



Schools & Libraries Cybersecurity Pilot Program: Competitive Bidding

Housekeeping

- Audio is available through your computer's speakers
- The audience will remain on mute
- **Enter questions at any time using the “Questions” box**
- If your audio or slides freeze, restart the webinar
- A copy of today's presentation is available in the handouts section of the GoToWebinar control panel

Pilot Program: Process and Timeline

Pilot Program Participants: Timeline



1

- Participants must complete a minimum 28-Day **Competitive Bidding** process using the Pilot FCC Form 470 to seek bids for **eligible** cybersecurity equipment and services.
- The Pilot FCC Form 470 is available in the Cybersecurity Pilot Program portal now and must be completed by August 18, 2025 to be timely filed.



2

- Participants submit Pilot Program **Funding Request(s)** using the Pilot FCC Form 471.
- Pilot Program FCC Form 471 application filing window runs from March 18 – September 15, 2025.



3

- Participants must also complete the **Pilot FCC Form 484 Part 2**.
- Participants must complete Part 2 by September 15, 2025 (the close of the Pilot FCC Form 471 application filing window) **and** submit the Pilot FCC Form 471 to be able to receive funding commitment decision letters (FCDL).

Pilot Program: Competitive Bidding

Pilot Program: Competitive Bidding

- Participating schools, libraries, and consortia must complete a minimum 28-day competitive bidding process using the Pilot FCC Form 470 to seek bids for eligible cybersecurity equipment and services.
- The competitive bidding process must be fair and open for all interested service providers.
- Participants must follow all applicable state, Tribal, or local procurement laws, in addition to the Pilot Program competitive bidding rules.
- Participants can begin the competitive bidding process now.

Pilot Program: Competitive Bidding

- Participants will use the Pilot FCC Form 470 available in the Cybersecurity Pilot Program portal to initiate competitive bidding.
- At a minimum, the Pilot FCC Form 470 should include the following:
 - A list of the specified cybersecurity services and/or equipment for which the participant requests bids. Participants may refer back to the Pilot FCC Form 484 Part 1 as they work to identify their needs on the Pilot FCC Form 470.
 - Sufficient information, including technical and network requirements, that will allow potential bidders to reasonably determine the needs of the participant.

Pilot Program: Competitive Bidding

- Participants can, but are not required to, issue a Request for Proposal (RFP) along with their Pilot FCC Form 470. If they choose to do so, they must upload the RFP into the Cybersecurity Pilot Program portal. If they choose not to issue an RFP, they must fill out the narrative text box to describe the cybersecurity services and/or equipment they seek.
- Pilot Program FCC Forms 470 and RFPs must be vendor neutral.
 - When completing the form or issuing an RFP, participants may not request a particular manufacturer's name, brand, product, or service unless they also use the words "or equivalent" in their descriptions to ensure prospective bidders are not discouraged from submitting potentially more cost-effective bids that use different manufacturer names, brands, products, or services.

Pilot Program: 28-Day Competitive Bidding Period

Pilot Program: 28-Day Competitive Bidding Period

- Participants must wait at least 28-days before selecting and entering into a legally binding agreement or contract with a service provider. This is known as the Allowable Contract Date (ACD).
- The 28-day competitive bidding period begins on the day that a participant certifies their Pilot FCC Form 470 in the Cybersecurity Pilot Program portal and it is posted to USAC's website.
- Participants can set a bid deadline as long as it allows for the full 28-day competitive bidding window.
- If a participant makes substantive changes to their Pilot FCC Form 470 and/or the accompanying RFP that materially affect the competitive bidding process, the participant must restart the 28-day bidding period.
- After waiting at least 28-days, participants can select a service provider after carefully reviewing all bids received and selecting the most cost-effective offering.

Pilot Program: Selecting a Service Provider

Pilot Program: Selecting a Service Provider

- After the competitive bidding period ends, participants must carefully evaluate all bids received using price of the eligible services and equipment as the primary factor.
 - Participants may use a bid evaluation matrix that weighs price as the primary (i.e., most heavily-weighted) factor to evaluate the bids.
- Participants can consider other factors in their bid evaluation, as long as the price of the eligible cybersecurity equipment and services is weighted more heavily than any other single factor.
- Once all bids have been evaluated, participants can select the most cost-effective offering and sign a contract or legally binding agreement with that service provider.
- Participants must retain a copy of their completed bid evaluation documents, including a copy of any bid evaluation matrix(ices), in accordance with FCC's record retention rules.

Pilot Program: Pilot FCC Form 470

Pilot Program: Pilot FCC Form 470

- Participants will use the Pilot FCC Form 470 in the Cybersecurity Pilot Program portal to initiate their competitive bidding activities.
- Only Account Administrators and other authorized persons who have full access rights to the Pilot FCC Form 470 may submit and/or certify the form on behalf of the participant.
- Participants will find the Pilot FCC Form 470 in their CBR Dashboard in the Cybersecurity Pilot Program portal, under the My Organization(s) tab.
- Participants can include eligible and ineligible equipment and services in their Pilot FCC Form 470, but only eligible cybersecurity equipment and services are reimbursable through the Pilot Program.
- Please note: Training is only eligible as a part of the installation of the equipment and services if it is basic instruction on the use of the eligible equipment and services, directly associated with equipment and services installation, and is part of the contract or agreement for the equipment and services.

Schools & Libraries Cybersecurity Master Service Agreements/Contracts

Pilot Program: Master Service Agreements/Contracts

- A Pilot participant that wishes to rely on a Master Services Agreement (MSA) or State Master Contract (SMC) that is negotiated by federal, state, Tribal, or local governmental entities on behalf of the participant will not be required to seek competitive bids if the MSA/SMC was awarded pursuant to the E-Rate FCC Form 470 process, as well as applicable federal, state, Tribal, or local competitive bidding requirements.

Pilot Program: Master Service Agreements/Contracts

- To qualify for this competitive bidding exemption (CBE), governmental entities (including state agencies) must submit their MSAs/SMCs to USAC for review within 60 days of the January 16, 2025 FCC Public Notice.
 - Non-governmental entities with existing MSAs that were awarded pursuant to the E-Rate FCC Form 470 process, as well as applicable federal, state, Tribal or local competitive bidding requirements, must seek a waiver from the FCC because they are not an eligible governmental entity under the CBE requirements.
- All MSAs/SMCs that qualify for the CBE will be posted on USAC's website with the establishing E-Rate FCC Form 470 for use by Pilot participants who qualify to use the contract.

Questions?

Pilot Program: Pilot FCC Form 470 Walkthrough

Pilot FCC Form 470 Walkthrough: Getting Started

My Applicant Landing Page



[Funding Request Report](#) | [FCC Form 470](#) | [FCC Form 471](#) | [FCC Form 486](#) | [Appeal](#) | [IDD Extension](#) | [FCC Form 500](#) | [SPIN Change](#) | [Service Substitution](#) | [Manage Users](#) | [Manage Organizations](#) | [EPC E-Rate Invoicing](#) | [USAC Website](#) | [Contact Us](#) | [Help](#)

Welcome, Applicant Name!

Pending Inquiries

Type

Application/Request

Funding Year

Pending COMAD Inquiries are not included.

Application/Request Number	Type	Nickname	Inquiry Name	Outreach Type	Date Sent	Due Date	<input type="checkbox"/> Extn.	Status
No items available								

Notifications

Notification Type

Status All
 Generated
 Not Generated

Funding Year

Notification	Description	Issued Date	Generated By	Generated On
No items available				

- Cybersecurity Pilot Program
- EPC Invoice

My Applicant Landing Page



[Funding Request Report](#) |
 [FCC Form 470](#) |
 [FCC Form 471](#) |
 [FCC Form 486](#) |
 [Appeal](#) |
 [IDD Extension](#) |
 [FCC Form 500](#) |
 [SPIN Change](#) |
 [Service Substitution](#) |
 [Manage Users](#) |
 [Manage Organizations](#) |
 [EPC E-Rate Invoicing](#) |
 [USAC Website](#) |
 [Contact Us](#) |
 [Help](#)

Welcome, Applicant Name!

Pending Inquiries

Type **Application/Request**
Funding Year

Pending COMAD Inquiries are not included.

Application/Request Number	Type	Nickname	Inquiry Name	Outreach Type	Date Sent	Due Date	↑	Extn.	Status
No items available									

Notifications

Notification Type **Status ?** All
Funding Year Generated
 Not Generated

Notification	Description	Issued Date	Generated By	Generated On
No items available				



Good Morning, Welcome to the Cybersecurity Pilot Program!

Name



My Organization(s)

My Forms and Requests

My Pending Tasks

My Pending Inquiries

Empty light blue bar

Search SL Applicant Entities

SEARCH



BEN	BEN Name	City	State	Entity Type	Action
000000	NAME	CITY	STATE	Library	ACTIONS



Good Morning, Welcome to the Cybersecurity Pilot Program!

Name



My Organization(s)

My Forms and Requests

My Pending Tasks

My Pending Inquiries

Empty light blue bar

Search SL Applicant Entities

BEN	BEN Name	City	State	Entity Type	Action
000000	NAME	CITY	STATE	Library	ACTIONS

- ⚡ Create CBR FCC Form 470
- ⚡ Create CBR FCC Form 484 Part 2

Pilot FCC Form 470 Walkthrough: Participant Type

CBR FCC Form 470 - Cybersecurity Pilot Program

NAME (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/2/2025 11:42 AM EST

Basic Information

Service Requests

Technical Contact Information

Procurement Information

FCC Form 470 Review

Certifications & Signature

Where applicable, we've completed this section of the form based on information from your Participant entity's profile. If any of the non-editable information is incorrect, or you wish to change the information, please update your profile first by going to your entity record, and clicking Manage Organization from the Related Actions menu. If you do not have access to Manage Organization, please contact your Participant entity's account administrator or create a customer service case to request updates to your Participant entity's profile.

Participant Type and Recipients of Service

Participant Type: Library

Number of Eligible Entities based on FCC Form 484 Part 1 1

Recipients of Service

Billed Entity Name	Billed Entity Number
NAME	000000

[BACK](#) [DISCARD FORM](#)

[SAVE & SHARE](#) [SAVE & CONTINUE](#)

AGENCY NAME (BEN: 000000) - User Guide Demo - Form #CBR420250000

Last saved: 12/30/2024 1:41 PM EST

Basic Information

Service Requests

Technical Contact
Information

Procurement Information

FCC Form 470 Review

Certifications & Signature

Where applicable, we've completed this section of the form based on information from your Participant entity's profile. If any of the non-editable information is incorrect, or you wish to change the information, please update your profile first by going to your entity record, and clicking Manage Organization and/or Manage Organization Relationships from the Related Actions menu. If you do not have access to these Related Actions, please contact your applicant entity's account administrator or create a customer service case to request updates to your Participant entity's profile.

▼ Participant Type and Recipients of Service

Participant Type: Government Agency

Please select which state you are applying for. *

--Select One--

Please select the entities that will be represented in this Application. *

- All public schools/districts in the state
- All non-public schools in the state
- All libraries in the state

Check all that apply.

BACK

DISCARD FORM

SAVE & SHARE

SAVE & CONTINUE

Pilot FCC Form 470 Walkthrough: Equipment & Service Requests

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/25/2025 9:57 AM EST

Basic Information

Service Requests

Technical Contact Information

Procurement Information

FCC Form 470 Review

Certifications & Signature

Before completing the rest of the Cybersecurity Pilot Program FCC Form 470, please review the different types of Cybersecurity Equipment and Services contained in the Pilot Eligible Services List as listed below. You will use this form to request bids for eligible Cybersecurity Equipment and Services.

If you have questions or would like more information about how to complete the Cybersecurity Pilot Program FCC Form 470, please visit [our website](#).

Type(s) of Cybersecurity Equipment and Services

Advanced/Next-Generation Firewalls

Equipment, services, or a combination of equipment and services that limits access between networks including equipment and services that may include the following features, substantially similar features, or their equivalents:

Endpoint Protection

Equipment and services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user school- and library-owned end-user devices, including desktop computers, laptops, and mobile devices, against cyber threats and

Identity Protection and Authentication

Equipment, services, or a combination of equipment and services that implement safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system

Monitoring, Detection, and Response

Equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats including equipment and services that may include the

- Logging practices/event logging
- Network access control
- Offsite/Immutable back-ups
- Multi-Factor Authentication (MFA)/phishing-resistant MFA
- Patching
- Password spraying
- Privileged identity management
- Secure Access Service Edge (SASE)
- Secure-By-Design equipment and services
- Security Information and Event Management (SIEM)
- Security Updates
- Single sign-on (SSO)
- Trusted Platform Module (TPM) and products with TPM chips
- Web Content Controls
- Wireless access controllers
- Zero Trust Architecture

Security Operations Center (SOC) for around the clock (24/7/365) monitoring, detection, and response

- Threat hunting/Updates and threat intelligence
- Vulnerability management

BACK

DISCARD FORM

SAVE & SHARE

SAVE & CONTINUE

Basic Information

Service Requests

Technical Contact
Information

Procurement
Information

FCC Form 470 Review

Certifications &
Signature

Participants are required to include sufficient information about their cybersecurity needs to allow bidders to submit responsive bids for requested services/equipment including any disqualification factors, additional details about eligible locations that will be receiving these services, and other information about the services requested that would help bidders develop bids that are responsive to your needs. Participants should provide additional information for each of the specific categories of cybersecurity services and equipment they are seeking support for that includes, for example, quantity of services/equipment needed, the type/model of the network or existing equipment that needs to be supported, number of end user devices/users/locations that will need to be supported, software and/or licenses that will be needed, etc. In lieu of using the narrative box that will be available for each service/equipment request, participants may upload a request for proposals (RFP) document providing additional information regarding the cybersecurity services and equipment being sought instead of completing the narrative box. When completing the narrative box(es) or an RFP(s), participants may not request a particular manufacturer's name, brand, product, or service unless they also use the words "or equivalent" in their descriptions to ensure prospective bidders are not discouraged from submitting potentially more cost-effective bids that use different manufacturer names, brands, products, or services.

If you are using an RFP(s) for any of the Cybersecurity Equipment and Services that you are requesting bids for, start by uploading them first.

RFPs for Cybersecurity Equipment and Service Requests

Is there an RFP(s) for any of the Cybersecurity Equipment and Services that you are requesting bids for? Please upload any RFP(s) here.*

YES

NO

RFPs for Cybersecurity Equipment and Service Requests

Is there an RFP(s) for any of the Cybersecurity Equipment and Services that you are requesting bids for? Please upload any RFP(s) here.

YES ✓

NO

If a participant decides to seek bids using a Request for Proposal (RFP), the RFP should include, at a minimum (as applicable):

- **Project Overview** – Sufficient information about your Pilot project to enable prospective bidders to understand your needs, including a description of the equipment and services you plan to seek Pilot Program funding for and the scope of your proposed project;
- **Technical Requirements** – A description of the technical network and data requirements necessary for the equipment and services you plan to purchase with Pilot Program funding to be effective;
- **Disqualification Factors** – Any factors that will result in submitted bids being disqualified without consideration;
- **Location and Site Information** – The names and addresses of any sites or locations that prospective bidders should include in their bids, along with any site-specific information that can help bidders provide responsive bids;
- **Pilot Program FCC Forms 470 and RFPs Must be Vendor Neutral** – When completing the narrative box(es) or an RFP(s), participants may not request a particular manufacturer's name, brand, product, or service unless they also use the words "or equivalent" in their descriptions to ensure prospective bidders are not discouraged from

Please upload all RFPs for the Cybersecurity Equipment and Services that you are requesting bids for. ?

UPLOAD



Drop file here

You must upload your actual RFP document. Uploading a document with a hyperlink to another website, including bid management sites, is not sufficient and can lead to funding denial.

RFPs for Cybersecurity Equipment and Service Requests

Is there an RFP(s) for any of the Cybersecurity Equipment and Services that you are requesting bids for? Please upload any RFP(s) here.

YES ✓

NO

If a participant decides to seek bids using a Request for Proposal (RFP), the RFP should include, at a minimum (as applicable):

- **Project Overview** – Sufficient information about your Pilot project to enable prospective bidders to understand your needs, including a description of the equipment and services you plan to seek Pilot Program funding for and the scope of your proposed project;
- **Technical Requirements** – A description of the technical network and data requirements necessary for the equipment and services you plan to purchase with Pilot Program funding to be effective;
- **Disqualification Factors** – Any factors that will result in submitted bids being disqualified without consideration;
- **Location and Site Information** – The names and addresses of any sites or locations that prospective bidders should include in their bids, along with any site-specific information that can help bidders provide responsive bids;
- **Pilot Program FCC Forms 470 and RFPs Must be Vendor Neutral** – When completing the narrative box(es) or an RFP(s), participants may not request a particular manufacturer's name, brand, product, or service unless they also use the words "or equivalent" in their descriptions to ensure prospective bidders are not discouraged from

Please upload all RFPs for the Cybersecurity Equipment and Services that you are requesting bids for. ?



RFP_1

PDF – 31.24 KB

UPLOAD



Drop file here

You must upload your actual RFP document. Uploading a document with a hyperlink to another website, including bid management sites, is not sufficient and can lead to funding denial.

RFPs for Cybersecurity Equipment and Service Requests

Is there an RFP(s) for any of the Cybersecurity Equipment and Services that you are requesting bids for? Please upload any RFP(s) here.

YES ✓

NO

If a participant decides to seek bids using a Request for Proposal (RFP), the RFP should include, at a minimum (as applicable):

- **Project Overview** – Sufficient information about your Pilot project to enable prospective bidders to understand your needs, including a description of the equipment and services you plan to seek Pilot Program funding for and the scope of your proposed project;
- **Technical Requirements** – A description of the technical network and data requirements necessary for the equipment and services you plan to purchase with Pilot Program funding to be effective;
- **Disqualification Factors** – Any factors that will result in submitted bids being disqualified without consideration;
- **Location and Site Information** – The names and addresses of any sites or locations that prospective bidders should include in their bids, along with any site-specific information that can help bidders provide responsive bids;
- **Pilot Program FCC Forms 470 and RFPs Must be Vendor Neutral** – When completing the narrative box(es) or an RFP(s), participants may not request a particular manufacturer's name, brand, product, or service unless they also use the words "or equivalent" in their descriptions to ensure prospective bidders are not discouraged from

Please upload all RFPs for the Cybersecurity Equipment and Services that you are requesting bids for. ?



RFP_1

PDF – 31.24 KB



RFP_2

PDF – 31.24 KB

UPLOAD



Drop file here

You must upload your actual RFP document. Uploading a document with a hyperlink to another website, including bid management sites, is not sufficient and can lead to funding denial.

RFPs for Cybersecurity Equipment and Service Requests

Is there an RFP(s) for any of the Cybersecurity Equipment and Services that you are requesting bids for? Please upload any RFP(s) here.

YES ✓

NO

If a participant decides to seek bids using a Request for Proposal (RFP), the RFP should include, at a minimum (as applicable):

- **Project Overview** – Sufficient information about your Pilot project to enable prospective bidders to understand your needs, including a description of the equipment and services you plan to seek Pilot Program funding for and the scope of your proposed project;
- **Technical Requirements** – A description of the technical network and data requirements necessary for the equipment and services you plan to purchase with Pilot Program funding to be effective;
- **Disqualification Factors** – Any factors that will result in submitted bids being disqualified without consideration;
- **Location and Site Information** – The names and addresses of any sites or locations that prospective bidders should include in their bids, along with any site-specific information that can help bidders provide responsive bids;
- **Pilot Program FCC Forms 470 and RFPs Must be Vendor Neutral** – When completing the narrative box(es) or an RFP(s), participants may not request a particular manufacturer's name, brand, product, or service unless they also use the words "or equivalent" in their descriptions to ensure prospective bidders are not discouraged from

Please upload all RFPs for the Cybersecurity Equipment and Services that you are requesting bids for. ?



RFP_1

PDF – 31.24 KB



RFP_2

PDF – 31.24 KB

UPLOAD



Drop file here

You must upload your actual RFP document. Uploading a document with a hyperlink to another website, including bid management sites, is not sufficient and can lead to funding denial.

provide responsive bids;

- **Pilot Program FCC Forms 470 and RFPs Must be Vendor Neutral** – When completing the narrative box(es) or an RFP(s), participants may not request a particular manufacturer’s name, brand, product, or service unless they also use the words “or equivalent” in their descriptions to ensure prospective bidders are not discouraged from submitting potentially more cost-effective bids that use different manufacturer names, brands, products, or services;
- **Bid Acceptance Period and Requirements** – Participants must wait at least 28 days after posting their Pilot Program FCC Form(s) 470 and RFP(s) on USAC’s website before making any commitments with selected providers of services and/or equipment. The period during which bids will be accepted is the Bid Acceptance Period; and
- **Constructing a Bid Evaluation** – To evaluate the bids received, participants must construct a bid evaluation matrix. Participants may decide which criteria they wish to consider in their bid evaluations and the weight assigned to each criterion. The price of eligible equipment and services need not be the only factor considered. However, the price of the eligible equipment and services must be weighted more heavily than any other single factor in the bid evaluation.
- **Note:** The information contained in a Pilot participant’s RFP(s) must be consistent with the services/equipment contained in the Pilot Program FCC Form 470.

BACK

DISCARD FORM

SAVE & SHARE

SAVE & CONTINUE

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/25/2025 10:47 AM EST

Basic Information

Service Requests

Technical Contact
Information

Procurement
Information

FCC Form 470 Review

Certifications &
Signature

Please add, edit, and remove service requests using the buttons below.

If you have questions or would like more information about how to complete the Cybersecurity Pilot Program FCC Form 470, please visit [our website](#).

Cybersecurity Equipment and Service Requests

Equipment and Service Types	Service Request Nickname	# of Entities Served	Installation, Initial Configuration, and Training	Associated RFPs	Narrative
-----------------------------	--------------------------	----------------------	---	-----------------	-----------

There are currently no service requests. Please enter a service request below by clicking the "Add New Service Request" button.

****Reminder:** All eligible equipment and services and related costs, including maintenance and operation, licenses, software, must be competitively bid.**

*******If you have questions about the types of network specification and other details to include here, please call the Customer Service Center at (888) 203-8100.*******

ADD NEW SERVICE REQUEST

EDIT SERVICE REQUEST

REMOVE SERVICE REQUEST

Please select the options below that match the Cybersecurity Equipment and Services for which you are seeking bids.

If you have questions or would like more information about how to complete the Cybersecurity Pilot Program FCC Form 470, please visit [our website](#).

Add New Cybersecurity Equipment and Service Request

Select a type of cybersecurity equipment and services *

Service Request Nickname *

Number of entities served *

Are you also seeking installation, activation, initial configuration, and/or training for this/these services(s)? *

- Yes
 No

Please select the RFP(s) that apply to this service request *

- RFP_1
 RFP_2

Please select the options below that match the Cybersecurity Equipment and Services for which you are seeking bids.

If you have questions or would like more information about how to complete the Cybersecurity Pilot Program FCC Form 470, please visit [our website](#).

Add New Cybersecurity Equipment and Service Request

Select a type of cybersecurity equipment and services *

Select a type ▼

Select a type

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

Are you also seeking installation, activation, initial configuration, and/or training for this/these services(s)? *

- Yes
- No

Please select the RFP(s) that apply to this service request *

- RFP_1
- RFP_2

Select a type of cybersecurity equipment and services *

Advanced/Next-Generation Firewalls ▼

Service Request Nickname *

Demo 4/255

Number of entities served *

2

Are you also seeking installation, activation, initial configuration, and/or training for this/these services(s)? *

Yes
 No

Please select the RFP(s) that apply to this service request *

RFP_1
 RFP_2

Narrative *

Please use the Narrative box below to describe and provide additional information regarding the service/equipment that you are seeking support for.

When completing the narrative text box(es), you may not include a particular manufacturer's name, brand, product, or services unless you also use the words "or equivalent" in your description to ensure that prospective bidders are not discouraged from submitting potentially more cost-effective bids that use different manufacturer names, brands, products, or services. Participants are required to include sufficient information about their

Advanced/Next-Generation Firewalls ▼

Equipment, services, or a combination of equipment and services that limits access between networks including equipment and services that may include the following features, substantially similar features, or their equivalents:

- Advanced Threat Detection and Prevention
- AI/ML Threat Detection and Response
- Application Awareness & Control
- Cloud-Delivered Threat Intelligence
- Comprehensive Network Visibility Software-defined Firewalls
- Deep Packet Inspection (DPI)
- Distributed-denial-of-service (DDoS) protection
- Firewall as a Service (FWaaS)
- Integrated Intrusion Prevention Systems (IIPS)
- Internet of Things (IOT) Security
- Intrusion prevention/detection
- Malware Detection
- Network Segmentation
- Patch Management Systems
- Virtual Private Network (VPN)

Select a type of cybersecurity equipment and services *

Advanced/Next-Generation Firewalls ▼

Service Request Nickname *

Demo 4/255

Number of entities served *

2

Are you also seeking installation, activation, initial configuration, and/or training for this/these services(s)? *

- Yes
- No

Please select the RFP(s) that apply to this service request *

- RFP_1
- RFP_2

Narrative

Please use the Narrative box below to describe and provide additional information regarding the service/equipment that you are seeking support for.

When completing the narrative text box(es), you may not include a particular manufacturer's name, brand, product, or services unless you also use the words "or equivalent" in your description to ensure that prospective bidders are not discouraged from submitting potentially more cost-effective bids that use different manufacturer names, brands, products, or services. Participants are required to include sufficient information about their cybersecurity needs to allow bidders to submit responsive bids for the requested services and equipment, including any disqualification factors.

Advanced/Next-Generation Firewalls ▼

Equipment, services, or a combination of equipment and services that limits access between networks including equipment and services that may include the following features, substantially similar features, or their equivalents:

- Advanced Threat Detection and Prevention
- AI/ML Threat Detection and Response
- Application Awareness & Control
- Cloud-Delivered Threat Intelligence
- Comprehensive Network Visibility Software-defined Firewalls
- Deep Packet Inspection (DPI)
- Distributed-denial-of-service (DDoS) protection
- Firewall as a Service (FWaaS)
- Integrated Intrusion Prevention Systems (IIPS)
- Internet of Things (IOT) Security
- Intrusion prevention/detection
- Malware Detection
- Network Segmentation
- Patch Management Systems
- Virtual Private Network (VPN)

RFP_1

RFP_2

- Intrusion prevention/detection
- Malware Detection
- Network Segmentation
- Patch Management Systems
- Virtual Private Network (VPN)

Narrative

Please use the Narrative box below to describe and provide additional information regarding the service/equipment that you are seeking support for.

When completing the narrative text box(es), you may not include a particular manufacturer's name, brand, product, or services unless you also use the words "or equivalent" in your description to ensure that prospective bidders are not discouraged from submitting potentially more cost-effective bids that use different manufacturer names, brands, products, or services. Participants are required to include sufficient information about their cybersecurity needs to allow bidders to submit responsive bids for the requested services and equipment, including any disqualification factors, additional details about eligible locations that will be receiving these services, and other information about the services requested that would help bidders develop bids that are responsive to your needs. Participants should provide additional information for each of the specific categories of cybersecurity services and equipment they are seeking support for that includes, for example, the quantity of services/equipment needed, the type/model of the network equipment that needs to be supported, the number of end-user devices/users/locations that will need to be supported, and any software and/or licenses that will be needed.

0/5000

CANCEL

SAVE & CREATE ANOTHER REQUEST

SAVE REQUEST

Please add, edit, and remove service requests using the buttons below.

If you have questions or would like more information about how to complete the Cybersecurity Pilot Program FCC Form 470, please visit [our website](#).

Cybersecurity Equipment and Service Requests

	Equipment and Service Types	Service Request Nickname	# of Entities Served	Installation, Initial Configuration, and Training	Associated RFPs	Narrative
<input type="checkbox"/>	Advanced/Next-Generation Firewalls	Demo	2	Yes	RFP_1	
<input type="checkbox"/>	Endpoint Protection	Demo 2	4	Yes		Yes

****Reminder: All eligible equipment and services and related costs, including maintenance and operation, licenses, software, must be competitively bid.****

*****If you have questions about the types of network specification and other details to include here, please call the Customer Service Center at (888) 203-8100.*****

[ADD NEW SERVICE REQUEST](#)[EDIT SERVICE REQUEST](#)[REMOVE SERVICE REQUEST](#)[BACK](#)[DISCARD FORM](#)[SAVE & SHARE](#)[SAVE & CONTINUE](#)

Pilot FCC Form 470 Walkthrough: Certification

CBR FCC Form 470 - Cybersecurity Pilot Program

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/26/2025 6:04 PM EST

Basic Information

Service Requests

Technical Contact
Information

Procurement
Information

FCC Form 470 Review

Certifications &
Signature

CBR FCC Form 470 Draft version of the PDF generation is in progress and it may take a few minutes to complete. Please click 'Refresh' once or twice a minute to check if the PDF generation is complete. If you don't want to wait, click 'Resume Task Later' to close the current screen, and CBR will assign you a task to continue the PDF review and certification process.

RESUME TASK LATER

REFRESH

CBR FCC Form 470 - Cybersecurity Pilot Program

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/26/2025 6:07 PM EST

Basic Information

Service Requests

Technical Contact Information

Procurement Information

FCC Form 470 Review

Certifications & Signature

Review

Please download and carefully review this Cybersecurity Pilot Program FCC Form 470 before certifying.

Download Document Link

[USAC_CBR_FCC_FORM_470_APPLICATION_CBR420250101_DRAFT_1/26/2025 6:04 PM EST.pdf](#)

By checking this box, I certify that the information in the PDF document above is correct.

BACK

DISCARD FORM

SEND FOR CERTIFICATION

CONTINUE TO CERTIFICATION

CBR FCC Form 470 - Cybersecurity Pilot Program

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/26/2025 6:07 PM EST

Basic Information

Service Requests

Technical Contact
Information

Procurement
Information

FCC Form 470 Review

Certifications &
Signature

Review

Please download and carefully review this Cybersecurity Pilot Program FCC Form 470 before certifying.

Download Document Link

[USAC_CBR_FCC_FORM_470_APPLICATION_CBR420250101_DRAFT_1/26/2025 6:04 PM EST.pdf](#)

By checking this box, I certify that the information in the PDF document above is correct.

BACK

DISCARD FORM

SEND FOR CERTIFICATION

CONTINUE TO CERTIFICATION

CBR FCC Form 470 - Cybersecurity Pilot Program

EXAMPLE SCHOOL DISTRICT

Last saved: 1/26/2025 6:07 PM EST

Basic Information

Service Re

NO

YES

470 Review

Certifications &
Signature

CBR420250000

Review

Please download and carefully review this Cybersecurity Pilot Program FCC Form 470 before certifying.

Download Document Link

USAC_CBR_FCC_FORM_470_APPLICATION_CBR420250101_DRAFT_1/26/2025 6:04 PM EST.pdf

By checking this box, I certify that the information in the PDF document above is correct.

BACK

DISCARD FORM

SEND FOR CERTIFICATION

CONTINUE TO CERTIFICATION

Certifications

I certify under oath that:

- I am authorized to submit this application on behalf of the above-named participant in the Schools and Libraries Cybersecurity Pilot Program and that based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this form has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this participant can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733).
- In addition to the foregoing, this participant is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities.
- By signing this application, I certify that the information contained in this form is true, complete, and accurate. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil, or administrative penalties for fraud, false statements, false claims, or otherwise. (U.S. Code Title 18, sections §§ 1001, 286–287 and 1341 and Title 31, sections §§ 3729–3730 and 3801–3812).
- The schools meet the statutory definition of “elementary school” or “secondary school” as defined in 47 C.F.R § 54.2000, do not operate as for-profit businesses, and do not have endowments exceeding \$50,000,000.
- Libraries or library consortia eligible for assistance from a State library administrative agency under the Library Services and Technology Act of 1996 do not operate as for-profit businesses and, except for the limited case of Tribal college or university libraries, have budgets that are completely separate from any school (including, but not limited to, elementary and secondary schools, colleges, and universities).
- The services and/or equipment that the school, library, or consortium purchases at discounts will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by 47 C.F.R § 54.2003(b).
- The school(s) and/or library(ies) listed on this FCC Form 470 will not accept anything of value, other than services and equipment sought by means of this form, from the service provider, or any representatives or agent thereof or any consultant in connection with this request for services.

Certifications

I certify under oath that:

- I am authorized to submit this application on behalf of the above-named participant in the Schools and Libraries Cybersecurity Pilot Program and that based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this form has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this participant can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733).
- In addition to the foregoing, this participant is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities.
- By signing this application, I certify that the information contained in this form is true, complete, and accurate. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil, or administrative penalties for fraud, false statements, false claims, or otherwise. (U.S. Code Title 18, sections §§ 1001, 286–287 and 1341 and Title 31, sections §§ 3729–3730 and 3801–3812).
- The schools meet the statutory definition of “elementary school” or “secondary school” as defined in 47 C.F.R § 54.2000, do not operate as for-profit businesses, and do not have endowments exceeding \$50,000,000.
- Libraries or library consortia eligible for assistance from a State library administrative agency under the Library Services and Technology Act of 1996 do not operate as for-profit businesses and, except for the limited case of Tribal college or university libraries, have budgets that are completely separate from any school (including, but not limited to, elementary and secondary schools, colleges, and universities).
- The services and/or equipment that the school, library, or consortium purchases at discounts will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by 47 C.F.R § 54.2003(b).
- The school(s) and/or library(ies) listed on this FCC Form 470 will not accept anything of value, other than services and equipment sought by means of this form, from the service provider, or any representatives or agent thereof or any consultant in connection with this request for services.

- ✓ The school, library, or consortium acknowledges that support under the Schools and Libraries Cybersecurity Pilot Program is conditional upon the school(s) and/or library(ies) securing access, separately or through this program, to all of the resources necessary to effectively use the requested equipment and services. The school, library, or consortium recognizes that some of the aforementioned resources are not eligible for support and certifies that it has considered what financial resources should be available to cover these costs.
- ✓ I will retain required documents for a period of at least 10 years (or whatever retention period is required by the rules in effect at the time of this certification) after the later of the last day of the applicable Pilot Program year or the service delivery deadline for the associated funding request. I also certify that I will retain all documents necessary to demonstrate compliance with the statute (47 U.S.C. § 254) and Commission rules regarding the form for, receipt of, and delivery of equipment and services receiving Schools and Libraries Cybersecurity Pilot Program discounts. I acknowledge that I may be audited pursuant to participation in the Pilot Program.
- ✓ I certify that the equipment and services that the participant purchases at discounts will be used primarily for educational purposes and will not be sold, resold, or transferred in consideration for money or any other thing of value, except as permitted by the Commission's rules at 47 C.F.R. § 54.2003(b). Additionally, I certify that the entity or entities listed on this form will not accept anything of value or a promise of anything of value, other than services and equipment sought by means of this form, from the service provider, or any representative or agent thereof, or any consultant in connection with this request for services.
- ✓ I acknowledge that support under this Pilot Program is conditional upon the school(s) and/or library(ies) I represent securing access, separately or through this program, to all of the resources necessary to effectively use the requested equipment and services. I recognize that some of the aforementioned resources are not eligible for support. I certify that I have considered what financial resources should be available to cover these costs.
- ✓ I certify that I have reviewed all applicable Commission, state, Tribal, and local procurement/competitive bidding requirements and that the participant will comply with all applicable requirements.

Name of Authorized Person Name

Title or Position of Authorized Person

BACK

DISCARD FORM

CERTIFY

- ✓ All bids submitted for eligible equipment and services will be carefully considered, with price being the primary factor, and the bid selected will be for the most cost-effective service offering.
- ✓ The school, library, or consortium and the school(s) and/or library(ies) securing the equipment and services. The school, library, or consortium certifies that it has considered what financial resources should be available to cover these costs.
- ✓ I will retain required documents for a period of 3 years (after the later of the last date of use of the equipment and services or the date of this certification) after the later of the last date of use of the equipment and services. I also certify that I will retain all documents for the form for, receipt of, and delivery of the equipment and services that I may be audited pursuant to public law 104-409.
- ✓ I certify that the equipment and services that the participant purchases at discounts will be used primarily for educational purposes and will not be sold, resold, or transferred in consideration for money or any other thing of value, except as permitted by the Commission's rules at 47 C.F.R. § 54.2003(b). Additionally, I certify that the entity or entities listed on this form will not accept anything of value or a promise of anything of value, other than services and equipment sought by means of this form, from the service provider, or any representative or agent thereof, or any consultant in connection with this request for services.
- ✓ I acknowledge that support under this Pilot Program is conditional upon the school(s) and/or library(ies) I represent securing access, separately or through this program, to all of the resources necessary to effectively use the requested equipment and services. I recognize that some of the aforementioned resources are not eligible for support. I certify that I have considered what financial resources should be available to cover these costs.
- ✓ I certify that I have reviewed all applicable Commission, state, Tribal, and local procurement/competitive bidding requirements and that the participant will comply with all applicable requirements.

To electronically sign and certify this form, click "Yes" below. By doing so, you affirm that you (1) understand the certifications you are making on this page and (2) have the authority to make the certifications on behalf of the entity/ies listed in this form.

NO

YES

Name of Authorized Person

Title or Position of Authorized Person

Certification Confirmation - Cybersecurity Pilot Program

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR420250000

Last saved: 1/26/2025 6:21 PM EST

Basic Information

Service Requests

Technical Contact
Information

Procurement
Information

FCC Form 470 Review

Certifications &
Signature

Certification Date

Date Submitted 1/21/2025 1:31 PM EST

Date Signed 1/26/2025 6:21 PM EST

Authorized Person

Name Name

Title

Employer EXAMPLE SCHOOL DISTRICT

Address 123 SCHOOL STREET

Phone 555-555-5555

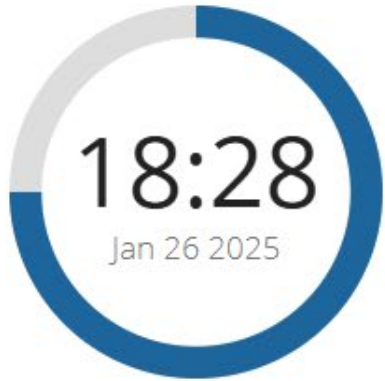
Email example@example.com

CLOSE

Pilot FCC Form 470 Walkthrough: Modifications



Good Evening, Welcome to the Cybersecurity Pilot Program!
NAME



[My Organization\(s\)](#)

[My Forms and Requests](#)

[My Pending Tasks](#)

[My Pending Inquiries](#)

Application Type

SEARCH

STATUS | Any



BEN	BEN Name	Application Number	Application Nickname	Status
000000	EXAMPLE SCHOOL DISTRICT	CBR420250000	Webinar Demo	Certified

Webinar Demo - CBR420250000

- Summary
- Certifications
- Documentation
- Related Actions

Application Information

Nickname	Webinar Demo	Created Date	12/30/2024 1:09 PM EST
Application Number	CBR420250000	Created By	Name
Funding Year	2025	Certified Date	1/26/2025 6:27 PM EST
Status	Certified	Certified By	Name
Allowable Contract Date	2/23/2025	Last Modified Date	1/26/2025 6:27 PM EST
		Last Modified By	Name

Billed Entity Information

Participant Name	EXAMPLE SCHOOL DISTRICT	Billed Entity Number	000000
Mailing Address	123 SCHOOL STREET	FCC Registration Number	000000000
Phone Number	555-555-5555	Email Address	example@example.com

Participant Type and Recipients of Service

Participant Type: School District

Number of Eligible Entities based on 0
FCC Form 484 Part 1

Webinar Demo - CBR420250000

Summary

Certifications

Documentation

Related Actions



Add an RFP Document

This function allows you to upload and associate an additional RFP to one or more Service Requests even if the RFP document did not exist at the time of certification.

Upload RFP

Changes to the CBR FCC Form 470, including uploading a new RFP document, may require applicants to restart the 28-day waiting period before selecting a service provider, signing a contract, or submitting and certifying an CBR FCC Form 471. Ministerial or clerical errors, such as updating contact information, do not require a reset of the 28-day waiting period. However, changes that materially affect the competitive bidding process, such as changing the services or equipment being requested, do require restarting the 28-day waiting period.

If you are requesting bids for additional equipment, services, or recipients of service not included on the original CBR FCC Form 470, you may need to file a new CBR FCC Form 470.

Please review the [USAC.org](https://www.usac.org) for additional guidance.

Does this new RFP constitute a substantial change to your CBR FCC Form 470? *

- Yes
- No

If you select yes, the 28-day waiting period will reset, and the Allowable Contract Date on your FCC Form 470 will be updated accordingly. If the new Allowable Contract Date prevents you from certifying the FCC Form 471 before the application window closes, you must request a waiver from the Commission after certifying the FCC Form 471.

Upload RFP

Changes to the CBR FCC Form 470, including uploading a new RFP document, may require applicants to restart the 28-day waiting period before selecting a service provider, signing a contract, or submitting and certifying an CBR FCC Form 471. Ministerial or clerical errors, such as updating contact information, do not require a reset of the 28-day waiting period. However, changes that materially affect the competitive bidding process, such as changing the services or equipment being requested, do require restarting the 28-day waiting period.

If you are requesting bids for additional equipment, services, or recipients of service not included on the original CBR FCC Form 470, you may need to file a new CBR FCC Form 470.

Please review the [USAC.org](https://www.usac.org) for additional guidance.

Does this new RFP constitute a substantial change to your CBR FCC Form 470? *


Yes

No

If you select yes, the 28-day waiting period will reset, and the Allowable Contract Date on your FCC Form 470 will be updated accordingly. If the new Allowable Contract Date prevents you from certifying the FCC Form 471 before the application window closes, you must request a waiver from the Commission after certifying the

accordingly. If the new Allowable Contract Date prevents you from certifying the FCC Form 471 before the application window closes, you must request a waiver from the Commission after certifying the FCC Form 471.

Uploading a new RFP document with substantial changes and not waiting the minimum 28 days may result in denial of funding.

Please add an RFP here *

UPLOAD



Drop file here

Service Request Grid


<input type="checkbox"/>	Equipment and Service Types	Service Request Nickname	# of Entities Served	Installation, Initial Configuration, and Training	Associated RFPs	Narrative
<input type="checkbox"/>	Advanced/Next-Generation Firewalls	Example 1	2	Yes	View RFP Documents	
<input type="checkbox"/>	Endpoint Protection	Example 2	2	Yes	View RFP Documents	Yes

CANCEL

SUBMIT

Accordingly, if the new Allowable Contract Date prevents you from certifying the FCC Form 471 before the application window closes, you must request a waiver from the Commission after certifying the FCC Form 471.

Uploading a new RFP document with substantial changes and not waiting the minimum 28 days may result in denial of funding.

Please add an RFP here *



NewRFP

PDF - 31.24 KB

Service Request Grid

<input type="checkbox"/>	Equipment and Service Types	Service Request Nickname	# of Entities Served	Installation, Initial Configuration, and Training	Associated RFPs	Narrative
<input type="checkbox"/>	Advanced/Next-Generation Firewalls	Example 1	2	Yes	View RFP Documents	
<input type="checkbox"/>	Endpoint Protection	Example 2	2	Yes	View RFP Documents	Yes

CANCEL

SUBMIT

accordingly. If the new Allowable Contract Date prevents you from certifying the FCC Form 471 before the application window closes, you must request a waiver from the Commission after certifying the FCC Form 471.

Uploading a new RFP document with substantial changes and not waiting the minimum 28 days may result in denial of funding.

Please add an RFP here *



NewRFP

PDF - 31.24 KB

Service Request Grid

<input type="checkbox"/>	Equipment and Service Types	Service Request Nickname	# of Entities Served	Installation, Initial Configuration, and Training	Associated RFPs	Narrative
<input checked="" type="checkbox"/>	Advanced/Next-Generation Firewalls	Example 1	2	Yes	View RFP Documents	
<input type="checkbox"/>	Endpoint Protection	Example 2	2	Yes	View RFP Documents	Yes

CANCEL

SUBMIT

Questions?

Pilot Program: Resources and Training

Pilot Program: Resources

- USAC will host [Pilot Program trainings](#)
- Sign up for Pilot Program [participant emails](#)
- [Pilot FCC Form 470](#) and [Pilot FCC Form 484 Part 2](#) User Guides
- [FCC Cybersecurity Pilot Program Website](#)
- [USAC Cybersecurity Pilot Program Website](#)

Pilot Program: Upcoming Trainings

- **Pilot FCC Form 484 Part 2 Webinar**
February 13 @ 3 p.m. E.T.
[Register](#)
- **Pilot FCC Form 471 Webinar**
March 18 @ 3 p.m. E.T.
[Register](#)

Thank You!





**Universal Service
Administrative Co.**