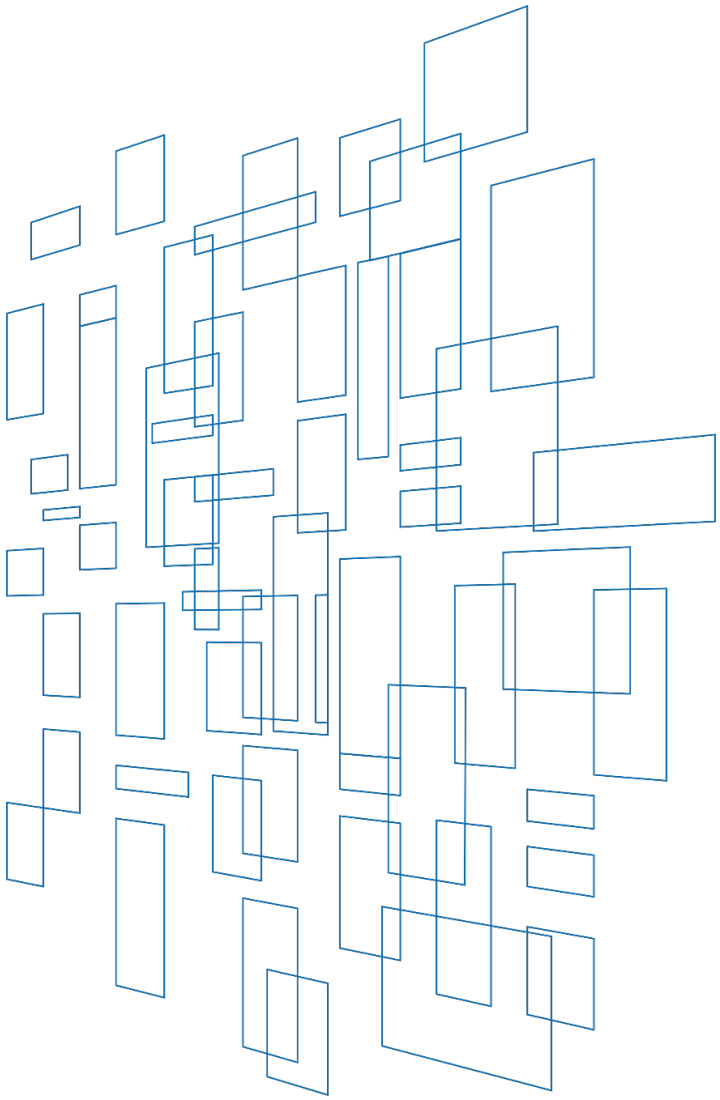


Schools and Libraries Cybersecurity Pilot Program Application User Guide

FCC Form 484 Part 1

Created/Revised September 2024

Contents

Pre-Application User Registration Requirements 5
One Portal 5
Logging in to One Portal for the First Time 5
EPC and Cybersecurity Pilot Program Account User Rights 6
User Accounts 6
User Roles and Permissions 6
Navigating to the CBR Dashboard 8
Starting the Application 9
Form Navigation 9
Progress Bar 9
Saving or Discarding the Form 10
Exiting the Form and Returning Later 10
Milestones and Sections 11
Required Fields 12
Pop-Up Confirmation Messages 12
FCC Form 484 Part 1 Form Overview 13
Start 13
Basic Information 13
Participant Selection – Members, Child Entities, and Individuals 14
Consortium Applicants – Selection of Members and Child Entities 14
School District and Library System Applicants – Selection of Child Entities 17
Individual School and Library Applicants 20
Proposed Plan 20
Project Details 24
Cybersecurity Application Pt. 1 26
Cybersecurity Application Pt. 2 27
Proposed Costs 31
Metrics 34
Supporting Documentation 35

Review 36
Review as a Partial Rights User 37
Review as a Full Rights User 37
Certifications 38
After Submitting 38
Resource Links 39
Free and Low-Cost Cybersecurity Resources 39
Education Department Free and Low-Cost Tools 39
CISA Free and Low-Cost Tools 39
Other Free and Low-Cost Tools 39
Cybersecurity Collaboration and Information-Sharing Groups 39
Form Assistance 40

This user guide is intended to help prospective applicants interested in the Federal Communication Commission's (FCC's) Schools and Libraries Cybersecurity Pilot Program (Pilot Program) understand the requirements and processes for submitting the FCC Form 484 Part 1. The FCC Form 484 Part 1 will be used to select Pilot Program participants. Part 2 of the FCC Form 484 will allow the FCC to gather the data needed from selected participants to help evaluate whether and how to use universal service funds to support the long-term cybersecurity needs of schools and libraries.

Before completing the FCC Form 484 Part 1, prospective applicants must ensure that they have established an account with the Universal Service Administrative Company (USAC) and provided general information about the schools and libraries (or consortia of schools and libraries) that will be seeking support. First, prospective applicants must establish an account and log into One Portal, USAC's single sign-on dashboard that allows applicants to access their online application(s). Next, prospective applicants must establish or access their account through the E-Rate Productivity Center (EPC), the account and application management portal for the E-Rate program.

After establishing or affirming their One Portal and EPC credentials, prospective applicants will be able to access the FCC Form 484 Part 1 and apply for the Pilot Program.

In Part 1 of the FCC Form 484 application, interested schools and libraries (and consortia comprised of schools and libraries) will provide basic information about their cybersecurity needs, experience, and plans to use the funding if selected for the Pilot Program. Unless an applicant is selected to participate in the Pilot Program, no further information will be required. This user guide focuses on the Part 1 requirements. Additional guidance will be provided to selected participants that are required to submit additional information through Part 2 of the FCC Form 484.

Help completing the FCC Form 484 and other forms associated with the Pilot Program will be available for applicants that need it. Directions to contact the USAC Customer Service Center are provided in the Form Assistance section of this user guide.

Pre-Application User Registration Requirements

Before completing the FCC Form 484 Part 1 to apply for the Pilot Program, prospective applicants must ensure that they have established an account with USAC in One Portal and the E-Rate Productivity Center (EPC).

One Portal

One Portal is USAC's single sign-on dashboard that allows applicants to access their online application(s). One Portal uses USAC's multi-factor authentication (MFA) system, which authenticates an online user during the login process by requiring the user to enter two or more separate pieces of information, such as a password known to the user and a code USAC generates and sends to the user by email or text. MFA helps safeguard access to data and applications and provides additional security consistent with federal information security guidelines.

To set up your credentials in One Portal, click the blue **Sign In** button at the top of any USAC page and follow the instructions.

If you already have an account in EPC, the account and application management portal for the E-Rate program, USAC has created an account for you in One Portal that uses your EPC contact email address as your username.

If you have a One Portal account but need to reset your password, click **Forgot Password**. For more information, watch the video How to Reset Your Password.

Logging in to One Portal for the First Time

The first time you sign into any USAC IT application, such as One Portal, the system will prompt you to set up MFA for your account. To do this:

1. Click the blue **Continue** button in the pop-up message.
2. On the login page, click the **Forgot Password** link.
3. Enter your **Username** (your EPC contact email address) and click **Reset via Email**.
4. When you receive the email, click the link to create a password. Your password must be at least eight characters long and include one lowercase letter, one uppercase letter, one number, and one special character.
5. Accept the system's terms of use and click **Sign In**.
6. On the next page, confirm the email associated with your account and click **Send Email**.
7. Check your email for a verification code.
8. Enter the code and click **Verify**.
9. The first time you log in to One Portal, you will need to accept the system terms and conditions.

After logging in, you will see USAC's One Portal dashboard if you have access to more than one application. On this page, you can access all of the Universal Service Fund (USF) applications associated with your login account. Navigate to EPC to view and complete Part 1 of the FCC Form 484.

EPC and Cybersecurity Pilot Program Account User Rights

User Accounts

In order to submit an FCC Form 484 Part 1 application, you must establish a user account in EPC, the account and application management portal used for the E-Rate, Emergency Connectivity Fund (ECF), and Schools and Libraries Cybersecurity Pilot Programs. To request an EPC user account, if your organization isn't registered in EPC, contact the USAC's Customer Service Center. If you need an EPC user account and your organization already uses EPC, request access from your Account Administrator.

To add users or reactivate a deactivated user as an Account Administrator, please see the EPC Account Administrator Guide.

User Roles and Permissions

Only your Account Administrator and other authorized persons that are given access rights, such as consultants and other employees, may submit and/or certify program forms on behalf of your organization. Permission rights are provided on a "form type" basis. Persons designated by the Account Administrator or other authorized person may have different rights for different FCC forms.

Available rights for the FCC Form 484 Part 1 include:

- **Full rights** – Users can fill out, edit, certify and submit the form.
- **Partial rights** – Users can fill out and edit the form, but cannot certify and submit the form. (Users with partial rights must choose to route the draft form to the organization's full-rights users for certification.)
- **View-only rights** – Users can view forms created by other users, but cannot fill out, edit, or certify and submit forms.
- **No Access** – Users cannot perform any form-related activity. A No Access user must request access to the form from the Account Administrator in order to obtain any of the access rights listed above.

Due to the sensitive nature of the data being collected in the Pilot Program, USAC has limited consultant access to applicants' FCC Forms 484. This means that, while the user management details contained in an applicant's E-Rate EPC Account Profile will be transferred to the Cybersecurity Pilot Program portal, consultants must be granted form-specific access by a school or library Account Administrator in order to access Pilot Program forms. There is a limit of three consultants permitted for each individual Pilot Program applicant account.

To designate permissions for Cybersecurity Pilot Program forms:

1. Log into EPC
2. From the landing page, click **Manage Users**
3. Check the checkbox for your entity and click **Manage User Permissions**
4. Select **CBR User Permissions**
5. Select the appropriate **CBR 484 Permission** for each user
6. Click **Submit**

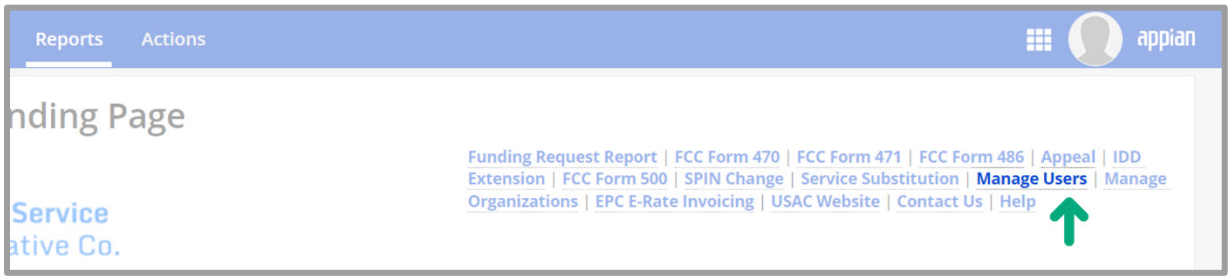


Figure 1 | From the EPC landing page, click Manage Users.

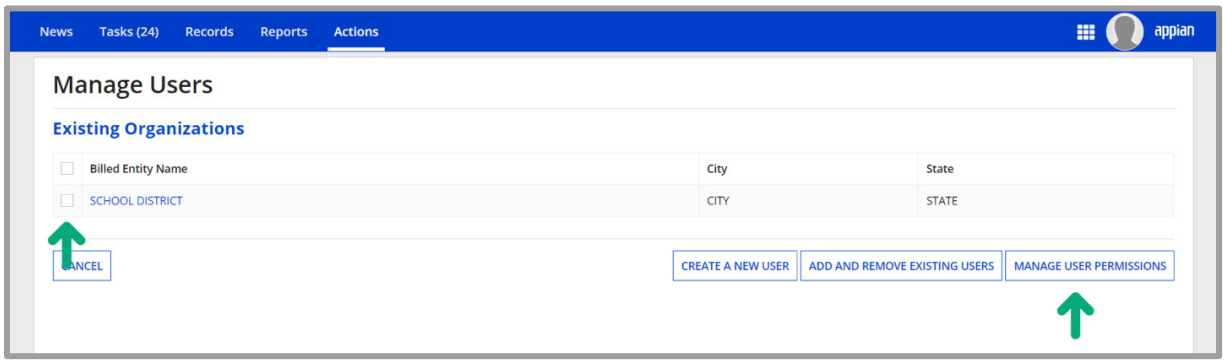


Figure 2 | On the Manage Users page, check the checkbox next to your entity and click Manage User Permissions.

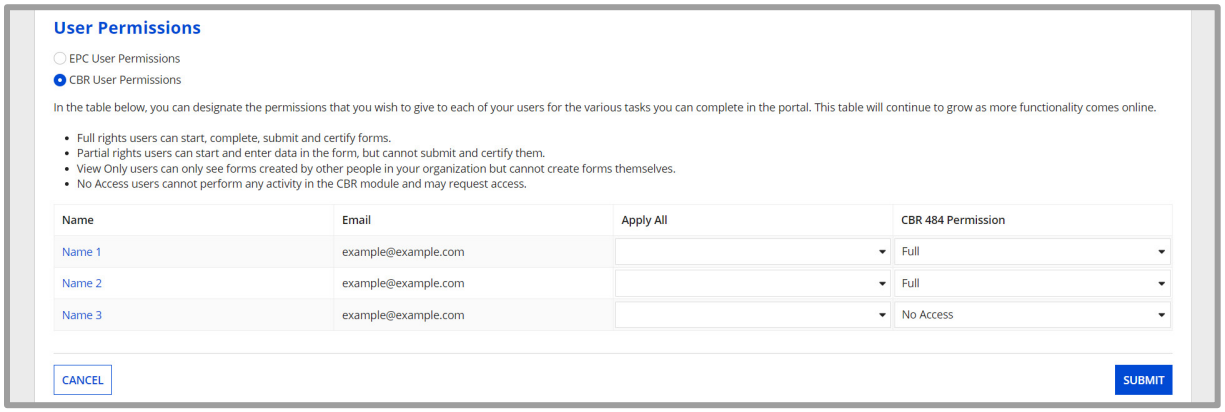


Figure 3 | On the Manage User Permissions page, select the permissions you wish to give to each user in the CBR 484 Permission column, then click Submit.

Navigating to the CBR Dashboard

The **CBR Dashboard** can be used to access the various forms needed to apply for and participate in the Pilot. To access the dashboard, log into EPC and click the navigation waffle to the left of your user image at the top of the screen. From the dropdown options, choose **Cybersecurity Pilot Program**.

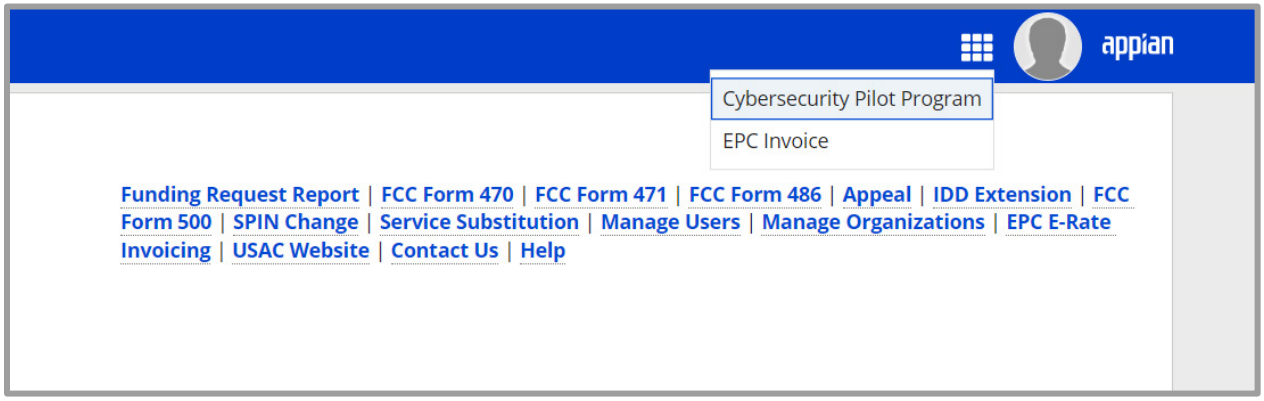


Figure 4 | From the EPC landing page, click the navigation waffle and choose Cybersecurity Pilot Program.

*Figure 5 | The four tabs on the CBR Dashboard are **My Organizations(s)**, **My Forms and Requests, My Pending Tasks,** and **My Pending Inquiries**.*

Starting the Application

In the **My Organization(s)** tab on the CBR Dashboard, click **File My FCC Form 484 Part 1** in the **Action** column.

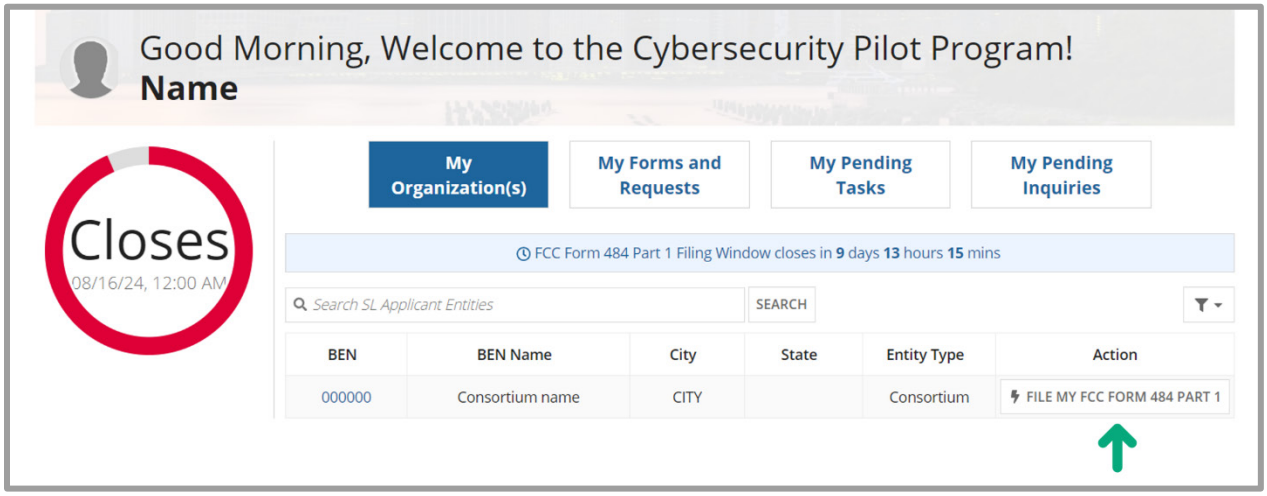


*Figure 6 | Click **File My FCC Form 484 Part 1** in the **Action** column on the CBR Dashboard to begin the application.*

Form Navigation

Progress Bar

The progress bar at the top of each form page helps you track your progress in completing the form. You can also use the progress bar to navigate between form pages.

*Figure 7 | In the progress bar, track progress and navigate between form pages: **Start**, **Basic Information**, **Participant Selection**, **Cybersecurity Plan**, **Supporting Documentation**, **Review**, and **Certifications**.*

Saving or Discarding the Form

The bottom of each page provides you with these options:

- **Back** – Go back to the previous page.
- **Save & Exit** – Save the form so it appears in the **My Pending Tasks** list on the CBR Dashboard with the most recent edits and exit the form.
- **Discard Form** – Discard the entire form. Note that when you confirm that you want to discard a form, the draft form will be deleted from USAC's system and cannot be retrieved.
- **Save and Continue** – Save the form so it appears in the **My Pending Tasks** list on the CBR Dashboard with the most recent edits and proceed to the next form page to continue entering information.

*Figure 8 | The options at the bottom of each page are: **Back**, **Save & Exit**, **Discard Form**, **Save & Continue**.*

Exiting the Form and Returning Later

Select **Save & Exit** to exit the form after saving changes. When you return, navigate to the CBR Dashboard and select the task name on the **My Pending Tasks** tab to resume where you left off completing the form. The prior information that you added is saved and you will still be able to edit it prior to submission of the form.

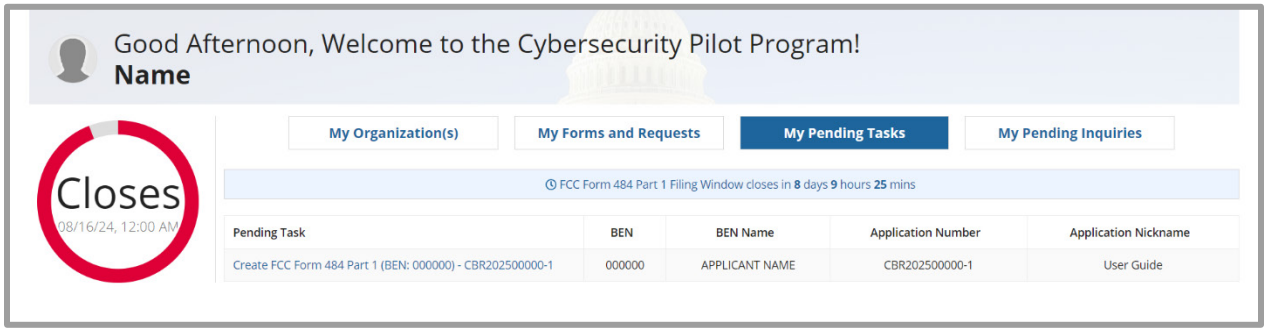


*Figure 9 | To resume editing, select the task name on the **My Pending Tasks** tab on the CBR Dashboard.*

Milestones and Sections

There are seven milestones that make up the form: **Start**, **Basic Information**, **Participant Selection**, **Cybersecurity Plan**, **Supporting Documentation**, **Review**, and **Certifications**. You can navigate between form milestones by using the progress bar or the **Save & Continue** and **Back** buttons at the bottom of the page.

Some milestones have multiple sections. For example, **Proposed Plan** is the first of six sections in the **Cybersecurity Plan** milestone. You can navigate between sections using the side navigation or the **Next** and **Previous** buttons at the bottom of the section.

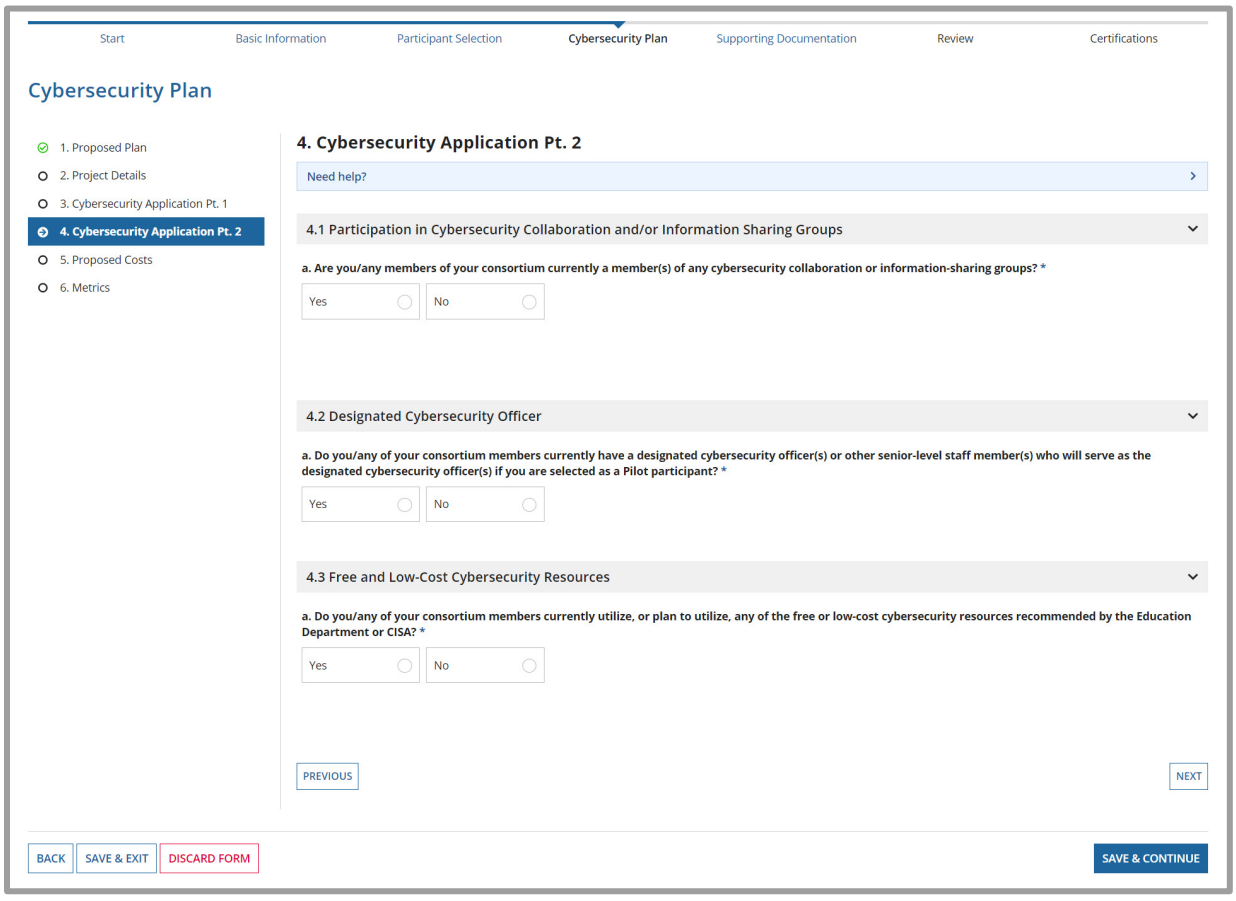


*Figure 10 | Navigate between milestones using the progress bar or the **Save & Continue** and **Back** buttons. Navigate between sections using the side navigation or **Next** and **Previous** buttons.*

Required Fields

Required fields are followed by a blue asterisk (*). You will be able to advance through the form if required fields are left blank. However, you will not be able to **certify** the form unless all required fields are completed.

Figure 11 | Required fields are followed by a blue asterisk.

Pop-Up Confirmation Messages

The system displays pop-up messages to verify that you want to take certain actions within the form. For example, if you do not wish to proceed, this pop-up message provides you with an opportunity to cancel a proposed action.

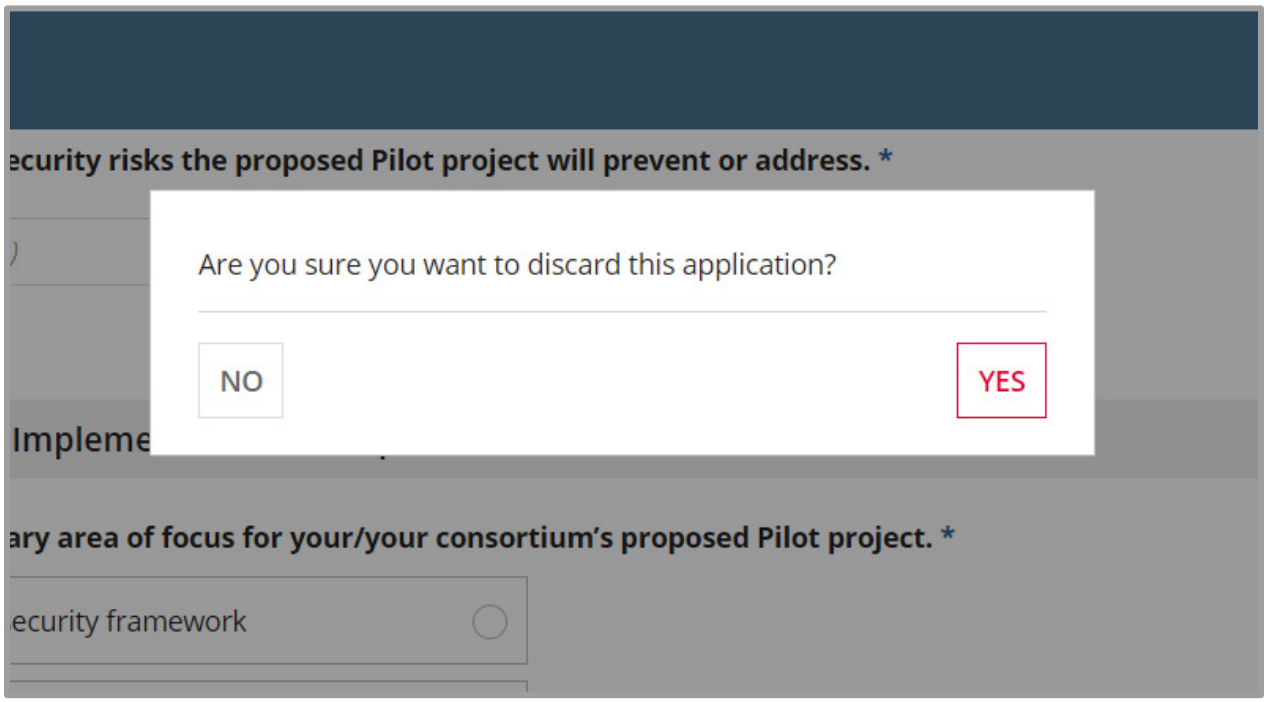


*Figure 12 | When you select **Discard Form,** a pop-up message asks you to confirm that you want to discard your application.*

FCC Form 484 Part 1 Form Overview

Applicants will use the FCC Form 484 Part 1 to provide a general level of cybersecurity information and answer questions about their proposed Pilot projects, including the eligible equipment and services they intend to seek funding for if selected for the Pilot Program – please be as **thorough** and **specific** as possible when completing the application.

Information that applicants submit about their about proposed project plans, including any equipment and/or services an applicant believes it may select, and information about estimated costs will be used by the FCC and USAC to ensure a diverse Pilot Program participant pool. The actual equipment and/or services a Pilot participant seeks reimbursement for and a participant's actual costs will be provided on the FCC Form 471, if an applicant is selected as a participant for the Pilot Program and after the participant has completed the competitive bidding process.

There are seven milestones that make up the FCC Form 484 Part 1: Start, Basic Information, Participant Selection, Cybersecurity Plan, Supporting Documentation, Review, and Certifications. Each milestone is discussed below.

Start

Review the FCC notice required by the Paperwork Reduction Act.

Basic Information

On the **Basic Information** page, identify the main contact person who will answer any questions about the information provided on the form. Contact information for each person is based on information in your entity's EPC Profile. Add contact information for the summer or holiday contact person, if it is different from the main contact person.

Where applicable, this section of the form will be auto-populated based on information from your entity's EPC Account Profile. If any of the non-editable information is incorrect or you wish to change the information, please update your entity's EPC Account Profile by selecting **Manage Organization** from the applicant landing page in EPC. If you do not have access to **Manage Organization**, please contact your entity's Account Administrator or create a customer service case to request updates to your entity's EPC Account Profile.

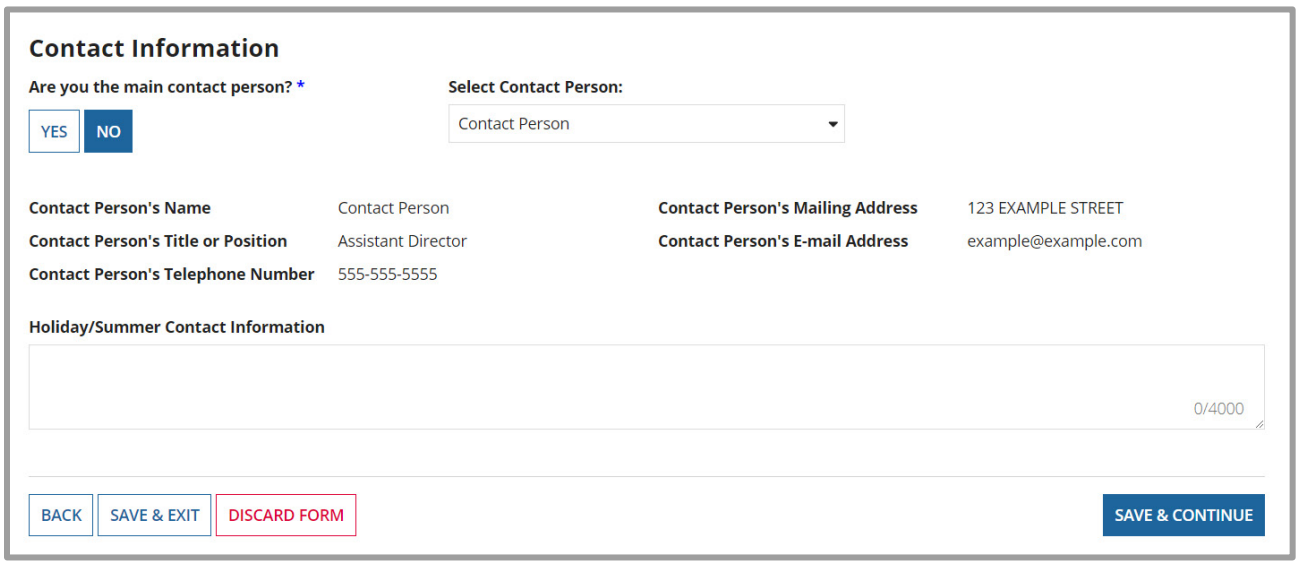


*Figure 13 | On the **Basic Information** page, select the person who will serve as the main contact for questions about the Cybersecurity Pilot Program. Contact information is pre-populated based on the applicant's EPC Account Profile.*

Participant Selection – Members, Child Entities, and Individuals

There are different versions of the **Participant Selection** page depending on who is submitting the application: consortia, school districts or library systems, or individual schools or libraries. Review the participant selection process for your entity type in the sections below.

Consortium Applicants – Selection of Members and Child Entities

A consortium (plural consortia or consortiums) is a group of school, school district, library, and/or library system entities that choose to submit an application and participate in the Pilot Program together. Pilot-eligible schools, school districts, libraries, and/or library systems may choose to form consortia in order to pool information and resources, as well as to aggregate demand in order to obtain lower prices and promote more efficient use of Pilot-eligible services and equipment.

In a consortium, schools, school districts, libraries, and library systems are known as consortium members. Some consortium members, like school districts and library systems, are made up of several individual entities that are referred to in a consortium application as child entities.

Applicants that wish to submit an application and participate in the Pilot Program as a consortium will need to select the specific members that will be included in the consortium application, as well as the members' specific child entities that will be included in the application. The members and child entities to be included in a consortium application should be identified on the form's **Participant Selection** page, along with the entity that will serve as the consortium lead.

For consortia, the member selection page will show a pre-populated list of members that you may wish to include in a consortium application. See Adding Members or Child Entities if you need to add new members that are not part of an existing consortium.

On the member selection page, you may choose whether you would like to add all of the members on the list to your consortium application or only specific members. If you would like to add all the members on the list to the consortium application, answer **Yes** to the question "Will every member in this consortium be part of your application to participate in the Cybersecurity Pilot Program?" Then click **Next**.

If you would like to add only specific members to the consortium application:

1. Answer **No** to the question "Will every member in this consortium be part of your application to participate in the Cybersecurity Pilot Program?"
2. In the **All Members** list, check the checkbox next to each member you wish to include in your consortium application. Ten available members are displayed on each page. Use the left and right arrows at the bottom of the list to move between pages and add the members you wish to include in your consortium application.
3. Once all members have been selected, click **Add**. Checked entities will be moved to the **Selected Members** list.
    - If you need to remove an entity from the selected entities list, check the checkbox in that row and click **Remove**.
4. Click **Next**.

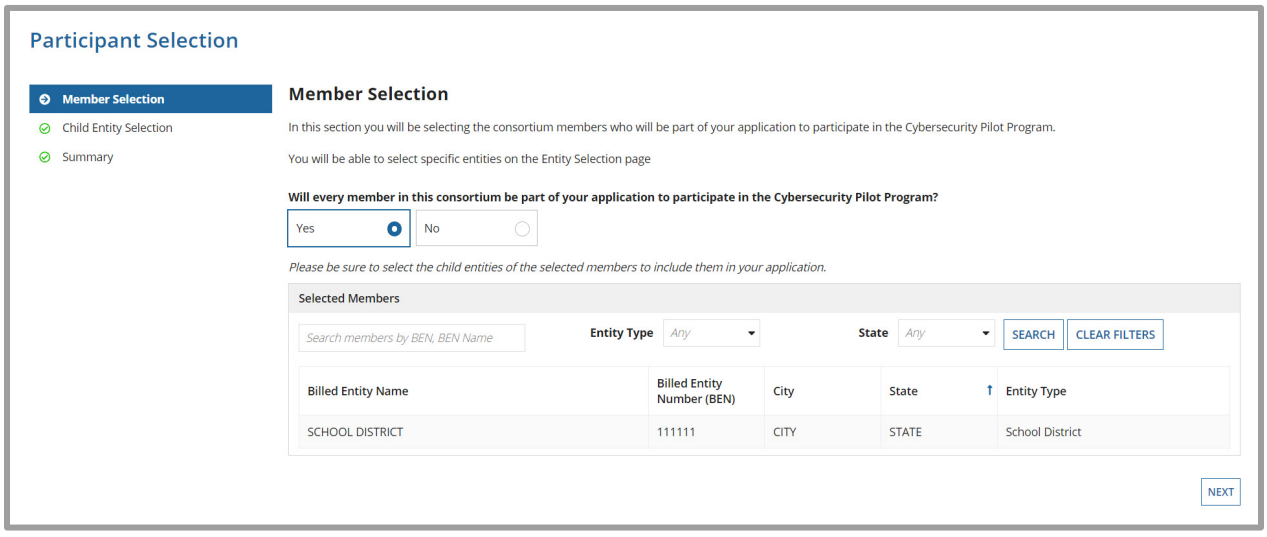


Figure 14 | Selecting members. Select the members to be included in your consortium application.

If any of the consortium members you select have child entities, you will need to select the child entities you wish to include in the consortium application on the **Child Entity Selection** page. You have the option to add all the child entities or add specific child entities. The steps to select child entities mirror the steps to select consortium members. You may filter the pre-populated child entities list by entity type (schools and libraries) to aid in your selection.

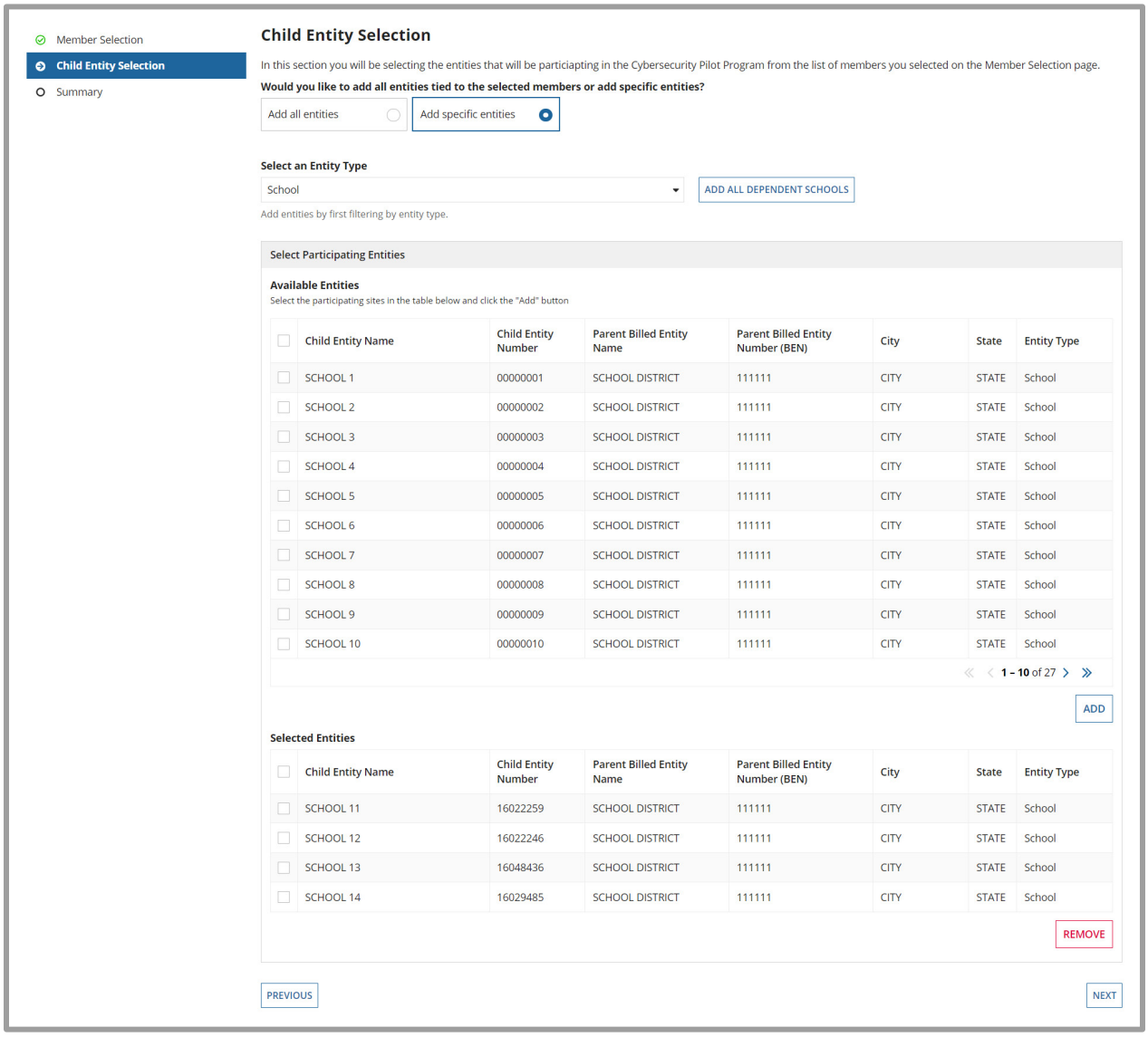


Figure 15 | Selecting child entities. Choose the child entities of selected consortium members that you wish to include in the consortium application.

Once you reach the **Summary** page, review the members and child entities you have selected for your consortium application. You may search the list of members and child entities included in the application (Participating Entities) by their Billed Entity Number (BEN) or name to confirm your selections. You may also click any column heading to sort by that column to confirm the entities that will participate in the Pilot.

Choose the consortium lead. The default consortium lead for the application is the entity that initiates the application in the Cybersecurity Pilot Program portal. To change the entity that is listed as the consortium lead, click on the **Lead Site Name** dropdown list and choose the entity that is to serve as the consortium lead.

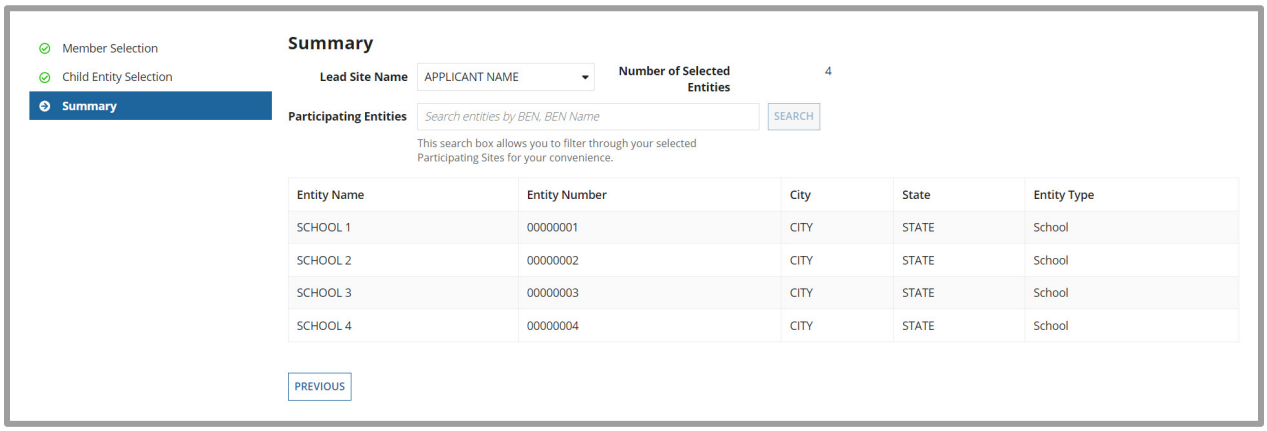


Figure 16 | Confirming selection of members and child entities included in consortium. On the Summary page, review your selected members and child entities and choose a consortium lead.

School District and Library System Applicants – Selection of Child Entities

School districts and library systems may apply for the Pilot Program by including all of the schools that make up a school district or all of the libraries that make up a library system. In the alternative, a school district or a library system may include a specific subset of its schools or libraries in its application. The individual schools that make up a school district and libraries that make up a library system are referred to as “child entities” on the Pilot Program application.

To apply to participate in the Cybersecurity Pilot Program as a school district or library system, you will need to select the child entities associated with the school district or library system that will be a part of the Pilot Program application. The **Child Entity Selection** page will show a pre-populated list of child entities that you may wish to include in an application. See Adding Members or Child Entities if you need to establish relationships with new child entities that are not already associated with your school district or library system in EPC.

Indicate whether you would like to include all of the child entities associated with your school district or library system on your application or whether you’d like to include only a specific subset of the child entities.

To add all associated child entities, click **add all entities**, then **Next**.

To add specific child entities:

1. Click **Add specific entities.**
2. In the **Available entities** list, check the checkbox next to each child entity that you would like to include in your application. Ten available child entities are displayed on each page. Use the left and right arrows at the bottom of the list to move between pages.
3. Once all child entities are selected, click **Add**. Checked entities move to the **Selected entities** list.
    - If you need to remove a child entity from the list of selected entities, check the checkbox in that row and click **Remove**.
4. Click **Next**.

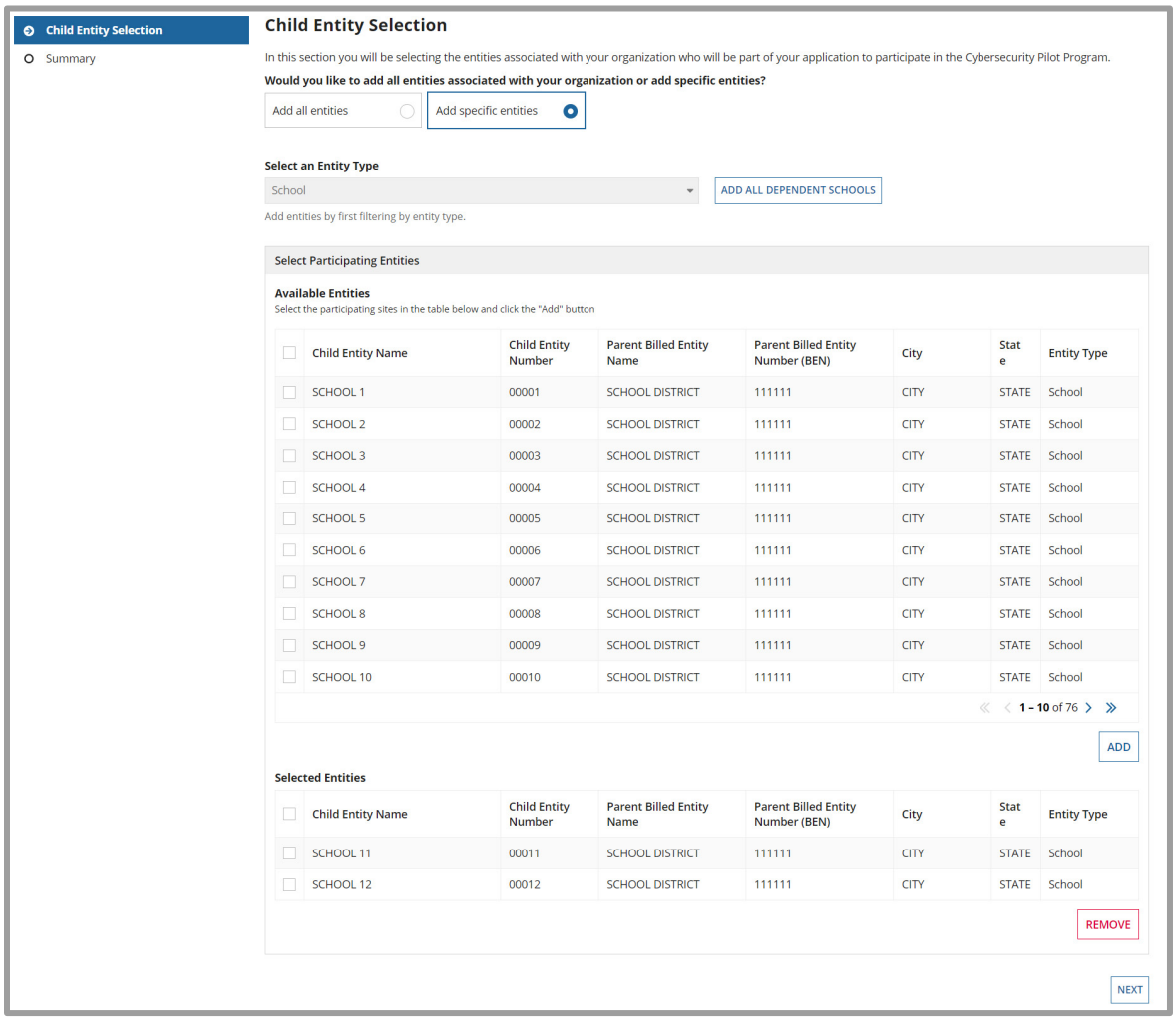


Figure 17 | Child entity selection for school districts and library systems. You will choose which child entities you want to include in your application. You may include all child entities or add specific child entities.

Once you reach the **Summary** page, review the child entities you have selected for your application. You may search the list of child entities by BEN or name to confirm your selections. You may also click any column heading to sort by that column to confirm the child entities that will you will include in your Pilot application.

The lead site for the application is the school district or library system that initiates the application in the Cybersecurity Pilot Program portal. School districts and library systems cannot change the lead site.

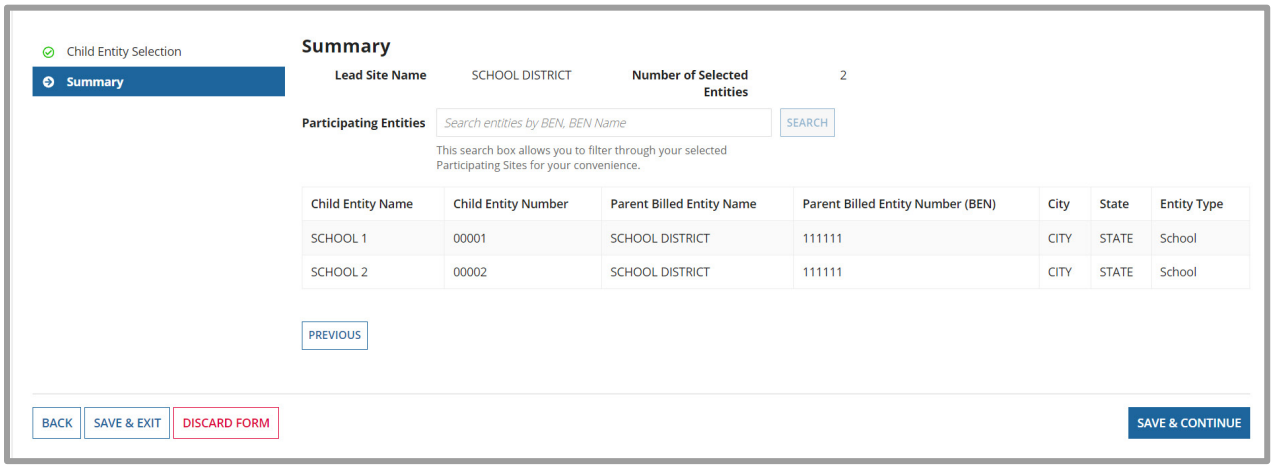


*Figure 18 | Confirming child entity selection for school districts and library systems. On the **Summary** page, review the selected child entities and choose a lead site.*

Adding Members or Child Entities – Consortia/School Districts and Library Systems

Existing relationships between consortia, school districts, and library systems, and their members and child entities are pulled into the Pilot Program forms from EPC. If you need to update the relationships between your school district, library system, or consortium and its members or child entities, you can do so in EPC.

If you are an Account Administrator, choose **Manage Organization Relationships** in the related actions menu from your applicant's entity record to add members or child entities to a school district, library system, or consortium. If you don't have access to **Manage Organization Relationships**, please contact your entity's Account Administrator.

Add any new members or child entities at least 24 hours before beginning your FCC Form 484 Part 1 to ensure time for the updated data to be included in EPC.

Individual School and Library Applicants

A school or library may apply to participate in the Pilot Program individually, as a single entity. As an individual school or library, your school or library is the only entity included in your application and is automatically set as the lead site for the application. Click **Save & Continue** to advance to the next form section.

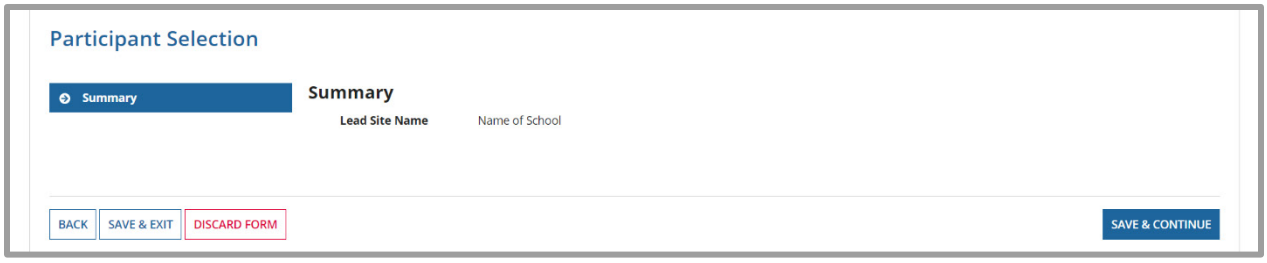


Figure 19 | Individual school or library selection. Your school or library is the only entity listed on the application.

Proposed Plan

To be considered for the Pilot Program, an applicant must include a plan that presents a clear strategy for addressing the cybersecurity needs of its K-12 school(s) and/or library(ies) and addresses how the project will accomplish the applicant's cybersecurity objectives. These plans should be tailored to the unique circumstances of each applicant.

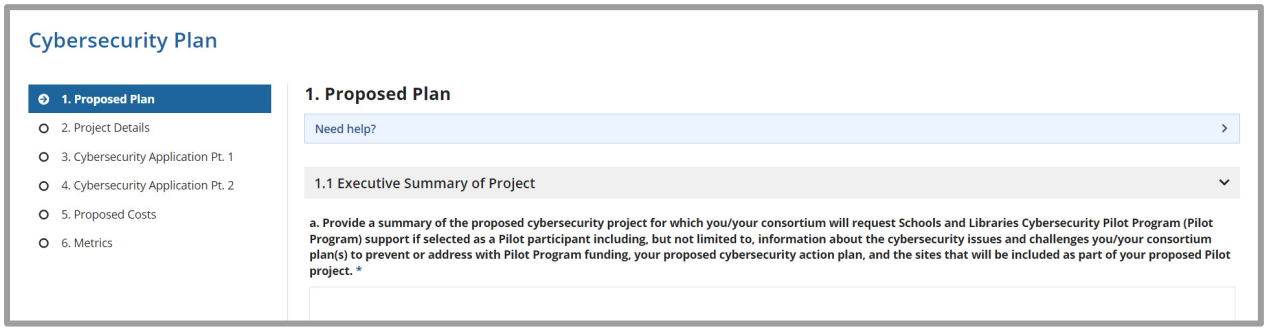


Figure 20 | Cybersecurity Plan - Proposed Plan.

Answering for a Consortium

If you are completing the first part of the Pilot Program application for a consortium, note that some questions in the Cybersecurity Plan milestone refer to **any** members of your consortium while others refer to **all** the members of your consortium. For example, you should answer yes to question 3.3 if **any** member of your consortium experienced a cybersecurity threat or attack in the last year. You should answer yes to question 6.1 only if **all** the members of your consortium are prepared to share the data and metrics they collect.

1.1 Executive Summary of Project

a. Provide a summary of the proposed cybersecurity project for which you/your consortium will request Schools and Libraries Cybersecurity Pilot Program (Pilot Program) support if selected as a Pilot participant including, but not limited to, information about the cybersecurity issues and challenges you/your consortium plan(s) to prevent or address with Pilot Program funding, your proposed cybersecurity action plan, and the sites that will be included as part of your proposed Pilot project. *5000-character limit; additional materials may be uploaded as needed*

Question Numbering

Parts of each question are given letters, beginning with a. You will see some questions with a part **a.** but no part **b.**, either because they have only one part or because additional parts will be included in Part 2 of the FCC Form 484 for selected participants.

1.2 Description of How Project Funding Will be Used

a. Select the equipment and services for which you/your consortium propose(s) to use Pilot funding. Select all that apply.
   - ☐ Advanced/Next-Generation Firewalls or similar
   - ☐ Endpoint Protection or similar
   - ☐ Identity Protection and Authentication or similar
   - ☐ Monitoring, Detection and Response or similar

b. Describe how the proposed Pilot project would use Pilot funding to protect the broadband network(s) and data of you/your consortium members and address your cybersecurity concerns, including, but not limited to, a discussion of the types of equipment and services you/your consortium plan(s) to purchase and how you/your consortium plan(s) to use the equipment and services to protect your broadband network(s) and data and manage and address cybersecurity risks. *5000-character limit; additional materials may be uploaded as needed*

Text Responses

Questions 1.1 and 1.2.b allow a text response of up to 5000 characters. Applicants can upload additional information as necessary in the **Supporting Documentation** form milestone.

1.3 Cybersecurity Risks Proposed Pilot Project will Prevent or Address

a. Select the cybersecurity risks the proposed Pilot project will prevent or address. Select all that apply.
   - ☐ Malware or similar
   - ☐ Viruses or similar
   - ☐ Spam or similar
   - ☐ Ransomware or similar
   - ☐ Distributed Denial-of-Service Attacks or similar
   - ☐ Insider/Privilege Misuse or similar
   - ☐ Email and Web Security Threats (e.g., phishing, password spraying, credential stuffing, etc.) or similar
   - ☐ Cloud Application Threats or similar
   - ☐ Network Threats, and Data Compromise and/or Loss or similar
   - ☐ None of the Above

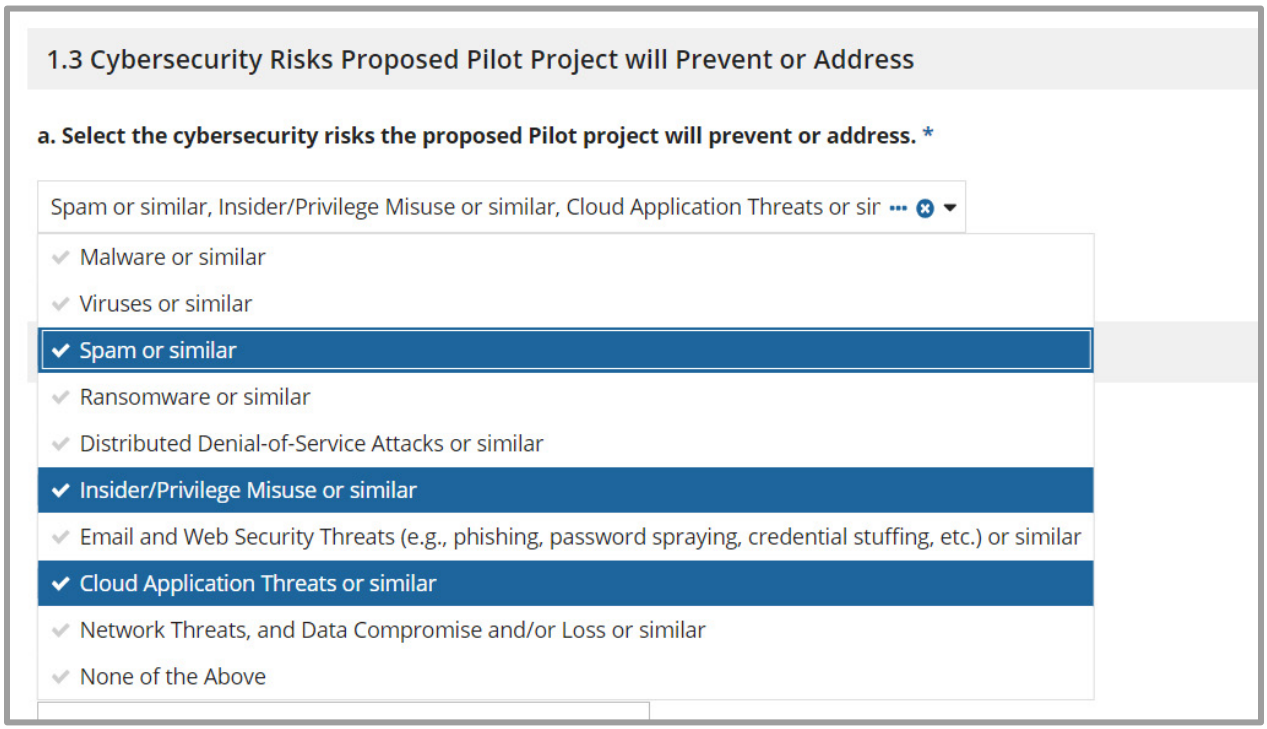


Figure 21 | Question 1.3.a. In this multiselect dropdown field, select the cybersecurity risks the proposed Pilot project will prevent or address.

Multiselect Dropdown Fields

Selected items are highlighted in blue and appear in the top row. Hover over the blue ellipsis in the top row to display all of the items you have selected for a particular question. Click the blue x to clear all selected items.

If you click **None of the Above**, all other items will be deselected.

1.4 Pilot Project Implementation and Operation

a. Identify the primary area of focus for your/your consortium's proposed Pilot project. Select one.

- ○ Create initial cybersecurity framework
- ○ Augment existing cybersecurity framework
- ○ Protect network(s) and data
- ○ Address past cybersecurity incident(s)/issue(s)
- ○ Address current cybersecurity incident(s)/issue(s)

1.5 Goals and Objectives

a. Select the goals and objectives for your/your consortium's proposed Pilot project. Select all that apply.

- ☐ Develop/implement/improve security and protection of E-Rate-funded broadband network(s)
- ☐ Develop/implement/improve network and data monitoring
- ☐ Develop/implement/improve incident detection and response
- ☐ Develop/implement/improve vulnerability scanning and patch management
- ☐ Develop/implement/improve protective controls
- ☐ Develop/implement/improve network segmentation
- ☐ Develop/implement/improve user access control
- ☐ Develop/implement/improve password management policies
- ☐ Develop/implement/improve IT security governance
- ☐ Obtain/supplement the cost of third-party cybersecurity management assistance

Moving Between Pages

When you use the next button to move to the next section of the **Cybersecurity Plan** milestone, you will land at the bottom of the page. Scroll to the top to make sure you have answered all questions.

Project Details

Schools and libraries will be required to answer a series of yes/no and multi-select questions to provide additional information about the cybersecurity project that they seek to implement if selected for the Pilot Program. Some of the questions are considered conditional, in that they will be hidden or displayed based on your answers to previous questions.

Conditional Questions

In this user guide, conditional questions appear with an "If" statement and a gray sidebar.

Conditional questions may load slowly. To avoid inadvertently skipping questions, re-check each section of your application for unanswered questions before moving on to the next page.

2.1 Recommended Cybersecurity Best Practices

a. Have you/any of your consortium members implemented recommended best practices from one or more cybersecurity organizations? Answer **Yes** or **No**.
Examples include the U.S. Department of Education, Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), a state Cybersecurity organization, or other entity

b. Do you/Does your consortium plan to implement recommended best practices from any cybersecurity organizations as part of your proposed Pilot project? Answer **Yes** or **No**.
Examples include the U.S. Department of Education, Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), a state Cybersecurity organization, or other entity

Recommended Cybersecurity Best Practices

Identify whether you have either implemented or plan to implement any recommended cybersecurity best practices. If you are participating as a consortium, you should answer yes if any of your members have either implemented or plan to implement best practices. Information regarding best practices can be found in the Resources section at the end of this user guide.

2.2 Ability of Proposed Pilot to be Self-sustaining

a. Will your/your consortium's proposed Pilot project be self-sustaining once the Pilot Program ends? Answer **Yes** or **No**.

> **If yes:**
> How will it remain self-sustaining? Select all that apply.
>
> ☐ With federal funding
> ☐ With state funding
> ☐ With local funding
> ☐ With Tribal funding
> ☐ With other funding, please specify
> **If other**: Please specify your source(s) of funding

Ability to be Self-Sustaining

A project is considered "self-sustaining" if it can remain operational without additional Pilot Program funds.

2.3 Network Equipment, Hardware, and Software Services

a. Using the Pilot Eligible Services List, select the cybersecurity equipment and services you/your consortium plan(s) to request as part of your proposed Pilot project. Select all that apply from each category.
Refer to Pilot Eligible Services List for answer options

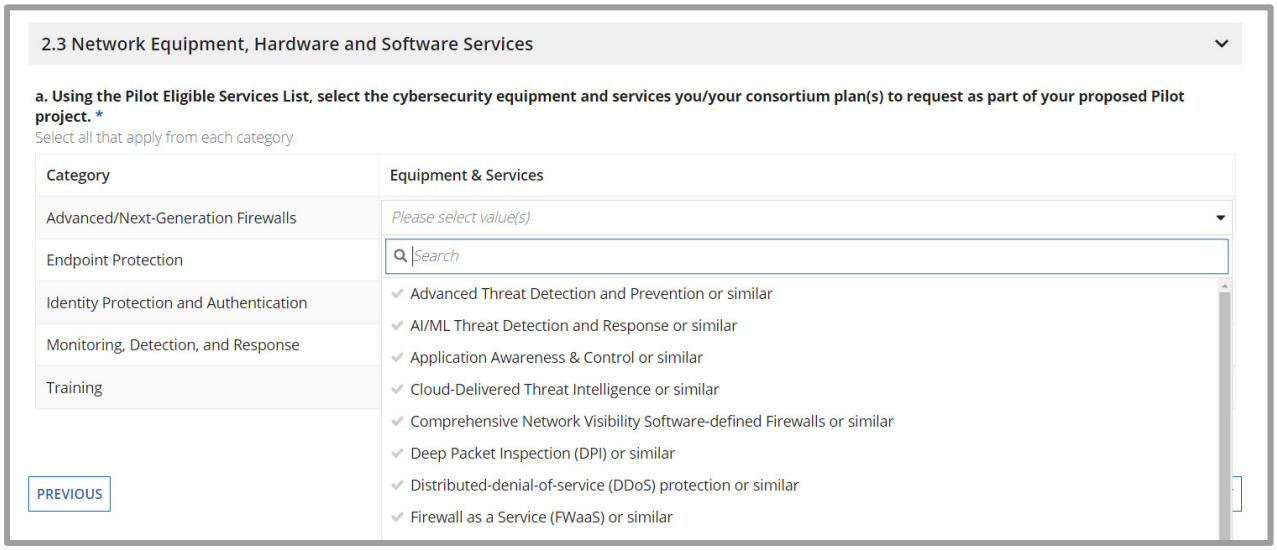


Figure 22 | Question 2.3.a. Select the cybersecurity equipment and services you plan to request from this group of multiselect dropdowns.

Multiselect Dropdown Groups

Multiselect Dropdown Groups are considered complete if at least one answer is selected. For example, Question 2.3.a is considered complete if you select at least one option from the five available categories (Advanced/Next-Generation Firewalls; Endpoint Protection; Identity Protection and Authentication; Monitoring, Detection, and Response; and Training). You do not need to select options in every category for the question to be considered complete.

Cybersecurity Application Pt. 1

Schools and libraries will be required to answer a series of yes/no questions to provide additional information about their cybersecurity experience, current resources, history of cybersecurity incidents and implementation of federal cybersecurity recommendations. Some of the questions are considered conditional, in that they will be hidden or displayed based on your answers to previous questions.

3.1 Previous Cybersecurity Experience

a. Do you/Does any member of your consortium have previous experience implementing cybersecurity protections/measures? Answer **Yes** or **No**.

> **If yes:**
> Select those protections/measures from the list of services/equipment below.
> *Refer to the Pilot Eligible Services List for more detail on the answer options.*
> On average, how many years of prior experience with the protections/measures do you/the members of your consortium have? (For consortia, answer this question using an average of all your consortium members.) Select **Less than a year**, **1 to 3 years**, **3 to 5 years**, or **More than 5 years**.

3.2 Current Cybersecurity Resources

a. Do you/Does any member of your consortium currently receive, or expect to receive, cybersecurity funding from any other federal, state, local, Tribal, or other cybersecurity program or source? Answer **Yes** or **No**.

> **If yes:**
> From which sources do you/your consortium members receive or expect to receive cybersecurity funding?
> Select all that apply: **Federal**, **State**, **Local**, **Tribal**, or **Other (please specify)**

3.3 Cyber Incidents

a. Have you/ Has any member of your consortium experienced a cybersecurity incident (e.g., a cybersecurity threat or attack) in the last year? Answer **Yes** or **No**.

3.4 Implementation of Department of Education or CISA Cybersecurity Recommendations

a. Have you/Has any member of your consortium implemented, or begun implementing, any of the U.S. Department of Education (Education Department) or Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) K-12 cybersecurity recommendations? Answer **Yes** or **No**.

Recommendations, Best Practices, and Resources

As used in Question 3.4, **recommendations** means any cybersecurity guidance provided by the Education Department or CISA, not just guidance pertaining specifically to K-12 schools and libraries. This is different from the **recommended best practices** referenced in question 2.1 of the application and discussed earlier in this user guide. It is also different from the **free and low-cost resources** referenced in question 4.1 of the application and discussed below.

Cybersecurity Application Pt. 2

Schools and libraries will be required to answer a series of multi-select questions to provide additional information about any collaboration or information-sharing groups they participate in, whether they currently have a cybersecurity officer and what free and low-cost resources that they currently utilize. The questions are considered conditional, in that they will be hidden or displayed based on your answers to previous questions.

Cybersecurity Application Pt. 1 and Cybersecurity Application Pt. 2

The questions that make up the **Cybersecurity Application** sections of the **Cybersecurity Plan** milestone are contained in the first part of the FCC Form 484 that is completed by Pilot Program applicants and are divided into two subsections, titled **Cybersecurity Application Pt. 1** and **Cybersecurity Application Pt. 2.**

Note that these subsections are not to be confused with the first and second parts of the of the application form itself, which are referred to as the FCC Form 484 Part 1 and FCC Form 484 Part 2.

4.1 Participation in Cybersecurity Collaboration and/or Information Sharing Groups

a. Are you/any members of your consortium currently a member(s) of any cybersecurity collaboration or information-sharing groups?

> **If yes:**
> Select the specific groups to which you/your consortium members currently belong. Select all that apply.
> *Refer to the Resources section at the end of this user guide for more detail on the answer options.*
>
> - ☐ MS-ISAC
> - ☐ K12 SIX
> - ☐ State and/or regional agency
> - ☐ State and/or regional school safety centers
> - ☐ State cybersecurity organizations
> - ☐ Cybersecurity industry association and/or organizations
> - ☐ Fusion centers
>
> What is the earliest date you/any of your consortium members joined any of the groups? *Enter a date or click the calendar button to choose a date from the calendar.*

> **If no:**
> Do you/any of the members of your consortium plan to join any cybersecurity collaboration or information-sharing groups? Select **Yes** or **No**.
>
> > **If yes:**
> > Select the specific group(s) you/your consortium members plan to join. Select all that apply.
> >
> > - ☐ MS-ISAC
> > - ☐ K12 SIX
> > - ☐ State and/or regional agency
> > - ☐ State and/or regional school safety centers
> > - ☐ State cybersecurity organizations
> > - ☐ Cybersecurity industry association and/or organizations
> > - ☐ Fusion centers
> >
> > What is the earliest date you/your consortium members anticipate joining any of the groups? *Enter a date or click the calendar button to choose a date from the calendar.*

If no:
If you/any of your consortium members do not plan to join a cybersecurity collaboration or information-sharing groups, please the indicate reason(s) why. Select all that apply.

- ☐ Lack of knowledge
- ☐ Lack of resources/staff
- ☐ External/additional approval needed to join third-party groups
- ☐ Unfamiliar with how/process to join
- ☐ Security/confidentiality concerns with sharing internal cybersecurity information with outside groups
- ☐ Internal policy/procedure that prohibits participation in these types of groups

4.2 Designated Cybersecurity Officer

a. Do you/any of your consortium members currently have a designated cybersecurity officer(s) or other senior-level staff member(s) who will serve as the designated cybersecurity officer(s) if you are selected as a Pilot participant? Select **Yes** or **No**.

If yes:

If consortium:
How many of your consortium members currently have a designated cybersecurity officer(s) or other senior-level staff member(s) who will serve as the designated cybersecurity officer(s)? Please select a value. (0% to 100%)

Select the specific tasks that the designated cybersecurity officer(s) or other senior-level staff member(s) will be responsible for during the Pilot. Select all that apply.

- ☐ Security systems development, testing, analysis, and implementation
- ☐ System vulnerability assessment and management
- ☐ Response to security threats, attacks, and similar events
- ☐ Development of threat prevention strategies
- ☐ Regular generation of reports for executives and administrators
- ☐ None of the above

4.3 Free and Low-Cost Cybersecurity Resources

a. Do you/any of your consortium members currently utilize, or plan to utilize, any of the free or low-cost cybersecurity resources recommended by the Education Department or CISA?

> **If yes:**
> Select the resources you/your consortium members currently utilize or plan to utilize for each category.
> *Refer to the Resources section at the end of this user guide for more detail on the answer options.*
> What is the earliest date you/your consortium members began utilizing or plan to utilize these resources? *Enter a date or click the calendar button to choose a date from the calendar.*

> **If no:**
> What is preventing you/your consortium members from using these resources? Select all that apply.
> - ☐ Lack of knowledge
> - ☐ Staffing/resource issues
> - ☐ Cannot be integrated with our current cybersecurity protections/measures
> - ☐ None of the above

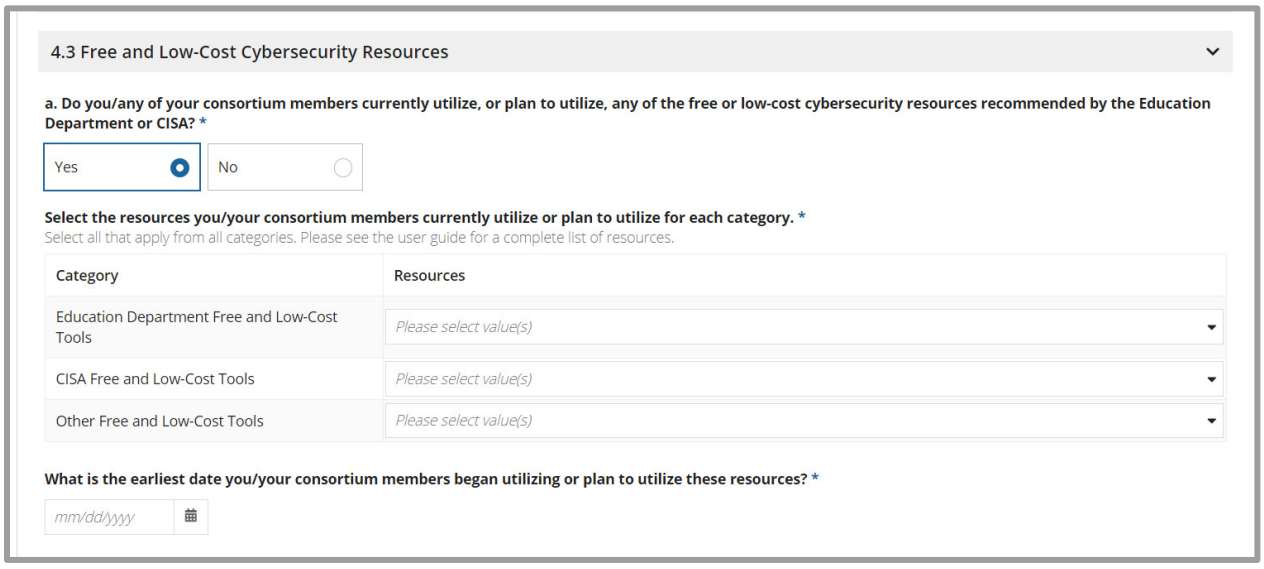


Figure 23 | Question 4.3. In this conditional question, if you answer yes, additional questions be displayed. You will then select the resources from the dropdowns and a date from the calendar.

Proposed Costs

Schools and libraries will be required to answer yes/no questions and provide information regarding their expected costs. Applicants should make a reasonable effort to estimate the costs associated with their Pilot project. The FCC expects to use this information to get a sense of the different sizes and types of projects that are being proposed, in order to ensure a diverse pool of participants. Where available, applicants can use published pricing or reports, past estimates or incurred costs, or other sources of information.

Once applicants have submitted their cost estimates on the FCC Form 484, they will not be able to modify them. However, Pilot Program participants will have an opportunity to adjust their projected costs after completing the competitive bidding process and making final decisions about the services and equipment to be purchased.

5.1 Funding for Non-cybersecurity Equipment and Services That Support Cybersecurity Equipment and Services

a. Do you/Does your consortium have access to funding to cover the cost of any non-cybersecurity equipment and services necessary to support the cybersecurity equipment and services you/your consortium plan(s) to request as part of your proposed Pilot project? Answer **Yes** or **No**.

5.2 Will Service Provider be Required to Include any No Cost Cybersecurity Equipment and/or Services

a. As part of your/your consortium's proposed Pilot project, do you plan to require your selected service provider(s) to provide any cybersecurity equipment and/or services at no cost to you? Answer yes or no.

> **If yes:**
> Using the Pilot Eligible Services List, please select the equipment and services you/your consortium plan(s) to require your service provider(s) to provide at no cost to you. Select all that apply from each category.
> *Refer to Pilot Eligible Services List for more detail on the answer options.*

Gift Rule

If you answer yes to question 5.2.a, USAC may contact you to confirm understanding of the Gift Rule. Please review the Gift Rule in the Schools and Libraries Cybersecurity Program Report and Order, FCC-24-63.

§ 54.2005(d)(1)
Subject to paragraphs (d)(3) and (4) of this section, a participant in the Schools and Libraries Cybersecurity Pilot Program may not directly or indirectly solicit or accept any gift, gratuity, favor, entertainment, loan, or any other thing of value from a service provider participating in or seeking to participate in the Schools and Libraries Cybersecurity Pilot Program. No such service provider shall offer or provide any such gift, gratuity, favor, entertainment, loan, or other thing of value except as otherwise provided herein. Modest refreshments not offered as part of a meal, items with little intrinsic value intended solely for presentation, and items worth $20 or less, including meals, may be offered or provided, and accepted by any individuals or entities subject to this rule, if the value of these items received by any individual does not exceed $50 from any one service provider per year. The $50 amount for any service provider shall be calculated as the aggregate value of all gifts provided during a year by the individuals specified in paragraph (d)(2)(ii) of this section.

5.3 Required Free and Low-Cost Cybersecurity Resources

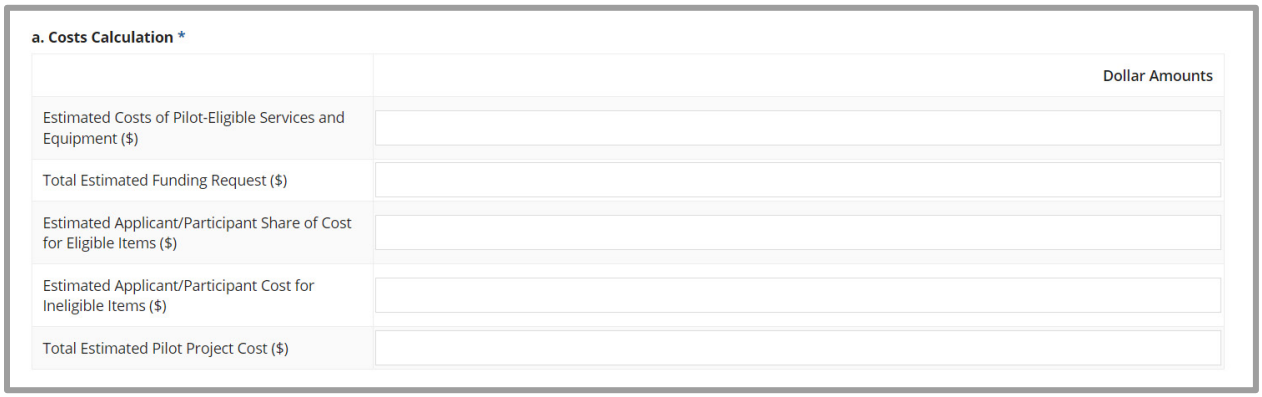
a. As part of your/your consortium's proposed Pilot project, do you plan to require your selected service provider(s) to utilize any free or low-cost Education Department, CISA, or other tools and/or resources? Answer yes or no.

> **If yes:**
> Select the free or low-cost Education Department, CISA, or other tools and/or resources you/your consortium plan(s) to require your service provider(s) to utilize.
> *Refer to the Resources section at the end of this user guide for more detail on the answer options.*

5.4 Costs

Enter dollar amounts for each of the following:

- Estimated Costs of Pilot-Eligible Services and Equipment ($)
- Total Estimated Funding Request ($)
- Estimated Applicant/Participant Share of Cost for Eligible Items ($)
- Estimated Applicant/Participant Cost for Ineligible Items ($)
- Total Estimated Pilot Project Cost ($)



a. Costs Calculation *

	Dollar Amounts
Estimated Costs of Pilot-Eligible Services and Equipment ($)	
Total Estimated Funding Request ($)	
Estimated Applicant/Participant Share of Cost for Eligible Items ($)	
Estimated Applicant/Participant Cost for Ineligible Items ($)	
Total Estimated Pilot Project Cost ($)	

Figure 24 | Question 5.4.a. Costs Calculation. Enter an estimated dollar amount in each row.

Costs Calculation

Enter a value greater than or equal to zero in each row. If any row is left blank, this question will be considered incomplete.

- **Estimated Costs of Pilot-Eligible Services and Equipment** is an estimate of the total costs of the eligible services and equipment the applicant plans to request for its Pilot project.
- **Total Estimated Funding Request** is an estimate of the total amount of USF funding the applicant plans to request for its proposed Pilot project.
- **Estimated Applicant/Participant Share of Cost for Eligible Items** is an estimate of the non-discount share of the costs of Pilot-eligible equipment and services that the applicant will be required to pay.
- **Estimated Applicant/Participant Cost for Ineligible Items** is an estimate of the costs for Pilot-ineligible equipment and services that the applicant will need to carry out its Pilot project.
- **Total Estimated Pilot Project Cost** is the total cost of eligible equipment and services (discount and non-discount shares) + the total cost of ineligible equipment and services + any other costs applicants/participants will incur to participate in the Pilot.

5.5 Sources of Support for Applicant's/Participant's Share of Cost for Eligible Items

a. Select the sources of financial support you/your consortium will use to pay the non-discount share of the cost of Pilot-eligible equipment and services. Select all that apply.
   - ☐ School or library resources
   - ☐ Local resources (non-grant)
   - ☐ State resources (non-grant)
   - ☐ Federal resources (non-grant)
   - ☐ Tribal resources (non-grant)
   - ☐ Local, state, or federal grants
   - ☐ None of the above

5.6 Plan to Cover Cost of Ineligible Items

a. Select the sources of financial support you/your consortium will use to pay for the cost of Pilot-ineligible equipment and services. Select all that apply.
   - ☐ School or library resources
   - ☐ Local resources (non-grant)
   - ☐ State resources (non-grant)
   - ☐ Federal resources (non-grant)
   - ☐ Tribal resources (non-grant)
   - ☐ Local, state, or federal grants
   - ☐ None of the above

Metrics

Schools and libraries will be required to answer yes/no questions regarding their willingness (and the willingness of their selected service provider) to collect and share data if selected to participate in the Pilot Program.

6.1 Data and Metrics Collected by Applicant

a. Are you/all the members of your consortium prepared to share the data you will collect and the metrics you will use to assess the outcome of your/your consortium's participation in the Pilot Program? Answer **Yes** or **No**.

6.2 Cost-Effectiveness Data and Metrics Collected by Service Provider

a. Will you/your consortium require your selected service provider(s) to collect, track, and measure data to determine the cost-effectiveness of the Pilot Program? Answer **Yes** or **No**.

> **If yes:**
> Are you/all the members of your consortium prepared to share that data and any available cost-effectiveness metrics as part of your participation in the Pilot Program for data collection purposes? Answer **Yes** or **No**

6.3 Awareness and Readiness Data and Metrics Collected by Service Provider

a. Will you/your consortium require your selected service provider(s) to collect, track, and measure data to determine the impact of participation in the Pilot Program on your/your consortium's current cybersecurity awareness and readiness? Answer **Yes** or **No**.

> **If yes:**
> Are you/all the members of your consortium prepared to share that data and any available cybersecurity awareness and readiness metrics as part of your participation in the Pilot Program? Answer **Yes** or **No**

Supporting Documentation

Please use this page to upload any supporting documentation that is requested or required by the application or will help us understand your proposed Pilot project or the cybersecurity services and equipment you propose to use.

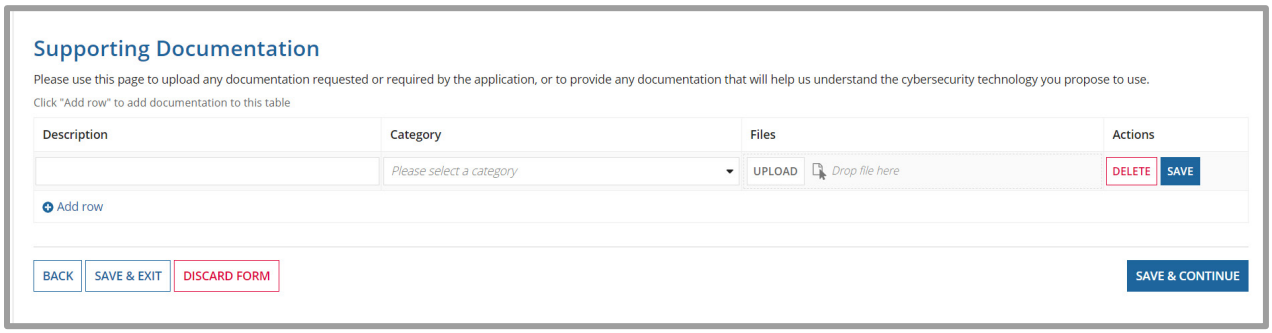


*Figure 25 | On the **Supporting Documentation** page, upload any supporting documents that are requested, required, or you want USAC and the FCC to consider along with your application. Enter a file description and select a category.*

To add supporting documentation:

1. Click **Add Row**.
2. Enter a **description** and choose a **category** (email, file, or image).
3. **Upload** the file.
4. Click **Save** in the **Actions** column. You will not be able to continue to the next page until you save changes in each row.

To edit or remove a saved document, click **Edit** in the Actions column. Click **Delete** to remove the row.

Review

When you reach the **Review** page, the system generates a PDF version of the form. It may take a few minutes for the system to generate and load the PDF. To check whether the generation of the PDF is complete, click **Refresh**. If you want to review the PDF at a later time, click **Resume Task Later** to close the screen. When you are ready to resume review, select the form from the **My Pending Tasks** list on the CBR dashboard to return to the **Review** page.

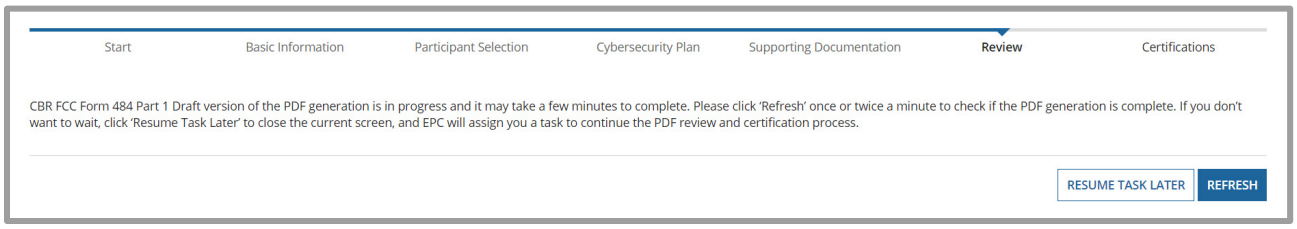


*Figure 26 | When you reach the **Review** page, it may take a few minutes for the system to generate and load a PDF version of the form.*

A message at the top of the **Review** page will alert you if there are unanswered questions on the form. If there are additional questions that you need to answer, click **Edit Form** to return to the **Basic Information** page. From there, re-review each section of the form and answer all required questions. Remember that you must select at least one option in each multi-select dropdown menu. If there is not a specific option that applies to you in a multi-select dropdown menu, select the **None of the Above** option.

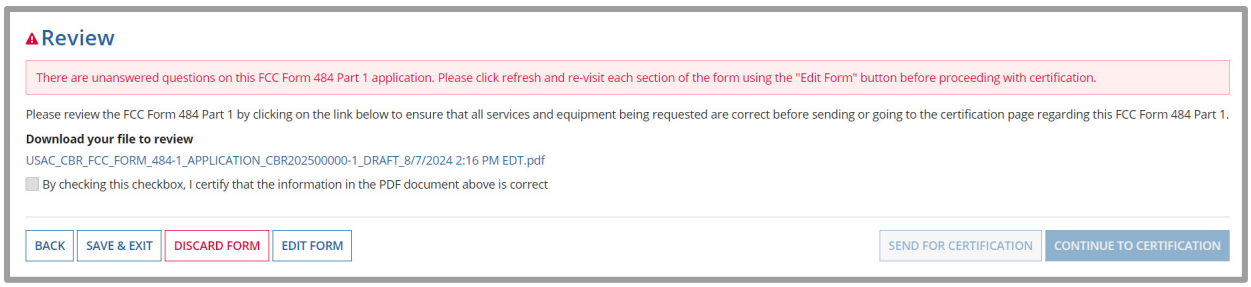


*Figure 27 | A message on the **Review** page will alert you if there are unanswered questions on the form. You will not be able to proceed to the **Certifications** page for the form until you answer all the required questions.*

Click the PDF file name to download the PDF version of your form for review.

Your Completed Application

If you are selected as a Pilot participant, you may need to refer to information from the FCC Form 484 Part 1 when completing the FCC Form 484 Part 2. The PDF containing your FCC Form 484 Part 1 information will remain available to you in the Cybersecurity Pilot Program portal and can be accessed if you are selected as a Pilot participant and need to complete Part 2 of the form.

Because Part 1 of the FCC Form 484 may include cybersecurity information that you consider to be sensitive, if you choose to download and save a copy of the form, you may wish to consider how protect and/or limit access to the saved copy (e.g., password-protecting the PDF to limit who has access to it).

The options on the **Review** page depend on your user permissions.

Review as a Partial Rights User

As a partial rights user, you don't have permission to certify the form and will need to send it to a full rights user for certification. To send the form to a full rights user, click **Send for Certification**. When the system notifies you that your form will be sent to the full rights users in your organization and asks if you wish to proceed, select **Yes** to send the form for certification. The form will disappear from your tasks list and you will not be able to re-open or revise the form.

Review as a Full Rights User

If you are a full rights user and will be certifying the form, select the checkbox to certify that the information in the PDF version of the FCC Form 484 Part 1 is correct. You have two options depending on whether you are the full rights user that will be certifying the form or you will be sending it to another full rights user for certification:

1. If you will be sending the form to another full rights user to certify: Select **Send for Certification** to send the form to other full-rights user(s) in your organization. If you choose this option, the form will disappear from your tasks list and you will not be able to re-open or revise the form. When the system notifies you that your form will be sent to the full rights user(s) in your organization and asks if you wish to proceed, select **Yes** to send the form for certification.
2. If you are the full rights user that will be certifying the form: Select **Continue to Certification** to continue to the **Certifications** page.

Certifications

On the Certifications page, carefully read the certification text. Click on each checkbox to confirm that you understand and will comply/have complied with the certification. After all boxes are checked, click **Certify**. This action is equivalent to providing your electronic signature. When the system asks if you are ready to certify your FCC Form 484 Part 1, select **Yes** to certify and submit.

When you select **Yes** in response to the confirmation message, the form will be certified and will be submitted to USAC. The form will disappear from your tasks list and you will not be able to re-open or revise the form after it has been certified.

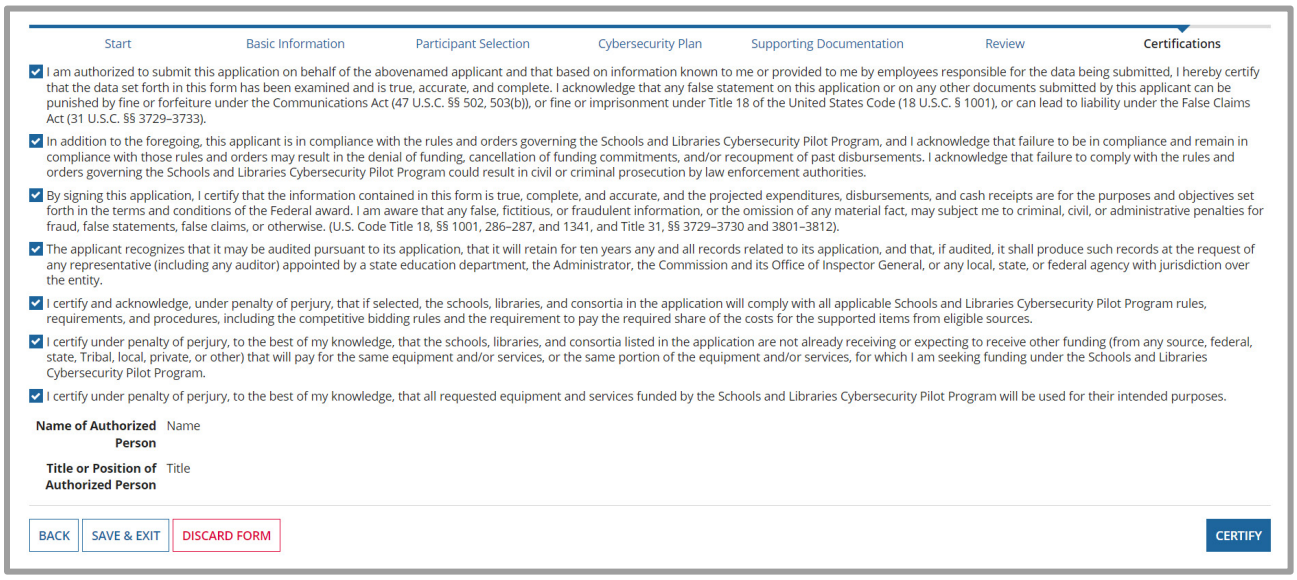


*Figure 28 | On the **Certifications** page, check each checkbox to confirm that you understand and will comply/have complied with each certification.*

After Submitting

After you have submitted your form and it is received by USAC, a notification will appear in the **News** feed for all members of your organization. This notification confirms that the form has been certified and submitted.

Once the Cybersecurity Pilot Program participants have been selected, the FCC will release a public notice announcing the selections. Selected participants will also receive a notification through the Cybersecurity Pilot Program portal. Applicants selected to participate in the Cybersecurity Pilot Program will then be invited to complete the FCC Form 484 Part 2 and initiate the competitive bidding process using the Cybersecurity Pilot Program FCC Form 470.

Resource Links

Free and Low-Cost Cybersecurity Resources

The resources listed below are also included in the answer options for questions 4.3.a and 5.3.a.

Education Department Free and Low-Cost Tools

- K-12 Cybersecurity 101 Risk Management Live and Virtual Trainings by Request
- Cybersecurity for K-12 Schools and School Districts: Developing a Cyber Annex
- Cybersecurity Tabletop Exercise
- Resources for Supporting School Safety Before, During, and After an Emergency
- Dear School Safety Partner: Cybersecurity and Cyber Safety

CISA Free and Low-Cost Tools

- Connect with CISA Regional Cybersecurity Advisor (CSA)
- Sign Up for Cyber-Hygiene Services
- Utilize CISA Cybersecurity Performance Goals (CPG)
- Other CISA tool

Other Free and Low-Cost Tools

- Free/low-cost tools from Free Non-CISA Cybersecurity Services list
- NIST Free and Low Cost Cybersecurity Learning Content
- Free MS-ISAC membership
- MS-ISAC Malicious Domain Blocking and Reporting (Protective Domain Name System)
- CIS Cyber Advisory Services Program
- Other CIS tools

Cybersecurity Collaboration and Information-Sharing Groups

The groups listed below are also the included in the answer options for question 4.1.a.

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- K12 Security Information eXchange (K12 SIX)
- Fusion centers

Form Assistance

If you have any questions about completing this form, please contact the USAC Customer Service Center (CSC) at (888) 203-8100 between 8 a.m. and 8 p.m. ET Monday through Friday.

You can also create a customer service case in the E-Rate Productivity Center (EPC) via the **Contact Us** link on your EPC landing page. On the customer service case form, select the topic **Cybersecurity Pilot.**

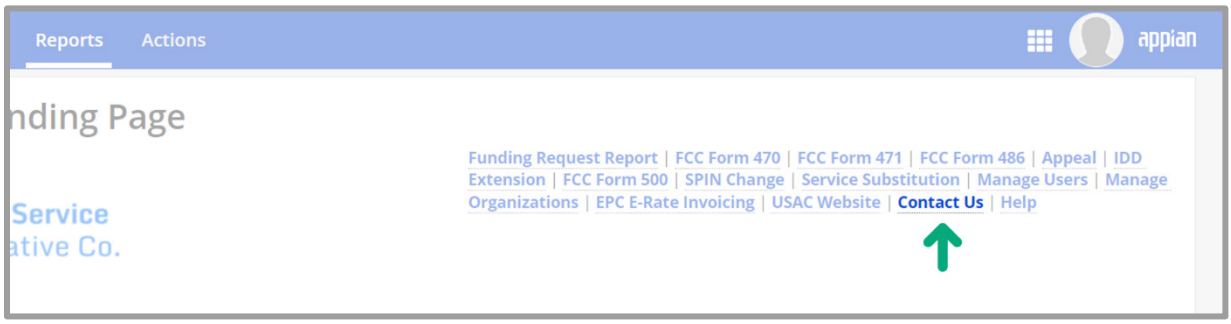


*Figure 29 | Click **Contact Us** on your EPC landing page to create a customer service case.*