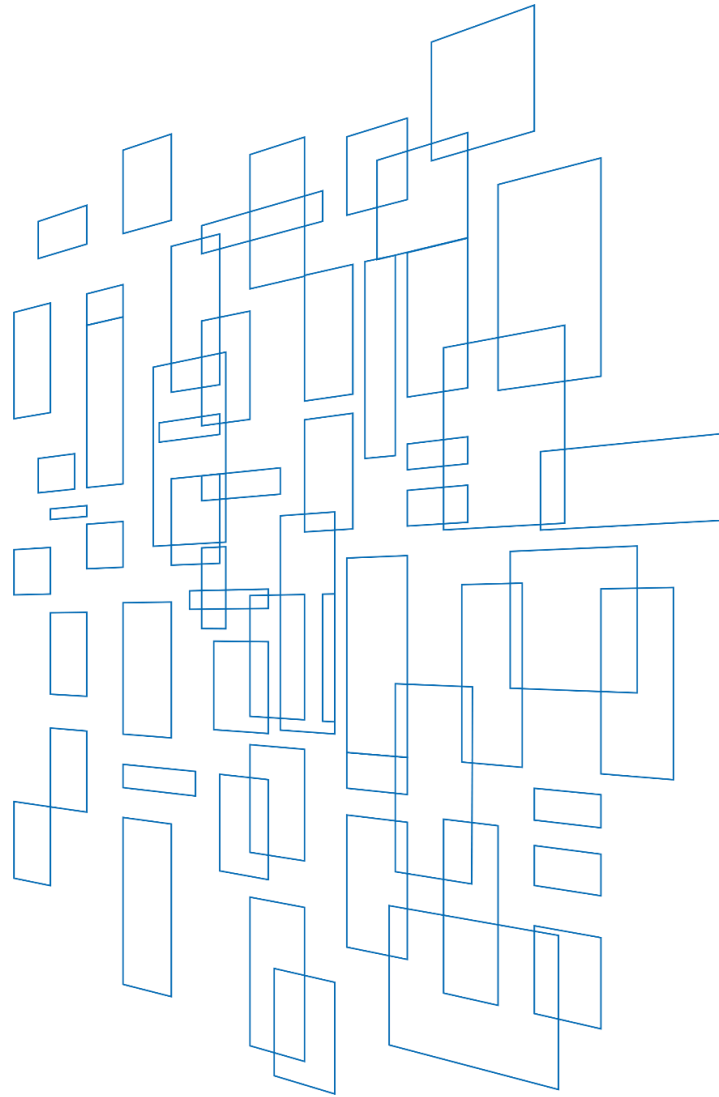




Schools and Libraries Cybersecurity Pilot Program Annual Reporting User Guide

Pilot FCC Form 484 Part 3

Created/Revised October 2026

Contents

File Pilot FCC Form 484 Part 3.....	4
User Roles and Permissions.....	4
Navigate to the Cybersecurity Pilot Program Portal.....	6
Start Pilot FCC Form 484 Part 3	7
Pilot FCC Form 484 Part 3 Navigation.....	7
Pilot FCC Form 484 Part 3 Form Overview	11
Start	11
Basic Information.....	11
Cybersecurity Plan – Part 1	11
Cybersecurity Plan – Part 2	11
Annual Reporting Questions.....	14
Person Completing Questionnaire	14
Student, Library Patron, and Staff Data	14
Current Cybersecurity Posture	15
Effectiveness: Advanced Firewalls.....	15
Effectiveness: Endpoint Protection	16
Effectiveness: Identity Protection and Authentication.....	17
Effectiveness: Monitoring, Protection, and Response.....	18
System Outage (Ransomware, DDOS, or other network-disabling attack)	20
Supporting Documentation.....	20
Review.....	21
Certifications	23
After Certifying and Submitting.....	25
Form Assistance	25

This Schools and Libraries Cybersecurity Pilot Program (Pilot Program or Pilot) Annual Reporting User Guide provides guidance to Pilot participants on the requirements and processes for preparing, completing, and submitting the Pilot FCC Form 484 Part 3. The data gathered from the Pilot will help the FCC evaluate whether, and to what extent, it should use the Universal Service Fund (USF) to support the cybersecurity needs of eligible schools and libraries going forward.

Pilot participants are required to complete the Pilot FCC Form 484 Part 3 to update information they provided in Part 1 and Part 2 of the Pilot FCC Form 484 and respond to new annual data reporting requirements. When completing the form, please be as thorough and detailed as possible.

We recognize that the cybersecurity-related information that is being requested and provided in the Pilot FCC Form 484 Part 3 may include sensitive business information and trade secrets. Accordingly, we will treat the information as presumptively confidential under our rules and will withhold it from routine public inspection. This information is being collected for the purposes described above and will not be shared with other federal agencies for incident reporting or compliance purposes. We further note that the Pilot FCC Form 484 Part 3 data will be protected by security protections built into USAC's Pilot portal.

Although the information contained in these reports will be presumptively confidential, the Wireline Competition Bureau may, at its discretion, create a version of the information collected on this form, which is aggregated, anonymized, or otherwise not subject to protection from disclosure, under the Freedom of Information Act for public release.

Help completing the Pilot FCC Form 484 Part 3 is available for Pilot participants that need it. Instructions on how to contact the USAC Customer Service Center are provided in the [Form Assistance](#) section of this user guide.

File the Pilot FCC Form 484 Part 3

This section provides guidance on how to complete and file the Pilot FCC Form 484 Part 3 in the Cybersecurity Pilot Program Portal.

User Roles and Permissions

Only the Pilot participant's Account Administrators, who have been assigned full access rights, or other authorized persons who have been assigned full access rights, such as consultants and school or library employees, can certify and submit Pilot Program forms. For the Pilot Program, user roles and permission rights are assigned on a per-form basis, which means that different users may have access to different Pilot Program forms.

For more information about how to add users or reactivate a deactivated user as an Account Administrator, please see the [E-Rate Productivity Center \(EPC\) Account Administrator Guide](#).

Available rights for the Pilot FCC Form 484 Part 3 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 route the draft form to the organization's full-rights user(s) 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 collected in the Pilot Program, USAC has limited consultant access to participants' Pilot FCC Forms 484. This means that, while the user management details contained in a participant'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 participant account.

To assign user roles and permission rights for Pilot Program forms, including the Pilot FCC Form 484 Part 3, an Account Administrator must:

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 Annual Reporting Permission** for each user
6. Click **Submit**



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

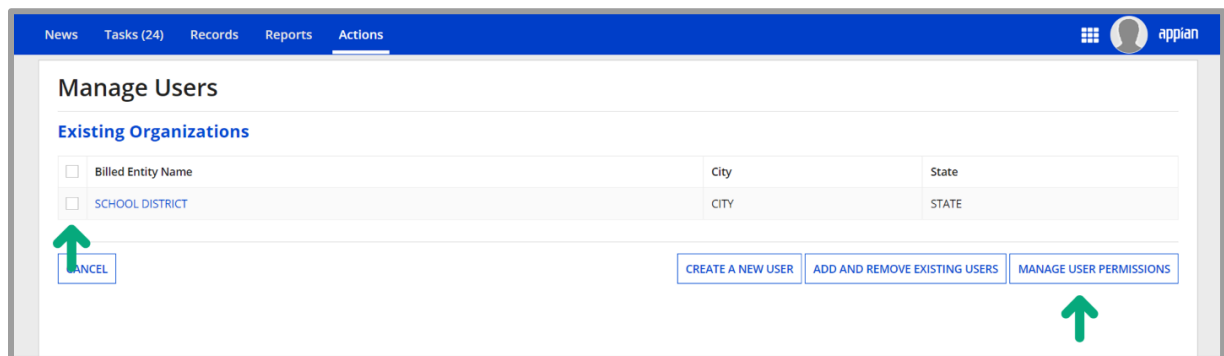


Figure 2 | On the Manage Users page, check the checkbox next to your entity and click **Manage User Permissions**.

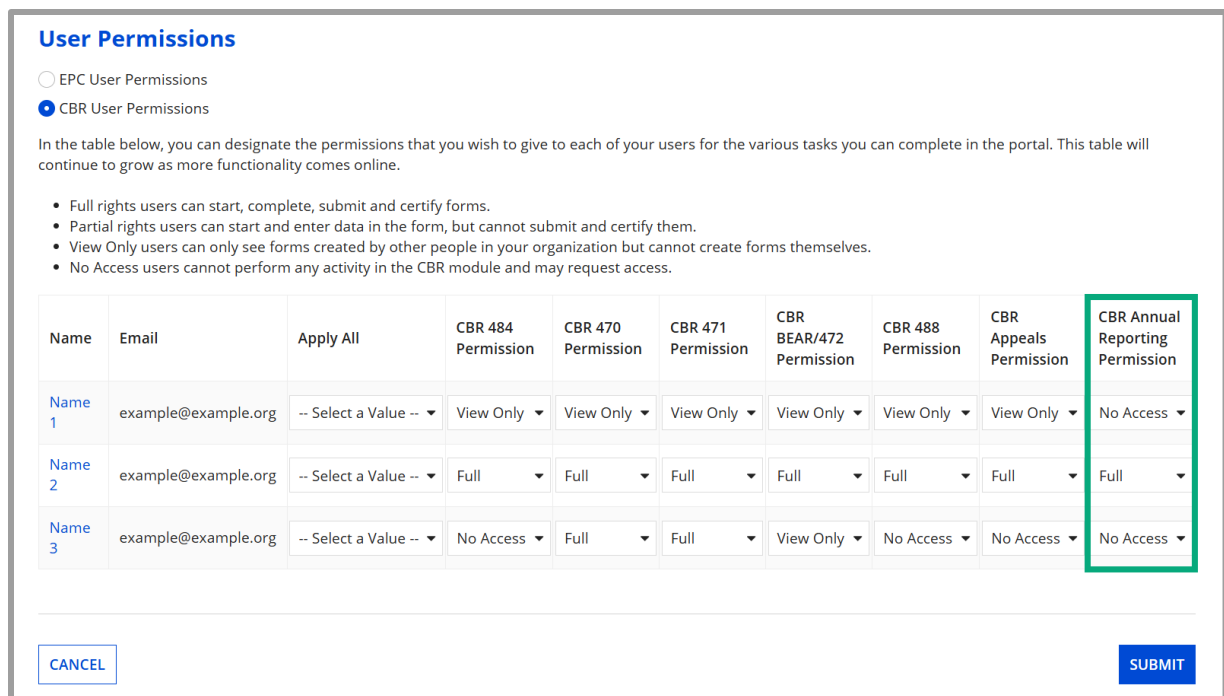


Figure 3 | On the User Permissions page, select the permissions you wish to give to each user in the **CBR Annual Reporting Permission** column, then click **Submit**.

Navigate to the Cybersecurity Pilot Program Portal

The Cybersecurity Pilot Program Portal (CBR Dashboard) can be used to access the various forms needed to participate in the Pilot Program. To access the dashboard, log into EPC and click the navigation waffle at the top right of the screen. From the dropdown options, choose **Cybersecurity Pilot Program**.

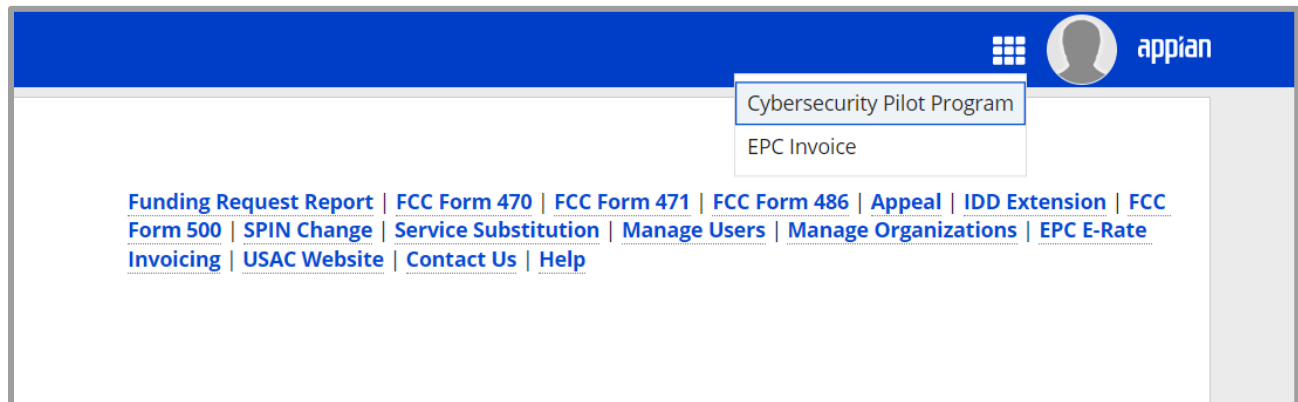


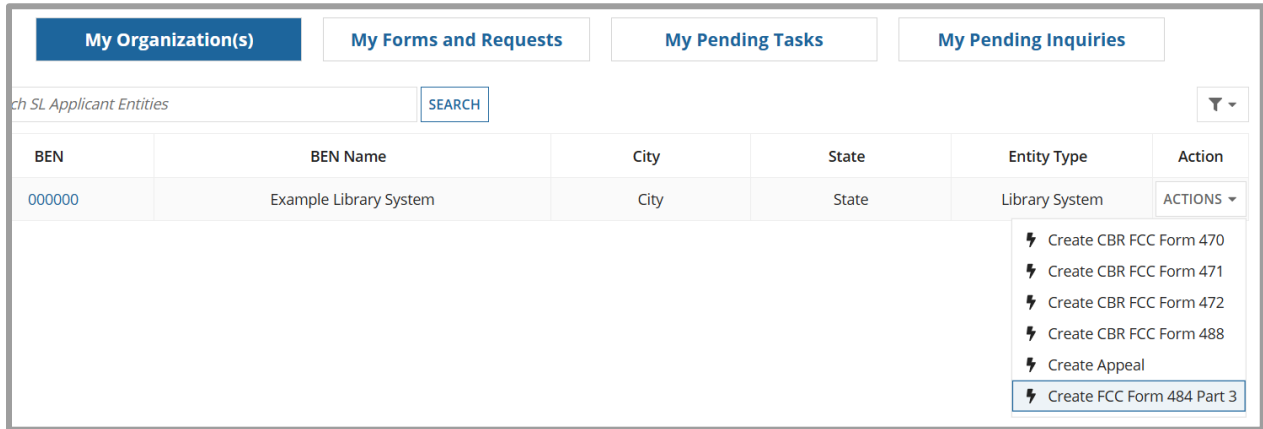
Figure 4 | From the EPC landing page, click the navigation waffle and choose **Cybersecurity Pilot Program**.



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 Pilot FCC Form 484 Part 3

In the **My Organization(s)** tab on the CBR Dashboard, click **Actions** in the **Action** column, then **Create CBR FCC Form 484 Part 3**.



My Organization(s) My Forms and Requests My Pending Tasks My Pending Inquiries

ch SL Applicant Entities SEARCH

BEN	BEN Name	City	State	Entity Type	Action
000000	Example Library System	City	State	Library System	ACTIONS ▾

- ⚡ Create CBR FCC Form 470
- ⚡ Create CBR FCC Form 471
- ⚡ Create CBR FCC Form 472
- ⚡ Create CBR FCC Form 488
- ⚡ Create Appeal
- ⚡ Create FCC Form 484 Part 3

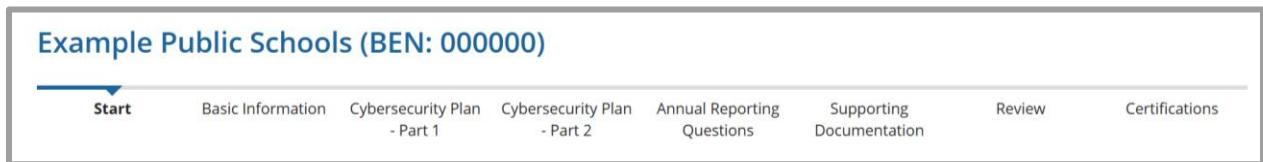
Figure 6 | Click **Actions**, then **Create FCC Form 484 Part 3** in the **Action** column on the CBR Dashboard to begin the form.

Form Navigation

This section provides an overview of navigation and input options within the Pilot FCC Form 484 Part 3.

Progress Bar

The progress bar at the top of each form page helps you track your progress in completing the form.



Example Public Schools (BEN: 000000)

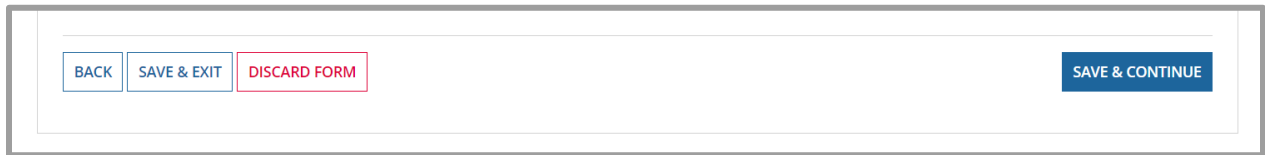
Start Basic Information Cybersecurity Plan - Part 1 Cybersecurity Plan - Part 2 Annual Reporting Questions Supporting Documentation Review Certifications

Figure 7 | In the progress bar, track progress between form sections: **Start, Basic Information, Cybersecurity Plan – Part 1, Cybersecurity Plan – Part 2, Annual Reporting Questions, Supporting Documentation, Review, and Certifications**.

Saving or Discarding the Pilot FCC Form 484 Part 3

The bottom of each Pilot FCC Form 484 Part 3 page provides you with the following 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 if you discard a form, the draft form will be deleted from USAC’s system and cannot be retrieved.
- **Save & 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.

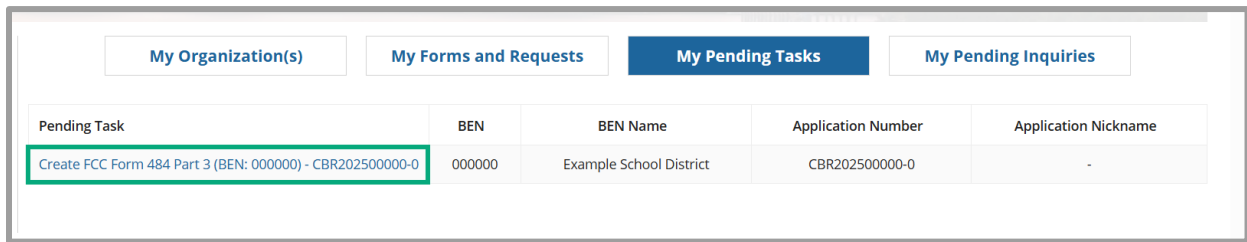


A screenshot of the bottom of the Pilot FCC Form 484 Part 3 page. It shows four buttons arranged horizontally: "BACK" (light blue), "SAVE & EXIT" (light blue), "DISCARD FORM" (red), and "SAVE & CONTINUE" (dark blue). The buttons are enclosed in a light gray border.

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

Exiting the Form and Returning Later

To save the information you have entered before exiting the form, select **Save & Exit**. When you return to the form, navigate to the CBR Dashboard and select the task name on the **My Pending Tasks** tab to resume where you left off. The prior information that you added is saved and you will still be able to edit it prior to submission of the form.



A screenshot of the CBR Dashboard. The top navigation bar has four tabs: "My Organization(s)", "My Forms and Requests", "My Pending Tasks" (which is selected and highlighted in blue), and "My Pending Inquiryies". Below the tabs is a table with the following data:

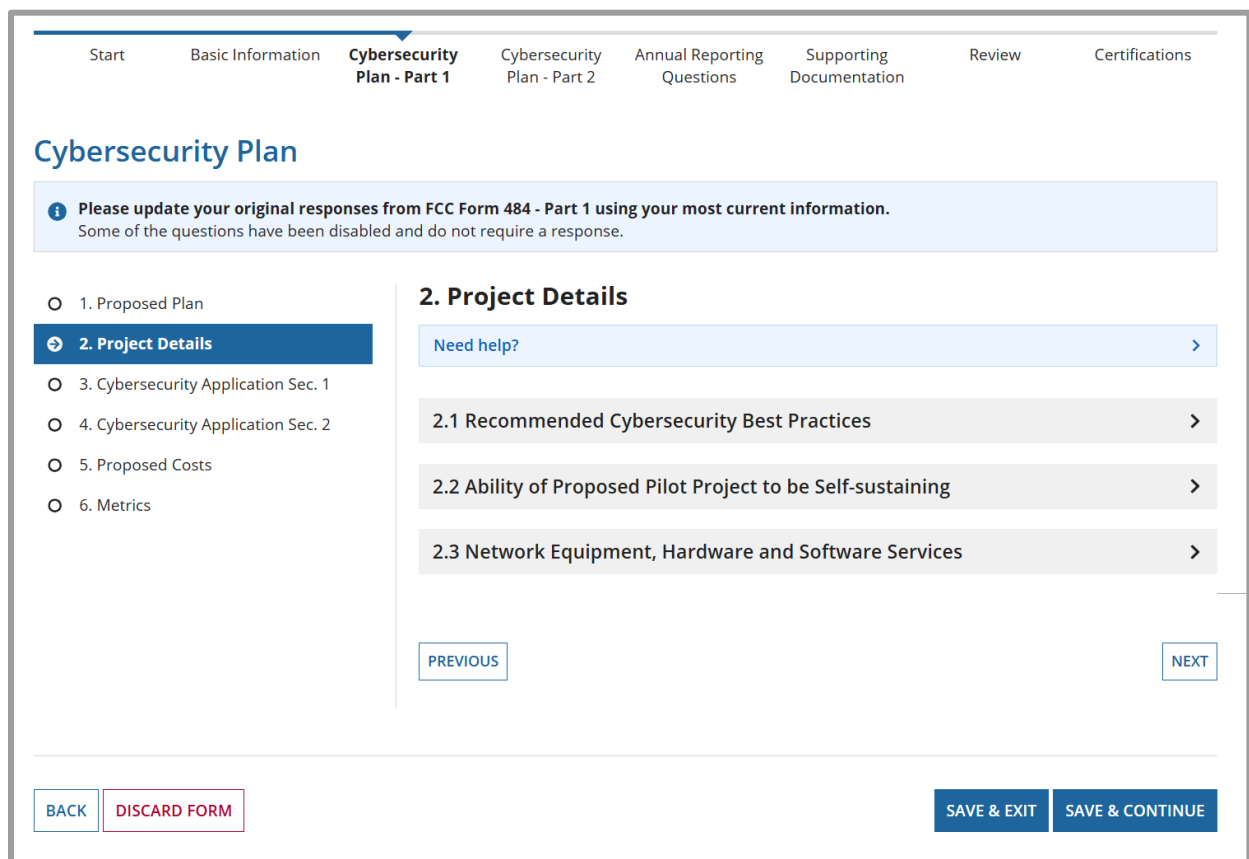
Pending Task	BEN	BEN Name	Application Number	Application Nickname
Create FCC Form 484 Part 3 (BEN: 000000) - CBR202500000-0	000000	Example School District	CBR202500000-0	-

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

Milestones and Sections

There are eight milestones that make up the form: **Start**, **Basic Information**, **Cybersecurity Plan – Part 1**, **Cybersecurity Plan – Part 2**, **Annual Reporting Questions**, **Supporting Documentation**, **Review**, and **Certifications**. You can navigate between form milestones using 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 – Part 1** milestone. You can navigate between sections using the side navigation or the **Next** and **Previous** buttons at the bottom of the section.



The screenshot displays the 'Cybersecurity Plan' milestone within a web application. At the top, a horizontal navigation bar lists eight milestones: Start, Basic Information, Cybersecurity Plan - Part 1 (active), Cybersecurity Plan - Part 2, Annual Reporting Questions, Supporting Documentation, Review, and Certifications. Below this, the 'Cybersecurity Plan' title is followed by an information box stating: 'Please update your original responses from FCC Form 484 - Part 1 using your most current information. Some of the questions have been disabled and do not require a response.' On the left, a side navigation menu lists six sections: 1. Proposed Plan, 2. Project Details (selected), 3. Cybersecurity Application Sec. 1, 4. Cybersecurity Application Sec. 2, 5. Proposed Costs, and 6. Metrics. The main content area for '2. Project Details' includes a 'Need help?' link and three expandable sections: '2.1 Recommended Cybersecurity Best Practices', '2.2 Ability of Proposed Pilot Project to be Self-sustaining', and '2.3 Network Equipment, Hardware and Software Services'. At the bottom of the main content area are 'PREVIOUS' and 'NEXT' buttons. The footer contains four buttons: 'BACK', 'DISCARD FORM', 'SAVE & EXIT', and 'SAVE & CONTINUE'.

Figure 10 | Navigate between milestones using 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.

Pop-Up Confirmation Messages

The system displays pop-up messages to verify that you want to take certain actions within the form. For example, the below pop-up message provides you with an opportunity to click **Yes** to discard the application or **No** if you wish to stay where you are in the form.

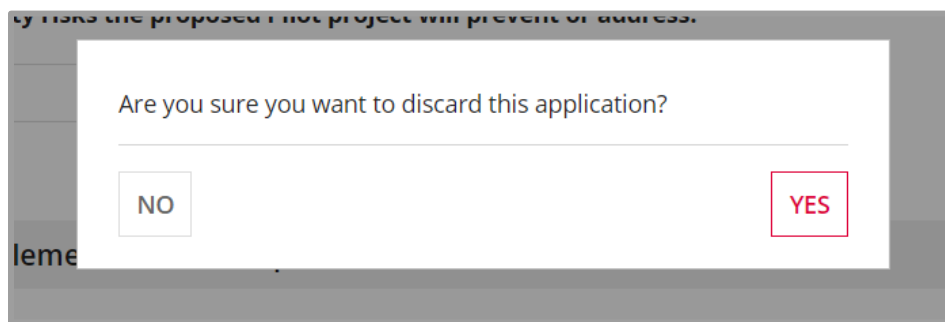


Figure 11 | When you select **Discard Form**, a pop-up message asks you to confirm that you want to discard your application.

Conditional Questions

Some questions are considered conditional, meaning that they will be hidden or displayed based on your answers to previous questions.

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.

Some conditional questions will also display text boxes. For example, if you select the answer **Other**, **please specify**, a text box will be displayed, and you will type your response in the text box.

Multiselect Dropdown Fields

You can select multiple options in some dropdown fields. These are indicated with the prompt **Select all that apply**.

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.

Pilot FCC Form 484 Part 3 Form Overview

There are eight sections that make up the Pilot FCC Form 484 Part 3: **Start**, **Basic Information**, **Cybersecurity Plan – Part 1**, **Cybersecurity Plan – Part 2**, **Annual Reporting Questions**, **Supporting Documentation**, **Review**, and **Certifications**. Each section is discussed below.

Start

On the **Start** page, be sure to review the Paperwork Reduction Act and Privacy Act Notices.

Basic Information

On the **Basic Information** page, enter an application nickname to help you easily identify your form. You will also 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 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 **Related Actions** menu on the landing page in EPC. 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 EPC Profile.

Cybersecurity Plan – Part 1

On the **Cybersecurity Plan – Part 1** page, you will update your original responses from the Pilot FCC Form 484 Part 1 using your most current information, as necessary. Your responses from the Pilot FCC Form 484 Part 1 will be pre-populated for each question. Some of the questions have been disabled and do not require a response.

Refer to the [Pilot FCC Form 484 Part 1 User Guide](#) or your form record for a list of the questions contained in this section. Access your Pilot FCC Form 484 Part 1 form record from the **My Forms and Requests** tab in the Cybersecurity Pilot Program Portal.

Cybersecurity Plan – Part 2

On the **Cybersecurity Plan – Part 2** page, you will update your original responses from the Pilot FCC Form 484 Part 2 using your most current information, as necessary. Your responses from Pilot FCC Form 484 Part 2 will be pre-populated for each question. Some of the questions have been disabled and do not require a response.

Refer to the [Pilot FCC Form 484 Part 2 User Guide](#) or your form record for a list of the questions contained in this section. Access your Pilot FCC Form 484 Part 2 form record from the **My Forms and Requests** tab in the Cybersecurity Pilot Program Portal.

In addition to questions populated from the Pilot FCC Form 484 Part 2, **Cybersecurity Plan – Part 2** includes several new questions that may be displayed on a conditional basis. These new conditional questions are provided below.

If you answered Yes to question 1.1.d: “Do you/does your consortium plan to use funding from the Pilot Program to conduct routine data backups?”

Is at least one copy of the back-up stored offline? (For consortia, please answer based on the majority of your consortium members.) Answer **Yes** or **No**.

What precautions are in place to ensure the integrity and security of the back-ups? (For consortia, please answer based on the majority of your consortium members.) Select all that apply.

- ☐ Encryption
- ☐ Multiple copies
- ☐ Regular updates/patching
- ☐ Secure location
- ☐ Limited access
- ☐ Regular testing of restore process
- ☐ Use MFA
- ☐ Comprehensive backup policy

If you answered Yes to question 2.1.c: “Do you/any members of your consortium currently have or plan to implement an incident response plan?”

Do you/any of your consortium members assess the effectiveness of your incident response plan? Answer **Yes** or **No**.

If Yes:

How often do you assess the effectiveness? (For consortia, please answer based on the majority of your consortium members.) Select one.

- ☐ Continuously, or more often than daily
- ☐ Daily
- ☐ Weekly
- ☐ Bi-Weekly
- ☐ Monthly
- ☐ Quarterly
- ☐ Annually
- ☐ Bi-Annually

If you answered greater than 0 to question 4.1.a: “How many cybersecurity incidents have you/your consortium members experienced in the last year? (For consortia, answer this question using an average of all your consortium members.)”

What was the mean time to detect? (For consortia, respond for the member with the most recent incident.)

What was the mean time to restore/recover? (For consortia, respond for the member with the most recent incident.)

Did the incident involve a third-party vendor solution (such as cloud services)? (For consortia, respond for the member with the most recent incident.)

If you answered Yes to question 5.1.a: “Do you/any of your consortium members currently provide cybersecurity training for school staff, students, or library staff?”

The existing conditional question “On average, how often do you/your consortium members provide cybersecurity training? (For consortia, answer this question using an average of all your consortium members.)” includes a new answer option: **one-time**.

The answer options for question 5.1.b: “Do you have one or more full-time dedicated cybersecurity staff?” have been updated. Select one:

- ☐ No
- ☐ No, part-time only
- ☐ Yes, 1-2
- ☐ Yes, 3 or more

If you answer No or No, part-time only:

How do you/your consortium members manage cybersecurity? (For consortia, please answer based on the majority of your consortium members.) Select all that apply.

- ☐ Part-time employee
- ☐ Managed service provider/third-party vendor
- ☐ School district
- ☐ Local/state government
- ☐ Ad hoc
- ☐ Other, please specify

Annual Reporting Questions

On the **Annual Reporting** page, you will answer new supplemental questions. Questions not applicable to your entity type will be disabled. You can disregard the disabled questions.

Answering for a Consortium

If you are completing the Pilot FCC Form 484 Part 3 for a consortium, review each question carefully for directions about how to answer on behalf of your consortium members. Some questions require you to provide an **average** for your consortium members, others ask you to answer based on the **majority** of your consortium members, and some ask you to answer based on **any** of your consortium members.

1. Person Completing Questionnaire

1.1 Person Completing Questionnaire

- What is the name of the person who is providing the answers on this Pilot FCC Form 484 Part 3?
- What is your primary job title?
- Are you a consultant? Answer **Yes** or **No**.
- Are you a consortium lead? Answer **Yes** or **No**.
- Are you the Designated Cybersecurity Officer? Answer **Yes** or **No**.

If no:

Please provide the name of the Designated Cybersecurity Officer.

- What is your email address?
- What is your phone number?
- How many years of network experience do you have?

2. Student, Library Patron, and Staff Data

2.1 Student, Library Patron, and Staff Data

- How many staff do you/your consortium members currently employ? (For consortia, respond with an average for your consortium members.)
- For libraries and library systems, how many patrons do you/your consortium members currently have? (For consortia, respond with an average for your consortium members.)
- For how many current and former school staff and students do you have a record on file? (For consortia, respond with an average for your consortium members.)
- For how many current and former library staff and patrons do you have a record on file? (For consortia, respond with an average for your consortium members.)

3. *Current Cybersecurity Posture*

3.1 Current Cybersecurity Posture

- a. Does your network/the networks of the majority of your consortium members have a virtual or physical partition or separation (like a router or a firewall) between your internal network (intranet) and the internet? Answer **Yes**, **No**, or **I Don't Know**.
- b. Is your network segmented by user type? (For consortia, please answer based on the majority of your consortium members.) Answer **Yes** or **No**.

If yes:

Which users is it segmented by? (For consortia, please answer based on the majority of your consortium members.) Select all that apply.

- ☐ Student
 - ☐ Staff
 - ☐ Admin
 - ☐ Other, please specify
- c. How is your network managed? (For consortia, please answer based on the majority of your consortium members.) Select all that apply.
 - ☐ Self-managed
 - ☐ Educational Services Agency (ESA) managed service provider
 - ☐ Non-profit managed service provider
 - ☐ For-profit managed service provider
 - ☐ Other, please specify

4. *Effectiveness: Advanced Firewalls*

4.1 Advanced Firewalls

- a. What percentage of your/your consortium members' total network traffic is protected by Advanced Firewalls? (For consortia, respond with an average for your consortium members.)

If greater than 0%:

Does your/any of your consortium members' Advanced Firewall solution provide a report about how much network traffic is protected each month (in gigabytes)? Answer **Yes** or **No**.

If yes:

How many gigabytes of traffic were protected in the last month? (For consortia, respond with an average for your consortium members.)

- b. Does your/any of your consortium members' Advanced Firewall report the number and type of threats prevented in the last year? Answer **Yes**, **No**, or **We don't have an advanced firewall**.

If yes:

How many total threats from insiders and outsiders were prevented by Advanced Firewall systems in the last year? (For consortia, respond with an average for your consortium members.)

How many threats from insiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

How many threats from outsiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

5. Effectiveness: Endpoint Protection

5.1 Endpoint Protection

- a. How many school-, library-, or consortium member-owned or leased end-user devices have access to the network? (For consortia, respond with an average for your consortium members.)
- b. What percentage of the total end-user devices with access to the network do school-, library-, or consortium member-owned or leased devices constitute? (For consortia, respond with an average for your consortium members.)
- c. How many school-, library-, or consortium member-owned or leased devices are protected by Endpoint Protection? (For consortia, respond with an average for your consortium members.)

If greater than 0:

How many servers are protected? (For consortia, respond with an average for your consortium members.)

What percentage of the total number of servers are protected? (For consortia, respond with an average for your consortium members.)

How many of the protected devices are Windows and Mac end-user devices? (For consortia, respond with an average for your consortium members.)

How many of the protected devices are Chromebook end-user devices? (For consortia, respond with an average for your consortium members.)

How many of the protected devices are Other (i.e., not Windows, Mac, or Chromebook) end-user devices? (For consortia, respond with an average for your consortium members.)

- d. Does your/any of your consortium members' Endpoint Protection solution provide a report on the number of threats prevented in the last year? Answer **Yes**, **No**, or **We don't have Endpoint Protection**.

If yes:

How many total threats from insiders and outsiders were prevented by Endpoint Protection systems or services in the last year? (For consortia, respond with an average for your consortium members.)

How many threats from insiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

How many threats from outsiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

6. *Effectiveness: Identity Protection and Authentication*

6.1 Identity Protection and Authentication

- a. On average, report the number of network users protected by Identity Protection and Authentication for the last year for each of the following categories (For consortia, respond with an average for your consortium members.):
- Students
 - Library Patrons
 - School Staff
 - Library Staff
- b. Are all registered users of the network protected by Identity Protection and Authentication software or services? (For consortia, please answer based on the majority of your consortium members.) Answer **Yes**, **No**, or **We don't have Identity Protection and Authentication**

If no:

Are all privileged/administrative users protected? (For consortia, please answer based on the majority of your consortium members.) Answer **Yes** or **No**.

Are all privileged/administrative users required to use MFA? (For consortia, please answer based on the majority of your consortium members.) Answer **Yes** or **No**.

Does your/any of your consortium members' Identity Protection and Authorization system(s) report the number and type of threats prevented in the last year? Answer **Yes**, **No**, or **We don't have Identity Protection and Authorization**.

How many total threats from insiders and outsiders were prevented by Identity Protection and Authorization systems or Services in the last year? (For consortia, respond with an average for your consortium members.)

How many threats from insiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

How many threats from outsiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

- c. Do you/the majority of your consortium members implement advanced protections such as Media Access Control (MAC) address filtering for access or blocking for Wi-Fi systems?

If yes:

Does that include blocking specific hardware devices by MAC address?

7. Effectiveness: Monitoring, Protection, and Response

7.1 Monitoring, Protection, and Response

- a. What portion of your/your consortium members' users are protected by Monitoring, Protection, and Response system(s)? (For consortia, respond with an average for your consortium members.) Select **All**, **Most**, **Some**, or **None**.
- b. Does your/any of your consortium members' Monitoring, Protection, and Response system(s) solution provide a report on the number of attempted attacks prevented in the last year? Answer **Yes**, **No**, or **We don't have Monitoring Protection and Response system**.

If yes:

How many total attacks from insiders and outsiders were prevented by Monitoring, Protection, and Response systems or services in the last year? (For consortia, respond with an average for your consortium members.)

How many attacks from insiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

How many attacks from outsiders were prevented in the last year? (For consortia, respond with an average for your consortium members.)

- c. Does your/any of your consortium members' Monitoring, Protection, and Response system(s) report the number and type of attack?

If yes:

Indicate the number of attacks in the last year for each of the types of attack listed below. If the same incident involved multiple attack types, please include that incident in the number reported for each applicable type of attack listed below. (For consortia, respond with an average for your consortium members.)

Answer for each attack type:

- 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, Data Compromise and Loss, or similar threats

- d. Do you/any of your consortium members ask students, staff, and/or patrons to report potential/suspected phishing attacks?

If yes:

How are suspected phishing attacks reported? (For consortia, please answer based on the majority of your consortium members.) Select all that apply.

- ☐ Automated
- ☐ Written email
- ☐ Other, please specify

How many phishing attacks were reported in the last year to IT personnel? (For consortia, respond with an average for your consortium members.)

- e. Have you/any members of your consortium conducted any test phishing attacks with students, staff, and/or patrons to test their ability to identify phishing emails in the last year? Answer **Yes**, **No**, or **I Don't Know**.

If yes:

What percentage of test attacks were handled incorrectly in the last year? (For consortia, respond with an average for your consortium members.)

8. System Outage (Ransomware, DDOS, or other network-disabling attack)

8.1 System Outage (Ransomware, DDOS, or other network-disabling attack)

- What percentage of your/your consortium's annual OVERALL BUDGET is spent on IT and cybersecurity? (For consortia, respond with an average for your consortium members.)
 - Total annual IT BUDGET?
 - Total annual CYBERSECURITY BUDGET, if tracked separately.
- If your/any of your consortium members' network(s) were to experience a network-disabling cyberattack, would the school or library need to close for the duration of the outage? Answer **Yes, No**, or **I Don't Know**.
- Do you/any members of your consortium have services hosted on-premise (e.g., email, student information system) that would be affected by a network-disabling attack? Answer **Yes, No**, or **I Don't Know**.
- How many school days were lost to a network-disabling attack last year (If you lost a portion of a day then enter the appropriate decimal, e.g. enter 0.5 for half a school day)? (For consortia, answer with an average of school days for your school and school district members.)
- What is the estimated cost of one make-up school day if a day is lost to a cyberattack-caused network outage? (For consortia, answer with an average cost for your school and school district members.)

Supporting Documentation

Use this page to upload any documentation that is requested or required by the application or will help us understand the information in the form.



Description	Category	Files	Actions
	Please select a category	UPLOAD Drop file here	DELETE SAVE
Add row			

BACK | SAVE & EXIT | DISCARD FORM | SAVE & CONTINUE

Figure 12 | 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 annual reporting form. Enter a file description and select a category.

To add supporting documentation:

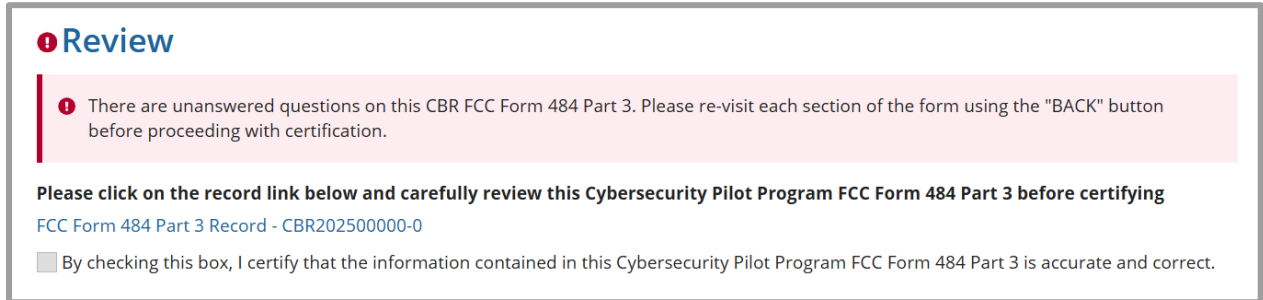
- Click **Add Row**.
- Enter a **description** and choose a **category** (email, file, or image).
- Upload** the file.
- Click **Save** in the **Actions** column. You will not be able to continue to the next page until you save changes in each row.

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 record of the form.

A message at the top of the **Review** page will alert you if there are unanswered questions on the form. You will not be able to proceed forward until all required questions are answered. To revisit a section of the form to review or complete a question, use the **Back** button.



Review

There are unanswered questions on this CBR FCC Form 484 Part 3. Please re-visit each section of the form using the "BACK" button before proceeding with certification.

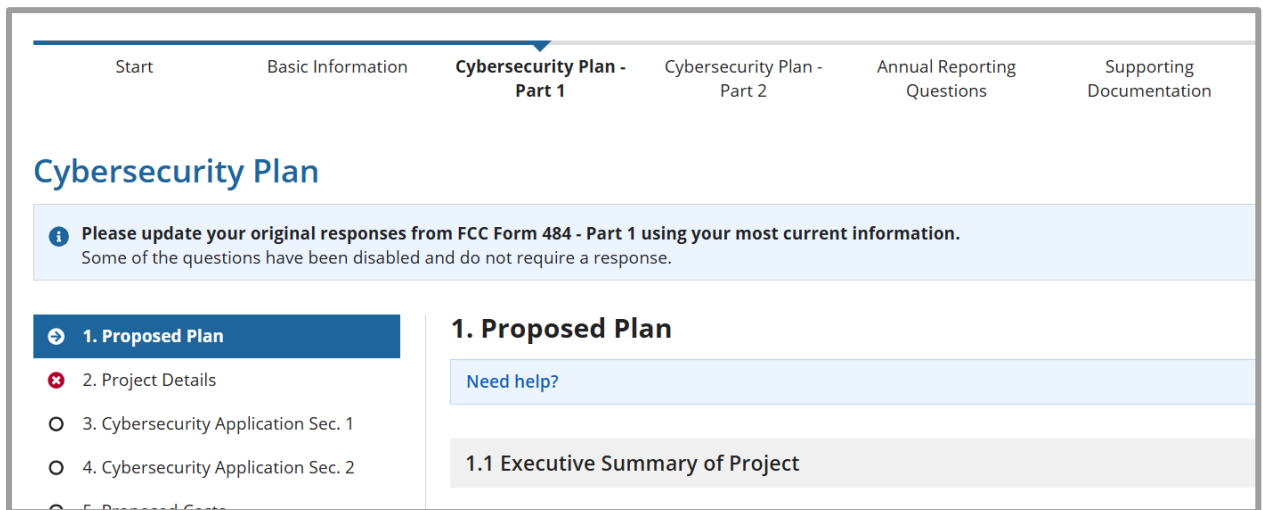
Please click on the record link below and carefully review this Cybersecurity Pilot Program FCC Form 484 Part 3 before certifying

[FCC Form 484 Part 3 Record - CBR202500000-0](#)

☐ By checking this box, I certify that the information contained in this Cybersecurity Pilot Program FCC Form 484 Part 3 is accurate and correct.

Figure 13 | 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 of the form until you answer all the required questions.

Pages with unanswered questions are marked with a red X in the side navigation menu. Please note that the form is not rechecked for completeness until you return to the Review page and, as a result, the red X will not automatically be cleared when you complete each page.



Start Basic Information **Cybersecurity Plan - Part 1** Cybersecurity Plan - Part 2 Annual Reporting Questions Supporting Documentation

Cybersecurity Plan

Please update your original responses from FCC Form 484 - Part 1 using your most current information. Some of the questions have been disabled and do not require a response.

1. Proposed Plan

2. Project Details

3. Cybersecurity Application Sec. 1

4. Cybersecurity Application Sec. 2

5. Proposed Costs

Need help?

1.1 Executive Summary of Project

Figure 14 | In this example, the **Project Details** page of the **Cybersecurity Plan – Part 1** milestone is incomplete.

To review the form:

1. Click the record link to access the record of your Pilot FCC Form 484 Part 3 for review.
2. The options on the **Review** page depend on whether you have been given partial or full-rights user permissions.

Review as a Partial Rights User

As a partial rights user, you do not have permission to certify the Pilot FCC Form 484 Part 3 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 user(s) 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 unless a full-rights user reassigns the form to you for further editing.

Review as a Full Rights User

If you are a full rights user that has received a Pilot FCC Form 484 Part 3 for certification, navigate to the **My Pending Tasks** tab in the Cybersecurity Pilot Program Portal to find the form that has been sent to you for certification.

Full rights users that receive a Pilot FCC Form 484 Part 3 from a partial rights user and full rights users that are completing the form for themselves have two options depending on whether they are the full rights user that will be certifying the form or will be sending it to another full rights user for certification. On the **Review** page:

1. If you will be sending the form to another full rights user for certification: Select **Send for Certification** to send the form to another full rights user(s) in your organization. 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. 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 unless a full rights user reassigns the form to you for further editing.
2. If you are the full rights user that will be certifying the form: Check the box to certify that the information in the record of the Pilot FCC Form 484 Part 3 is correct. Select **Continue to Certification** to continue to the **Certifications** page.

Certifications

Carefully read the certification text. Check each box 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 Pilot FCC Form 484 Part 3, select **Yes** to certify and submit.

When you select **Yes** in response to the confirmation message, the form will be certified and 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.

Certifications

I certify under oath that:

- ☒ I am authorized to submit this application on behalf of the above-named participant 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, and the projected expenditures, disbursements, and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. 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, §§ 1001, 286-287, and 1341, and Title 31, §§ 3729-3730 and 3801-3812).
- ☒ The participant recognizes that it may be audited pursuant to its application, that it will retain for ten years any and all records related to its application, and that, if audited, it shall produce such records at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.
- ☒ I certify and acknowledge, under penalty of perjury, that the schools, libraries, and/or consortia will comply with all applicable Schools and Libraries Cybersecurity Pilot Program rules, requirements, and procedures, including the competitive bidding rules and the requirement to pay the required share of the costs for the supported items from eligible sources.
- ☒ I certify under penalty of perjury, to the best of my knowledge, that the schools, libraries, and/or consortia are not already receiving or expecting to receive other funding (from any source, federal, state, Tribal, local, private, or other) that will pay for the same equipment and/or services, or the same portion of the equipment and/or services, for which I am seeking funding under the Schools and Libraries Cybersecurity Pilot Program.
- ☒ I certify under penalty of perjury, to the best of my knowledge, that all requested equipment and services funded by the Schools and Libraries Cybersecurity Pilot Program will be used for their intended purposes.
- ☒ I certify that I have complied with all responsibilities of participants regarding covered transactions doing business with other persons listed in 2 CFR § 180.300 et seq., including requirements to, among other things, verify that the persons with whom I intend to do business are not excluded or disqualified; and notify the FCC and USAC whether a principal to the transaction is presently excluded or disqualified, has an applicable criminal or civil judgment, is presently indicted for an applicable civil or criminal charge, or has had one or more public transactions terminated in the preceding three years for cause or default. I certify that I have either made the required notifications in writing to the FCC and USAC, or that no notification is required. I have communicated the requirement to comply with these laws to applicable contractors, subcontractors, suppliers, consultants, or their agents when these parties had a material role relating to this supported transaction, are considered a "principal," or the amount of the transaction is at least \$25,000.

Figure 15 | On the **Certifications** page, check each checkbox to confirm that you understand and will comply/have complied with each certification.

Certifications

Certification text follows for your reference.

I certify under oath that:

- I am authorized to submit this application on behalf of the above-named participant 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, and the projected expenditures, disbursements, and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. 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, §§ 1001, 286-287, and 1341, and Title 31, §§ 3729-3730 and 3801-3812).
- The participant recognizes that it may be audited pursuant to its application, that it will retain for ten years any and all records related to its application, and that, if audited, it shall produce such records at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.
- I certify and acknowledge, under penalty of perjury, that the schools, libraries, and/or consortia will comply with all applicable Schools and Libraries Cybersecurity Pilot Program rules, requirements, and procedures, including the competitive bidding rules and the requirement to pay the required share of the costs for the supported items from eligible sources.
- I certify under penalty of perjury, to the best of my knowledge, that the schools, libraries, and/or consortia are not already receiving or expecting to receive other funding (from any source, federal, state, Tribal, local, private, or other) that will pay for the same equipment and/or services, or the same portion of the equipment and/or services, for which I am seeking funding under the Schools and Libraries Cybersecurity Pilot Program.

- I certify under penalty of perjury, to the best of my knowledge, that all requested equipment and services funded by the Schools and Libraries Cybersecurity Pilot Program will be used for their intended purposes.
- I certify that I have complied with all responsibilities of participants regarding covered transactions doing business with other persons listed in 2 CFR § 180.300 *et seq.*, including requirements to, among other things, verify that the persons with whom I intend to do business are not excluded or disqualified; and notify the FCC and USAC whether a principal to the transaction is presently excluded or disqualified, has an applicable criminal or civil judgment, is presently indicted for an applicable civil or criminal charge, or has had one or more public transactions terminated in the preceding three years for cause or default. I certify that I have either made the required notifications in writing to the FCC and USAC, or that no notification is required. I have communicated the requirement to comply with these laws to applicable contractors, subcontractors, suppliers, consultants, or their agents when these parties had a material role relating to this supported transaction, are considered a “principal,” or the amount of the transaction is at least \$25,000.

After Certifying and Submitting

After you have certified your Pilot FCC Form 484 Part 3 and it is received by USAC, it is considered submitted and all users with full, partial, or view-only access rights to the form will receive a certification acknowledgement email. This notification confirms that the form has been certified and submitted.

Form Assistance

If you have any questions about completing the Pilot FCC Form 484 Part 3, please contact the USAC Customer Service Center (CSC) at (888) 203-8100 between 8 a.m. and 8 p.m. E.T. Monday through Friday.

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

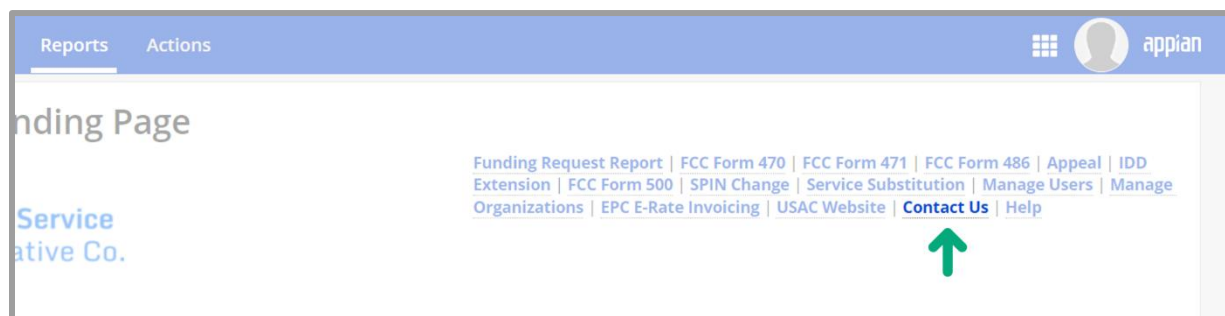


Figure 16 | Click **Contact Us** on your EPC landing page to create a customer service case.