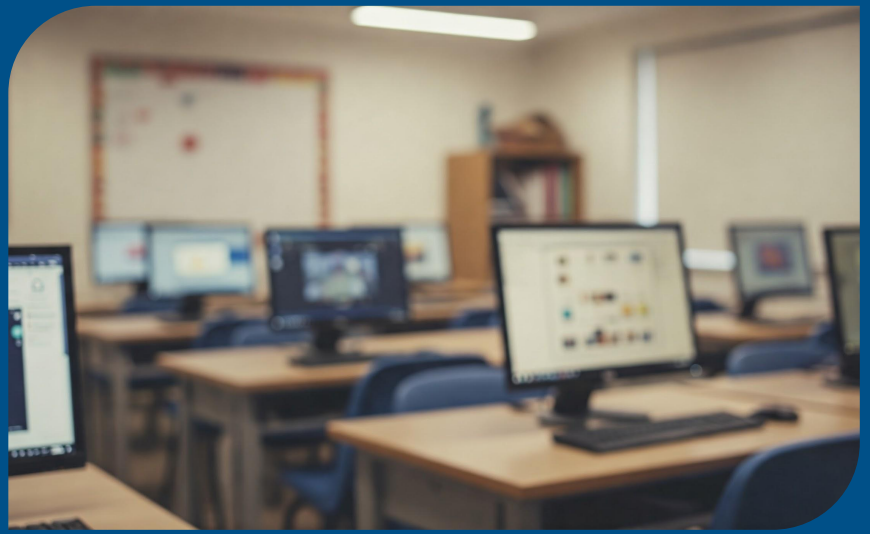
03.17.25

# Federal Funding for Cybersecurity in Education



## Georgia Leaders of Education Technology

CyberCon 2025

Schools, Health & Libraries Broadband Coalition | GLET Presentation

# Meet the Speakers

## Kristen Corra

Policy Counsel

Schools, Health & Libraries Broadband Coalition (SHLB)

## Michael Flood

Founder & CEO

Alpine Frog, LLC

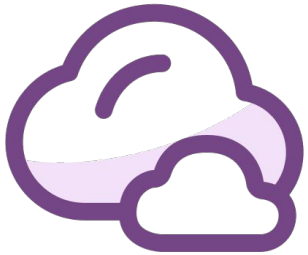
# Agenda

1. Federal Policy Landscape (Snapshot)
2. FCC's Cyber Pilot Program
3. Other Federal & Georgia Funding
4. Future Risks & Opportunities
5. Resources

# Audience Poll

# Join at slido.com
# #6691778

# Rate your district’s overall Cybersecurity posture. How do you feel about cybersecurity?



# In 1 word, what is your biggest obstacle to improving your cybersecurity posture?

# Does your district have a designated Chief Information Security Officer (CISO) or cybersecurity lead?

1. **Federal Policy Landscape**
2. FCC's Cyber Pilot Program
3. Other Federal & Georgia Funding
4. Future Risks & Opportunities
5. Resources

# Federal Policy Landscape (A Snapshot)

**E-Rate:** Covers “basic” firewalls

**Public Interest:** (February 2021) CoSN, SHLB, & others filed petitions with FCC

**Cyber Attacks Gaining National Attention:** (September 2022) LAUSD ransomware attack

**CISA:** (January 2023) cybersecurity study released

**White House, Dept. of Ed:** (August 2023) Holds K-12 cybersecurity summit; releases digital infrastructure briefs

**FCC:** (December 2022/November 2023) Rulemaking efforts to determine school needs

# Federal Policy Landscape (A Snapshot)

## SCHOOL CYBER ATTACKS GAINING NATIONAL ATTENTION

**September 2022**

**Los Angeles Unified School District (second largest school district in the nation) suffered a significant ransomware attack.**

LAUSD followed the FBI's strict no-ransom payment advice and denied the ransom payment.

The hackers published the stolen data on the dark web. Around 2,000 student assessment records were stolen from LAUSD's systems, including sensitive data.

September 21, 2022

The Honorable Jessica Rosenworcel, Chairwoman
The Honorable Brendan Carr, Commissioner
The Honorable Geoffrey Starks, Commissioner
The Honorable Nathan Simington, Commissioner

Federal Communications Commission
45 L Street NE
Washington, D.C. 20554

**RE: Local Educational Agencies and Organizations Across the Country Urge the FCC Authorize the Use of E-Rate Funds to Combat Cyber Security Threats at Public Schools**

Dear Chairwoman Rosenworcel and Commissioners:

The recent cyberattack on the Los Angeles Unified School District – the second largest school district in the nation – serves as an important reminder for federal officials to take immediate action to protect our nation's educational entities from cyber-attacks. On behalf of over 1,100 local and state education agencies, national organizations and the students and communities we serve across the United States, we urgently request the Federal Communications Commission (FCC) immediately authorize the ongoing, permanent use of existing E-Rate Program funds to bolster and maintain IT security infrastructure.

While Los Angeles Unified's ability to intercept the attack by deactivating all of their systems was the swift and prudent action to avoid a catastrophic breach, this ransomware attack demonstrates vulnerabilities that leave school districts nationwide susceptible to future attacks. It exposes the significant risk of disruption to instruction, home to school transportation, or access to nutritious meals that would be catastrophic for students and their learning.

Many of our school districts have previously joined national organizations in urging the FCC to update the E-Rate program by including cybersecurity costs under the E-Rate Eligible Services List (ESL). For instance, we have asked FCC to modernize its definition of firewalls to make eligible the advanced technologies and software necessary to help school districts prepare for the increase in cyberattacks and enable school districts to strengthen their security protections. Currently, school districts and libraries nationwide are fighting increasingly sophisticated cyberattacks and their aftermath with funding meant to be used for meeting the instructional and socio-emotional needs of our students. We feel that supporting cybersecurity tools 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 scope of the attack on Los Angeles Unified.

*LAUSD -with education and technology leaders- wrote a letter to the FCC, asking it to "immediately authorize" the use of E-Rate Program funds to strengthen school IT security infrastructure.*

# Federal Policy Landscape (A Snapshot)

## CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

**October 2021: Congress passed the K-12 Cybersecurity Act of 2021.**

The Act required the Cybersecurity and Infrastructure Security Agency (CISA) to study current cybersecurity risks and challenges facing schools, and develop recommendations, guidelines, and online training toolkits to assist schools in facing rising threats of cybersecurity incidents.

**January 2023: CISA released a study called Partnering to Safeguard K-12 Organizations from Cybersecurity Threats.**

Three main recommendations, including 1) investing in impactful cybersecurity measures, 2) addressing resource constraints, and 3) building collaboration and information sharing.

## WHITE HOUSE, DEPT. OF EDUCATION

**March 2023: National Cybersecurity Strategy**

The White House released the National Cybersecurity Strategy, recognizing the need for robust collaboration, particularly between the public and private sectors.

**August 2023: Back to School Safely: Cybersecurity for K-12 Schools**

The White House held a summit, convening administration leaders, school administrators, educators, and education technology providers to discuss how to strengthen school cybersecurity amidst growing ransomware attacks.

**August 2023: K-12 Digital Infrastructure Brief: Privacy Enhancing, Interoperable, and Useful**

The US Department of Education Office of Education Technology released K-12 Digital Infrastructure Briefs that cover the role of interoperability, cybersecurity, and privacy.

# Federal Policy Landscape (A Snapshot)

## WHITE HOUSE: CURRENT CYBERSECURITY EFFORTS

**January 2025**

**The Biden Administration issued Executive Order ("EO") 14144 on "Strengthening and Promoting Innovation in the Nation's Cybersecurity."**

This expands on a previous Biden National Cybersecurity Strategy and EO (called Improving the Nation's Cybersecurity) from 2021.

**The Trump Administration rescinded 78 EOs issued by President Biden, but did not rescind/modify President Biden's first or second cybersecurity EOs.**

Does this signal a willingness to continue support for efforts established under the previous administration?

# Federal Policy Landscape (A Snapshot)

## FCC RULEMAKING EFFORTS

**Rulemaking: Advanced Firewalls Supported by E-Rate**

December 2022: FCC initiated a public comment proceeding asking for information about E-Rate eligibility for K-12 cybersecurity services like advanced firewalls.

**FCC Adopts the Schools and Libraries Cybersecurity Pilot Program**

June 2024: The FCC adopted the Schools and Libraries Cybersecurity Pilot Program and released the final Report and Order setting out the rules for schools and libraries wishing to apply.


**Rulemaking: Information About Proposed Cyber Pilot Program**

November 2023: The FCC initiated another public comment proceeding. It proposed creating  a cybersecurity “pilot program” that would allow the agency to better understand exactly what services a school or library needs.

1. Federal Policy Landscape
2. **FCC's Cyber Pilot Program**
3. Other Federal & Georgia Funding
4. Future Risks & Opportunities
5. Resources

# FCC's Cybersecurity Pilot Program

**Adopted:** June 2024

**Funding Mechanism:** Universal Service Fund (USF) - Outside of E-Rate

**Total Budget:** $200 million

**Timeframe:** 3 years

**Pays For:** Cybersecurity resources to schools and libraries not currently covered by E-Rate

**Goal:** Assess needs for a future (permanent?) funding structure.

# FCC's Cybersecurity Pilot Program

## WHAT'S ELIGIBLE?

**Four general categories of technology:**

- Advanced/next-generation firewalls
- Endpoint protection
- Identity protection and authentication
- Monitoring, detection, and response

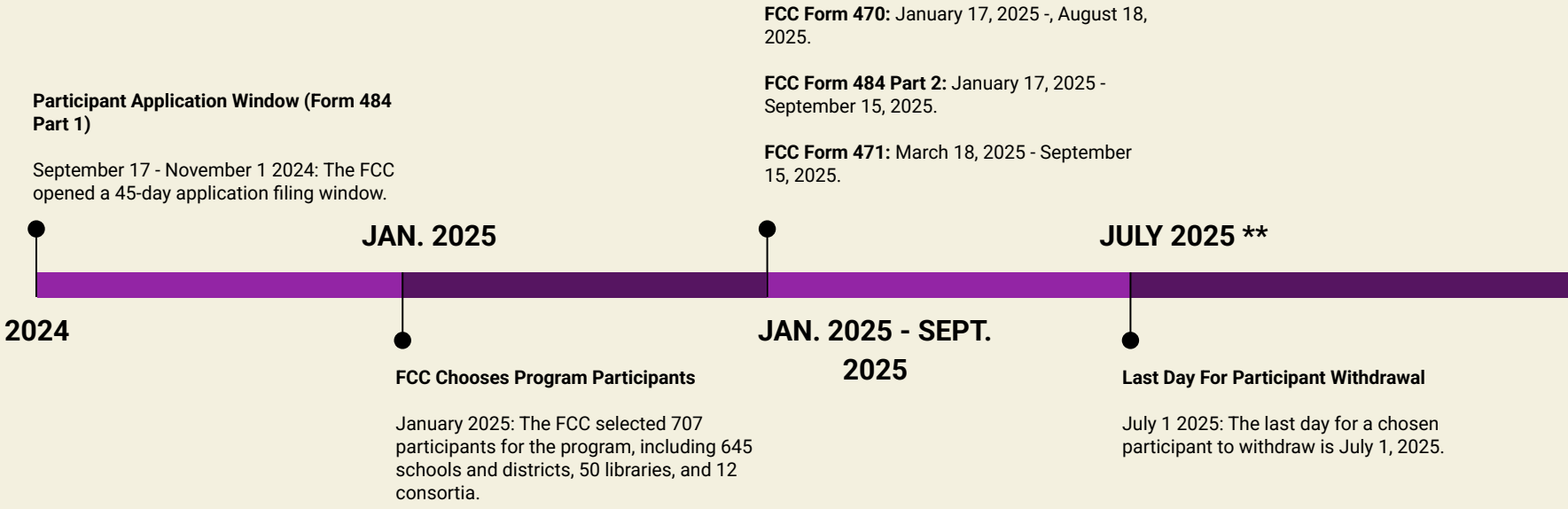
**The FCC adopted a non-exhaustive "Pilot Eligible Services List" (P-ESL) with examples of eligible services/equipment under these categories.** The FCC wants to remain flexible in what tools are funded - it deems services and/or equipment eligible if they "constitute a protection designed to improve or enhance the cybersecurity of a K-12 school, library, or consortia."

## WHAT'S INELIGIBLE?

- Services/equipment/associated costs already eligible under E-Rate
- Anything which has, or will be, reimbursed through other USF or federal, state, local program
- End-user devices (like tablets, laptops)
- Staff salaries and labor costs
- Beneficiary and consulting services not related to the installation and configuration of the eligible equipment and services
- Equipment on FCC's Covered List (e.g. Huawei, ZTE)

# FCC’s Cybersecurity Pilot Program

## TIMELINE



Total 484 Applications: 2,734 (~93% schools, 4% libraries, 3% consortia)

Total Funding Requests: $3.7 billion

Eligible Schools/Libraries/Consortia: 707

Who Applied? All 50 states, Puerto Rico, & D.C.

**November 8, 2024 - Former FCC Chairwoman Jessica Rosenworcel**

*"The overwhelming response to our pilot program makes clear that the cybersecurity threats impacting school systems are widespread. The Pilot Program provides an excellent opportunity to both learn from these varied experiences, and also test out solutions in different environments."*

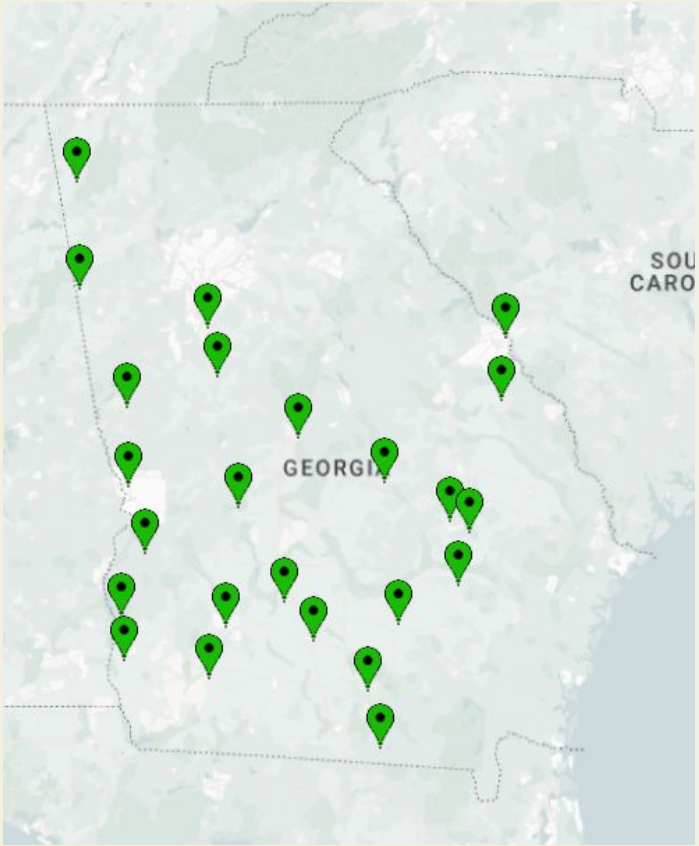
# FCC’s Cybersecurity Pilot Program

## GEORGIA PARTICIPANTS

**25 selected participants**

- 22 county school districts
- 2 city school districts
- 1 library system

All projects received the full funding amount available under the program’s formula.



1. Federal Policy Landscape
2. FCC's Cyber Pilot Program
3. **Other Federal & Georgia Funding**
4. Future Risks & Opportunities
5. Resources

# Other Federal & Georgia Funding

**State and Local Cybersecurity Grant Program**

- From the Infrastructure Investment and Jobs Act of 2021
- Four-year program appropriated $1B total
  - $200M in FY 2022
  - $400M in FY 2023
  - $300M in FY 2024
  - $100M in FY 2025
- At least 80% of grant funds must benefit local governments
- Of that 80% share, at least 25% must benefit rural areas.
- GEMA/HS is the State Agency Administrator (SAA) in GA
- GTA is involved in application evaluation
- Most recent deadline was **February 28, 2025**

**Links:**

https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program
https://www.cisa.gov/cybergrants/slcgp
https://gema.georgia.gov/state-and-local-cybersecurity-grant-program
https://gta.georgia.gov/policies-and-programs/cybersecurity

Note: There is an additional and separate version of this program for federally recognized tribal governments

# Other Federal & Georgia Funding

**Homeland Security Grant Program**

- ~$1B per year across three sub-programs:
  - State Homeland Security Program (SHSP);
  - Urban Area Security Initiative (UASI); and
  - Operation Stonegarden (OPSG).
- GEMA/HS is the State Agency Administrator (SAA) in GA
  - SAAs are required to pass-through at least 80% of SHSP and UASI funding to local or tribal units of government.
- At least 30% must be spent on National Priority Areas, including "Enhancing Cybersecurity"
- Most recent deadline was **April 30, 2024**

**Links:**

https://www.fema.gov/grants/preparedness/homeland-security
https://gema.georgia.gov/homeland-security-grant-program

Note: There is an additional and separate version of this program for federally recognized tribal governments

# Other Federal & Georgia Funding

**Nonprofit Security Grant Program**

- $454.5M in FY 2024
- GEMA/HS is the State Agency Administrator (SAA) in GA
    - GEMA lists "*Schools and educational institutions*" as eligible entities on the program page
- The Goal, Objectives, and Priorities of the program NOFO highlights both physical *and cybersecurity* measures.
- In FY 2024, there were two rounds in June and January
- Most recent deadline was **January 2, 2025**

**Links:**

https://www.fema.gov/grants/preparedness/nonprofit-security
https://gema.georgia.gov/nonprofit-security-grant-program
https://gema.georgia.gov/nonprofit-security-grant-program-national-security-supplemental

# Other Federal & Georgia Funding

**Stronger Connections Grant Program / Safer Georgia Schools**

- Funded via additional appropriations to ESEA Title IV-A in the Bipartisan Safer Communities Act (BSCA)
- $31.7M in three rounds from Oct 2023 thru May 2024
- Funded thru the State Education Agency (SEA) - GaDOE
  - Office of Whole Child Supports in Georgia
- Included multiple cybersecurity related areas
  - Cybersecurity tools and/or risk assessment services
  - Internal and external penetration testing
  - Content filtering, Firewall, Backup, SSO, and MFA solutions
  - Endpoint, email or network detection, response, and mitigation
  - Cybersecurity training
- Most recent deadline was **March 29, 2024**

**Links:**

https://resources.finalsite.net/images/v1684423245/cherokeek12net/jgbghjdkhxhjwirhfpow/SaferGeorgiaSchoolsGrantRFP.pdf
https://gadoe.org/grants-awards-diploma-seals/grant-allocations/
(Whole Child Support -> FY 24)

Note: Governor Kemp has included $50M in additional funding for School Safety Grants in his Amended FY 2025 Budget Proposal

# Other Federal & Georgia Funding

**Georgia School Board Association Safety Grants**

- Smaller Grant Program, 9 years running
- $5,000 maximum per grant limit
- Funded thru the Georgia School Boards Association (GSBA)
  - Must be a GSBA, Risk Management Services member
- Included cybersecurity examples in past recipients
  - Updates and/or additional security for district cyber protections
  - Additional Cyber Protection to the district technology areas
- Most recent deadline was **November 1, 2024**

GSBA
Georgia School Boards Association

**Links:**

https://gsba.com/risk-management/safety-grant-application/
https://gsba.com/wp-content/uploads/2024/08/Safety-Grant-Application-2024-2025.pdf

1. Federal Policy Landscape
2. FCC's Cyber Pilot Program
3. Other Federal & Georgia Funding
4. **Future Risks & Opportunities**
5. Resources

# Future Risks & Opportunities

**New Administration:** Will the Trump administration and 119th Congress recognize K-12 cybersecurity needs and support continued federal resources?

**Funding Mechanism:** Are USF & E-Rate safe?

**Demonstrating the Impact & Need:** Schools and libraries have the opportunity to show the FCC and Congress how critical the USF & E-Rate are.

Participants and Service Providers in the Schools & Libraries Cybersecurity Pilot Program will influence a future, permanent program

# Future Risks

## CHALLENGES TO THE UNIVERSAL SERVICE FUND

### Contribution Mechanism

**USF is currently funded through contributions from telecommunications services**, but the base keeps shrinking.

**Second quarter 2025 - 36.6%**

**How do we fund the USF going forward?**

- Appropriations
- BB Internet Service Providers
- Edge providers (Google, Amazon)
- Spectrum auction revenue

### The Courts

**Consumers' Research case currently at the Supreme Court**

5th Circuit found the USF contribution mechanism to be unconstitutional.

New theory of "double delegation" problem:

- Statutory authority from Congress to the FCC
- Authority from FCC to USAC (third party administrator of the fund)

### Congress

**USF Reform Efforts**

Concerned with contribution reform and constitutionality of the funding mechanism.

Will certain members try to undermine the continued need for E-Rate?

- Waste, fraud, abuse?
- Do internet services improve student learning?
- What are today's overarching principles of "universal service"?

# Future Opportunities

## PRESERVE THE UNIVERSAL SERVICE FUND

**We need to ensure that federal funding opportunities are preserved and stable.**

**Lawmakers might know about the USF (generally), but do they know about E-Rate?**

- How can we translate E-Rate dollars into direct community benefits?
- Storytelling and education is critical
  - Filing comments with the FCC - develops a record
  - State and local advocacy days
  - Federal (D.C.) Fly-Ins

April 9 - 11

SHLB is organizing a D.C. fly-in where members can share information about the USF.

How does E-Rate benefit communities? What would happen if it went away?

1. Federal Policy Landscape
2. FCC's Cyber Pilot Program
3. Other Federal & Georgia Funding
4. Future Risks & Opportunities
5. **Resources**

# Resources

**Links:** There are a lot of (often free!) cybersecurity resources available

**What Can You Do?:** You have the on-the-ground knowledge to educate D.C.

**Who is SHLB?:** Advocacy and policy organizations are already keeping up with these issues. How can you utilize them?

# Resources

## LINKS

https://www.cisa.gov/K12Cybersecurity

https://www.k12six.org/

https://www.cisecurity.org/ms-isac

https://rems.ed.gov/Cyber

https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity

https://www.cosn.org/edtech-topics/cybersecurity/

https://www.cosn.org/edtech-topics/cybersecurity/cosns-nist-cybersecurity-framework-resources-alignment-for-k-12/

# Resources

## WHAT CAN YOU DO?

**Stay informed**

- Keep up to date on new FCC rules/initiatives

**Gather Data**

- Gather information and data about your programs, cybersecurity needs, etc.
- What's working?

**Educate lawmakers**

- Your voice matters – how does E-Rate help your school & community? What cybersecurity needs do you have?

## WHO IS SHLB?

**Non-profit Advocacy Organization**

- Anchor Institutions keep people connected

**Member supported**

- Have over 300 members from all over the US
- They support our mission

**We educate lawmakers!**

- We advocate for policies that support anchor institutions and their communities
- We bring your voice to D.C.
- We keep you informed about what is going on

# Questions?


## Kristen Corra

Policy Counsel, SHLB
kcorra@shlb.org

## Michael Flood

CEO, Alpine Frog
mflood@alpinefrog.net