This submission is being made pursuant to 44 U.S.C. § 3507 of the Paperwork Reduction Act of 1995 (PRA) to obtain Office of Management and Budget (OMB) approval for new information collection requirements due to a Federal Communications Commission (Commission or FCC) rulemaking proceeding to establish a new Universal Service Fund pilot program, as explained further below. The forms for the Schools and Libraries Cybersecurity Pilot Program are modeled after FCC Forms 470, 471, 472, and 474 and the corresponding Emergency Connectivity Fund (ECF) forms. This information collection will leverage certain processes and FCC forms contained in information collections OMB Control Nos. 3060-0806 (FCC Forms 470 and 471), 3060-0856 (FCC Forms 472 and 474), and in the ECF information collection 3060-1286 (FCC ECF Forms 471, 472, 474, and 488) to avoid collecting duplicate information. As part of this information collection, there will also be a new FCC Form, the Schools and Libraries Cybersecurity Pilot Program Application (FCC Form 484), that will be used by schools, libraries, and consortia seeking to participate in this new pilot program.

## SUPPORTING STATEMENT

This information collection establishes requirements for the Schools and Libraries Cybersecurity Pilot Program (Cybersecurity Pilot Program or Pilot). The information collection proposes to collect information from applicants that will be used by the Commission to evaluate and select Pilot participants to receive funding under the Cybersecurity Pilot Program, and will be used by the Commission and the Universal Service Administrative Company (USAC or the Administrator) to reimburse schools, libraries, and consortia of schools and libraries (consortia) for the purchase of eligible cybersecurity services and equipment necessary to protect their broadband networks and data. *See Schools and Libraries Cybersecurity Pilot Program*, WC Docket No. 23-234, Report and Order, FCC 24-63, (adopted June 6, 2024) (*Cybersecurity Pilot Report and Order*).

### A. Justification:

1. *Circumstances that make the collection necessary.* Sections 254(1), (c)(3), (h)(1)(B), and (h)(2) of the Communications Act of 1934, as amended (Communications Act), grant the Commission authority to specify the services that will be supported using universal service funds and to design the specific mechanisms for support. The E-Rate program (formally known as the schools and libraries universal service support mechanism) provides funding for category one services, which include services and equipment needed to support broadband connectivity to schools and libraries, and category two services, which include services and equipment needed to support broadband connectivity within the schools and libraries. Basic firewall service is the only cybersecurity service currently funded by the E-Rate program. Specifically, basic firewall service provided as part of the vendor's Internet service is funded as a category one service, and separately-priced basic firewalls and services are funded as a category two service subject to the E-Rate applicants' five-year category two budget. The program defines a firewall as a hardware and software combination that sits at the boundary between an organization's network and the outside world, and protects the network against unauthorized access or intrusions. Under the E-Rate program, eligible schools, school districts, libraries, and consortia that include eligible schools and libraries may apply for discounts ranging from 20 percent to 90 percent of the pre-discount price of eligible services. The level of discounts may change depending on the category of eligible services selected, urban/rural designation, and level of need (based on the applicant's percentage of students participating in the National School Lunch Program (NSLP)).

Schools and libraries are increasingly targets of cyber attackers who disrupt their ability to educate, and who illegally obtain sensitive student, school staff, and library patron data, and hold the school

and library broadband networks hostage to extract ransom payments. During the COVID-19 pandemic, many E-Rate stakeholders submitted petitions asking the Commission to reconsider the eligibility of advanced firewall and other network security services given the increased use of schools' broadband networks to provide remote learning to their students.

In the *Cybersecurity Pilot Program Report and Order*, the Commission establishes a three-year Cybersecurity Pilot Program to ascertain whether supporting cybersecurity services and equipment with universal service support could advance the key universal service principles of providing quality Internet and broadband services to K-12 schools and libraries at just, reasonable, and affordable rates; and to ensure schools' and libraries' access to advanced telecommunications as provided by Congress in the Telecommunications Act of 1996.

The Cybersecurity Pilot Program will be a separate program from the E-Rate program, which has long provided funding for broadband services delivered to and within schools and libraries. The Cybersecurity Pilot Program will also be separate from the ECF program which was an emergency program established through the American Rescue Plan Act of 2021. In the interest of efficiency and simplicity, however, the goals and measures, rules, and processes adopted for the Cybersecurity Pilot Program will leverage the Commission's experience with the E-Rate and ECF programs, including adapting the E-Rate and ECF program forms and processes for use in the Cybersecurity Pilot Program. This method will streamline the Cybersecurity Pilot Program application and reimbursement processes for applicants, participants, and service providers; expedite the processing of applications and reimbursement requests; and lessen administrative burdens on participants and service providers participating in the Cybersecurity Pilot Program.

Specifically, all schools, libraries, and consortia of eligible schools and libraries that are interested in participating in the Cybersecurity Pilot Program will submit the first part of an application (Schools and Libraries Cybersecurity Pilot Program Application, FCC Form 484) that collects general information about how they would use the Pilot funds and provides a broad overview of their proposed Cybersecurity Pilot projects. Eligible entities will then be selected to participate in the Cybersecurity Pilot Program from the set of applicants that file the first part of the Cybersecurity Pilot Program Application, FCC Form 484. Applicants who are selected as Pilot participants will file the second part of the Cybersecurity Pilot Program Application, FCC Form 484. The second part of the application will collect a more detailed level of cybersecurity data and Pilot project information, but only from Cybersecurity Pilot Program participants. The Cybersecurity Pilot Program Application, FCC Form 484, is included with this submission and is split into its component parts.

Once selected, Pilot participants seek bids for their requested eligible cybersecurity services and equipment by filing the Schools and Libraries Cybersecurity Pilot FCC Form 470 (FCC Form 470 - Cybersecurity) with USAC, the current administrator of the E-Rate and ECF programs. After entering into agreements for eligible cybersecurity services and equipment, applicants apply for funding by filing the Schools and Libraries Cybersecurity Pilot FCC Form 471 (FCC Form 471 - Cybersecurity) application form, including supporting documentation, with the Administrator during the application filing window(s). Applicants will also be required to provide certifications regarding their compliance with the Schools and Libraries Cybersecurity Pilot Program rules on these forms. FCC Form 470 – Cybersecurity and FCC Form 471 – Cybersecurity are included with this submission. The approval for the information collection associated with the Schools and Libraries Cybersecurity Pilot FCC Form 470 can be found in the OMB Control No. 3060-0806. The approvals for the information collections associated with the Schools and Libraries Cybersecurity Pilot FCC Form 471 can be found in the OMB Control Nos. 3060-0806 and 3060-1286.

Upon receipt of eligible cybersecurity services or equipment, participants or service providers, must submit requests for reimbursement (Schools and Libraries Cybersecurity Pilot FCC Forms 472 and 474 (FCC Forms 472 - Cybersecurity and 474 – Cybersecurity) along with supporting invoicing documentation, to request disbursements through the Cybersecurity Pilot Program. The authorized person submitting the form will also be required to provide certifications regarding their compliance with the Schools and Libraries Cybersecurity Pilot Program. The Schools and Libraries Cybersecurity Pilot FCC Form 472 - Cybersecurity and FCC Form 474 – Cybersecurity are included with this submission. The approvals for the information collections associated with the Schools and Libraries Cybersecurity Pilot FCC Forms 472 and 474 can be found in the OMB Control Nos. 3060-0856 and 3060-1286.

Participants will also be able to request post-commitment changes to their FCC Form 471 - Cybersecurity funding requests by submitting the Cybersecurity Pilot Program post-commitment change request FCC Form 488 to USAC for review and approval (ECF FCC Form 488, as adapted for use in the Cybersecurity Pilot Program). Participants will be able to amend service start and end dates, reduce or cancel funding requests, substitute equipment or services, or change service providers through this process. Service providers are also allowed to submit this form to make certain changes to the funding requests as well. The Cybersecurity Pilot Program FCC Form 488 is included in this submission. The Schools and Libraries Cybersecurity Pilot FCC Form 488 is based on the approved information collection associated with OMB Control No. 3060-1286, ECF FCC Form 488 (using FCC Forms 471, 486, and 500) (FCC Form 488 – Cybersecurity).

Collection of the information is necessary so that the Commission and the Administrator have sufficient information to determine if entities are eligible for funding and complying with the Commission's rules. In addition, the information is necessary for the Commission to evaluate the extent to which the Pilot is meeting the statutory objectives specified in section 254(h) of the Communications Act, as amended.

Statutory authority for this collection of information is contained in sections 1-4, 201-202, 254, 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201-202, 254, 303(r), and 403.

This information collection does not affect individuals or households. Therefore, there is no impact under the Privacy Act.

**SCHOOLS AND LIBRARIES CYBERSECURITY PILOT PROGRAM NEW INFORMATION COLLECTION REQUIREMENTS**

The following are the proposed new information collection requirements associated with the proposed Schools and Libraries Cybersecurity Pilot Program:

a. Schools and Libraries Cybersecurity Pilot Program Application (FCC Form 484)

In order to be considered for participation in the Cybersecurity Pilot Program, eligible school, library, and consortium applicants must electronically submit the first part of an application, Schools and Libraries Cybersecurity Pilot Program FCC Form 484 (FCC Form 484), through an online system for the Cybersecurity Pilot Program. The information submitted will be used by the Commission to select Pilot participants and make preliminary funding determinations. The Wireline Competition Bureau (Bureau) will announce the opening of the Pilot Participant Selection Application Window. Eligible recipients shall submit an FCC Form 484 following the

opening of the window. The Bureau shall announce those eligible applicants that have been selected to participate in the Cybersecurity Pilot Program following the close of the window.

- Online Access for Streamlined Filing – Once information is pre-populated into the first part of the FCC Form 484, applicants will be able to check and provide corrections and updates to the information. The online portal asks for basic information about the applicant such as name, address, email address, and website information, and pre-populates these and other components of information already known about the applicant from prior submitted basic entity-related data into the online Cybersecurity Pilot Program Application form (FCC Form 484). This information comes from the applicant's information that was pre-filed and stored in the system, minimizing the burden of collecting this basic information. Specifically, in the first part of the FCC Form 484 applicants will be asked to provide:

    - Name, entity number, FCC registration number, employer identification number, addresses, and telephone number for each school, library, and consortium member that will participate in the proposed Pilot project, including the identity of the lead site for any proposals involving consortium. (This information will be pre-populated if available.)
    - Contact information for the individual(s) who will be responsible for the management and operation of the proposed Pilot project, including name, title or position, telephone number, mailing address, and email address. (This information will be pre-populated if available.)
    - Applicant number(s) and entity type(s), including Tribal information, if applicable, and current E-Rate participation status and discount percentage, if applicable. (This information will be pre-populated if available).
    - A broad description of the proposed Pilot project, including a description of the applicant's goals and objectives for the proposed Pilot project, a description of how Pilot funding will be used for the proposed project, and the cybersecurity risks the proposed Pilot project will prevent or address.
    - The cybersecurity equipment and services the applicant plans to request as part of its proposed project, the ability of the project to be self-sustaining once established, and whether the applicant has a cybersecurity officer or other senior-level staff member designated to be the cybersecurity officer for its Pilot project.
    - Whether the applicant has previous experience implementing cybersecurity protections or measures, how many years of prior experience the applicant has , whether the applicant has experienced a cybersecurity incident within a year of the date of its application, and information about the applicant's participation or planned participation in cybersecurity collaboration and/or information-sharing groups.
    - Whether the applicant has implemented, or begun implementing, any U.S. Department of Education or Cybersecurity and Infrastructure Security Agency best practices recommendations, a description of any U.S. Department of Education or Cybersecurity and Infrastructure Security Agency free or low-cost cybersecurity resources that an applicant currently utilizes or plans to utilize, or an explanation of what is preventing an applicant from utilizing these available resources.
    - An estimate of the total costs for the proposed Pilot project, information about how the applicant will cover the non-discount share of costs for the Pilot-eligible services,

and information about other cybersecurity funding the applicant receives, or expects to receive, from other federal, state, local, or Tribal programs or sources.

- Whether any of the ineligible services and equipment the applicant will purchase with its own resources to support the eligible cybersecurity equipment and services it plans to purchase with Pilot funding will have any ancillary capabilities that will allow it to capture data on cybersecurity threats and attacks, any free or low-cost cybersecurity resources that the applicant will require service providers to include in their bids, and whether the applicant will require its selected service provider(s) to capture and measure cost-effectiveness and cyber awareness/readiness data.
- A description of the applicant's proposed metrics for the Pilot project, how they align with the applicant's cybersecurity goals, how those metrics will be collected, and whether the applicant is prepared to share and report its cybersecurity metrics as part of the Pilot Program.

In order to participate in the Cybersecurity Pilot Program, eligible school, library, and consortium applicants who are selected as Pilot participants must electronically submit the second part of the FCC Form 484 through an online system for the Cybersecurity Pilot Program. The information submitted will be used by the Commission to make more definitive funding determinations and collect baseline cybersecurity data. The Bureau will notify Pilot participants of the deadline for completing the second part of the FCC Form 484 through a Public Notice.

- Online Access for Streamlined Filing – Once information is pre-populated into the second part of the FCC Form 484, participants will be able to check and provide corrections and updates to the information. For the second part of the FCC Form 484, the online portal asks for the following additional (or substantially similar) cybersecurity information, as applicable:

  - Information about correcting known security flaws and conducting routine backups, developing and exercising a cyber incident response plan, and any cybersecurity changes or advancements the participant plans to make outside of the Pilot-funded services and equipment.
  - A description of the participant's current cybersecurity posture, including how the school or library is currently managing and addressing its current cybersecurity risks through prevention and mitigation tactics.
  - Information about a participant's planned use(s) for other federal, state, or local cybersecurity funding (i.e., funding obtained outside of the Pilot).
  - Information about a participant's history of cybersecurity threats and attacks within a year of the date of its application; the date range of the incident; a description of the unauthorized access; a description of the impact to the school or library; a description of the vulnerabilities exploited and the techniques used to access the system; and identifying information for each actor responsible for the incident, if known.
  - A description of the specific U.S. Department of Education or Cybersecurity and Infrastructure Security Agency cybersecurity best practices recommendations that the participant has implemented or begun to implement.

- Information about a participant's current cybersecurity training policies and procedures, such as the frequency with which a participant trains its school and library staff and, separately, information about student cyber training sessions, and participation rates.
- Information about any non-monetary or other challenges a participant may be facing in developing a more robust cybersecurity posture.

- Participants must provide certifications along with the first and second parts of their Cybersecurity Pilot Program FCC Forms 484. These certifications are required to protect the integrity of the Cybersecurity Pilot Program, and to ensure compliance with the Commission's rules.

b. Schools and Libraries Cybersecurity Pilot Program FCC Form 470 "Description of Services Requested and Certification" (FCC Form 470 – Cybersecurity)

- Cybersecurity Pilot Program participants will submit a Schools and Libraries Cybersecurity Pilot Program FCC Form 470 (FCC Form 470 - Cybersecurity) to the Administrator to initiate their competitive bidding process, if not subject to a competitive bidding exemption. The FCC Form 470 - Cybersecurity shall include, at a minimum, a list of specified services and/or equipment for which the school, library, or consortium requests bids and sufficient information to enable bidders to reasonably determine the needs of the participant and provide responsive bids. The FCC Form 470 - Cybersecurity will be submitted electronically through the Cybersecurity Pilot Program online system and available information in the portal will be migrated to the FCC Form 470 - Cybersecurity to lessen the administrative burden on the participant. The Cybersecurity Pilot Program FCC Form 470 - Cybersecurity relies on the data that is collected on the E-Rate FCC Form 470 (approved under OMB Control Number 3060-0806).

- Applicants must provide certifications along with their Cybersecurity Pilot Program FCC Form 470 - Cybersecurity. These certifications are required to protect the integrity of the Cybersecurity Pilot Program and to ensure compliance with the Commission's rules.

- USAC will post each certified Cybersecurity Pilot Program FCC Form 470 - Cybersecurity on its website and send confirmation of the posting to the participant requesting services and/or equipment. Participants must wait at least 28 days from the date on which its description of services and/or equipment is posted on the USAC's website before entering into contracts and agreements with the selected providers of services and/or equipment. The confirmation from USAC will include the date after which the Cybersecurity Pilot Program participant may select its service provider(s) and sign a contract with its chosen provider(s).

c. Schools and Libraries Cybersecurity Pilot Program FCC Form 471 "Services Ordered and Certification" (FCC Form 471 – Cybersecurity)

For the Cybersecurity Pilot Program, participants will file a Cybersecurity Pilot Program FCC Form 471 (FCC Form 471 - Cybersecurity) to notify USAC of the services and/or equipment that have been or will be purchased, the service provider(s) with whom the participant has entered into an agreement, and an estimate of the funds needed to reimburse the costs of the eligible services and equipment through the Cybersecurity Pilot Program.

- Online Access for Streamlined Filing – Once information is prepopulated into the FCC Form 471- Cybersecurity, participants will be able to check and provide corrections and updates to the information. The online portal asks for basic information about the participant such as name, telephone number, address, email address, and website information, and pre-populates these and other components of information already known about the applicant from previously submitted data that will be migrated to the online FCC Form 471- Cybersecurity. This information comes from the participant's profile information that was pre-filed and stored in the system, minimizing the burden of collecting this basic information. The portal may also ask other questions related to the FCC Form 471 as the participant completes and submits the online Cybersecurity Pilot Program FCC Form 471- Cybersecurity. The Cybersecurity Pilot Program FCC Form 471- Cybersecurity relies on the data that is collected on both the E-Rate FCC Form 471 (approved under OMB Control Number 3060-0806) and the ECF FCC Form 471 (approved under OMB Control No. 3060-1286). Access to the portal and pre-population of data is expected to expedite the FCC Form 471- Cybersecurity filing process for participants to request Cybersecurity Pilot Program support for eligible services and equipment to support the program goals of: (1) improving the security and protection of E-Rate-funded broadband networks and data; (2) measuring the costs associated with cybersecurity services and equipment, and the amount of funding needed to adequately meet the demand for these services if extended to all E-Rate participants; and (3) evaluating how to leverage other federal K-12 cybersecurity tools and resources to help schools and libraries effectively address their cybersecurity needs.

- Customized Applications – In general, the FCC Form 471- Cybersecurity is customized to the type of participant and/or the type of selections made during the filing process.

- Integrated Instructions – Guidance for filling out the form is integrated into the online system to provide filers a roadmap to complete the FCC Form 471- Cybersecurity. Wherever applicable and possible, filers will be provided explanatory text regarding the selections they choose during filing, and additional text to remind them where they may have to provide additional information or meet special requirements.

- Requesting Services – In addition to information previously asked of participants to request funding for services and equipment in this collection, participants may need to supply additional information and documentation to enable USAC and the Commission to determine if the participant is compliant with the Cybersecurity Pilot Program rules and the requested services and equipment are eligible for support.

- Other Documentation Requirements – Schools, libraries, and consortia are required to maintain inventories of services and equipment purchased or reimbursed through the Cybersecurity Pilot Program. All eligible schools, libraries, and consortia that choose to participate may be required to collect and submit data as part of the funding request process, at regular intervals during the Cybersecurity Pilot Program, and at the end of the Pilot. The collection of this information, which may go beyond that provided in the Cybersecurity Pilot Program FCC Forms 484 and 471- Cybersecurity, is necessary to evaluate the impact of the Pilot, including whether the Pilot achieves its goals. This includes the proposed evaluation process, as well as annual and final progress reports detailing the use of funds and effectiveness of the Cybersecurity Pilot Program.

- Streamlined Communications – Once an FCC Form 471- Cybersecurity has been filed, filers receive a notice through the user online portal to confirm receipt.

- The Commission's rules require participants to certify on the Cybersecurity Pilot Program FCC Form 471 – Cybersecurity their compliance with the requirements for the Cybersecurity Pilot Program (47 C.F.R. § 54.2006(a)(2)(i)-(xvi)). These certifications are required to protect the integrity of the Cybersecurity Pilot Program, and to ensure compliance with the Commission's rules.

d. Schools and Libraries Cybersecurity Pilot Program FCC Form 472/474 "Request for Reimbursement" (FCC Form 472/474 – Cybersecurity)

- For the Cybersecurity Pilot Program, participants and/or service providers will submit a Cybersecurity Pilot Program Request for Reimbursement Form (Request for Reimbursement or FCC Form 472/474 - Cybersecurity) to receive disbursements from the Program. Much of the requested information will be pre-populated through the online portal. USAC will review and approve the requests for reimbursement. The Cybersecurity Pilot Program Request for Reimbursement relies on the data that is collected on both the E-Rate FCC Form 472 and FCC Form 474 (approved under OMB Control Number 3060-0856) and the ECF FCC Form 472/474 (approved under OMB Control No. 3060-1286), including information about the amount paid for approved services delivered on or after the actual service start date and approved services and equipment, as reported on the FCC Form 471- Cybersecurity.

- Participants and/or service providers will also be required to provide invoices and other supporting documentation for the services and equipment that are included in the Cybersecurity Pilot Program Request for Reimbursement. This requirement will help to ensure that the Cybersecurity Pilot Program is being used as intended and will protect the integrity of the Cybersecurity Pilot Program.

- Participants and/or service providers must provide certifications along with their Cybersecurity Pilot Program Requests for Reimbursement. (47 C.F.R. § 54.2008(a)(1)(i)-(xiii); § 54.2008(a)(2)(i)-(xiii)). These certifications are required to protect the integrity of the Cybersecurity Pilot Program, and to ensure compliance with the Commission's rules.

- Participants and/or service providers will receive electronic notifications as to the status of their Cybersecurity Pilot Program Requests for Reimbursement.

e. Schools and Libraries Cybersecurity Pilot Program FCC Form 488 "Post-Commitment Change Request" (based on ECF FCC Form 488) (FCC Form 488 – Cybersecurity)

- After USAC reviews the funding request and commitments are issued to fund the eligible services and equipment requested in the Cybersecurity Pilot Program FCC Form 471- Cybersecurity, participants may make adjustments to previously filed FCC Forms 471 - Cybersecurity, such as changing the service start date or service end date, cancelling or reducing the amount of a funding request approved, requesting a service or equipment substitution and requesting a service provider change. Service providers are also allowed to make certain post-commitment changes to their FCC Form 471- Cybersecurity funding requests. (*See* 47 C.F.R. § 54.2006(b) (allowing participants to submit service substitutions for approval by USAC)). This Cybersecurity Pilot Program Post-Commitment Change Request (FCC Form 488 – Cybersecurity) can be used by participants to make these necessary changes to their previously approved and committed Cybersecurity Pilot FCC Forms 471- Cybersecurity. The change request for use in the Cybersecurity Pilot Program is included in this submission. This change request is based on the approved information

collection for the ECF FCC Form 488, OMB Control No. 3060-1286 to create a streamlined process for making post-commitment changes in the Cybersecurity Pilot Program. The participant or service provider will request these changes by logging into the online portal, making changes to the selected Cybersecurity Pilot Program FCC Form 471- Cybersecurity, and then re-certifying the requested changes to the selected FCC Form 471- Cybersecurity in the online portal. *See, e.g.*, 47 C.F.R. **§** 54.2006(b) (allowing service and equipment substitutions).[1]

f. Recordkeeping, Reporting, and Audits. All participants in the Cybersecurity Pilot Program will be required to retain all documentation accumulated during the Pilot for at least ten (10) years from the last date of service or delivery of equipment. All Cybersecurity Pilot Program participants shall maintain asset and inventory records of services and equipment purchased sufficient to verify the actual location of such services and equipment for a period of 10 years after purchase. All participants in the Cybersecurity Pilot Program will produce these records upon request of any representative (including any auditor) appointed by a state education department, USAC, the Commission and its Office of Inspector General or any local, state, or federal agency with jurisdiction over the entity. Cybersecurity Pilot Program participants may also be subject to compliance audits to ensure they are complying with Cybersecurity Pilot Program rules and certification requirements. (47 C.F.R. §§ 54.2009(a)-(b), 54.2010(a)-(b)).

2. *Use of information*. The information collected is designed to obtain information from applicants and service providers that will be used by the Commission and/or USAC to evaluate the applications and select participants to receive funding under the Cybersecurity Pilot Program, and make funding determinations and disburse funding in compliance with applicable federal laws for payments made through the Cybersecurity Pilot Program. The Commission will begin accepting applications to participate in the Cybersecurity Pilot Program after publication of its *Cybersecurity Pilot Program Report and Order* and notice of OMB approval of the Cybersecurity Pilot Program information collection in the Federal Register.

3. *Use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology*. In an effort to reduce any burden created by the information collection requirements, respondents will be required to submit their applications and forms electronically through an online portal on the USAC website. The online data collections do not, in non-material respects, exactly resemble the representation or template of the form charts included with this submission. The online interface will permit applicants, participants, and service providers to input data in required fields and auto-populate data where applicable, reducing their filing burden.

4. *Efforts to identify duplication*. There will be no duplication of information. The information sought is unique to each applicant, participant, or service provider and similar information is not already available. To the extent some information is already available through the E-Rate and ECF portals, it will be migrated into the Cybersecurity Pilot Program online portal.

5. *Impact on small entities*. Entities directly subject to the requirements in this information collection are primarily schools, libraries, school districts, and consortia thereof. This information collection is designed to impose the least possible burden on the respondents while ensuring that the Commission has the information necessary to evaluate applications for the Cybersecurity Pilot Program, select participants for the program to receive funding, and evaluate participants' and service providers'

[1] *Cybersecurity Pilot Program Report and Order* at Appendix A.

requests for reimbursement. Specifically, the Commission has limited the information requirements to those necessary for the purposes for which the information will be used.

6. *Consequences if information is not collected*. The information collected will be used to evaluate applications, make Pilot participant selections, and issue funding commitments and disbursements under the Cybersecurity Pilot Program. Without the requested information, the Commission will not be able to assess either applicant eligibility or the extent to which funds are properly used by Cybersecurity Pilot Program participants.

7. *Special circumstances*. There are no special circumstances associated with this information collection.

8. *Federal Register notice; efforts to consult with persons outside the Commission*. The Commission published a Federal Register Notice on December 29, 2023, 88 FR 90141, seeking comments on the new information collection requirements contained in the *Cybersecurity Pilot NPRM* Supporting Statement. To date, no comments have been received from the public.

9. *Payments or gifts to respondents*. The Commission does not anticipate providing any payment or gifts to respondents.

10. *Assurances of confidentiality*. The funding recipient's name, address, unique entity identifier (UEI) number, and business type will be disclosed in accordance with the Federal Funding Accountability and Transparency Act/Digital Accountability and Transparency Act (FFATA/DATA) reporting requirements. Commitment and disbursement information also will be made public. We intend to keep other information private to the extent permitted by law. Further, sensitive cybersecurity information contained in the Schools and Libraries Cybersecurity Pilot Program Application (FCC Form 484), as well as information provided in Pilot participants' initial, annual, and final reports will be presumptively confidential; however, we do plan to use aggregated, anonymized, and/or non-specific school or library data as a tool to evaluate the success and impact of the Pilot, including whether and how to fund schools' and libraries' cybersecurity needs through the E-Rate program or another universal service program on an ongoing basis.

11. *Questions of a sensitive nature*. We recognize that FCC Form 484 applications could contain sensitive information. As such, the USAC cybersecurity platform that applicants, and participants once selected for the Pilot, will use to submit their FCC Form 484 applications will be a closed system that can only be accessed by the applicant or participant, or persons designated by the applicant or participant, USAC, and the FCC. Applicants and participants will not be able to view each other's FCC Form 484 applications and the sensitive cybersecurity information on the FCC Form 484 data will not be made available to the public. However, the other Pilot form data, FCC Forms 470, 471, and 472/474 data, may be publicly available as federal funding is being provided to the Pilot participants, and the public data may include the name of the Pilot participant, services and equipment requested, names of service providers, and the amount of Pilot funding committed and disbursed. To address those concerns, the *Cybersecurity Pilot Program Report and Order* directs Commission and USAC staff to abide by all applicable federal and state laws in carrying out the Pilot and any audits of the program and treat information provided as presumptively confidential.

12. *Estimates of the hour burden of the collection to respondents.* The following represents the hour burden on the collection of information:

a. **Submission of Schools and Libraries Cybersecurity Pilot Program FCC Form 484 "Application".**

(1) Number of respondents: Approximately 23,000 respondents.

(2) Frequency of response: Once.

(3) Total number of responses per respondent: 1

(4) Hourly burden per respondent: 14

14 hours (to fill out the form to comply with reporting requirements)

(5) Total annual burden: 322,000

23,000 (number of respondents) x 1 (estimated number of submissions) x 14 hours = 322,000

(6) Total estimate of in-house cost to respondents: $15,800,540

(7) Explanation of Calculation: We estimate that:

(a) It will take approximately 14 hours to fill out the FCC Form 484 for the reporting requirements (23,000 respondents x 14 hours x 1 Form =322,000).

(b) Approximately 23,000 respondents will spend approximately 14 hours to comply with requirements preparing and submitting the FCC Form 484 at a cost of $49.07 per hour.

322,000 hours x $49.07/hour = $15,800,540 cost for the reporting requirements

**Summary of Estimated Total Annual Burden Hours for FCC Form 484.**

**Total Number of Respondents: 23,000 respondents**

**Total Number of Reponses: 23,000 responses**

**Total Annual Hourly Burden: 322,000 hours**

322,000 hours for reporting requirements

b. **Submission of Schools and Libraries Cybersecurity Pilot Program FCC Form 470 - "Description of Services Requested and Certification" (FCC Form 470 – Cybersecurity).**

(1) Number of respondents: approximately 23,000

(2) Frequency of response: Once.

(3) Total number of responses per respondent: 1

(4) Hourly burden per respondent: 3

3 hours (to fill out the form to comply with reporting requirement).

(5) Total annual burden:

23,000 (number of respondents) x 1 (estimated number of submissions) x 3 hours = 69,000

(6) Total estimate of in-house cost to respondents: $3,385,830

(7) Explanation of calculation: We estimate that:

a) It will take approximately 3 hours to fill out the FCC Form 470 - Cybersecurity for the reporting requirements (23,000 respondents x 3 hours x 1 Form = 69,000).

b) Approximately 23,000 respondents will spend approximately 3 hours to comply with requirements preparing and submitting the FCC Form 470 - Cybersecurity at a cost of $49.07 per hour.

69,000 hours x $49.07/hour = $3,385,830 cost for the reporting requirements

**Summary of Estimated Total Annual Burden Hours for FCC Form 470 - Cybersecurity:**

**Total Number of Respondents: 23,000 respondents**

**Total Number of Reponses: 23,000 responses**

**Total Annual Hourly Burden: 69,000 hours**

69,000 hours for reporting requirements

c) **Submission of Schools and Libraries Cybersecurity Pilot Program FCC Form 471 - "Services Ordered and Certification" (FCC Form 471 – Cybersecurity).**

(1) Number of respondents: approximately 23,000

(2) Frequency of response: Once.

(3) Total number of responses per respondent: 1.7

(4) Hourly burden per respondent: 4

4 hours (to fill out the form to comply with reporting requirement)

(5) Total annual burden:

23,000 (number of respondents) x 1.7 (estimated number of submissions) x 4 hours = 156,400

(6) Total estimate of in-house cost to respondents: $7,674,548

(7) Explanation of calculation: We estimate that:

(a) It will take approximately 4 hours to fill out the FCC Form 471- Cybersecurity for the reporting requirements (23,000 respondents x 4 hours x 1.7 Forms = 156,400).

(b) Approximately 23,000 respondents will spend approximately 4 hours to comply with requirements preparing and submitting the FCC Form 471- Cybersecurity at a cost of $49.07 per hour).

156,400 hours x $49.07/hour = $7,674,548 cost for the reporting requirement.

**Summary of Estimated Total Annual Burden Hours for FCC Form 471 - Cybersecurity:**

**Total Number of Respondents: 23,000 respondents**

**Total Number of Responses: 39,100 responses**

**Total Annual Hourly Burden: 156,400**

156,400 hours for reporting requirements.

d. **Submission of Schools and Libraries Cybersecurity Pilot Program Request for Reimbursement (FCC Form 472/FCC Form 474 - Cybersecurity).**

(1) Number of respondents: Approximately 23,000 respondents.

(2) Frequency of response: On occasion.

(3) Total number of responses per respondent: 4

(4) Hourly burden per respondent: 1

1 hour (to fill out the form to comply with reporting requirement)

(5) Total annual burden: 92,000

23,000 (number of respondents) x 4 (estimated number of submissions) x 1 hours = 92,000

(6) Total estimate of in-house cost to respondents for the hour burdens for collection of information: $4,514,440

(7) Estimate of Calculation: We estimate that:

(a) It will take approximately 1 hour to fill out the FCC Form 472/474 - Cybersecurity for the reporting requirement (23,000 respondents x 1 hour x 4 Forms = 92,000).

(b) Approximately 23,000 respondents will spend approximately 1 hour to comply with requirements preparing the FCC Forms 472/474 - Cybersecurity at a cost of $49.07 per hour.

92,000 hours x $49.07/hour = $4,514,440 cost for reporting requirements.

**Summary of Estimated Total Annual Burden Hours for FCC Form 472/474 - Cybersecurity:**

**Total Number of Respondents:** 23,000 respondents.

**Total Number of Responses:** 92,000 (23,000 respondents x 4 Forms = 92,000)

**Total Annual Hourly Burden:** (23,000 respondents x 4 Form submissions x 1hours) = 92,000

92,000 hours for reporting requirements.

e. **Submission of Schools and Libraries Cybersecurity Pilot Program Post-Commitment Change Request Form (streamlined information collection based on the ECF Change Request Form (using FCC Forms 471/486/500/) for use in the Cybersecurity Pilot Program) (FCC Form 488 – Cybersecurity).**

(1) Number of respondents: Approximately 1,000 respondents.

(2) Frequency of response: On occasion.

(3) Total number of responses per respondent: 1

(4) Hourly burden per respondent: 1 hour (to fill out the form to comply with reporting requirement)

(5) Total annual burden: = 1,000

1,000 (number of respondents) x 1 (estimated number of submissions) x 1 hour = 1,000

(6) Total estimate of in-house cost to respondents: $49,070

(7) Explanation of calculation: We estimate that:

(a) It will take approximately 1 hour to provide data for the FCC Form 488 - Cybersecurity for the reporting requirements (1,000 respondents x 1 hour x 1 Form = 1,000).

(b) Approximately 1,000 respondents will spend approximately 1 hour to comply with requirements preparing the FCC Form 488 - Cybersecurity at a cost of $49.07 per hour.

1,000 hours x $49.07/hour = $49,070 cost for reporting requirements.

**Summary of Estimated Total Annual Burden Hours for FCC Form 488 - Cybersecurity:**

**Total Number of Respondents:** 1,000 respondents

**Total Number of Responses:** 1,000 (1,000 respondents x 1 Form = 1,000)

**Total Annual Hourly Burden:** 1,000 (1,000 respondents x 1 Form submission x 1 hours)

1,000 hours for reporting requirements.

f. **Submission of Schools and Libraries Cybersecurity Pilot Program Recordkeeping.**

(1) Number of respondents: approximately 23,000

(2) Frequency of response: Annual recordkeeping requirement.

(3) Total number of responses per respondent: 1

(4) Hourly burden per respondent: 4.50

4.5 hours (to comply with recordkeeping requirements).

(5) Total annual burden:

23,000 (number of respondents) x 1 (estimated number of submissions) x 4.50 hours = 103,500

(6) Total estimate of in-house cost to respondents: $5,078,745

(7) Explanation of calculation: We estimate that:

(a) Approximately 23,000 respondents will spend approximately 4.50 hours to comply with the ten-year recordkeeping requirement at a cost of $49.07 per hour.

(b) 103,500 hours x $49.07/hour = $5,078,745 cost for the recordkeeping requirements.

**Summary of Estimated Total Annual Burden Hours for FCC Recordkeeping Requirements:**

**Total Number of Respondents: 23,000 respondents**

**Total Number of Reponses: 23,000 responses**

**Total Annual Hourly Burden: 103,500 hours**

103,500 hours for recordkeeping requirements.

**The estimated respondents, responses, and burden hours are listed below:**

| Information Collection Requirements | Number of Respondents | Total Number of Responses | Hourly Burden Per Response | Total Annual Hourly Burden | Total In-House Cost to the Respondents |
|---|---|---|---|---|---|
| a. Schools and Libraries Cybersecurity Pilot Program FCC Form 484 | 23,000 | 23,000 | 14 | 322,000 | $15,800,540 |
| b. Schools and Libraries Cybersecurity Pilot Program FCC Form 470 - Cybersecurity | 23,000 | 23,000 | 3 | 69,000 | $3,385,830 |
| c. Schools and Libraries Cybersecurity Pilot Program FCC Form 471 – Cybersecurity | 23,000 | 39,100 | 4 | 156,400 | $7,674,548 |
| d. Schools and Libraries Cybersecurity Pilot Program FCC Forms 472/474 - Cybersecurity | 23,000 | 92,000 | 1 | 92,000 | $4,514,440 |
| e. Schools and Libraries Cybersecurity Pilot Program FCC Form 488 - Cybersecurity | 1,000 | 1,000 | 1 | 1,000 | $49,070 |
| f. Schools and Libraries Cybersecurity Pilot Program Recordkeeping | 23,000 | 23,000 | 4.5 | 103,500 | $5,078,745 |
| **Grand Total** | 23,000 unique respondents | 201,100 | 27.5 | 743,900 | $36,503,173 |

13. *Total Annual Costs to Respondents*. Estimates for the cost burden of the collection to respondents. There are no outside contracting costs for this information collection. See the total in item 12 above for the estimated in-house costs to respondents.

14. *Estimates of the Cost Burden to the Commission*. There will be few, if any, additional costs to the Commission because notice, enforcement, and policy analysis associated with the Universal Service Fund are already part of the Commission's duties. Moreover, there will be minimal cost to the Federal government because a third party, USAC, administers the Universal Service Fund and support mechanisms.

15. *Program Changes or Adjustments.* If the Commission adopts the new information collection requirements as proposed in a final rulemaking, the following burdens/increases will be added to OMB's Active Inventory: 23,000 total respondents, 201,100 total annual responses, and 743,900 total annual burden hours.

16. *Collections of information whose results will be published.* The Commission will publish the selected participants for the Cybersecurity Pilot Program and may publish funding request (FCC Form 471 - Cybersecurity) and funding disbursement (FCC Forms 472/474 - Cybersecurity) data. At this time, the Commission has no plans to publish data collected for statistical use or other reports. However, the Commission may publish such data in the future, to the extent that the data's confidentiality is not protected under law, in the course of carrying out the Commission's policymaking responsibilities.

17. *Display the expiration date for OMB approval of the information collection*. The Commission seeks approval to not display the expiration date for OMB approval of this information collection. OMB control numbers and expiration dates for the Commission's information collection requirements assigned by OMB pursuant to the Paperwork Reduction Act of 1995, Public Law 104–13 can be found at *https://www.reginfo.gov/public/do/PRAMain* *See* 47 CFR § 0.408.

18. *Exceptions to certification statement for Paperwork Reduction Act Submissions*. There are no exceptions to the Certification Statement.

## B. Collections of Information Employing Statistical Methods:

The Commission does not anticipate that the collection of information will employ statistical methods.