Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of:	)	
	)	
Schools and Libraries Cybersecurity Pilot Program	)	WC Docket No. 23-234
	)	
	)	

COMMENTS ON PROPOSED SCHOOLS AND LIBRARIES CYBERSECURITY PILOT PROGRAM (WC DOCKET NO. 23-234; FCC 23-94)

I. Introduction

The Michigan Statewide Educational Network (MISEN or SEN) is a statewide fiber-optic research and education backbone network[1]. Its vision is to connect all of the State's Intermediate School Districts (ISDs), Local Education Agencies (LEAs), and Public School Academies (PSAs) to high-speed broadband connectivity to enable each entity to achieve their classroom educational goals. MISEN strives to eliminate the digital divide between urban and rural, North and South, impoverished and wealthy, and provide Michigan's 1.44 million students access to an equitable and robust learning environment, unhindered by socioeconomics or geography. While the efforts thus far have focused on broadband connectivity, the need to protect the data traversing the SEN has grown commensurate with increasing levels of cyberthreats.

[1] MISEN has participated in the FCC's Schools & Libraries, aka E-Rate, Program as a consortium applicant since Funding Year 2016. In those eight years, MISEN has received $31.84M in committed funding for high-speed broadband on behalf of its members. Leveraging economies of scale, MISEN offers Internet access at $.09/Mbps (pre-discount amount) to its participating consortium members.

Since its inception, MiSEN has maintained a profile of collaboration. As an E-Rate applicant, MISEN is a "super consortium", which is a statewide consortium made up of many smaller consortia. In addition to the natural cooperation necessary as a consortium lead of 56 ISDs and over 530 school districts, MISEN regularly collaborates with state agencies and stakeholder groups including the Michigan Department of Technology, Management and Budget (DTMB), the Michigan Educational Technology Leaders (METL), the Michigan Association of Intermediate School Administrators (MAISA), and the Michigan Collaboration Hub (MiCH). MISEN was created through a state-level General Fund allocation to lower broadband costs through economies of scale while also addressing equity concerns (cost and access) for schools across the State. Library entities, while not considered in MISEN's original mission, are also now counted in the growing number of applicants served by SEN-provided broadband.

MISEN is encouraged by the FCC's desire to take action to protect E-Rate program participants from loss caused by cyberattacks and is pleased to submit comments and data to help shape the Schools and Libraries Cybersecurity Pilot program (Pilot, the Pilot) and, subsequently, the future of the E-Rate Program.

II. Summary of Comments

MISEN appreciates the FCC's attention to the current deficiencies of supporting funds for cybersecurity measures for K12 and Library entities. These initial comments set forth numerous suggestions to shape the Pilot program, help the FCC meet the Pilot program goals, address concerns about applicants leveraging other available cybersecurity resources, and, in turn, shape the future of the E-Rate program for all applicants.

The following list summarizes MISEN's recommendations in these initial comments:

- The length of the proposed Pilot program is too long and will stifle affordable access to widely adopted cybersecurity measures for most E-Rate applicants. The FCC should consider making certain products and services eligible for E-Rate in FY2025.
- The allocated $200M for the Pilot may prove insufficient to significantly impact or gather substantial data, depending on the final number of Pilot members selected. Expanding the existing E-rate eligibility criteria to include current-generation firewalls and Multi-Factor Authentication (MFA) would enhance the Pilot's ability to study a broader range of services.
- The FCC should adopt an encompassing and generalized Eligible Services List to allow program applicants the flexibility to determine which cybersecurity tools best meet their current needs.
- Consortia entities should be specifically identified as eligible Pilot program applicants.
- Shared resources should be incentivized in Pilot program participants. Applicants should be encouraged to be creative in launching partnerships with other agencies and groups for the benefit of the greater good.

III. A Three-Year Pilot Program Will Delay Delivery of Desperately Needed Cybersecurity Funding

Three years for a pilot program is too long for all schools to wait. A three-year pilot is an acceptable time period only when information is limited regarding cost(s), process, implementation, and outcomes. However, the K-12 community has been utilizing cybersecurity measures as long as

the internet has existed. There is a wealth of data available to the FCC on firewall costs through current E-Rate Category 2 funding requests. We believe that the FCC, using that data, could reasonably expand the E-Rate Eligible Services List (ESL) as early as Funding Year 2025 to include current-generation firewalls and components. MISEN agrees with others who have proposed the same.[2] MISEN further urges the FCC to consider immediate inclusion of Multi-Factor Authentication (MFA) in the E-Rate ESL. MFA for network access and applications has proven to be highly effective at stopping, or reducing, cyberattacks. Proof of an active MFA solution is also required of entities seeking to maintain Cyber Liability insurance, a practice that no school can afford to go without. This is equivalent to an unfunded mandate from the private sector as a requirement for protection.

The FCC has previously brought sweeping changes and improvements without first running a pilot program. The Commission's First and Second E-Rate Modernization Orders are recent examples of this. Many of the implemented changes from the Modernization Orders were based on commenter-submitted experiences and data. This Cybersecurity NPRM process is likely to bear similar fruit, empowering the Commission to take action to make in FY2025 current-generation firewalls, features, and components using the comments and data submitted by the field and noted as publicly available.

Cybersecurity is no longer a luxury, but rather a requirement for I-rated Internet access in function. Therefore, it is an overdue consideration for the FCC through its E-Rate Program. MISEN

[2] METL's comments in response to DA 22-1315. "METL urges the Commission to grant full eligibility for current generation firewall solutions, improving upon the limited support for "basic" firewalls as granted in the Sixth Report and Order."

implores the FCC to make well-examined cybersecurity measures, like advanced firewalls and MFA, eligible through the E-Rate program for all applicants as soon as possible, beginning in Funding Year 2025. This will provide the opportunity for essential protection of the entire K-12 and library communities considerably sooner. The need for action is immediate, and with every year that passes, the greater the exposure of attack to the applicant community.

IV. The Allocated Funds for Pilot Program Fall Short of Making Any Real Impact

MISEN fears the Pilot program's budget of $200 million will fall short of providing real impact to the applicant community in this time of crisis. For K-12 schools, cyber incidents are so prevalent that, on average, there is more than one incident per school, per day.[3] Cybersecurity and Infrastructure Security Agency (CISA) Assistant Director for Stakeholder Engagement, Alaina Clark, stated that "The continued impact of cyber intrusions is threatening the nation's ability to educate our children while also placing personal information and school data at risk. We can, and must, do better for our nation's youngest learners."

According to Cybercrime Magazine, cybercrime, if measured as a country, would be the world's third-largest economy after the United States and China[4]. Statistics predict that cybercrime will cost the global economy more than 20 trillion U.S dollars by 2026, representing a 1.5 times increase compared to figures in 2022[5]. Furthermore, schools and libraries currently lack dedicated

[3] https://www.cisa.gov/K12Cybersecurity
[4] Cybercrime To Cost The World $10.5 Trillion Annually By 2025. (2020, November). https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.
[5] Source: Statista,https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/

funding to support cybersecurity needs. Per-pupil funding in Michigan, stagnant for over a decade until recent increases, does not include a calculation for cybersecurity protections.[6]

Library Services and Technology Act (LSTA) grant dollars lack a calculation for general internal information technology operations, much less cybersecurity. E-Rate has been the only dedicated and recurring source of funding for firewall protection, albeit basic, representing the bare-minimum in cybersecurity protections. The current ESL's restrictive definitions and firewall manufacturers' fluctuating equipment eligibility percentages have limited the E-Rate program's effectiveness in protecting the very service it helps fund: access to high-speed broadband. Schools, which are data rich and security poor, have become soft targets for cyber criminals.

The Commission, through USAC, has access to costs associated with firewall purchases supported by the E-Rate program. Recent purchases by one Michigan ISD and on Michigan LEA shed some additional light.

COST EXAMPLES:

- One ISD purchased a current-generation firewall solution in October 2023, including equipment and three-year license updates, for $490,000.[7] The state of Michigan has 56 ISD entities.

[6] State of MI per-pupil funding for 2022-23 school year increased to $9,150 and will further increase in 2023-24 to $9,608. These represent the highest ever per-pupil funding available to MI schools. http://legislature.mi.gov/doc.aspx?mcl-388-1620

[7] Redundant (2) PaloAlto 5410s with maintenance, basic ATP subscription, global connect for VPN license and SFPs and installation

    - 56 entities x $490,000 = $27,440,000 to provide a first layer of defense at the ISD level for themselves and districts they serve at a cost of $9,146,666 per year
    - $9,146,666 / 56 ISD entities = $163,333 per ISD entity per year
- One LEA purchased a current-generation firewall solution in 2023, including equipment and three-year licenses for $25,830.[8] The state of Michigan has 830 LEA entities.
    - 830 entities x $25,830 = $21,438,900 to provide a layer of defense at the district level for themselves and the buildings they serve at a cost of $7,146,300 per year
        - $7,146,300 / 830 LEA entities = $8,610 per LEA per year
- The State of Michigan has a combined total of 886 entities made up of ISDs and LEAs. Using the numbers listed above as a guide, we can extrapolate costs of deployment:
    - Estimated ISD level firewall equipment and license costs over three years:
        - $27,440,000
    - Estimated LEA level firewall equipment and license costs over three years:
        - $21,438,900
    - Estimated Total Cost at the ISD and LEA level per year over three years:
        - $163,333 per ISD + $8,610 per LEA x 3 years = $515,829

MISEN believes the Pilot program's funding will fall short of making any real impact and that the Commission could make current-generation firewalls, related components, and licensing and Multi-Factor Authentication immediately eligible for E-Rate, thereby stretching the pilot funding. The FCC can make eligible advanced firewalls and MFA under current Category 2 budgets, and let applicants make their purchasing decisions. This will bring no additional burden to the Fund.

[8] Single FortiGate-200F Hardware plus 3 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP), VPN license, SFPs and installation

Of note, every cybersecurity solution has a human component necessary for the implementation, management, and maintenance of the solution. Cybersecurity is not just a network issue; it is a network and human issue. Before applicants can implement any solution, they will have to make a substantial investment in the hiring, training, and certification of their staff to manage, monitor, and maintain it. Substantial funding for tangible equipment and services through the cybersecurity pilot and E-Rate program is going to be mission critical for applicants who already have significant costs incurred in staff and outsourced professional services.

The next Category 2 budget cycle, beginning in FY2026, will require the FCC to carefully consider an increase to the per-pupil/square foot multiplier to ensure applicants have access to the funding necessary to maintain, upgrade, and protect their high-speed networks. Using the existing E-Rate program to fund firewalls and MFA will benefit many more applicants almost immediately with no additional drain to the Program and will allow the pilot program's limited $200M to fund and study the benefits of additional protection measures outlined our proposed Eligible Products and Services below.

V. Eligible Products and Services

MISEN encourages the FCC to allow the applicant community to make the purchasing decisions that are in their best protective interests relative to cybersecurity with a broader rather than more specific Eligible Services List. MISEN suggests making eligible categories and allowing Pilot participants to select any product and/or services that fall into any of the eligible categories. The categories suggested for the ESL include items in bold below. The bulleted items under each

category are listed as examples of currently available solutions and are not intended to be an exhaustive list:

Identity & Access

- Multi-Factor Authentication support
- Tools and training to implement Zero Trust architecture.
- Identity Management

Monitoring/Warning/Response

- Security Operation Centers - increasingly relied on and potentially required by Cyber Insurers in the future
- Security Information and Event Management (SIEM) Logging solutions
- Active countermeasure tools
- Intrusion Detection & Protection Systems (IDS/IPS)
- Web content controls
- Application awareness, monitoring, and controls
- Network traffic analysis
- Internal and external vulnerability scanning
- Network Detection Response (NDR)
- Data Loss Prevention

Network Infrastructure Hardening

- Virtual Private Networks (VPN)

- External threat intelligence
- Network Segmentation
- ”Next Generation” (current-generation/advanced) Firewalls
- Deep Packet inspection
- Malware detection
- Patch Management systems
- Network Access Control
- Offsite, immutable backups

Training and Human Resources

- Staff & Student Cybersecurity Awareness
- Incident Response Planning
- Communications Templates
- Forensic support
- Cybersecurity Assessments
- Negotiation (Counsel)
- Cybercrime Insurance Premiums
- Risk Assessments
- Tabletop Drills
- Penetration testing
- Red Team exercises

VI. Benefits of Consortia as Pilot Project Participants

Just as the Second E-Rate Modernization Order advocated the consortium model for program applicants, so too should the Cybersecurity Pilot Program allow for consortium solutions in both purchasing of equipment and service and the implementation and reporting of those protections.

By acknowledging consortia as eligible participants in the Pilot, the Commission will stretch the limited proposed Pilot funding and increase the impact to more students and schools through wider participation. A consortium provides a mechanism to increase support while decreasing cost using the influence of volume to achieve economical procurement and service delivery. A consortium of consortia, like MISEN, can act as a force multiplier and reduce implementation costs and replication of service at multiple entities across the state.

As noted previously, MISEN, as an established consortium lead, currently acts as a procurement entity for applicants across Michigan for Category One eligible services. SEN-purchased broadband reaches entities in every county in the state. Recipients of service include large urban and suburban districts, and single-room, rural schools. Allowing MISEN, for example, to procure needed cybersecurity equipment and services on behalf of its members would provide protections and, to the Commission’s benefit, valuable data on needs, solutions, and cost from a broad applicant pool. The potential for a wealth of data around the process (procurement and distribution), cost-savings through a bulk purchasing model, and the impacts on a diverse set of applicants (geographically and demographically) would align with the Commission's goals for this Pilot.

VII. Benefits of Leveraging Existing Partnerships While Forging New

MISEN agrees with the Commission's goals for Pilot applicants to forge partnerships to leverage available resources and is positioned well to do so. Michigan's K=12 community is set to benefit from state leaders with the understanding that we must protect our students from cybercriminals. In the 2023 School Aid Act, the Michigan legislature included Section 97(g)[9] to help fund a statewide Managed Detection and Response (MDR) solution for K=12 entities. The result was the creation of the legislatively required MiSecure Advisory Board to "oversee the function of MiSecure Operation Center. The Advisory team is made up of ISD technology leaders, State of Michigan Police, DTMB Security Engineers, [and] members of other statewide broadband initiatives." Currently, MiSecure is awaiting the release of funds to support the purchase of MDR solutions for all K-12 entities within the state.

When mature, MiSecure will provide schools with MDR software to monitor and protect critical servers 24x7x365 against cybersecurity threats. The cost for MDR software has typically been the barrier to adoption at the local level; however, by leveraging this statewide funding opportunity, schools will be able to make significant gains in their cybersecurity strategy. MDR software is only one component of an overall cybersecurity strategy, and the MiSecure Operations Team is tasked to provide leadership and advocacy addressing each of these components. One such component is the implementation of edge firewalls on school networks. Full-featured firewall licenses which include Intrusion and Protection Services (IPS) and Intrusion Detection Services (IDS), adequate logging and reporting, remote access (e.g. VPN), deep packet inspection, malware detection, and other services are often cost prohibitive to schools. The State's MiSecure effort **does not** address all these needs. Fortunately, most Michigan schools are connected to the State

[9]388.1697g Statewide Security Operations Center; Managed Detection and Response solution cybersecurity risk assessments (http://legislature.mi.gov/doc.aspx?mcl-388-1697g)

Education Network (MISEN), which can be adapted to provide for state-level protections supported by the MiSecure team. Such support and coordination is specifically referenced in the 97g legislation: "Partner with K to 12 statewide connectivity partners to install and monitor intrusion detection systems[10]."

MISEN and MiSecure

MISEN and MiSecure fit well to share resources, brainstorm solutions, partner in implementation, support shared monitoring and reporting.

MISEN, MiSecure, METL, and REMC

The Michigan Education Technology Leaders (METL) cybersecurity task force has partnered with MISEN and MiSecure, as well as the Regional Educational Media Center Association of Michigan[11] (REMC), to develop free resources on cybersecurity planning and preparedness. These resources include the publications: *Essential Cybersecurity Practices for Education,*[12] the *MiSecure Quick Self-Audit,*[13] *Edupaths Cybersecurity Online Courses,*[14] REMC's free cybersecurity resources collection,[15] and plan to create Cybersecurity Incident Response templates. These human-side resources are proactive and support the understanding and use of basic technologies to protect against the constant threats faced by the K12 community.

---

[10] Sec. 97g, Subsection 4(b) http://legislature.mi.gov/doc.aspx?mcl-388-1697g

[11] The Regional Educational Media Center Association of Michigan is a 501(c)(3) nonprofit organization established in 1969. Its members are the 28 local Regional Educational Media Centers operated through the Intermediate School District structure.

[12] https://misecure.org/wp-content/uploads/2019/07/Essential-Cybersecurity-Practices-for-K12.pdf

[13] https://misecure.org/selfaudit/

[14] https://www.edupaths.org/catalog?Search=How%20to%20Become%20a%20Human%20Firewall

[15] https://www.remc.org/educator-resources/mi-cybersecurity-resources/

If MISEN were able to leverage E-Rate funding to purchase cybersecurity tools, such as fully featured firewalls, integrated with cybersecurity subscriptions and network layer defenses (e.g IPS, VPN, MFA, net flow, logging), the State-funded MiSecure effort could then provide support and administration to monitor and respond. A joint MISEN/MiSecure effort during the Pilot, and beyond, will help develop further strategies to secure the network, limit attack vectors, and provide support and training would provide additional protections to most schools and libraries in Michigan.

VIII. Conclusion

MISEN is encouraged by the Commission's decision to make cybersecurity a priority and is thankful for the opportunity to submit these comments. The FCC can take immediate actions to affect real change across the E-Rate applicant pool, sooner than three to five years, by making advanced firewalls E-rate eligible using available cost data from the E-Rate program. For the Pilot, consortium applicants should be specifically included as eligible participants to allow funding to go further, help more applicants, and provide broader data. Finally, we support Pilot applicants being asked to identify opportunities for collaboration and detail their current efforts to ensure fiscal responsibility and greater reach of funding and resources. Michigan understands the significance of cybercrime and the impact it has on its citizens. It will continue its collaborative efforts across all sectors, with MISEN and other K-12 entities on the front line.

Respectfully submitted,

Merri Lynn Colligan
Director of MISEN
Michigan Statewide
Educational Network
(810) 591-4453
MColligan@misen.org

Luke Wittum (Jan 29, 2024 15:44 EST)

Luke Wittum
Assistant Superintendent
Genesee ISD
Chair
Michigan Statewide Educational
Technology Leaders
(810) 591-4436
lwittum@geneseeisd.org

Matt McMahon (Jan 29, 2024 14:47 EST)

Matt McMahon
Director
MiSecure Operations
Center
(989) 715-3233
mmcmahon@gomaisa.org

Dated: January 29, 2024