Privacy Impact Assessment (PIA)
for the

IES Data Center (IESDC)
November 17, 2021

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

Contact Point

Contact Person/Title: Ed Vaden
Contact Email: Ed.Vaden@ed.gov

System Owner

Name/Title: Brian Taylor, IES Director of Technology
Principal Office: IES

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

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

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

The Institute of Education Sciences (IES) Data Center (IESDC) serves as the survey data collection tool and storage database for IES surveys. In addition, IESDC provides public-facing websites that provide deidentified data for research purposes. IES is comprised of four Centers, which are organizations that provide integrated, multifunctional tools for data collection, dissemination, and analysis. The four Centers include:

1. **National Center for Education Evaluation and Regional Assistance (NCEE)**
   NCEE conducts unbiased, large-scale evaluations of education programs supported by federal funds; provides technical assistance; and supports the development and use of research and evaluation throughout the United States.
2. **National Center for Education Research (NCER)**
   NCER supports research activities to improve the quality of education and thereby, increase student academic achievement, reduce the achievement gap between high-performing and low-performing students, and increase access to and completion of postsecondary education. NCER also funds predoctoral and postdoctoral research training programs to invest in the training and development of the next generation of education researchers.
3. **National Center for Education Statistics (NCES)**
   NCES fulfills a Congressional mandate to collect, collate, analyze, and report complete statistics on the condition of American education; conduct and publish reports; and review and report on education activities internationally.
4. **National Center for Special Education Research (NCSER)**
   NCSER supports research on infants, toddlers, children, and youth with and at risk for disabilities through advancing the understanding of and practices for teaching, learning, and organizing education systems.

IESDC collects information through computer-assisted data collection tools[1] (i.e., surveys) for respondents[2] to provide data to IES for studies conducted by the U.S. Department of Education (Department). The IESDC environment consists of 60 backend servers and databases to collect, maintain, and disseminate information. In addition to the collection tools, the system provides four features on the public-facing websites for each of the Centers:

- Information about studies conducted by the Department;
- Official statistics and research results for studies conducted by the Department;
- Data analysis tools to allow the public to generate their own reports on deidentified data; and
- Publications to share official results from Department studies with the public.

IESDC manages the dissemination of information from studies to the public differently depending on the types of data collected, as detailed below.

Unrestricted Public Consumption of Deidentified Datasets that include Microdata[3]
For some studies, IESDC provides unrestricted public-facing microdata sets when those data can be properly deidentified. Examples of such studies include the High School Longitudinal Study (HSLS) and National Household Education Survey (NHES). The microdata can be downloaded by the public in a deidentified form.

Unrestricted Public Consumption of Deidentified Datasets that do not include Microdata
For some studies, IESDC provides unrestricted public-facing datasets that do not include microdata. Prior to posting such data, IES has performed aggregative analyses to convert the microdata to the aggregate level, as well as applied strict disclosure protections to ensure that the data are deidentified. Examples of such studies include National Postsecondary Student Aid Study (NPSAS), Baccalaureate and Beyond Longitudinal Study (B&B), and Beginning Postsecondary Students Longitudinal Study (BPS). For these datasets, IESDC allows the public to generate deidentified statistics and view them online without disclosing any identifiable data to the public. IESDC also hosts websites

[1] Computer-assisted data collection tools refers to automated instruments comprised of a series of questions that instruct respondents as to what information is being requested, automatically determines what questions should be asked next based on responses to prior questions, and stores responses in structured databases.
[2] K-12, postsecondary, and adult students; K-12 and postsecondary faculty and staff; K-12 and postsecondary institutions; families of preschool through grade 12 students.
[3] Microdata are data that describe individual respondents (e.g., respondent 1 has attribute x) before aggregative analyses are applied to convert the data to the aggregate level (e.g., x% of respondents have attribute y). If microdata are publicly downloadable from IESDC, they have been deidentified.

describing these studies and public-facing analysis of data collected through the studies for public consumption.

Public Consumption of Institution Datasets

Some IES studies collect non-identifiable data from institutions. IESDC makes these non-identifiable datasets available on the public-facing websites. Examples of such studies include Integrated Postsecondary Education Data System (IPEDS) and Private School Survey (PSS). In addition to hosting public-use data for these studies, IESDC also hosts public-facing school searches and comparison tools.

Restricted Use Datasets[4]

IESDC hosts a website that allows researchers to apply for access to restricted-use[5] data from certain studies. IES "loans" restricted-use data to qualified organizations in the United States which meet specific criteria. Individual researchers must apply through an organization (e.g., a university, a research institution, or company). To qualify, an organization must provide a justification for access to the restricted-use data, submit the required legal documents, agree to keep the data safe from unauthorized disclosures at all times, and agree to participate fully in unannounced, unscheduled inspections of the researcher's office to ensure compliance with the terms of the License and the Security Plan form. For data that is loaned to a researcher, the researcher is responsible for purging all copies or subsets of the subject data from any computer system used in the research project when the License is closed.

1.2. Describe the purpose for which the personally identifiable information (PII)[6] is collected, used, maintained, or shared.

IES provides parents, educators, students, researchers, policymakers, and other members of the general public with reliable information about:

- the condition and progress of education in the United States, including early childhood education and special education;
- educational practices that support learning and improve academic achievement and access to educational opportunities for all students; and
- the effectiveness of Federal and other education programs.

[4] IES uses the restricted-use data License as a mechanism for making more detailed data available to qualified researchers.

[5] Federal agencies collect survey data containing personally identifiable information that are confidential and protected by law. IES uses the restricted-use data License as a mechanism for making more detailed data available to qualified researchers without making identifiable data available to the broader public, consistent with requirements in law.

[6] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

Data collections managed through IESDC enable IES to provide education datasets, data tools, reports, educator's practice guides, summaries of completed and in-progress research and evaluation projects, videos, and infographics to achieve the goals listed above.

Data collected through IESDC may also include PII for purposes of following up with respondents during later stages of multi-timepoint data collections and to support matching to administrative record data from other sources. Administrative record matching helps reduce respondent burden during the survey and typically provides more accurate information than a respondent might be able to provide during a relatively short survey.

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

Currently Operating System

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

Updated PIA

The PIA is being updated because, under Department policy, PIAs are required to be reviewed and updated every two years and the prior IESDC PIA was due for review and update.

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

Contractor

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

□ N/A

Yes

2. Legal Authorities and Other Requirements

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

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

IES is authorized by 20 U.S.C. Ch. 76 – Education Research, Statistics, Evaluation, Information, and Dissemination, Subchapter I – Education Sciences Reform Act of 2002. This statute authorizes the IES data collection activities through IESDC and the use of the data by the Office of Postsecondary Education (OPE).

SORN

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

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[7] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The following SORNs cover the maintenance of the information for IESDC:

- National Center for Education Statistics Longitudinal Studies and the School and Staffing Surveys (83 FR 56831, 11/14/2018, ~~ED-2017-IES-0131~~SORN Number: 18–13–01)
- National Longitudinal Transition Study-2 (NLTS2) (74 FR 56826, 11/03/2009, SORN Number: 18–13–23~~E9-26430~~)

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

☑ N/A

Click here to enter text.

Records Management

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

[7] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

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

NARA records retention schedules associated with IES are currently being updated. Data produced by IES for statistical analyses and reporting are generally considered permanent records. Until the record retention schedules are approved, data will be retained indefinitely and will not be destroyed.

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

Yes

3. Characterization and Use of Information

Collection

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

The specific PII elements will depend on the particular IES survey. For access to information regarding the different surveys, users can visit the Institute of Education Sciences (IES) Home Page. The various IESDC data collections may include information on the analysis of education programs, student assessments, education program offerings and program participation, education program staffing, qualifications of staff, individual characteristics of respondents (e.g., age, race/ethnicity, gender), salaries, financial information for postsecondary students and K-12 and postsecondary institutions (depending on the study), transcript information for K-12 and postsecondary students (depending on the study), and Social Security number[8] (if required by the study).

For study contact purposes, name, address (home and/or institutional depending on the study), phone number (home and/or work depending on the study), and email address (personal and/or work depending on the study) may be collected.

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

[8] For example, the Beginning Postsecondary Student Longitudinal Study (BPS) collects SSN to allow correct linking to student loan data collected by FSA.

Yes

The information collected is the minimum needed to provide parents, educators, students, researchers, policymakers, and other members of the general public with reliable data about education in the United States and other countries, to follow up with respondents, and to support matching to administrative record data from other sources. No additional information is collected.

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

Information is collected directly from individuals invited to participate in a survey such as students, parents, teachers, school administrators, childcare providers, or educational entities, federal agencies, and private organizations, such as the College Board. Information is also collected from schools and institutions, federal agency data systems, and commercial vendors.

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

The mode of data collection depends on the specific study and the ability of respondents to respond using different communication tools. The more common modes of data collection include web-based data collection tools, paper forms, telephone interviews, and in-person interviews. Information collected outside the web-based data tools are entered into IESDC manually, often by scanning paper forms.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[9] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The records that are collected and maintained in IESDC are not used for the purpose of providing a benefit to or making a determination about any individual. Therefore, invalid records maintained in the IESDC is not a significant privacy concern. However, these records are collected to provide official statistics, data, and other information to support the work and research of policy makers, education practitioners, researchers, the general

[9] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

public, and a wide range of additional stakeholders. To this end, IES applies different techniques[10] to ensure the quality of the data.

Use

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

The collection of PII through IESDC facilitates the creation of data sets, tools, reports, educator's practice guides, summaries of completed and in-progress research and evaluation projects, videos, and infographics. These are posted to publicly accessible websites to allow the general public to gain information on education programs and practices. Information related to education in the United States and other nations is collected and analyzed to develop studies and provide related data to the general public and policy makers.

The information is also used to contact panel study members of longitudinal studies undertaken by the agency. Data and information from the longitudinal studies are hosted in IESDC. Public-facing information from the studies can be found in publications on the websites hosted in IESDC and through data analysis tools in IESDC. The PII is not made available to the public, however, other than the provision of restricted-use data to qualified researchers. The PII is also used to link IES studies to other extant data sources to improve the usefulness of the studies for policy makers and the public. These include links to geographic information such as that provided by U.S. Census Bureau data products, data holdings of the Department, and data owned by private organizations such as the College Board. Information from these linked sources is then reflected in aggregate statistics made available through the same means as those described for the longitudinal studies.

The PII can be accessed for research purposes through the IES restricted-use data license process. Please see https://nces.ed.gov/statprog/instruct.asp for data security procedures and requirements regarding restricted-use data.

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

No

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

[10] Examples include noise additive, condensation-based, and geometric data perturbations.

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

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

Yes

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

□ N/A

Not all collections include the collection of SSNs. If SSNs are collected, they are collected with Office of Management and Budget (OMB) approval for the express purpose of record linkage with Department records systems and, in some cases, State or local student records. In longitudinal studies, SSNs may also be used for tracking study respondents as they change schools and/or geographic locations over the course of the study (e.g., to follow study respondents as they transition from the completion of baccalaureate program into the workforce or additional higher education).

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

□ N/A

IES keeps abreast of studies that focus on the use of names for such linkages and follow-up studies, but the return rate on matches based on other forms of identification remain substantially lower than that obtained through the use of SSNs. Therefore, at this time, there are no alternatives to the use of SSNs that would suffice to achieve the objectives of the studies.

4. Notice

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

In the case of surveys conducted in educational institutions, advance letters are sent to the administrator of the institution describing the study, explaining the voluntary nature of the study, and describing the pledge of data confidentiality. In addition, every IES data collection that includes PII also includes a Privacy Act Statement, description of the voluntary nature of the data collection and a pledge of confidentiality, per OMB standards and NCES Statistical Standard 4.2.

The text of the pledge of confidentiality includes the following: *Your answers may be used only for statistical or research purposes and may not be disclosed, or used, in identifiable form for any other purpose except as required by law.*

Furthermore, the routine statistical purposes for which the data may be used must be explained. If an individual educational institution requires informed consent from parents or adult students, that is included in the data collection procedures, otherwise each respondent is informed of the voluntary nature of their participation as it applies to both the entire data collection and to individual questions within the data collection. In the event of legally mandated participation in a data collection, the data provider (usually a representative of an institution) is provided a description of the legal requirement and all data protections that are afforded are provided, if the institutional data include data that are potentially disclosive of individual characteristics IES uses professional best practices to protect the identity of individuals in an institution when publishing data from the collection.

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

□ N/A

The notice is tailored to specific respondent types and will vary by study. For an example of the notices, please see the following teacher questionnaire for the Early Childhood Longitudinal Study, Kindergarten Class of 2010-11 at https://nces.ed.gov/ecls/pdf/secondgrade/Spring_2013_Teacher_Ques_Teacher_Level.pdf.

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

Every IES data collection that includes PII includes a description of the voluntary nature of the data collection and a pledge of confidentiality per OMB standards and NCES Statistical Standard 4.2. Each respondent is informed of the voluntary nature of their participation as it applies to both the entire data collection and to individual questions within the data collection.

Statements like the following are shared with respondents before they provide information, "*If you have comments or concerns regarding the status of your individual response to this survey, write directly to: ... Participation is voluntary. You may skip questions you do not wish to answer;... All responses that relate to or describe identifiable characteristics of individuals 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. Data will be combined to produce statistical reports. No individual data that links your name, address, telephone number, or identification number with your responses will be included...*"

For a complete example of how this is conveyed to respondents, please see language on the first page of the example cited in response to question 4.2 above.

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

Yes

5. Information Sharing and Disclosures

Internal

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

Yes

The IESDC hosts survey collections and data dissemination websites for the Office of Postsecondary Education (OPE). These OPE websites are related to Integrated Postsecondary Education Data System (IPEDS) websites. IPEDS is part of NCES.

5.2. What PII will be shared and with whom?

□ N/A

For study contact purposes, name, address (home and/or institutional depending on the study), phone number (home and/or work depending on the study), and email address (personal and/or work depending on the study) may be shared with OPE.

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

□ N/A

The IESDC hosts survey collections and data dissemination websites for the Office of Postsecondary Education (OPE).

External

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

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[11]

Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

□ N/A

Data collected in IESDC may be shared with the general public, in deidentified form, as described in response to question 1. Restricted use data are shared with staff within IES on a need-to-know basis and with other federal agencies through a memorandum of understanding (MOU) that mirrors the requirements described above for the data licensing program (see discussion of IES restricted data licenses in 3.6). Note that SSNs are never shared. A recent example of such an MOU is one with the U.S. Census Bureau to link an IES study of college graduates to employment data to study relationships between college degree attainment and career trajectories.

In addition, IESDC hosts a website that allows researchers[12] to apply for access to restricted-use data from these studies. IES loans restricted-use data only to qualified organizations in the United States. Individual researchers must apply through an

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

[12] IES loans restricted-use data only to qualified organizations in the United States. Individual researchers must apply through an organization (e.g., a university, a research institution, or company). To qualify, an organization must provide a justification for access to the restricted-use data, submit the required legal documents, agree to keep the data safe from unauthorized disclosures at all times, and agree to participate fully in unannounced, unscheduled inspections of the researcher's office to ensure compliance with the terms of the License and the Security Plan form.

organization (e.g., a university, a research institution, or company). To qualify, an organization must provide a justification for access to the restricted-use data, submit the required legal documents, agree to keep the data safe from unauthorized disclosures at all times, and agree to participate fully in unannounced, unscheduled inspections of the researcher’s office to ensure compliance with the terms of the License and the Security Plan form.

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

□ N/A

The information is shared for statistical or research purposes in alignment with question 1.2.

5.7. Is the sharing with the external entities authorized?

□ N/A

Yes

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

□ N/A

Yes

The IESDC tracks disclosures made to any external entity through the MOU/License process, which includes the use of a legally binding agreement with the other federal office, agency, or institution.

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

□ N/A

All public access data have been approved for release by IES senior management based upon analyses overseen and directed by the IES Disclosure Review Board. Each MOU with another federal program and each license with a qualified external researcher includes a description of the planned research and a statement explaining why publicly available data are not sufficient for the proposed analysis. The MOU/License process includes the use of a legally binding agreement with the other federal office, agency or institution; affidavits of nondisclosure from each authorized data user on the MOU/License; verification that the computer system on which the data will be used has full certification and accreditation in the case of a federal agency, alternatively verification that the data will only be used on a standalone computer in the case of a license; participation in unannounced security/compliance inspections; compliance with IES reporting standards for the specific data file; and the submission of all work products to IES for disclosure review prior to release to anyone not permitted access to the data through the researcher’s MOU/License agreement. Typically, information shared with another federal program will be done manually through secure email.

Data that do not require MOU or License agreements have had PII removed and have been subject to additional data perturbations to prevent indirect identification. Researchers, policymakers, and other stakeholders use these data for their own research and information purposes. Similarly, the public can access information through published reports through websites hosted by the IESDC. These reports do not contain PII.

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

□ N/A

Yes

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

□ N/A

Yes

6. Redress

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

Per the SORNs listed in question 2.2.1, if someone wants access to a record in this system of records, they must provide the system manager with their name, contact information, and any other identifying information requested to distinguish between individuals with the same name and date of birth. Requests for access to a record must meet the requirements of 34 CFR 5b.5, including proof of identity.

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

Per the SORNs listed in question 2.2.1, if someone wishes to amend a record, they must contact the system manager with their name, date of birth, and any other identifying information requested to distinguish between individuals with the same name and date of birth. Requests for access to a record must meet the requirements of 34 CFR 5b.5, including proof of identity

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

Both the SORN and this PIA, as well as the Department's regulations, at 34 CFR 5b.7, provide information and procedures for correcting inaccurate information.

7. Safeguards

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

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

Yes

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

Yes

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

□ N/A

Moderate

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

IESDC houses the survey collection and data dissemination websites for IES. IESDC is hosted in a secure environment in the Amazon Web Services (AWS) GovCloud (US region). AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. It is Federal Risk and Authorization Management Program (FedRAMP) certified. IESDC is connected to the Internet via a certified Managed Trusted Internet Protocol Services (MTIPS) connection which includes a security operation center (SOC) as well as EINSTEIN monitoring. IESDC is rated Moderate by the FIPS 199 Security Categorization. IESDC received an

ATO on November 18, 2020. The system complies with IT security requirements in the Federal Information Security Modernization Act (FISMA), OMB circulars, and the National Institute of Standards and Technology (NIST) standards and guidelines. The system's security and privacy are evaluated in yearly FISMA self-assessments. IESDC uses Access Control Lists (ACLs), firewalls, NTFS permissions, Microsoft BitLocker, McAfee ePO and Virus Scan, and BigIP filtering to protect the information.

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

Yes

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

Yes

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

IESDC received an ATO November 18, 2020, after a FISMA Security Assessment. These assessments take place every 3 years. IESDC participates in yearly FISMA self-assessments during the years that the full assessments do not take place. IESDC performs monthly internal and external vulnerability scans on all systems. Additional vulnerability scans take place as necessary to make sure system changes do not cause security issues. IESDC runs daily quick virus scans and weekly full virus scans on all systems. System changes are tracked through the IES Members Site's change control system.

8. Auditing and Accountability

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

All public access data have been approved for release by IES senior management, based upon the analysis and recommendations from the IES Disclosure Review Board. In addition, in those instances in which data are made available for analysis through the use of an online analysis tool, internal controls are programmed into the analysis tools to avoid potential disclosure of any identifying information (e.g., the suppression of small cells, limitations on the specific types of analyses available, constraints on the publication of unrounded and unweighted sample size, and electronic protections of the underlying data). Users of public-facing data are notified that use of such data for purposes other than statistical or research purposes (e.g., trying to identify individuals in a study) is subject to severe criminal and civil penalties. More sensitive data that are shared are governed by IES MOU or restricted-use data licenses. Each MOU or license with an approved qualified agency or researcher includes a description of the planned research and a statement explaining why publicly available data are not sufficient for the proposed analysis. IES reviews all analyses generated through such MOUs or licenses for disclosure risk before information is shared beyond those named in the MOU or license agreement.

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

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?
One privacy risk identified is unauthorized access to the PII contained in in IESDC. This PIA details the privacy controls and safeguards implemented for this system to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary to achieve the business purposes. Additionally, Question 8.1 describes how data perturbations, specific adjustments to online analysis tools, and legal protections further prevent disclosure risks.

Another privacy risk is the potential for unintended uses of the data that are collected. If data from a collection can be used for evaluation and research purposes not initially envisioned when collection occurred, IES would conduct the new research or enter into a restricted-use license agreement with academic researchers through the IES restricted-use license procedures. In both situations, resulting analyses that would be made publicly available would be reviewed before release and go through formal Disclosure Review Board clearances. By law, data in the systems cannot be used for other than statistical purposes.