Universal Service Administrative Co.

Cybersecurity Plan

Your responses in the Cybersecurity Plan milestone will help the FCC evaluate whether, and to what extent, it should use the Universal Service Fund to support the cybersecurity needs of eligible schools and libraries going forward. Please be as thorough and specific as possible.

Answering for a Consortium

If you are completing the Pilot FCC Form 484 Part 2 for a consortium, review each question carefully for directions about how to answer on behalf of your consortium members. Some questions in the Cybersecurity Plan milestone refer to **any** members of your consortium while others refer to **all** the members of your consortium.

For example, you should answer **yes** to question 1.1.c if **any** member of your consortium currently conducts routine data backups. For question 4.1.a, you should provide the average number of cybersecurity incidents experienced in the last year for **all** members of your consortium.

1. Proposed Plan

1.1 Correction of Known Security Flaws and Routine Backups

a. Have you/any of the members of your consortium identified any cybersecurity flaws with your network(s) and/or data systems in the past year? Answer **Yes** or **No**.

> **If yes:**
> Have you/any of the members of your consortium made any updates to your network(s) and/or data systems in the past year (including legacy and advanced security features beyond simply updating the operating system) to address any of the cybersecurity flaws? Answer **Yes** or **No**.

b. Do you/does your consortium plan to use funding from the Pilot Program to correct known cybersecurity flaws in your/your members' network(s) and/or data systems? Answer **Yes** or **No**.

> **If yes:**
> What cybersecurity flaws do you/your consortium members plan to correct with Pilot Program funding? Select all that apply.
>
> ☐ Lack of Advanced/Next-Generation Firewalls or similar
> ☐ Lack of Endpoint Protection or similar
> ☐ Lack of Identity Protection and Authentication or similar
> ☐ Lack of Monitoring, Detection, and Response or similar

Universal Service Administrative Co.

c. Do you/any of your consortium members currently conduct routine data backups? Answer **Yes** or **No**.

> **If yes:**
> On average, how often do you/does your consortium conduct routine data backups? For consortia, answer this question using an average of all your consortium members. Select one.
>
> ○ Continuously, or more often than daily
> ○ Daily
> ○ Weekly
> ○ Monthly
> ○ Quarterly
> ○ Annually

d. Do you/does your consortium plan to use funding from the Pilot Program to conduct routine data backups? Answer **Yes** or **No**.

> **If yes:**
> How often will you/your consortium conduct the routine data back-ups? For consortia, answer this question using an average of all your consortium members. Select one.
>
> ○ Continuously, or more often than daily
> ○ Daily
> ○ Weekly
> ○ Monthly
> ○ Quarterly
> ○ Annually

2. Project Details

2.1 Recommended Cybersecurity Best Practices

a. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members have implemented. Select all that apply.

☐ U.S. Department of Education (Education Department)
☐ Department of Homeland Security Cybersecurity & Infrastructure Agency (CISA)
☐ National Institute of Standards and Technology (NIST)
☐ Other, please specify
☐ We have not implemented any recommended cybersecurity best practices

Universal Service Administrative Co.

If any organization(s) are selected:
Indicate which recommended best practices you/your consortium members have implemented from the selected organization(s) above. Select all that apply.

Organization	Best Practices
Education Department	☐ Develop and exercise a cyber incident response plan or a cybersecurity annex ☐ Implement multi-factor authentication ☐ Prioritize patch management ☐ Perform and test backups ☐ Minimize exposure to common attacks ☐ Create a training and awareness campaign at all levels ☐ None of the above
CISA	☐ Deploy multi-factor authentication (MFA) ☐ Mitigate known exploited vulnerabilities ☐ Implement and test backups ☐ Regularly exercise an incident response plan ☐ Implement a strong cybersecurity training program ☐ Recognize and actively address resource constraints ☐ Focus on collaboration and information sharing ☐ None of the above
NIST	☐ Identify systems, assets, data, capabilities, and risk profile ☐ Protect confidentiality, integrity, and availability of critical infrastructure ☐ Detect suspicious behavior ☐ Respond to damage caused by detected anomalies using response strategies and processes ☐ Recover by getting systems up and running and restoring routine operations ☐ None of the above

Universal Service Administrative Co.

Changing Your Organization Selections

If you make any changes to the organization(s) selected in 2.1.a, 2.1.b, or 2.1.c, all selected best practices in the conditional question that follows will be cleared.

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. Select all that apply.
   - ☐ U.S. Department of Education (Education Department)
   - ☐ Department of Homeland Security Cybersecurity & Infrastructure Agency (CISA)
   - ☐ National Institute of Standards and Technology (NIST)
   - ☐ Other, please specify
   - ☐ We have not implemented any recommended cybersecurity best practices

> **If any organization(s) are selected:**
> Indicate which recommended best practices you/your consortium plan(s) to implement. Select all that apply.
> *See question 2.1.a for answer options*

c. Do you/any members of your consortium currently have or plan to implement an incident response plan? Answer **Yes** or **No**.

> **If yes:**
> Do you/does your consortium leverage or intend to leverage recommended best practices for your incident response plan from any of the cybersecurity organizations selected in the FCC Form 484 Part 1? Answer **Yes** or **No**.
>
> > **If yes:**
> > Indicate which recommended best practices you/your consortium incorporates or plan(s) to incorporate into your incident response plan(s). Select all that apply.
> > *See question 2.1.a for answer options*

Universal Service Administrative Co.

Recommended Best Practices

The lists of best practices used as answer options for questions 2.1.a, 2.1.b, and 2.1.c come from the following sources and are not an exhaustive list:

- Cybersecurity Preparedness for K-12 Schools and Institutions of Higher Education (Education Department)
- Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (CISA)
- Understanding the NIST Cybersecurity Framework (NIST)

2.2 Cybersecurity Protections for Broadband Networks and Data Outside of the Pilot Program

a. Do you/any of your consortium members plan to obtain or upgrade any of your current cybersecurity protections/measures regardless of whether you receive funding from the Pilot Program? Answer **Yes** or **No**.

> **If yes:**
> Select the cybersecurity protections/measures you/the majority of your consortium members intend to obtain or upgrade regardless of whether you receive funding from the Pilot Program. Select all that apply.
>
> ☐ Advanced/Next-Generation Firewalls or similar
> ☐ Endpoint Protection or similar
> ☐ Identity Protection and Authentication or similar
> ☐ Monitoring, Detection, and Response or similar

Universal Service Administrative Co.

3. Cybersecurity Application Sec. 1

3.1 Current Cybersecurity Practices and Resources

a. Are you/any of your consortium members currently utilizing or implementing any cybersecurity protections/measures? Answer **Yes** or **No**.

> **If yes:**
> Which protections/measures are you/your consortium members utilizing or implementing? Select all that apply.
>
> ☐ Advanced/Next-Generation Firewalls or similar
> ☐ Endpoint Protection or similar
> ☐ Identity Protection and Authentication or similar
> ☐ Monitoring, Detection, and Response or similar

b. Do you/any of your consortium members currently have processes and/or procedures in place to manage and address cybersecurity risk? Answer **Yes** or **No**.

> **If yes:**
> What are those processes and procedures? Select all that apply.
>
> ☐ Cyber incident response plan/cybersecurity annex
> ☐ Multi-factor authentication (MFA)
> ☐ Patch management
> ☐ Implementing/performing/testing backups
> ☐ Minimizing exposure to common attacks
> ☐ Training and awareness
> ☐ Mitigating known exploited vulnerabilities
> ☐ Addressing resource constraints
> ☐ Collaboration and information sharing
> ☐ Monitoring/detecting/responding to suspicious behavior
> ☐ Recovery processes and procedures for compromised network(s) and data
> ☐ Ability to restore routine operations after a cyber threat or attack
> ☐ Other

Universal Service Administrative Co.

c. If you indicated in the FCC Form 484 Part 1 that you have other sources of cybersecurity funding, what purpose(s) do you/your consortium members plan to use that funding (i.e., funding that is not received from the Pilot Program) for? Select all that apply.

- ☐ Advanced/Next-Generation Firewalls or similar
- ☐ Endpoint Protection or similar
- ☐ Identity Protection and Authentication or similar
- ☐ Monitoring, Detection, and Response or similar
- ☐ Not applicable/no other sources of cybersecurity funding

d. Will any of the funding you receive from the Pilot Program be used for the same or similar cybersecurity equipment and services that you/any of your consortium members have purchased or will purchase using other cybersecurity funding? Answer **Yes** or **No**.

> **If yes:**
> For which cybersecurity equipment and services that are the same/similar will you/your consortium members use the other cybersecurity funding? Select all that apply.
>
> - ☐ Advanced/Next-Generation Firewalls or similar
> - ☐ Endpoint Protection or similar
> - ☐ Identity Protection and Authentication or similar
> - ☐ Monitoring, Detection, and Response or similar

Equipment and Services

For Cybersecurity Pilot Program purposes, the term “product” is synonymous with “equipment” and/or “services.”

Universal Service Administrative Co.

4. Cybersecurity Application Sec. 2

4.1 History of Cyber Threats and Attacks

a. How many cybersecurity incidents have you/your consortium members experienced in the last year? (For consortia, answer this question using an average of all your consortium members.) Select one.

- ○ 0
- ○ 1-3
- ○ 4-6
- ○ 6+

Cyber Incident

For questions in this section, "cyber incident" is defined as "an occurrence that actually or potentially results in adverse consequences to an information system or information that the system processes, stores, transmits and that may require a response action to mitigate or eliminate the consequences." *See* 47 CFR § 54.2000.

If 1 or more:
What was the type and/or nature of the most recent cybersecurity incident/threat/attack? (For consortia, respond for the member with the most recent incident.) Select one.

- ○ Malware or similar
- ○ Viruses or similar
- ○ Spam or similar
- ○ Ransomware or similar
- ○ Distributed Denial-of-Service Attacks or similar
- ○ Insider/Privilege Misuse or similar
- ○ Email and Web Security Threats (e.g., phishing, password spraying, credential stuffing, etc.) or similar
- ○ Cloud Application Threats or similar
- ○ Network Threats, and Data Compromise and/or Loss or similar

Universal Service Administrative Co.

How long did the most recent cybersecurity incident(s) last from time of detection to resolution? (For consortia, respond for the member with the most recent incident.) Select one.

- ○ Less than one hour
- ○ One hour
- ○ A few hours
- ○ One day
- ○ A few days
- ○ One week
- ○ More than one week

Cybersecurity Incident Time Period

In question 4.1.a, the **start** of the incident is defined as the moment it was detected.

The **end** of the incident is defined as the time when functionality is restored (not necessarily the restoration of data).

When did the most recent cybersecurity incident begin? (For consortia, respond for the member with the most recent incident.) Select one.

- ○ During the school day
- ○ After the school day
- ○ During a school holiday or other school break
- ○ During library hours
- ○ After library hours
- ○ During a holiday or other library closure

Were you/the affected consortium member able to identify the malicious cybersecurity actor(s)? Answer **Yes** or **No**.

Universal Service Administrative Co.

If yes:
How did you/the affected consortium member identify the malicious cybersecurity actor(s)? Select all that apply.

- ☐ Advanced/Next-Generation Firewalls or similar
- ☐ Endpoint Protection or similar
- ☐ Identity Protection and Authentication or similar
- ☐ Monitoring, Detection, and Response or similar

How long did it take you/the affected consortium member to detect and respond to the most recent cybersecurity incident? Choose the answer that best describes the time interval. (For consortia, respond for the member with the most recent incident.) Select one.

- ○ Less than one hour
- ○ Between one hour and one day
- ○ Between one day and one week
- ○ Between one week and one month
- ○ Between one month and three months
- ○ Between three months and six months
- ○ More than six months

Universal Service Administrative Co.

What was the estimated direct cost of the most recent cybersecurity incident on you/the affected consortium member? (For consortia, respond for the member with the most recent incident.) Select one.

- ○ $0-$99
- ○ $100-$499
- ○ $500-$999
- ○ $1,000-$4,999
- ○ $5,000-$19,999
- ○ $20,000-$49,999
- ○ $50,000-$99,999
- ○ $100,000-$499,999
- ○ $500,000-$999,999
- ○ $1 million-$19.9 million
- ○ $20 million-$49.9 million
- ○ $50 million or more

Direct Cost

The direct cost includes money and money equivalents (including crypto currency) paid out such as ransom payments, immediate system repair costs, remediation payments to victims of data loss, and quantifiable payments that are the direct result of an attack.

Universal Service Administrative Co.

What was the estimated indirect cost of the most recent cybersecurity incident on you/the affected consortium member? (For consortia, respond for the member with the most recent incident.) Select one.

- ○ $0-$99
- ○ $100-$499
- ○ $500-$999
- ○ $1,000-$4,999
- ○ $5,000-$19,999
- ○ $20,000-$49,999
- ○ $50,000-$99,999
- ○ $100,000-$499,999
- ○ $500,000-$999,999
- ○ $1 million-$19.9 million
- ○ $20 million-$49.9 million
- ○ $50 million or more

Indirect Cost

The indirect cost includes cost indirectly related to the attack that may not be easily quantifiable, such as costs of system downtime, and additional expenses related to the attack such as overtime paid to employees for make-up school days.

Universal Service Administrative Co.

How did the most recent cybersecurity incident impact your/the affected consortium member's operations, network, and/or data? Select all that apply.

- ☐ We had to shut down the school or library temporarily
- ☐ Our sensitive data was lost or compromised
- ☐ We had to pay a ransom to regain access/recover data
- ☐ We had to pay remediation to victims of a data breach
- ☐ We had to pay to restore and repair a damaged or disabled network(s)
- ☐ We had to pay employees overtime to make up for lost time due to the network outage
- ☐ Other, please specify

5. Cybersecurity Application Sec. 3

5.1 Cybersecurity Training

a. Do you/any of your consortium members currently provide cybersecurity training for school staff, students, or library staff? Answer **Yes** or **No**.

If yes:
On average, how often do you/your consortium members provide cybersecurity training? (For consortia, answer this question using an average of all your consortium members.) Select one.

- ○ Weekly
- ○ Bi-Weekly
- ○ Monthly
- ○ Quarterly
- ○ Annually
- ○ Bi-Annually

Bi-Weekly and Bi-Annually

In question 5.1.a, bi-weekly means every other week and bi-annually means every two years.

Universal Service Administrative Co.

On average, what are your/your consortium members' training participation rates? (For consortia, answer this question using an average of all your consortium members.) Select one.

- ○ Less than 25%
- ○ 25%-49%
- ○ 50%-74%
- ○ 75%-99%
- ○ 100%

On average, how many school staff, students, or library staff participate in the cybersecurity training? (For consortia, answer this question using an average of all your consortium members.) Select one.

- ○ 0-9
- ○ 10-19
- ○ 20-49
- ○ 50-99
- ○ 100 or more

What training format(s) do you/the majority of your consortium members use to provide cybersecurity training? Select all that apply.

- ☐ Online
- ☐ In Person
- ☐ Hybrid

b. Do you have one or more full-time dedicated cybersecurity staff? Select one.

- ○ Part-Time Only
- ○ 1-2
- ○ 3 or more

Universal Service Administrative Co.

6. Cybersecurity Challenges

6.1 Non-monetary Challenges

a. In the past year, have you/any of your consortium members faced non-monetary challenges in attempting to IMPLEMENT cybersecurity protections/measures? Answer **Yes** or **No**.

> **If yes:**
> Select all of the non-monetary challenges you/the majority of your consortium members have faced in attempting to IMPLEMENT cybersecurity protections/measures. Select all that apply.
>
> ☐ Lack of time
> ☐ Lack of staff
> ☐ Lack of cybersecurity-specific knowledge
> ☐ Not a high-priority item for the school or library
> ☐ Not sure where to start
> ☐ How quickly broadband technology evolves
> ☐ How quickly cybersecurity threats and attacks evolve
> ☐ Other, please specify

b. In the past year have you/any of your consortium members faced any non-monetary challenges in attempting to MAINTAIN your current cybersecurity protections? Answer **Yes** or **No**.

> **If yes:**
> Select all of the non-monetary challenges you/the majority of your consortium members have faced in attempting to MAINTAIN your current cybersecurity protections/measures. Select all that apply.
>
> ☐ Lack of time
> ☐ Lack of staff
> ☐ Lack of cybersecurity-specific knowledge
> ☐ Not a high-priority item for the school or library
> ☐ Not sure where to start
> ☐ How quickly broadband technology evolves
> ☐ How quickly cybersecurity threats and attacks evolve
> ☐ Other, please specify