSO and to each P/T and support staff person of the Licensee who will have access to subject data and shall require each of those individuals to execute an Affidavit of Nondisclosure (Attachment No. 4).

2. The Licensee must ensure that each individual who executes an Affidavit of Nondisclosure reads and understands the materials provided to her or him before executing the Affidavit.

3. Licensee shall ensure that each Affidavit of Nondisclosure is notarized upon execution.

4. Licensee may not permit any individual specified in paragraph II.A. to have access to subject data until the procedures in paragraphs IV.B.1. through 3 of this License are fulfilled for that individual.

5. Licensee shall promptly, after the execution of each Affidavit, send the original Affidavit to the IES Data Security Office and shall maintain a copy of each Affidavit at the Licensee's secured facility protected under this License.

C. Notification regarding authorized individuals to IES.

1. Licensee shall promptly notify the IES Data Security Office when the SSO, or any P/T or support staff who has been authorized to have access to subject data no longer has access to those data.

D. Publications made available to IES.

1. Licensee shall provide the IES Data security Office a copy of each publication containing information based on subject data or other data product based on subject data before they are made available to individuals who have not executed an Affidavit of Nondisclosure.

2. Because the publication or other release of research results could raise reasonable questions regarding disclosure of individually identifiable information contained in subject data, copies of the proposed publication or release must be provided to the IES Data Security Office before that disclosure is made so that IES may advise whether the disclosure is authorized under this License and the provisions of section 183 of the Education Sciences Reform Act of 2002; CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Privacy Act of 1974; and the Family Educational Rights and Privacy Act. Licensee agrees not to publish or otherwise release research results provided to IES if IES advises that such disclosure is not authorized.

E. Licensee shall notify the IES Data Security Office immediately upon receipt of any legal, investigatory, or other demand for disclosure of subject data.

F. Licensee shall notify the IES Data Security Office immediately upon discovering any breach or suspected breach of security or any disclosure of subject data to unauthorized parties or agencies.

G. Licensee agrees that representatives of IES have the right to make unannounced and unscheduled inspections of the Licensee's facilities, including any associated computer center, to evaluate compliance with the terms of this License and the requirements of section 183 of the Education Sciences Reform Act of 2002; CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Privacy Act of 1974; and the Family Educational Rights and Privacy Act.

V. SECURITY REQUIREMENTS

A. Maintenance of, and access to, subject data.

1. Licensee shall retain the original version of the subject data at a single location and may make no copy or extract of the subject data available to anyone except the SSO or a P/T staff member as necessary for the purpose of the statistical research for which the subject data were made available to the Licensee.

2. Licensee shall maintain subject data (whether maintained on a personal computer or on printed or other material) in a space that is limited to access by the PPO, SSO, and authorized P/T staff.

3. Licensee shall ensure that access to subject data maintained in computer memory is controlled by password protection. Licensee shall maintain all print-outs, CD-ROMS, personal computers with subject data on hard disks, or other physical products containing individually identifiable information derived from subject data in locked cabinets, file drawers, or other secure locations when not in use.

4. Licensee shall ensure that all printouts, tabulations, and reports are edited for any possible disclosures of subject data.

5. Licensee shall establish security procedures to ensure that subject data cannot be used or taken by unauthorized individuals.

6. Licensee shall not permit removal of any subject data from the limited access space protected under the provisions of this License as required in the attached Security Plan (Attachment No. 3.), without first notifying, and obtaining written approval from, IES.

B. Retention of subject data.

Licensee shall return to the IES Data Security Office all subject data, or destroy those data under IES supervision or by approved IES procedures when the statistical analysis, research, or evaluation that is the subject of this agreement has been completed or this License terminates, whichever occurs first. Licensee, as part of its responsibilities discussed herein, agrees to submit a completed Close-out Certification Form to the IES Data Security Office.

C. Compliance with established security procedures.

Licensee shall comply with the security procedures described in the Security Plan (Attachment No. 3 to this License).

VI. PENALTIES

A. Any violation of the terms and conditions of this License may subject the Licensee to immediate revocation of the License by IES.

1. The IES official responsible for liaison with the Licensee shall initiate revocation of this License by written notice to Licensee indicating the factual basis and grounds for revocation.

2. Upon receipt of the notice specified in paragraph VI.A.1 of this License, the Licensee has thirty (30) days to submit written argument and evidence to the Director of IES indicating why the License should not be revoked.

3. The Director of IES shall decide whether to revoke the License based solely on the information contained in the notice to the Licensee and the Licensee's response and shall provide written notice of the decision to the Licensee within forty-five (45) days after receipt of Licensee's response. The Director of IES may extend this time period for good cause.

B. Any violation of this License may also be a violation of Federal criminal law under the Privacy Act of 1974 (5 U.S.C. 552a(i)); section 183 of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573(d)(2); and/or CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.). Alleged violations under section 183 of the Education Sciences Reform Act of 2002 and CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.) are subject to prosecution by the Offices of the United States Attorney. The penalty for violation of section 183 of the Education Sciences Reform Act of 2002 and CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.), is a fine of not more than $250,000 and imprisonment for a period of not more than five years.

VII. PROCESSING OF THIS LICENSE

A. The term of this License shall be for_____years. If, before the expiration of this License, the Director of IES establishes regulatory standards for the issuance and content of Licenses, the Licensee agrees to comply with the regulatory standards.

B. This License may be amended, extended, or terminated by mutual written agreement between the Licensee and the Director of IES. Any amendment must be signed by a Senior Official specified in paragraph VII.C. of this License, PPO, and the Director of IES and is effective on the date that all required parties have signed the amendment.

C. The Senior Official (SO), who cannot be the same individual designated as the PPO, having the legal authority to bind the organization to the terms of the License, shall sign this License below. The SO certifies, by his/her signature, that -

1. The organization has the authority to undertake the commitments in this License;

2. The SO has the legal authority to bind the organization to the provisions of this License; and

3. The PPO is the most senior subject matter officer for the Licensee who has the authority to manage the day-to-day statistical, research, or evaluation operations of the Licensee.

_____ _____
Signature of the Senior Official Date

_____
Type/Print Name of Senior Official

Title:_____Telephone: (____)_____

D. The individual described in paragraph II.A1. as the PPO shall sign this License below. If the SO also acts as the chief statistical officer for the Licensee; viz. as the PPO, the SO shall likewise sign under this paragraph as well as having signed under paragraph VII.C.

_____ _____
Signature of the Principal Project Officer Date

_____
Type/Print Name of the Principal Project Officer

Title:_____Telephone: (____)_____

E. The Director of the Institute of Education Sciences or Designee issues this License to

_____. The License is effective as of the date of the Director of IES or Designee's signature below, or such other period specified in the Licensee's request for the License.

_____
Signature of Director of IES or Designee

_____
Title

_____
Type/Print Name of Director of IES or Designee

_____
Date

IES License Control Number: _____

Appendix H

Security Plan Form

Institute of Education Sciences (IES)
Restricted-use Data

Name of Institution / Organization: _____

PPO Name: _____

PPO Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

PPO Phone Number: _____

Type of Security Plan: New ☐ Renewal ☐ Modification ☐

License Number: _____

Physical Location of Data

Project Office Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

Project Office Phone Number: _____

Note: *The restricted-use data and computer must be secured and used **only** at this location. When the data are not being used, the data must be stored under lock and key at this location. Only authorized users of the data, as listed on the License, may have key access to this secure project office/room.*

Physical Security of Data

Describe Building Security:
(Describe building security arrangements where project office is located.)

Describe Project Office Security:
(Describe project office security arrangements for the room where the computer and data will be located.)

Computer Security Requirements

Describe Computer System:
*(Please read the **Note** below. Computer security must follow the requirements listed below.)*

Computer Operating System: _____

Anti-Virus Software Installed on Computer: _____

***Note:** The restricted-use data must be copied to and run on a standalone, desktop computer. **Use of a laptop computer, external hard drive, or USB memory stick is strictly prohibited.** Absolutely no restricted-use data may be copied onto a server or computer that is attached to a modem or network (LAN) connection. Prior to attaching the computer to a modem or LAN connection, the restricted-use data must be purged and overwritten on the computer.*

The following physical location and computer security procedures must be implemented when in possession of restricted-use data. By checking the box next to each security procedure, you signify that these security procedures will be implemented for the duration of the project and License period:

- Only authorized users listed on the License will have access to the secure room. Access will be limited to the secure room/project office by locking the office when away from the office. ☐
- Data will only be secured, accessed and used within the secure project office/room (as specified on page 1 of this plan). ☐
- A password will be required as part of the computer login process. ☐
- The password for computer access will be unique and contain 6 to 8 characters with at least one non-alphanumeric character. ☐

- The computer password will change at least every 3 months or when project staff leave. ☐
- Read-only access will be initiated for the original data. ☐
- An automatic password protected screensaver will enable after 5 minutes of inactivity. ☐
- No routine backups of the restricted-use data will be made. ☐
- Project office room keys will be returned and computer login will be disable within 24 hours after any user leaves the project. The PPO will notify IES of staff changes. ☐
- Restricted-use data will **not** be placed on a server (network), laptop computer, USB memory stick, or external hard drive. ☐
- The data will be removed from the project computer and overwritten, whether at the end of the project or when reattaching a modem or LAN connection. ☐
- Post Warning notification: During the computer log-in process, a warning statement (shown below) will appear on the computer screen before access is granted. If it is not possible to have the warning appear on the screen, it must be typed and attached to the computer monitor in a prominent location. ☐

WARNING

U.S. Government Restricted-use Data

Unauthorized Access to Data (Individually Identifiable Information) on this Computer is a Violation of Federal Law and will Result in Prosecution.

Do You Wish to Continue? (Y)es or (N)o

Signature Page – Management Review and Approval

I have reviewed the requirements of the License agreement and the security procedures in this plan that describe the required protection procedures for securing, accessing and using the restricted-use data.

I hereby certify that the computer system, physical location security procedures, and access procedures meet all of the License requirements and will be implemented for the duration of the project and License period.

Senior Official Signature	Date
Senior Official Name & Title (print)	Phone Number
Principal Project Officer Signature	Date
Principal Project Officer Name & Title (print)	Phone Number
System Security Officer Signature	Date
System Security Officer Name & Title (print)	Phone Number

Note: The National Center for Education Statistics (NCES) processes licenses and disseminates restricted-use data for all centers in the Institute of Education Sciences (IES) including the National Center for Education Research (NCER), the National Center for Education Statistics (NCES), the National Center for Education Evaluation (NCEE), and the National Center for Special Education Research (NCSER).