

**STATEMENT OF
COMMISSIONER GEOFFREY STARKS**

Re: *Schools and Libraries Cybersecurity Pilot Program*, Report and Order, WC Docket No. 23-234 (June 6, 2024).

Our schools possess massive amounts of data about students, including their social security numbers, health records, disciplinary records, and other personally identifiable information. Accordingly, schools are target rich environments for cyberattacks, such as ransomware, and are low hanging fruit because they are often resource constrained and lack cyber expertise. Bad actors know this, and take advantage of it. According to Verizon's 2024 Data Breach Investigations Report,¹ the education services sector experienced 1,780 attacks in 2023, up 258% from last year.² CISA and the Department of Education have developed free resources to help schools protect their networks, which I applaud, but our schools and libraries need additional help.

I'm proud to support today's E-Rate Cybersecurity Pilot that will make \$200 million available to schools and libraries to protect their networks against the threats they face every day. The E-Rate program is one of the Commission's most important and successful programs. But the connectivity we support must be secure. This Pilot will provide us with the information necessary to analyze whether and how the Commission should update our E-Rate program to help schools and libraries help themselves against the ongoing cyber threat.

I continue to work diligently to ensure our networks are secure in the United States, and I thank the Chairwoman for her leadership in considering how E-Rate can be an asset to protect school and library networks. I also thank her for taking my edits regarding the budget, as well as ensuring the Pilot produces the type of data necessary to analyze the Pilot's success. I want to thank the staff who worked on this item. I approve.

¹ See Verizon 2024 Data Breach Investigations Report, available at <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>.

² Reports about school or library system attacks abound. Major districts such as the Los Angeles Unified School District, Baltimore County Public Schools, Broward County Public Schools, the Minneapolis Public School system, the Fulton County School District, and the Albuquerque Public Schools have publicly announced attacks in recent years, impacting hundreds of thousands of current and past students. See Howard Blume, *L.A. Unified data breach last year includes at least 2,000 student records, officials say*, Los Angeles Times, Feb. 22, 2023, <https://www.latimes.com/california/story/2023-02-22/lausd-cyber-attack-includes-at-least-2-000-student-records>; Luke Barr, *Baltimore schools cyber attack cost nearly \$10M: State IG*, ABC News, Jan. 25, 2023, <https://abcnews.go.com/US/baltimore-schools-failed-fully-act-security-recommendations-cyber/story?id=96671802>; Amanda Batchelor, *Hackers post filed after Broward school district refuses to pay ransom*, Local10.com, Apr. 20, 2021, <https://www.local10.com/news/local/2021/04/20/hackers-post-files-after-broward-school-district-doesnt-pay-ransom/>; Alexandra Simon, Jennifer Hoff, *Minneapolis Public Schools confirms hackers release personal data*, KARE11, Mar. 17, 2023, <https://www.kare11.com/article/news/local/minneapolis-public-schools-confirms-hackers-released-personal-data/89-8e682442-2da4-434f-8e03-19f5d08009fe>; *Fulton County Schools investigating possible security breach of computer systems*, FOX5 Atlanta, Jan. 31, 2024, <https://www.fox5atlanta.com/news/fulton-county-schools-security-breach-computer-systems>; *A cyberattack in Albuquerque forces schools to cancel classes*, NPR, Jan. 14, 2022, <https://www.npr.org/2022/01/14/1072970219/cyber-attack-in-albuquerque-latest-to-target-public-schools>.