DORIS O. MATSUI
6TH DISTRICT, CALIFORNIA

COMMITTEE ON ENERGY AND COMMERCE

SMITHSONIAN INSTITUTION, BOARD OF REGENTS

Congress of the United States
House of Representatives
Washington, DC 20515-0506

WASHINGTON OFFICE
2311 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-0506
(202) 225-7163

DISTRICT OFFICE
ROBERT T. MATSUI U.S. COURTHOUSE
501 I STREET, SUITE 12-600
SACRAMENTO, CA 95814
(916) 498-5600

http://matsui.house.gov

December 8, 2022

The Honorable Jessica Rosenworcel
Chairwoman
Federal Communications Commission
45 L Street, N.E.
Washington, D.C. 20554

Dear Chairwoman Rosenworcel,

As cyber incidents targeting K-12 institutions grow more frequent and severe, I write to urge the Federal Communications Commission (FCC) to reevaluate its abilities and limitations in combating this threat. While the FCC has certain targeted tools to protect K-12 institutions, it is imperative that these tools keep pace with modern technological advances and compliment other federal cybersecurity efforts to keep our students and educators safe.

Resource-constrained K-12 institutions are struggling to keep up with cybercriminals that employ rapidly evolving tactics to steal sensitive data, disrupt learning, and threaten school safety. On September 6, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the MultiState Information Sharing and Analysis Center (MS-ISAC) released a Cybersecurity Advisory (CSA) outlining the significant cyber threat facing K-12 institutions. The CSA notes that certain cyber criminals are "disproportionately targeting the education sector with ransomware attacks," and that "the FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks." This warning is reinforced by the rise in ransomware attacks documented by the 2022 State of K-12 Cybersecurity Annual Report which found that 2022 was "the third straight year that there have been more than 50 publicly disclosed K-12 ransomware attacks and the first year it was the most frequently experienced type of cyber incident cataloged by the K-12 Cyber Incident Map."

In 1999, the FCC added cybersecurity capabilities to the schools and libraries universal service support program (E-rate) by including "basic firewalls or firewall services" as an eligible expense. Since then, firewall technologies and the complexity of cyber threats facing schools have advanced significantly. And, though these basic firewalls may be productive in preventing some of the most routine and unsophisticated cyberthreats, they fall far short of adequately addressing the threat landscape schools face today. While the E-rate program must continue to

prioritize expanding broadband connections for students, there is still an urgent need to help under resourced schools acquire the cyber protections they need.

Many federal partners have responsibilities in K-12 cybersecurity including the FCC and a concerted government approach is needed. To determine whether and how E-rate may be modernized, I urge you to coordinate with other federal agencies as you consider an appropriate path forward. Regular consultation with other federal agencies will help ensure any E-rate updates avoid duplication with other government efforts and balance E-rate's focus on connections while allowing the existing cybersecurity capability to stay relevant.

I appreciate your attention to this important issue and look forward to working with you to provide students and teachers with the safe, high quality broadband connections they need to succeed.

Sincerely,

Doris Matsui
Member of Congress