July 25, 2023

Vanessa Wrenn
Chief Information Officer
Technology Services and Digital Learning
North Carolina Department of Public Instruction

Via email

Dear Ms. Wrenn,

Thank you for the July 11, 2023, response to our letter sent June 20, 2023 outlining questions from the education technology industry regarding the process for Public-School Unit (PSU) data integration set to go into effect August 1, 2023. Our members are working with their PSU customers across the state of North Carolina in advance of the August 1 deadline but continue to have concerns about the process and requirements that may be difficult for vendors to meet. We respectfully request some additional guidance from the Department of Public Instruction (DPI) and flexibility for PSUs and vendors to adequately protect the privacy and security of student data by the deadline.

By way of background, SIIA is the principal trade association for the software and digital content industry. Our members serve customers in North Carolina and include the nation's leading publishers and innovative developers of digital products and services for K-20 education, including digital instructional materials, education software and applications, online educational programs, professional development and related technologies and services for use in education.

In our June letter, we asked, "how will vendor security and system architecture information be protected by DPI to avoid the risk of the roadmaps getting accessed by bad actors." The response was, "this information would be delivered to the PSU and not to the DPI. Therefore, we would not receive any information." We have not seen any guidance from DPI for PSU's on how to protect the required disclosure of vendor security and system architecture information. We are concerned that the requirements to outline fairly detailed security practices will lead to unnecessary breaches of student data if the information is improperly stored at the PSU level, or, for example, intellectual property disclosed in the form of system design documentation. It would be helpful to either allow vendors to certify that they align to the requirements or to have specific requirements for protecting this data at the PSU level.

We also asked in our June letter if all ed tech companies will need to comply with the standards. There continues to be confusion about which vendors need to sign the Data Confidentiality and Security Agreement for Online Service Providers and Public School Units ("Agreement"). The response from your office said that "Any

company that receives student data from a state system will have to follow this process." Some PSU's are requiring all vendors to sign, even those that do not receive or send data to the statewide system.

We've also heard some PSU's are adding additional requirements beyond the scope of the Agreement. The response to our question about modifications to the agreement said, "There are to be no changes to the Data Security Agreement." Current practices in the state differ from guidance from the office. We respectfully request clarification again for both vendors and PSU's looking to comply with the new guidelines.

Additional clarification regarding the requirement of an attestation or certification from a third-party regarding security standards and requesting a complete list of acceptable security standards is needed. It is not clear if the list provided in the Agreement and the Vendor Readiness Assessment Report are exhaustive. For example, is NIST-CSF an acceptable framework?

Vendor compliance with the third-party assessment standard will take significant time, in excess of the brief notification period allotted between May 15, 2023 and August 1, 2023, to help ensure alignment with internal operational processes. Granting a compliance grace period would help enable appropriate vendor alignment with the standard and would help minimize PSUs' risk of losing access to software vendors' services at the start of the 2023-2024 academic year.

The lack of ability to modify the Agreement presents several problems for vendors and are onerous to both vendors and the PSU. When enacted in August, the new requirements will have substantial cost implications in staffing, which will overhaul customer and technical support models. It will also impact the costs of technological services through additional mandated components and management costs. We've outlined some problems below and ask for some flexibility to negotiate the terms. Negotiation would not be used to lessen security protections but would allow for more precise contracts so vendors can actually meet the requirements. Alternatively, a clarification from DPI that vendors and PSU's may add addendums to the Agreement to clarify confusing terms would be helpful. Examples of some of the areas of concern are outlined below:

- The definition of shared data goes beyond the scope of data defined by the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99) and in North Carolina statute (Chapter 115C Article 29). Further, there are references to "restricted" and "highly restricted" data, however the terms are not defined nor clarified within the examples. Allowing vendors and PSU's to define the scope of data to be protected as they negotiate the terms of the contract would be more precise for the specific tool used and allow for alignment to state and federal law.

- The requirement to request advance written approval of a subcontractor from a PSU is unnecessary paperwork and puts the onus and the burden on the PSU. A requirement to ensure that the subcontractor adheres to specific practices would be a more streamlined approach that would continue to protect the data and lessen the burden on schools and vendors.

- The breach disclosure timeframe and requirements may be difficult to meet, if not impossible to meet. The Agreement requires 24 hours' notice which may not be enough time to identify what data was impacted nor the extent of the breach. This could lead to incomplete notification and disrupt the vendor's process to contain a suspected breach. Additionally, this section in the Agreement also outlines that the PSU may require the vendor to provide notice of a breach. This does not consider the fact that the vendor may not have the contact information for the student, parent, or employee and would be unable to complete that requirement without additional disclosure of information from the PSU. We would appreciate flexibility to work with the PSU to define the roles and responsibilities in the event of a data breach.

- Requirements limiting data storage and access may prevent companies that provide services like customer support outside of the continental United States to meet the terms of this contract. Flexibility to adapt the terms of the contract of when data may be accessed outside of the United States - such as for customer support - would be helpful.

- Requirement to maintain a log of all student data received under the Security Agreement is burdensome and will require additional resources. Alternatively, including a list of categories of data shared and maintained throughout the terms of the agreement would accomplish the task.

We appreciate your time and attention to these concerns. We understand that the deadline is fast approaching and would again appreciate additional flexibility so vendors and PSU's can successfully protect student information.

Regards,

Sara Kloek
Vice President, Education and Children's Policy
Software & Information Industry Association