615 Martin Luther King Jr. Blvd • Bristol, TN 37620
(423) 652-9451 • Fax (423) 652-9238 • www.btcs.org

Meeting of the Committee on Education and the Workforce, May 17, 2018
U.S. House of Representatives

Written Testimony of Gary Lilly, Ed.D.
Director of Schools, Bristol Tennessee City Schools

Good morning, I am Gary Lilly, superintendent of schools in Bristol, TN. I am honored to be here.

School systems educate a very popular demographic. From businesses to youth rec leagues, it sometimes seems like everyone wants to get access to our students. What keeps me awake at night is knowing that there are bad actors around the world who are actively working to find, compromise, and sell student data that should be kept private.

And, schools typically collect a lot of data about students:

> To register a student, we need his or her basic demographic information, such as their name, address, phone number, gender, and race. But we also have to be able to differentiate one John Smith from another John Smith, either within our own district, or from the district down the road. That means either collecting their social security number or assigning some other unique identifier.
>
> We ask for their parents' information, emergency contacts, and any medical conditions they may have.
>
> And, all of that is just to get them enrolled. Over the course of their K-12 educational career, we amass even more data. We store the classes they take, the grades they make, their attendance, standardized test scores, if they're eligible for free or reduced lunch, any disabilities they may have, and log their behavior.

My district keeps all of this information in an online database, which is stored on a secured server behind two firewalls. Even so, the state I'm from, Tennessee, requires districts to sync information to their statewide system daily.

Hopefully, you're seeing that student data is accessible to many people on various systems legitimately. Like most districts, we are taking steps to protect that data to the extent that we can. We check and vet all of our employees before hiring them and also restrict the type of data they can access based on their role.

We have quarterly meetings to discuss student and employee data and privacy protections. The problem is that it's difficult to think like a criminal if you're not one, so we use a service called BrightBytes Digital Privacy, Safety & Security that leads administrators through a questionnaire and offers support and documentation that helps us think about changes we should consider to our policies, professional development programs, systems and infrastructure, and incident response.

We also use a managed internet service provider, Educational Networks of America, which uses traffic pattern analysis and other methods to identify attacks and mitigate their impact.

We do work with a number of educational service providers that store student data. We are currently working on verbiage for contracts with outside vendors to ensure there are safeguards for data stored off-site. We want to know how they are using that data: Where is it stored? To whom is it disclosed? And, when we no longer have a contract, how will it be disposed?

Internally, we continually attempt to educate both employees and students about the importance of protecting their data and digital citizenship.

Earlier this year, we actually hired a firm to run a phishing test on our employees so we could better target individual opportunities for development. Because we talk about it all the time, I was sure that we wouldn't have many, if any, fall for a phishing attempt.

I was shocked when the results suggested that almost 20% of our folks were "phish-prone!" – And, even that is supposedly a good bit lower than the industry average. It was definitely eye-opening and a good reminder that we need to stay vigilant.

I appreciate that you all want to assist with the work that we are doing to protect our students. Title IV(a) in ESSA allows districts the flexibility to do what we need to do to assess and harden data systems. It is also imperative that we have support to educate both students and employees about how to safeguard data and privacy.

The Family Educational Rights and Privacy Act also needs to be regularly reviewed and updated to keep up with the pace of technology. Ideally, the federal policy will align with and complement state and local efforts. I encourage you to see what works, what doesn't, and explore any unintended consequences that might create impediments for districts. I further encourage you to begin by clearly defining what is considered an education record, including digital files. Currently, there is considerable confusion regarding what must, may, or may not be disclosed.

For the first time ever, our district purchased a cyber-protection insurance policy this year. It is my sincere hope and prayer that we never have a need for it. Any help you can provide to make the policy unnecessary will be greatly appreciated.

Thank you!