Val Verde Unified School District
975 W Morgan Street • Perris, CA 92571 • 951-940-6100

Dear Chairwoman Rosenworcel and Commissioners:

The Val Verde Unified School District requests that cybersecurity equipment, licenses and services be added to the E-Rate Eligible Services List (ESL). Cybersecurity incidents have grown far beyond the capabilities of most school districts and directly impact the mission of E-Rate, to the point where almost daily another school district's network is damaged or completely shut down anywhere from a few weeks to months, directly impacting the ability of students to access educational resources.

As a medium sized suburban school district within California with over 19,300 students of a diverse socioeconomic background, we are incredibly proud of our students, their achievements and our staff's ability to employ transformative instructional practices supported by modern technology. Our commitment to impacting the lives of our students and community has earned exclusive recognition at both the state and national level. However, much like our peers across the country, our ability to continue to fund and provide a safe and stable technology environment is under direct threat from cybersecurity attacks.

The federal Cybersecurity & Infrastructure Security Agency (CISA) found that in August and September of 2020, 57% of all ransomware incidents reported to MS-ISAC involved K12 schools. *(Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data | CISA www.cisa.gov/uscert/ncas/alerts/aa20-345a)*

In the 2022 Sophos report on The State of Ransomware in Education 2022, 56% of K12 education institutions were hit by ransomware, demonstrating a sharp increase from just the previous year. Of these, nearly 72% resulted in the encryption of data, a much higher percentage than that of commercial companies. These attacks had a devastating impact on the organizations, with the cost to remediate the attack averaging $1.58 million and 26% taking 1-6 months to recover. *(The State of Ransomware in Education 2022 | Sophos www.sophos.com/en-us/whitepaper/state-of-ransomware-in-education)*

This increase in attacks is largely due to vast bandwidth and extensive amount of technology, rivaling many large companies, such as instructional programs providing one or more devices *per student*, STEAM technology devices in labs and classrooms, sophisticated security systems including smart cameras and visitor screening systems, indoor and outdoor wireless infrastructure to support the vast network, growing IoT devices for students and facilities, and ever increasing amounts of private sensitive data. As a result, school districts are a rich ecosystem of modern technology that is ripe for exploitation if not sufficiently protected.

Unfortunately, by stark contrast, school districts do not have dedicated funding for skilled 24/7 cybersecurity staff. In fact, most school districts rely on general technology staff, a small number of engineers and the technology director to stay abreast of cybersecurity trends and implement protections. This is often extremely difficult to balance between limited time and funding, while also serving the technology needs to support the district mission.

In addition, insurance companies, notably in California, are exiting the cybersecurity insurance space due to the limited defense posture of their clients and the increasing incident costs involved, often amounting to several million dollars for a single event. Those few companies who continue to offer cybersecurity insurance are increasing premiums to unprecedented levels and requiring reasonable, yet significant, protections. These requirements include not only standard network hardware such as next generation firewalls, but also include holistic protection and prevention including endpoint protection, infrastructure monitoring and prevention, penetration testing, multi-factor authentication (MFA) for *all* staff (including part-time and occasional substitute staffing), mandatory annual cybersecurity training and simulated phishing attacks.

Val Verde Unified School District
975 W Morgan Street • Perris, CA 92571 • 951-940-6100

This lack of available insurance providers and increasing costs have sparked several risk management industry experts to compare the cybersecurity insurance space with California wildfire insurance. The ability for school districts to obtain insurance is quickly becoming unstable between the lack of providers, the cost of premiums for those that remain and the cost of implementing adequate protection.

We feel that supporting cybersecurity tools and services through the E-Rate program is not only appropriate under the FCC's existing goals for Universal Service, but also has reached a critical point as illustrated by the increasing attacks on school districts, notably the recent attack on the Los Angeles Unified School District. It is also important to recognize that eligibility needs to include broader holistic services as mentioned above, potentially including 24/7 fully managed cybersecurity monitoring and remediation services. Simply funding additional security licensing on top of current network equipment, such as next generation firewalls, only addresses one area of recommended surface attack protections.

While successfully funding cybersecurity services might be a complex task, over the last several years the total demand for E-Rate funding has fallen short of the allocated funding. Based on the Commission's annual announcements of the E-Rate program cap, available carry forward funds, and program demand, it appears that there is an opportunity for the Commission to revisit the per-student Category Two funding allocations to equitably distribute leftover funds to support cybersecurity.

Historic E-Rate Program Available Funds Compared to Demand (in Billions):

Year	Program Cap*	Carry Forward Funds	Total Available Funds (Cap Plus Carry Forward)	Category One Demand	Category Two Demand	Total Demand	Leftover Funds
2016	$3.94	$1.90	$5.84	$2.33	$1.28	$3.61	$2.23
2017	$3.99	$1.20	$5.19	$2.30	$0.90	$3.20	$1.99
2018	$4.06	$1.20	$5.26	$2.03	$0.75	$2.77	$2.49
2019	$4.15	$1.00	$5.15	$1.91	$0.99	$2.90	$2.25
2020	$4.23	$0.50	$4.73	$1.74	$1.17	$2.91	$1.82
2021	$4.27	$0.50	$4.77	$1.69	$1.34	$3.03	$1.74
2022	$4.46	$0.50	$4.96	$1.64	$1.51	$3.15	$1.81

On behalf of our students and communities we serve, we request the Federal Communications Commission authorize the ongoing, permanent use of E-Rate Program funds for cybersecurity equipment, licenses, and services.

Sincerely,

Michael McCormick
Superintendent

Matt Penner
Director of Information & Instructional Technology

Daniel Whitfield
Director of Risk Management