MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

September 17, 2020

The Honorable Betsy DeVos
Secretary
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202

Dear Secretary DeVos:

I write to you about the need for effective cybersecurity in the context of our nation's K-12 education system. As COVID-19 has placed a strong emphasis on remote learning throughout the United States, this new normal also highlights the heightened need to protect education infrastructure from cyber-attacks, provide measurable standards, and ensure educators are equipped to manage cybersecurity risk.

Virginia's Fairfax County Public Schools, a local school division with nearly 200,000 students and over 24,000 employees, was recently the target of a cyber and ransom attack that included theft of protected information. While an investigation proceeds, the incident in Fairfax County demonstrates the need for schools to be prepared with cybersecurity defenses and resilience. A ransomware attack on a school system in normal times can be disruptive and costly; in the context of a global public health emergency, with unprecedented reliance on remote learning, it is debilitating.

Sophisticated cyber-attacks and more opportunistic forms of malware, like ransomware, are widespread today and require sustained vigilance. Defending against these persistent attacks requires a consistent and holistic approach. The public sector is particularly at risk given constrained state and local budgets. It is too late to wait for a cyber-attack before taking action to ensure school systems and personal data is secure and available.

I urge the U.S. Department of Education to develop baseline cybersecurity standards for K-12 schools and institutions of higher education and to work with school districts to develop a risk-based and comprehensive appropriations request for FY2022. Many school districts do not currently have sufficient guidance to implement an effective cybersecurity program. Fortunately, there is cybersecurity guidance available that could be tailored for education. Existing cybersecurity frameworks, such as National Institute of Standards and Technology (NIST) and Cybersecurity and Infrastructure Security Agency (CISA) guidance, can be adapted and applied for our school systems. We have seen a range of sectors develop customized Framework Profiles that tailor the NIST Cybersecurity Framework to the particular risks, resources, and circumstances of a particular sector.

I recommend providing schools with guidance that includes awareness campaigns, risk management, threat mitigation, cybersecurity posture reviews, and resiliency. Awareness campaigns for both educators and students can focus on the importance of recognizing threats, such as phishing attacks, ransomware, malware, and social engineering methods. Regular evaluations can determine the effectiveness of awareness campaigns to address any gaps. Threat mitigation includes developing sufficient safeguards to ensure data security and access control. Detection capabilities are also needed to continuously monitor for anomalies and cybersecurity events. Schools should review these capabilities, plus their readiness to respond and recover from attacks. For example, tabletop exercises can validate processes and test procedures used before, during, and after an attack. Cyber resiliency ensures systems have an ability to continue operating in case of attack, while full restoration takes place. Many of these objectives will require new funding from Congress, particularly in the wake of the devastating impact COVID-19 has had on school system budgets.

In addition to protecting school infrastructure, I urge you to develop guidance and disseminate best practices to states and localities seeking to teach cybersecurity in the K-12 setting. For example, the Cyberspace Solarium Commission recommends that the U.S. Government promote professional development programs to model safe, secure, and privacy-aware internet practices in classrooms. The Commission also recommends incorporating effective digital literacy curricula in American classrooms at the K-12 level and beyond, including critical thinking and problem solving skills.[1]

Finally, I urge the Department of Education to work with educators, industry, and CISA to encourage a consortium or Information Sharing and Analysis Center (ISAC) for K-12 schools to exchange cybersecurity threat information and best practices for defense. Such an organization could be a counterpart to the existing Research and Education Networks ISAC that focuses on higher education. Because K-12 schools have very different missions and resources than higher education institutions, I would encourage particular attention to ensuring such efforts meet K-12 educators where they are – with information sharing, best practices, and action items tailored to account for capabilities and constraints of K-12 schools.

Our nation faces increasing cybersecurity threats on our infrastructure. As the recent Fairfax County Public Schools incident demonstrates, our schools need vigilant defenses from these threats, similar to private industries and government. Adversaries have shown a willingness to attack our education facilities, and schools must be proactive, attentive, and proficient at cybersecurity. While the nation confronts the COVID-19 public health emergency, an increased reliance on remote learning makes the need for effective threat defense paramount.

[1] U.S. Cyberspace Solarium Commission Final Report (March 2020).

Schools have a unique strategic role in our nation’s cybersecurity posture through educating students and tomorrow’s leaders of essential cybersecurity practices. I urge you to take necessary steps to ensure schools have adequate guidance to defend attacks and provide a cybersecurity education. Thank you for your consideration of these issues and your timely response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator