United States Senate

WASHINGTON, DC 20510-3205

August 19, 2025

The Honorable Linda E. McMahon
Secretary
U.S. Department of Education
400 Maryland Ave., SW
Washington, D.C. 20202

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
3801 Nebraska Avenue, NW
Washington, DC 20528

Dear Secretary McMahon and Secretary Noem,

We write to respectfully raise concerns over recent cuts affecting K-12 cybersecurity and digital infrastructure. In recent years, K-12 school districts have experienced an increase in data breaches and cyberattacks, posing a serious threat to student safety and privacy. For this reason, we urge the administration to take immediate action to restore funding and staffing levels for Cybersecurity and Infrastructure Security Agency (CISA) K-12 cybersecurity programs and programs within the Department of Education (ED) that support the critical need for K-12 cybersecurity.

A resilient digital infrastructure is foundational to the integrity of our education system and safeguarding our students and faculty. Under the Family Educational Rights and Privacy Act, school districts are obligated to safeguard a vast quantity of personally identifiable information (PII), including student and faculty names, birth dates, Social Security numbers, health information, and financial details. This data is especially valuable to cyber criminals who use PII to commit fraudulent behavior that can have detrimental long-term effects on students and families. Cutting funding for schools and eliminating federal programs and resources that support cybersecurity for K-12 leaves personally identifiable information vulnerable to cyberattacks.

K-12 schools are a prime target for cyber criminals because they are perceived as having valuable data and weak cybersecurity infrastructures. From July 2023 to December 2024, approximately 82% of schools reported experiencing at least one cyber incident, with over 9,300 confirmed incidents across an estimated 5,000 K-12 institutions.[1] A 2024 Department of Homeland Security threat assessment identified K-12 school districts as being a "near constant ransomware target" because of a lack of resources that affect their ability to prevent and respond to cyberattacks.[2] This is primarily because schools do not have a dedicated funding stream to maintain resilient digital infrastructure, or the personnel needed to navigate a complex digital

[1] https://www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report
[2] https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

landscape. A recent report by the Consortium for School Networking showed that approximately 61% of school districts use general funds to pay for their cybersecurity efforts and about 44% outsource cybersecurity monitoring because of limited funds and personnel.[3]

Additionally, cyberattacks impose a significant financial burden on schools and school districts. According to a 2022 U.S. Government Accountability Office (GAO) report, school districts lose between $50,000 and $1 million per cyberattack.[4] This is not the time to cut programs and resources at CISA or ED. As schools face significant funding and staffing cuts this upcoming school year, many will be left without the resources, personnel, or funds to navigate an increasingly complex digital threat environment on their own. Students and school personnel will suffer as a result.

Despite the growing threat to K-12 cybersecurity across the country, the administration is taking steps to weaken federal support for K-12 cybersecurity and digital infrastructure. We urge the administration to reverse course and reinstate the programs to their previous funding and staffing levels. Specifically, we ask you to:

- Reject the proposal in the President's budget to slash $491 million from CISA and reduce its workforce by over 1,000 positions and restore full funding and staffing levels to the Agency.[5]
- Reverse funding cuts to CISA's Multi-State Information Sharing and Analysis Center (MS-ISAC) by $10 million to allow the program to continue conducting K-12 outreach, real-time incident response, and threat intelligence sharing – all valuable resources that many school districts could previously obtain at no cost.
- Restore ED's K-12 Cybersecurity Government Coordinating Council, which aligned resources and facilitate collaboration with state and local education systems to share key intelligence information that is not easily accessible to schools.
- Restore ED's Office of Education Technology (OET) which helped support K-12 schools adopt and implement cybersecurity measures, maintain a resilient digital infrastructure, and implement new technologies in schools.

Eliminating these resources makes school systems more vulnerable to what would've been preventable threats under proper guidance and support.

Students, faculty, and staff at K-12 schools should never have to fear that their personal safety and privacy is at risk. The federal government has a responsibility to protect high-risk sectors that are increasingly susceptible to cyberattacks, especially when the primary individuals at risk are minors. As such, we urge ED and DHS to establish a dedicated stream of funding for K-12

---

[3] https://www.cosn.org/wp-content/uploads/2025/05/EdTechLeadership_2025_F2.pdf
[4] https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done
[5] https://cyberscoop.com/trump-administration-proposed-cisa-budget-cuts/

schools and reinstate programs that provided essential technical assistance, guidance, and support for K-12 cybersecurity efforts. We request responses to the following questions by XXX:

1. What actions is ED taking to ensure K-12 schools are prepared to prevent and respond to cyber incidents ahead of the upcoming school year?
    a. Are there any planned actions to update guidance, toolkits, or provide technical assistance to schools ahead of the upcoming school year?
2. How has ED been communicating with state and local education systems to ensure a coordinated and effective response to cyberattacks?
3. What resources are available to help school districts, especially those in rural or underserved areas, conduct risk assessments and adopt security measures?
4. Will ED commit to restoring or replacing the K-12 Cybersecurity Government Coordinating Council or the Office of Educational Technology?
    a. If not, what plans are there to support resilient digital infrastructure, digital equity, and effective cybersecurity measures? Which office within ED currently has primary responsibility for cybersecurity?
5. Will DHS commit to restoring funding for MS-ISAC?
    a. If not, what plans are thereto replace the K-12 outreach, incident response, and threat intelligence sharing functions carried out by MS-ISAC for which MS-ISAC will have reduced capacity following cuts?
6. What are the administration's plan to ensure long-term cyber resilience in schools, including technical assistance and funding to schools to train or hire personnel?

Sincerely,

Kirsten Gillibrand
United States Senator

Elissa Slotkin
United States Senator

Amy Klobuchar
United States Senator

Richard Blumenthal
United States Senator

Lisa Blunt Rochester
United States Senator

Mark R. Warner
United States Senator

Jacky Rosen
United States Senator

Tina Smith
United States Senator

Jon Ossoff
United States Senator