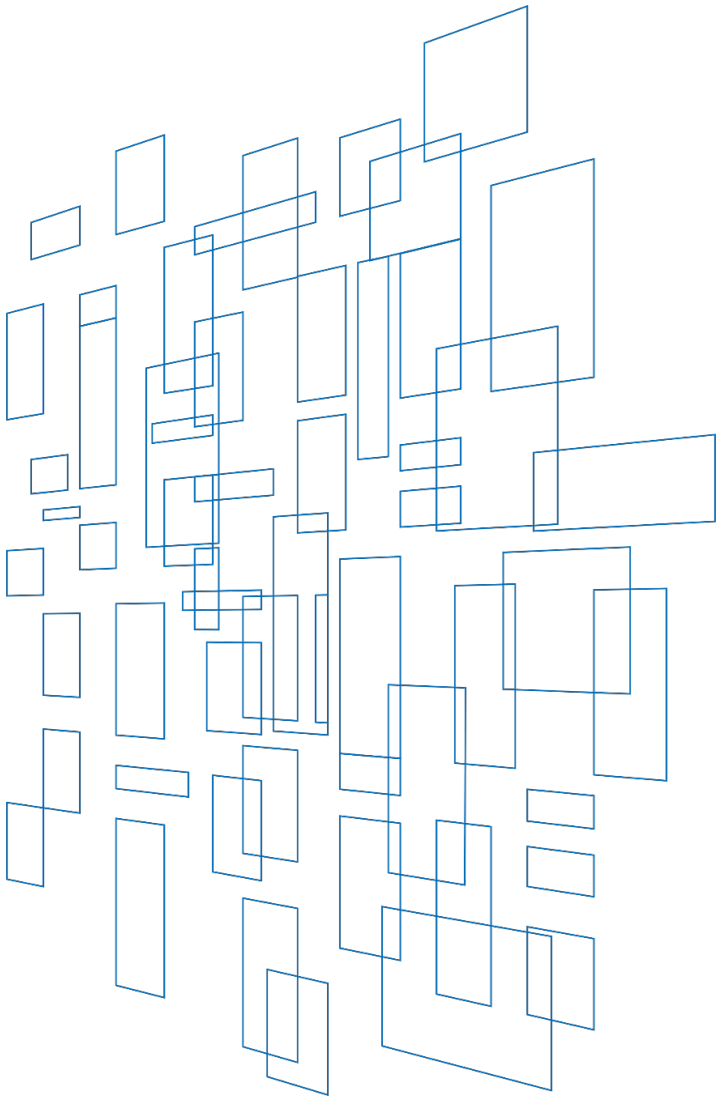

Schools and Libraries Cybersecurity Pilot Program Application User Guide

FCC Form 484 Part 2

Created/Revised January 2025

Universal Service Administrative Co.

Contents

User Roles and Permissions 4
Navigating to the CBR Dashboard 6
Starting the Pilot FCC Form 484 Part 2 7
Form Navigation 7
Progress Bar 7
Saving or Discarding the Pilot FCC Form 484 Part 2 8
Exiting the Form and Returning Later 8
Milestones and Sections 9
Required Fields 10
Pop-Up Confirmation Messages 10
Conditional Questions 10
Multiselect Dropdown Fields 11
Pilot FCC Form 484 Part 2 Form Overview 12
Start 12
Basic Information 12
Participant Selection 12
Cybersecurity Plan 13
1. Proposed Plan 13
2. Project Details 14
3. Cybersecurity Application Sec. 1 18
4. Cybersecurity Application Sec. 2 20
5. Cybersecurity Application Sec. 3 25
6. Cybersecurity Challenges 27
Supporting Documentation 28
Review 28
Certifications 30
After Certifying and Submitting 30
Form Assistance 31

Universal Service Administrative Co.

This Schools and Libraries Cybersecurity Pilot Program (Pilot Program or Pilot) Application User Guide provides guidance on the requirements and processes for submitting and completing the Pilot FCC Form 484 Part 2 for selected Pilot participants.

In contrast to the Pilot FCC Form 484 Part I, Pilot FCC Form 484 Part 2 collects more detailed cybersecurity data and Pilot project information, but only from those who are selected as Pilot participants. The data gathered from the Pilot will help the FCC evaluate whether, and to what extent, it should use the Universal Service Fund to support the cybersecurity needs of eligible schools and libraries going forward.

We recognize that the cybersecurity-related information that is being requested and provided in the Pilot FCC Form 484 Part 2 supplemental questions 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 2 data will be protected by security protections built into USAC's Pilot portal.

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

Universal Service Administrative Co.

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 2 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 being 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 2, 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 484 Permission** for each user
6. Click **Submit**

Universal Service Administrative Co.

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

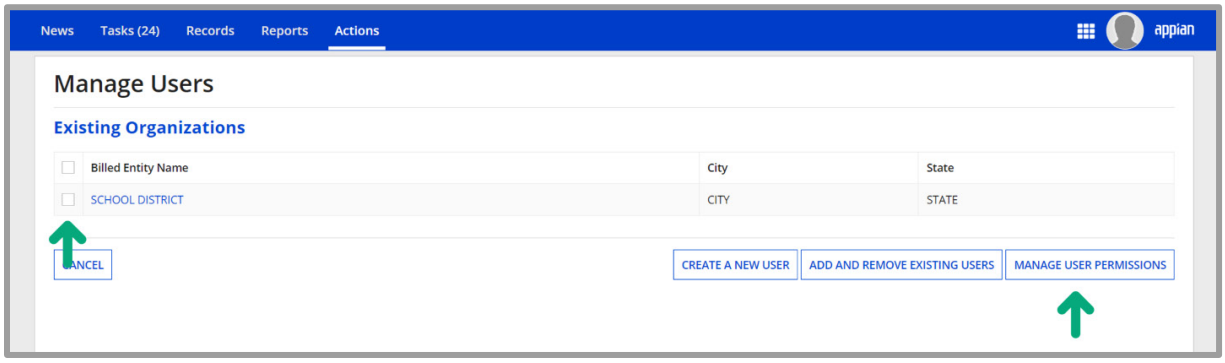

Figure 2 | On the Manage Users page, check the checkbox next to your entity and click Manage User Permissions.

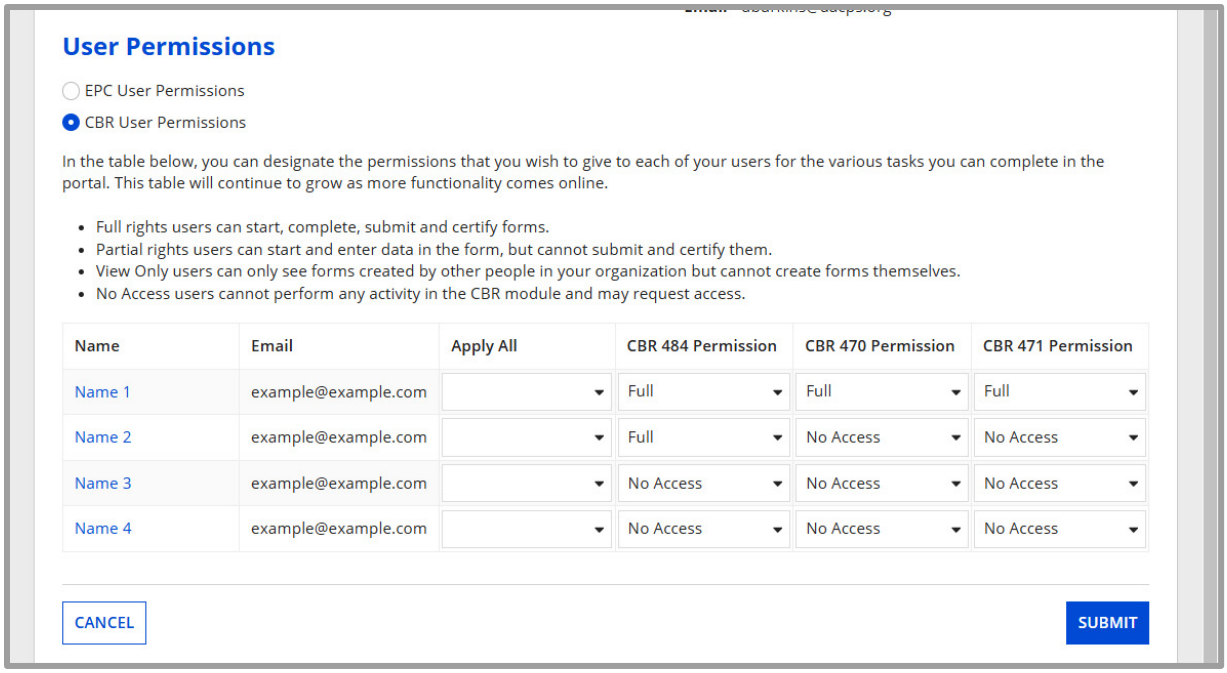

Figure 3 | On the Manage User Permissions page, select the permissions you wish to give to each user in the CBR 484 Permission column, then click Submit.

Universal Service Administrative Co.

Navigating to the CBR Dashboard

The **CBR Dashboard** can be used to access the various forms needed to 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**.

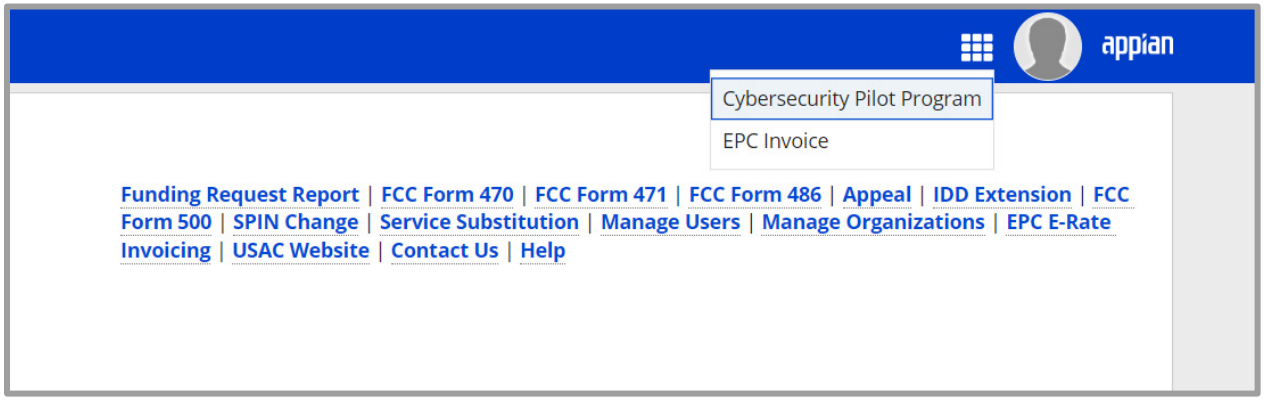

Figure 4 | From the EPC landing page, click the navigation waffle and choose Cybersecurity Pilot Program.

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

Universal Service Administrative Co.

Starting the Pilot FCC Form 484 Part 2

In the **My Organization(s)** tab on the CBR Dashboard, click **Actions** in the **Action** column, then **Create CBR FCC Form 484 Part 2**.

*Figure 6 | Click **Actions**, then **Create CBR FCC Form 484 Part 2** in the **Action** column on the CBR Dashboard to begin the form.*

Form Navigation

Progress Bar

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

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

Universal Service Administrative Co.

Saving or Discarding the Pilot FCC Form 484 Part 2

The bottom of each Pilot FCC Form 484 Part 2 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 & 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 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.

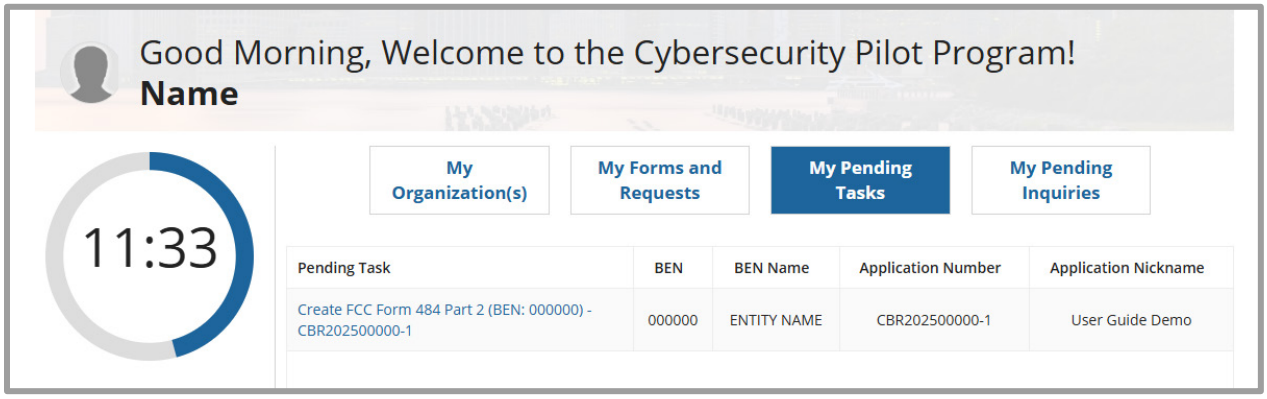

*Figure 9 | To resume editing the form, select the task name on the **My Pending Tasks** tab on the CBR Dashboard.*

Universal Service Administrative Co.

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 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** milestone. You can navigate between sections using the side navigation or the **Next** and **Previous** buttons at the bottom of the section.

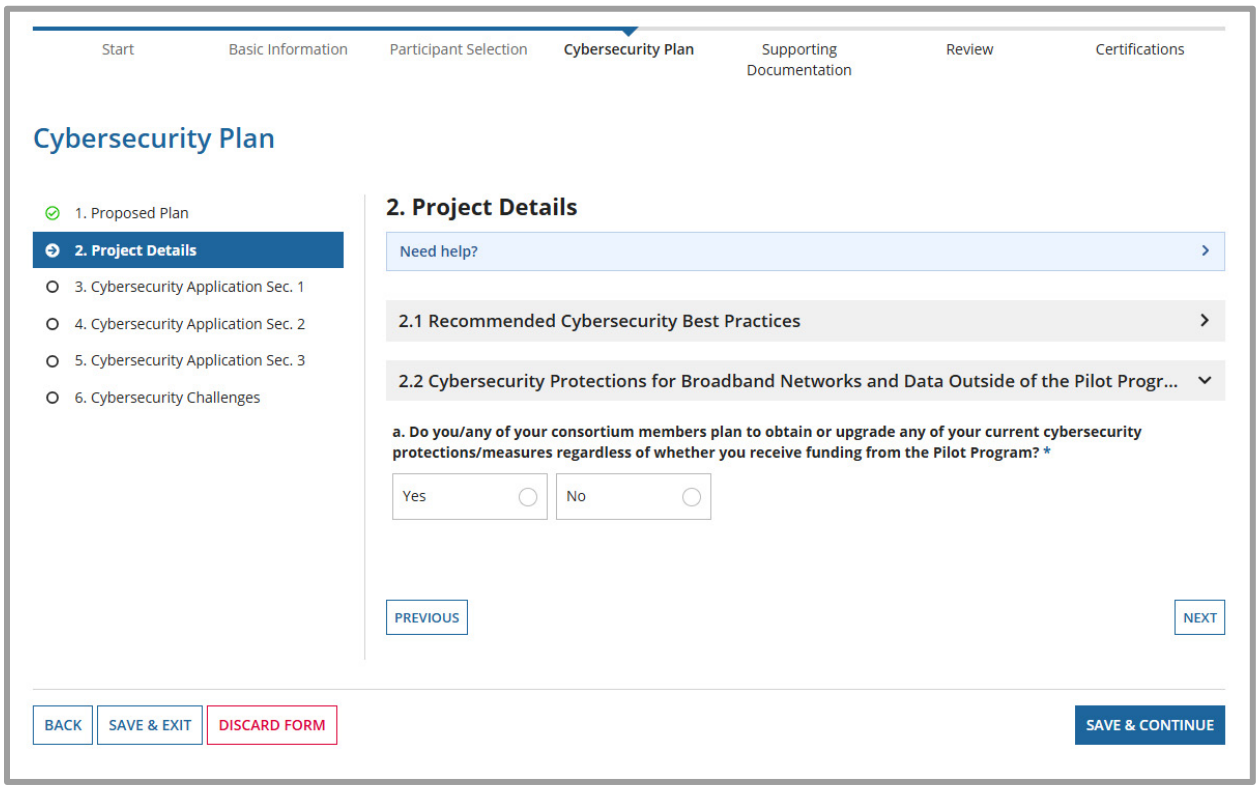

*Figure 10 | Navigate between milestones using the progress bar or the **Save & Continue** and **Back** buttons. Navigate between sections using the side navigation or **Next** and **Previous** buttons.*

Universal Service Administrative Co.

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, 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.

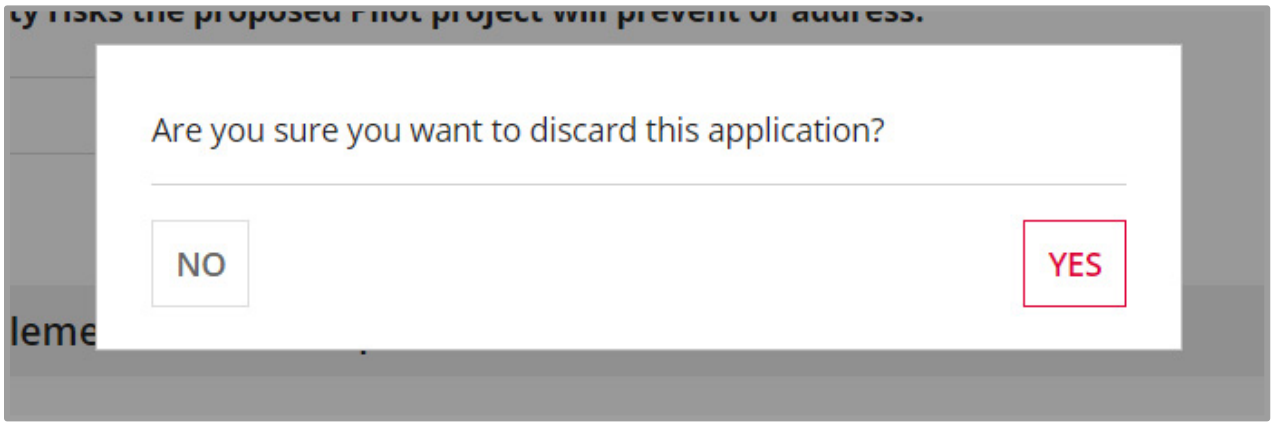

*Figure 12 | When you select **Discard Form,** a pop-up message asks you to confirm that you want to discard your application.*

Conditional Questions

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

In this User Guide, conditional questions are indicated by 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.

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.

Universal Service Administrative Co.

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.

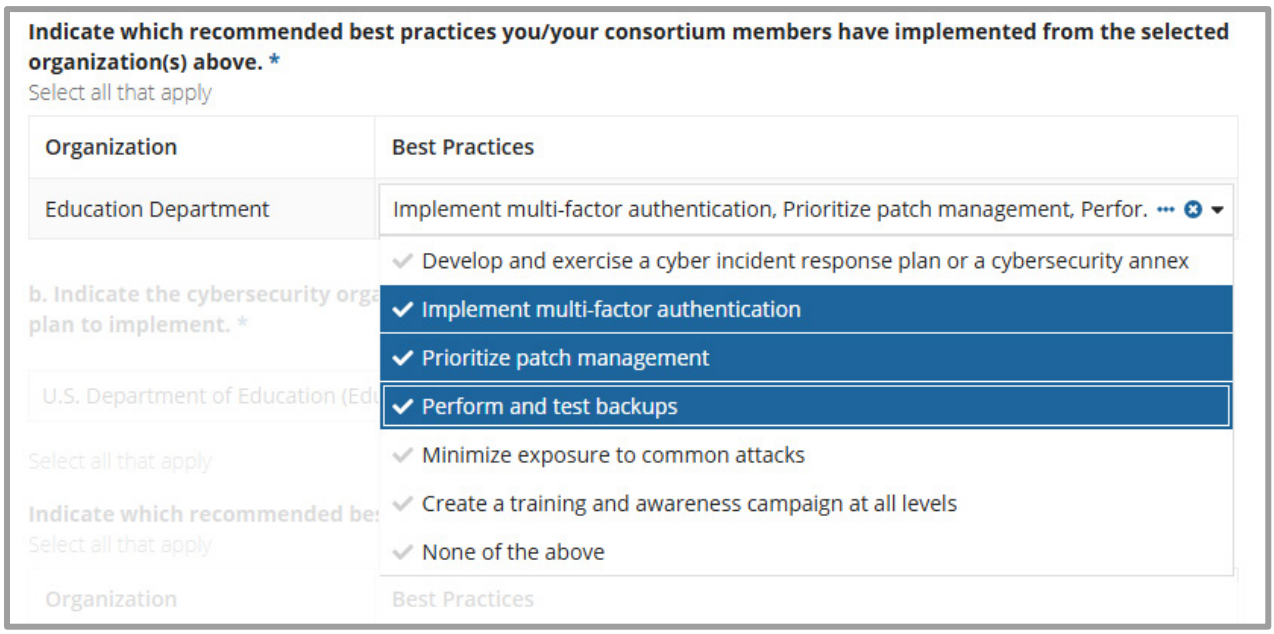

Figure 13 | In a multiselect dropdown field, selected items are highlighted in blue and appear in the top row.

Universal Service Administrative Co.

Pilot FCC Form 484 Part 2 Form Overview

Please reference your Pilot FCC Form 484 Part 1 as you complete this form. To download a PDF version of your certified and submitted Pilot FCC Form 484 Part 1:

1. Navigate to the **My Forms and Requests** tab on the CBR Dashboard.
2. From the **Application Type** dropdown, choose FCC Form 484 Part 1.
3. Click the application number.
4. This takes you to the FCC Decision Copy tab on the Summary page. Click **Generated Documents** in the left-side navigation pane to download your Certified PDF.

There are seven milestones that make up the **FCC Form 484 Part 2: Start**, **Basic Information**, **Participant Selection**, **Cybersecurity Plan**, **Supporting Documentation**, **Review**, and **Certifications**. Each milestone is discussed below.

Start

On the **Start** page, 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.

Participant Selection

On the **Participant Selection** page, review the list of participating entities. If you are completing the Pilot FCC Form 484 Part 2 for a consortium, school district, or library system, this page displays all entities you selected on the Pilot FCC Form 484 Part 1 to be included in your application to participate in the Pilot Program. If you are completing the form as an individual school or library, only your school or library will be listed on this page.

The information on the Participant Selection page cannot be edited. Members and child entities cannot be changed from the selections made in the Pilot FCC Form 484 Part 1.

Universal Service Administrative Co.

Cybersecurity Plan

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

Answering for a Consortium

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

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

1. Proposed Plan

1.1 Correction of Known Security Flaws and Routine Backups

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

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

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

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

Universal Service Administrative Co.

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

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

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

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

2. Project Details

2.1 Recommended Cybersecurity Best Practices

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

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

Universal Service Administrative Co.

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

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

Universal Service Administrative Co.

Changing Your Organization Selections

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

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

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

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

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

Universal Service Administrative Co.

Recommended Best Practices

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

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

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

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

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

Universal Service Administrative Co.

3. Cybersecurity Application Sec. 1

3.1 Current Cybersecurity Practices and Resources

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

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

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

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

Universal Service Administrative Co.

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

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

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

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

Equipment and Services

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

Universal Service Administrative Co.

4. Cybersecurity Application Sec. 2

4.1 History of Cyber Threats and Attacks

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

- ○ 0
- ○ 1-3
- ○ 4-6
- ○ 6+

Cyber Incident

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

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

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

Universal Service Administrative Co.

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

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

Cybersecurity Incident Time Period

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

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

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

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

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

Universal Service Administrative Co.

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

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

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

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

Universal Service Administrative Co.

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

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

Direct Cost

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

Universal Service Administrative Co.

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

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

Indirect Cost

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

Universal Service Administrative Co.

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

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

5. Cybersecurity Application Sec. 3

5.1 Cybersecurity Training

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

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

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

Bi-Weekly and Bi-Annually

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

Universal Service Administrative Co.

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

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

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

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

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

- ☐ Online
- ☐ In Person
- ☐ Hybrid

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

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

Universal Service Administrative Co.

6. Cybersecurity Challenges

6.1 Non-monetary Challenges

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

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

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

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

Universal Service Administrative Co.

Supporting Documentation

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

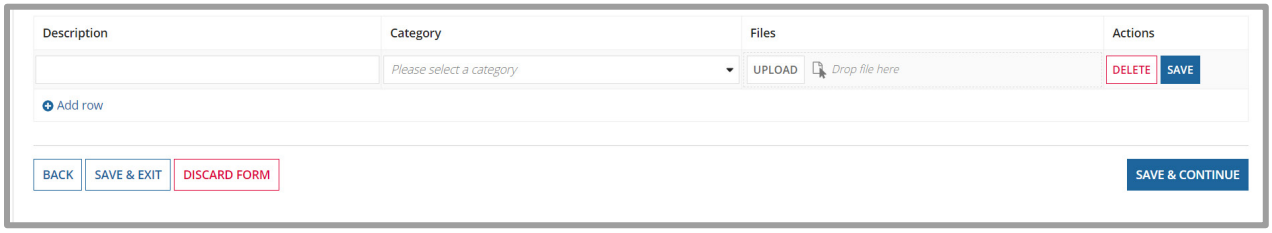

*Figure 14 | On the **Supporting Documentation** page, upload any supporting documents that are requested, required, or you want USAC and the FCC to consider along with the second part of your application. Enter a file description and select a category.*

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 a PDF has been successfully generated, 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.

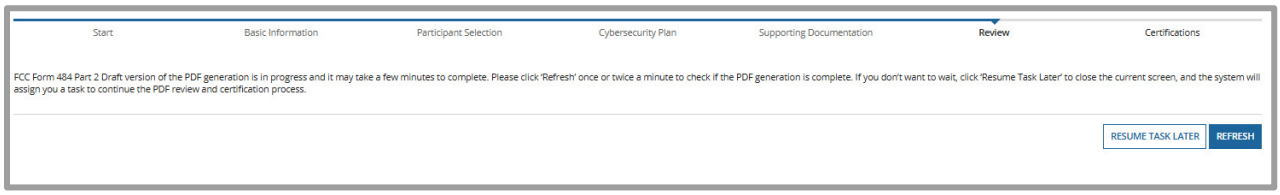

*Figure 15 | When you reach the **Review** page, it may take a few minutes for the system to generate and load a PDF version of the form.*

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.

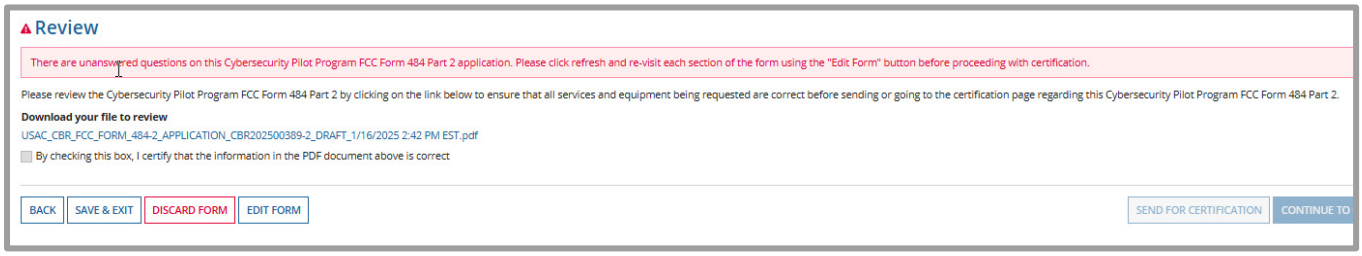

*Figure 16 | A message on the **Review** page will alert you if there are unanswered questions on the form. You will not be able to proceed to the **Certifications** page for the form until you answer all the required questions.*

To review the form:

1. Click the PDF file name to download the PDF version of your Pilot FCC Form 484 Part 2 for review.
2. The options on the **Review** page depend on whether you have been given partial or a full-rights user permissions.

Review as a Partial Rights User

As a partial rights user, you don't have permission to certify the Pilot FCC Form 484 Part 2 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.

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 Pilot FCC Form 484 Part 2 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 for certification: Select **Send for Certification** to send the form to other 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.
2. If you are the full rights user that will be certifying the form: Check the box to certify that the information in the PDF version of the Pilot FCC Form 484 Part 2 is correct. Select **Continue to Certification** to continue to the **Certifications** page.

Universal Service Administrative Co.

Certifications

On the Certifications page, 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 2, 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.

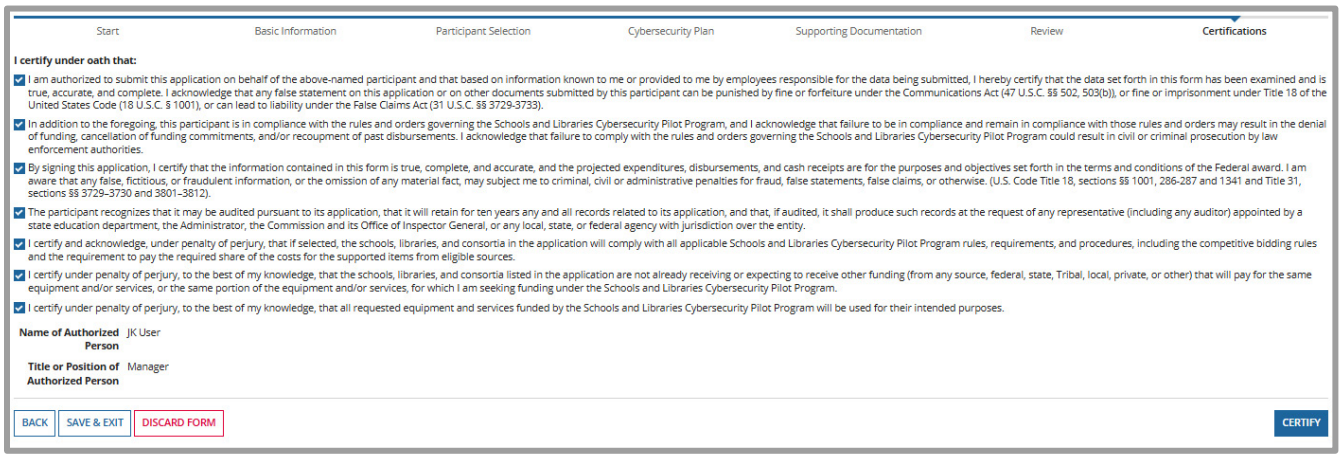

*Figure 17 | On the **Certifications** page, check each checkbox to confirm that you understand and will comply/have complied with each certification.*

After Certifying and Submitting

After you have certified your Pilot FCC Form 484 Part 2 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.

Universal Service Administrative Co.

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. 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.**

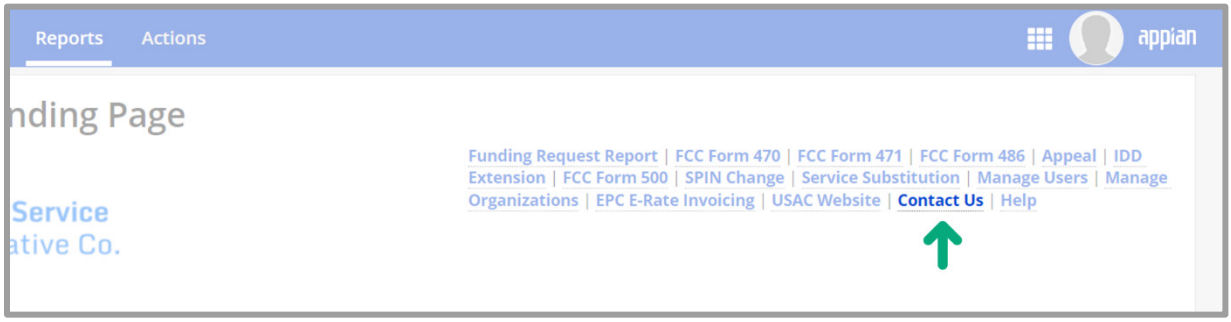

*Figure 18 | Click **Contact Us** on your EPC landing page to create a customer service case.*