THE SCHOOL SUPERINTENDENTS ASSOCIATION

1615 Duke Street | Alexandria, VA 22314
Phone: 703.528.0700 | Fax: 703.841.1543
www.aasa.org

April 19, 2023

United States Senate
The Honorable Bernie Sanders, Chair
The Honorable Bill Cassidy, Ranking Member
Senate Health, Education, Labor, and Pensions (HELP) Committee

428 Senate Dirksen Office Building
Washington, DC 20510

RE: Request for Information on Reauthorization of the *Education Sciences Reform Act*

Dear Chair Sanders and Ranking Member Cassidy,

This letter is in response to the Senate HELP Committee's bipartisan Request for Input (RFI) on a potential reauthorization of the Education Sciences Reform Act (ESRA), including the Educational Technical Assistance Act and the National Assessment of Education Progress Authorization Act. We write today on behalf of AASA, The School Superintendents Association and the AASA Student and Child Privacy Center (SCPC). AASA is the national organization representing the nation's 13,000 public school superintendents and the districts and students they serve. In our work on student data and privacy, we collaborate with the Public Interest Privacy Center (PIPC), an organization that equips stakeholders with the insights, training, and tools needed to cultivate effective, ethical, and equitable privacy safeguards for all children and students. We appreciate the opportunity to provide feedback on the important work of updating and improving the Education Sciences Reform Act (ESRA).

AASA strongly supports using data and research to improve teaching and learning and to inform decision-making at every level, including superintendents and state and federal policymakers. Research improves practices, adds to and addresses gaps in knowledge, provides empirical support for new policies to improve education, and ensures equity and the quality of education for all children.

Research is not only relevant to the core education mission of our members' schools: it plays an indispensable role in identifying the most effective strategies, utilizing resources responsibly, sustaining the global competitiveness of our education system, and equipping all students success now and in the future.[1] However, the effectiveness of research is dependent on its results being provided to practitioners - something that districts have not received, despite written agreements that require it.

Student privacy and data security are also integral to effective and trusted education research. Education research should always incorporate key ethical data practices such as the Fair Information Practices (FIPs), which are the basis of many federal and state privacy laws in the US and worldwide. The FIPs

[1] Roadmap for Effective Data Use and Research Partnerships between State Education Agencies and Education Researchers, DQC

principles–data minimization, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability–can provide a "structure for using data effectively and for granting researcher access to data in consistent, accountable, transparent, and secure ways"[2] These protections must be codified in law to better assist districts in holding researchers accountable for upholding these standards. agreed-upon data collection, use, and sharing protections, as well as the researcher's responsibility to provide the findings of their research back to their district partner.

AASA appreciates the Senate HELP Committee's interest in advancing the field of education research to better serve schools and students. Enacted in 2002 and expired since 2008, ESRA is a 20-year-old statute not only past-due for reauthorization, but also seriously outdated in terms of the massive changes in the student privacy landscape in that time: over 130 state student privacy laws have been passed in 47 states in the past 10 years alone. The student privacy landscape continues to change rapidly–in just the past three months child privacy was mentioned in the State of the Union; was discussed at three Congressional hearings; related amendments to FERPA and PPRA were included in the Parents Bill of Rights Act that passed the House, and child privacy was prioritized in numerous other state and federal bills.

As is the case with any reauthorization, Congress has an opportunity to make strategic and critical updates and improvements to ESRA that work to strengthen the underpinnings of the original law while updating and improving federal policy to reflect the ever-changing environment of education, research, data and privacy. Our feedback is a combination of guiding principles Congress should focus on, direct responses to the questions in the RFI, and potential legislative changes.

When Congress reauthorized No Child Left Behind into the Every Student Succeeds Act, they appropriately reframed the federal role in K12 education to use federal policy as a flashlight or guardrail, moving away from the 'carrot and stick' approach. This intentional design was aimed at establishing clear goals and priorities while also ensuring room for flexibility, something that is equally important in the field of education research. As you move forward with the ESRA work, those framing or 'guardrail' parameters should include:

- improving the timeliness of the evidence and data;
- expanding the usability and accessibility of education evidence and data;
- using federal policy to grow state and local capacity to generate and use evidence and data;
- clarifying how/when federal education research and data collections can be created/expanded and responsibility of federal government to consider burden on state and local education agencies; and
- modernizing education research infrastructure to be better aligned with the student privacy landscape.

AASA urges the Committee to modernize the field of education research to better align with the evolving student privacy landscape by incorporating privacy and security requirements into ESRA. This may be accomplished through adding provisions emphasizing the importance of privacy and security in the education research process such as adding individuals with expertise in privacy and security to the boards authorized by ESRA and requiring data privacy and security training for researchers and teachers. Further, we support the Committee including a formal authorization of the Privacy Technical

[2] Roadmap for Effective Data Use and Research Partnerships between State Education Agencies and Education Researchers, DQC

Assistance Center (PTAC) in ESRA to provide much needed technical assistance on changing student privacy issues to states.

AASA has addressed its comments to areas in which we have expertise, responding specifically to questions 2, 3, 5, 6, and 8. Where we have identified opportunities for key recommendations to be incorporated through specific legislative language changes, we have included bullet points referencing the relevant sections of the US Code. AASA would be happy to discuss the proposals offered in this letter, please feel free to contact Noelle Ellerson Ng (nellerson@aasa.org) or Amelia Vance (avance@aasa.org).

Sincerely,

Noelle Ellerson Ng
Associate Executive Director
AASA, The School Superintendents Association

Amelia Vance
Chief Counsel, Student & Child Privacy Center

Technical Responses

2. What specific changes could Congress make to improve the efficiency and effectiveness of the Federal technical assistance centers, including the Comprehensive Centers, operated by the U.S. Department of Education (ED) to improve their utility to State and local education leaders and policymakers?

Requiring boards authorized under ESRA, including the Comprehensive Centers, to include individuals with privacy and security expertise improves the efficiency and effectiveness of Federal technical assistance centers by increasing institutions' ability to protect student data. Privacy and security professionals can provide valuable insights and guidance that ensure that privacy and security considerations are integrated into all aspects of education research. Board and committee members with privacy and security expertise can help identify and address emerging issues as technology advances to ensure education research remains effective in protecting personal information. Here are areas based on the current law where this suggestion can be implemented:

- § 9516(c)(3): add (G) - the director of the Student Privacy Policy Office at the U.S. Department of Education
- § 9516(c)(4)(A): add (iii) - not fewer than 3 individuals with expertise in privacy, confidentiality, and cyber-security [or "with expertise in protecting personally identifiable information and data minimization"]
- § 9516(d)(2): add (D) - experts in privacy and security
- § 9602(g)(3): add (C) - "at least 3 individuals with expertise in student or child privacy, educational ethics, and cybersecurity in the education context"
- § 9605(b)(1): add (D) - contain at least 5 individuals with expertise in student or child privacy, educational ethics, and cybersecurity in the education context."

- § 9621(b)(1)(C): add “with expertise in student data privacy and security”
- § 9621(b)(1)(N): add “with expertise in student data privacy and security”

3. How could Congress strengthen the functionality, relevance, and role of the National Board for Education Sciences in leading IES research activities as well as education research performed across the Federal government?

As discussed in our answer to Question 2, it is important to require boards authorized under ESRA to include individuals with privacy and security expertise to increase institutions’ ability to protect student data. We have identified areas where there are opportunities to increase the privacy expertise of board memberships in our answer to Question 2.

5. How could Congress ensure better coordination among all Federal agencies conducting education research outside of IES?

To ensure better coordination among all Federal agencies conducting education research, ESRA should support, prioritize, and require that federal agencies look to minimize–if not avoid–requiring similar or identical data multiple times; rather, ESRA should establish a process to incentivize the federal government to improve efficiency within and between existing datasets–(both intra- and inter- agency) and aim to eliminate redundancy and unnecessary administrative burden at the state and local level. ESRA should also include clear indication of the extent to which NCES can create or implement data collections from state and local education agencies beyond what is authorized in federal statute.

Additionally, Congress could include a provision in ESRA formally authorizing PTAC and strengthening it to provide much needed privacy technical assistance for states and other entities/partners conducting education research. PTAC has played a vital role in providing technical assistance and best practices to districts, states, companies, and privacy advocates. Prior to PTAC’s creation in 2010, stakeholders were often afraid to ask the office that enforced FERPA – the Family Policy Compliance Office (FPCO) – for technical assistance or help in applying FERPA since they felt they might be penalized for asking clarifying questions. In addition, stakeholders would frequently not hear back from FPCO in a timely manner. Having a separate office that deals with questions from SEAs, LEAs, and other stakeholders – and generally responds within a week of receiving any question – has helped remedy those problems.

The student privacy legal and practical landscape is undergoing rapid, continual change–as seen in the over 130 new state student privacy laws passed since 2014 and new federal regulations on the horizon. States are struggling to navigate these changes, and PTAC’s rich technical assistance has improved student data privacy nationally by helping public and private education leaders better understand the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendments (PPRA), while also helping schools and other data holders implement privacy best practices. PTAC has been especially useful as states have changed their laws in helping stakeholders determine how their laws and practices work with FERPA and other federal privacy laws.

At the same time, PTAC has been overloaded with requests for technical assistance. Limited technical assistance leaves states sometimes opting not to do useful data analysis that federal law already allows them to do because of uncertainty about what is allowed in the current legal landscape. With more attention being paid to privacy and technology issues at all levels, there is a growing critical need for

accessible and practical guidance and technical assistance. Privacy technical assistance for states can be greatly improved by including a formal authorization of PTAC in ESRA. In authorizing PTAC, ESRA could strengthen PTAC by allocating the freedom, authority, and funding necessary to provide privacy technical assistance for states.

6. How could IES better support field-initiated research that promotes continuous improvement and timelier and more actionable research?

At the risk of stating the obvious, the most important thing that IES can do to promote more timely–and therefore, more actionable–research is to ensure that valid, reliable, and secure aggregate data and research findings are available as soon as possible. As the ability to collect, analyze and report data becomes easier and quicker, it is imperative ESRA support any and all effort to ensure that data is collected and available as quickly as possible, and as much as in 'real time' as possible. Related to this, to the extent that ESRA wants to support the use of federal education research by school-based practitioners, we cannot emphasize enough the importance of accurate data that can be used as close to in real time as possible. The longer the delay between submission and public availability, the less timely, and therefore less relevant and actionable, the research.

IES can also better support field-initiated research that promotes continuous improvement of the overall quality of education research by directing researchers to incorporate privacy and security best practices into their work. Incorporating privacy and security best practices into education research makes the findings more reliable and thus more actionable. Here are areas based on the current law where privacy and security best practices can be implemented:

- § 9512: add (7) - promote privacy, security, and confidentiality of student data
- § 9515(a)(2): add (D) - privacy and security harms are mitigated…
- § 9531(b)(1): add (E) - promote privacy, security, and confidentiality in education research
- § 9541(b)(3): add (C) - promotes privacy, security, and confidentiality
- § 9561(b): add (5) - to promote privacy, security, and confidentiality in education research and evaluation
- § 9567(b): add (4) - to promote privacy, security, and confidentiality in education research

8. How could IES bolster partnerships with the full range of partners – including but not limited to educators, school systems, institutions of higher education, including minority-serving institutions, public and private entities, localities and States, researchers, and the Federal government – to more effectively utilize, scale, and commercialize education research to improve teaching and learning?

To bolster partnerships when conducting education research, it is necessary to ensure that there is adequate trust amongst a full range of partners. Providing understandable privacy and security protections helps build that trust and mitigate the risks of data collection in education research. Here are areas based on the current law where additional privacy and security protections can be added:

- § 9533(a)(6): add "including privacy and security standards"
- § 9533(a)(10): add (E) - research on how educational service agencies mitigate privacy and security harms related to technology implementation, including

        - (i) the protection of student information from unauthorized access, destruction, use, modification, or disclosure;
        - (ii) the implementation and maintenance of reasonable security procedures and practices to protect student information; and
        - (iii) the implementation and maintenance of reasonable privacy controls
- § 9533(c)(2): add (L) - Privacy and security
- § 9534(a): add (5) - Develop standards for data security and privacy policies, and seek the input of experts, including those from security, cyber-security, and education fields that have experience with personal data protection, in developing such standards and policies.
- § 9534(b)(2): add (C) - develop procedures to evaluate the compliance of each recipient of an award of a research grant, contract, or cooperative agreement with applicable privacy, security, and ethical standards
- § 9562(a)(2)(D): add 'and privacy and security practices that protect student data'
- § 9563(a)(1): add (H) - conduct or support evaluations of privacy and security policies, practices, and trainings
- § 9573(b): change references to "individually identifiable information" to "personally identifiable information"
- § 9573(c)(1)(A): add ", including standards for data security and privacy policies. The Director shall seek the input of experts, including those from security, cyber-security, and education fields that have experience with personal data protection, in developing such standards and policies."
    - (i) The standards for data security and privacy policies shall include, but not be limited to:
        - (a) data privacy protections, including criteria for determining whether a proposed use of personally identifiable information would benefit students and educational agencies, and processes to ensure that personally identifiable information is not included in public reports or other public documents;
        - (b) data security protections, including data systems monitoring, data encryption, incident response plans, limitations on access to personally identifiable information, safeguards to ensure personally identifiable information is not accessed by unauthorized persons when transmitted via communication networks, and destruction of personally identifiable information when no longer needed; and
        - (c) application of all such restrictions, requirements and safeguards to third-party contractors.
- § 9573(d)(5)(A): change "individually identifiable information" to "personally identifiable information" with the same definition as FERPA in 34 CFR § 99.3

Additionally, requiring privacy and security training for researchers is essential to protecting privacy and building trust. Privacy and security training can help ensure that researchers understand the importance of protecting personal information and are equipped with the skills and knowledge to do so. Here are areas based on the current law where additional privacy and security training can be added:

- § 9534(a): add (6) - ensure that all researchers are trained in appropriate privacy, security, and ethical standards and requirements for conducting research
- § 9543(a)(1)(F): add (iii) - data on training provided to teachers and administrators related to privacy and security requirements and best practices in education
- § 9564(e)(5): "laboratories are consistent with the research and training standards described in section 9534 and the evaluation standards adhered to pursuant to section 9563(a)(2)(A)."

- § 9564(f)(1)(B)(iii): add “including best practices to preserve the privacy and increase protection of student data”
- § 9564(f)(1): add (D) - templates for data sharing agreements and contracts with researchers that prioritize and protect student privacy
- § 9602(f)(1)(A): add (iv) - privacy and security risks associated with education technology and education research
- § 9602(f)(1)(C): add “including privacy and security best practices”

Partnerships with the full range of partners aiming to more effectively utilize, scale and make widely available education research must focus efforts on shortening the lag between data collection and data availability. As discussed in our answer to Question 6, it is imperative ESRA support any and all effort to ensure that data is collected and available as much as in ‘real time’ as possible, especially to the extent that ESRA wants to support the use of federal education research by school-based practitioners. While it may be feasible to evaluate a given program using data with a five year lag, that is simply not functional for classroom- and school-level educators, who will rightfully be most interested in accessing data that can truly and directly inform the work they are doing with the students in their classrooms today.

Furthermore, we would like to note that including the word “commercialize'' in this question may not be the most appropriate way to frame the goal of having more scalable education research because prioritizing privacy protections for students in education research may come at the cost of having to make decisions that do not align with commercial goals. Additionally, framing scalability in terms of commercialization does not align with FERPA. FERPA protects students' privacy rights. While districts can hold student personally identifiable information (PII), FERPA generally requires schools to have written consent before a school can disclose PII from education records to third parties. However, FERPA includes several exceptions that allow PII to be disclosed without written consent. A lot of education research falls under the FERPA studies exception which allows for schools to share PII with researchers without parental consent. The studies exception requires a written agreement that mandates the destruction of PII when it is no longer needed for the study purposes. Entities cannot go from a researcher to a vendor contractually upfront without giving up the benefits of the studies exception - meaning researchers would have to get parental consent before students can participate in studies if they want to seamlessly transition to being a commercial vendor later on. There are many barriers standing in the way of parental consent that may prevent marginalized students from participating in education research if parental consent were required. Falling under the studies exception is crucial to education research because findings would not be effective in tackling intractable teaching and learning challenges disproportionately affecting marginalized populations without those populations being widely able to participate in the research - something that could be jeopardized if parental consent is required.