K-12 Cybersecurity Fact Sheet

Request: Support the bipartisan *Enhancing K-12 Cybersecurity Act (H.R.2845 and S.1191)* introduced by Rep. Matsui, Rep. Nunn, Sen. Blackburn, and Sen. Warner to help school districts and state education agencies enhance their schools' cybersecurity readiness, mitigate risks, prevent breaches, and protect their networks and confidential data from ransomware and other cyberattacks. In addition, encourage the Federal Communications Commission to update the E-rate program's firewall definition and ensure applicants can use the program's Category 2 funds to acquire advanced or next generation firewalls.

Background: Cyberattacks on K-12 schools have grown steadily in recent years, including a surge of new attacks in 2022. These costly attacks cause loss of instructional time, disrupt administrative activities, compromise confidential student and employee data, and severely impact school budgets.

Given the persistent and increasing number of these attacks, federal and state policymakers have considered dozens of bills and approved several new laws designed to address the issue. CoSN's annual K-12 cybersecurity legislative trends report shows that legislators in 36 states introduced at least 232 cybersecurity bills that focused directly or indirectly on the education sector. 18 states adopted 37 cybersecurity laws with direct or indirect application to the education sector. At the federal level, legislators introduced 22 cybersecurity bills, including two bills focused on elementary and secondary education and four measures focused on postsecondary institutions. Additionally, the FCC invited public comment about whether the E-rate program should be modernized to cover advanced or next generation firewalls.

Talking Points:

- School districts and state education agencies often lack the significant resources and expertise required to defend school networks and confidential data from sophisticated cyberattacks. Lower wealth communities are at a particular disadvantage relative to their better resourced peers when it comes to assembling the technical, human, and other safeguards that are part of a multifaceted K-12 cybersecurity strategy.
- According to CoSN's 2023 annual leadership survey, only 16% of districts have a full-time employee dedicated to network security. Further, 13% of districts do not provide cybersecurity training to their teachers, 12% do not provide training to administrators, 14% do not provide it to support staff, and, perhaps most alarmingly, 33% do not provide training to students.
- Dedicated federal funding, technical resources, and leadership are needed to ensure that school districts can acquire the technology and expert staff required to monitor and protect networks and data.
- State education agencies and school districts would greatly benefit from a more coordinated response to cybersecurity which would help them leverage their limited resources and funding. New mandates without resources are not helpful.