Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Eligible Services List (ESL)	)	WC Docket No. 13-184
For The Schools And Libraries	)	
Universal Service Support Mechanism	)	
	)	

COMMENTS OF THE COUNCIL OF THE GREAT CITY SCHOOLS

The Council of the Great City Schools is pleased to submit comments in response to the Public Notice on the Proposed Eligible Services List for the FY 2023 E-Rate Program (WC Docket No. 13-184; DA 22-878) and urges the Commission to make all firewall components and services eligible for E-Rate support under Category Two budgets for the upcoming program year.

The Council of the Great City Schools includes 77 school districts, or less than one-half of one percent of the approximately 14,000 school districts in the U.S., but as the nation's largest urban school systems, our members enroll approximately 8 million students, including approximately 28 percent of the nation's Hispanic students, 29 percent of the nation's African American students, and 25 percent of the nation's children living in poverty. The value of the E-Rate is apparent every day to the districts in the Council, as we serve the highest numbers and concentrations of disadvantaged children, employ the largest number of teachers, and operate in the greatest number of outdated and deteriorating buildings.

E-Rate Support Needed to Prevent Cyberattacks

The Council once again requests that the Commission consider the inclusion of advanced firewall components and services as part of the E-Rate's Eligible Services List. Cyberattacks on urban school districts have continued since our request last year, with the nation's second largest school system, the Los Angeles Unified School District, the most recent victim. Cyberattacks and ransomware demands not only threaten the exposure of records containing student, staff and financial data, but can result in the loss of instructional and operational time. The federal Cybersecurity and Infrastructure Security Agency (CISA) noted in their September 6, 2022 National Cyber Awareness System Alert that malicious actors have been, "disproportionately targeting the education sector with ransomware attacks."

In the 2019 Category Two Report and Order, the Commission declined to make any additional services eligible, noting that applicants should prioritize their Category Two funding requests on deploying high-speed broadband. Since that time, however, the COVID-19 pandemic increased 1:1 instruction, moved a large portion of teaching and learning online, and expanded educator reliance on content-rich media sources. Even with most students and staff returning to physical classrooms last year, school districts are working diligently to ensure the benefits of digital learning continue to be a part of their educational offerings. With the increase in disruptive threats and online services, a robust and safe network is needed

to maintain the volume of learning platforms and blended instructional approaches that are in place, as well as ensuring continuity of district services. School districts cannot sacrifice one for the other and must prioritize both broadband access and security.

A recent Council report on Best Practices in Procurement included a chapter on cybersecurity, highlighting the importance of educating staff about phishing and emphasizing password and authentication security, but most importantly, investing in proper cybersecurity. Urban school districts are doing what they can to train and inform the school community about online behavior, but the importance of having the right cybersecurity software, encryption devices, and firewalls cannot be overstated. Having a strong first line of defense in place is costly but can help prevent these types of attacks.

Urban school districts have taken a proactive role in preventing attacks, and Council members have shared best practices in cybersecurity among themselves, alerted each other of breaches in their systems, and facilitated discussion about plans and tools to prevent further security incidents. IT professionals know it is incumbent upon them to develop a formalized strategy for maintaining a secure network, identify and close gaps in network vulnerabilities, educate all individuals within their school community about their role in cyber secruity, and find recurring funding sources to invest in needed network security tools. A coordinated federal effort is needed to ensure that school districts are protected from cyber threats and disruptions, and the Commission should lead the way with E-Rate support.

Petitioners for Rulemaking on Cybersecurity Agree on the Need for E-Rate Support

Last year, the Council joined the Consortium for School Networking (CoSN), the State Educational Technology Directors Association, the Schools, Health & Libraries Broadband (SHLB) Coalition, the State E-rate Coordinators Alliance, and the Alliance for Excellence in Education in filing a Petition for Rulemaking. That submission described the importance of helping school districts prepare for the increase in cyberattacks and advocated for updating the E-Rate to help school districts tackle their increasing security needs. We repeat the request made in that filing in these comments: the Commission should update the E-Rate's ESL to define all firewall and related features as "basic," increase the Category 2 budget cap, and adopt a broadband definition inclusive of cybersecurity.

In their comments on last year's ESL, CoSN explained that the E-Rate's inadequate support for cybersecurity should be strengthened, as the program currently provides protection "in name only." Urban school districts must bear the cost of these services almost entirely on their own, and as CoSN explained, "This programmatic shortcoming limits the cybersecurity tools available to E-rate recipients that lack the resources to acquire even basic cyber protections like firewalls." The SHLB Coalition highlighted the financial implications for school districts in their ESL comments, sharing that, "The FBI issued a joint advisory last December 2020 based on an increase in ransomware attacks against K-12 educational institutions. Many cyber-attacks try to obtain confidential student data and threaten to leak it unless organizations pay a ransom."

The CISA Alert discussed above repeated these warnings again in their September 6th bulletin, sharing that, "Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff." The SHLB's comments from last year also noted a CISCO report which cited an increase in the percentage of reported ransomware incidents involving K-12 schools from 28% in the first half of 2020 to

57% in the fall. The September 6th alert from CISA reiterated 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."

E-Rate Support Can Protect Networks and Control Rising Costs

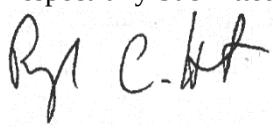
In response to the rising attacks in recent years, many districts have been forced to purchase Cyber Liability Insurance. E-Rate firewall support will not only directly increase the security for schools nationwide, but the availability of more widespread protection may also help stabilize the cost of cybersecurity insurance premiums, which have increased by as much as 100-150% for some urban districts in the past year. Coverage for the financial consequences of electronic security incidents and data breaches is costly, but E-Rate support for firewall services can help lower the risk that insurance companies cite for rising premiums, as well as the number of targets nationwide.

The technology needs that existed in school districts nationwide became plainly apparent when the COVID-19 pandemic resulted in school closures, hybrid learning, and synchronous/asynchronous instruction. The increased digital access that has followed provides clear academic advantages, but the growing number of online users, devices connected to our networks, and demand for technical support has only added to the security-related costs that school districts have been bearing almost entirely on their own.

Conclusion

Urban schools are grateful for the efforts by the Commission to connect students and families off-campus through the Emergency Connectivity Fund and Affordable Connectivity Program, as well as the historic and ongoing support that E-Rate provides to connect our classrooms. As we work with the Commission to deploy reliable and high-speed internet access that our school districts need, all stakeholders must ensure that the networks our school districts rely on for teaching, learning, and operations are protected from malicious actors and the growing threats of cyberattacks. We urge the Commission to lead the way with federal support for the cybersecurity costs our districts are facing to undertake these efforts.

Respectfully Submitted,



Raymond Hart, Executive Director
Council of the Great City Schools

Address:
Council of the Great City Schools
Suite 1100N
1331 Pennsylvania Avenue, NW
Washington, DC 20004

Member districts: Albuquerque, Anchorage, Arlington (Texas), Atlanta, Aurora, Austin, Baltimore, Birmingham, Boston, Bridgeport, Broward County (Ft. Lauderdale), Buffalo, Charleston County, Charlotte-Mecklenburg, Chicago, Cincinnati, Clark County (Las Vegas), Cleveland, Columbus, Dallas, Dayton, Denver, Des Moines, Detroit, Duval County (Jacksonville), East Baton Rouge, El Paso, Fayette County (Lexington), Fort Worth, Fresno, Guilford County (Greensboro, N.C.), Hawaii, Hillsborough County (Tampa), Houston, Indianapolis, Jackson, Jefferson County (Louisville), Kansas City, Long Beach, Los Angeles, Miami-Dade County, Milwaukee, Minneapolis, Nashville, New Orleans, New York City, Newark, Norfolk, Oakland, Oklahoma City, Omaha, Orange County (Orlando), Palm Beach County, Philadelphia, Phoenix, Pinellas County, Pittsburgh, Portland, Providence, Puerto Rico, Richmond, Rochester, Sacramento, San Antonio, San Diego, San Francisco, Santa Ana, Seattle, Shelby County (Memphis), St. Louis, St. Paul, Toledo, Toronto, Tulsa, Washoe County (Reno), Washington, D.C., and Wichita, and Winston-Salem (Forsyth County).