Available for Public Use

Schools & Libraries Cybersecurity Pilot Program: Pilot FCC Form 484 Part 2

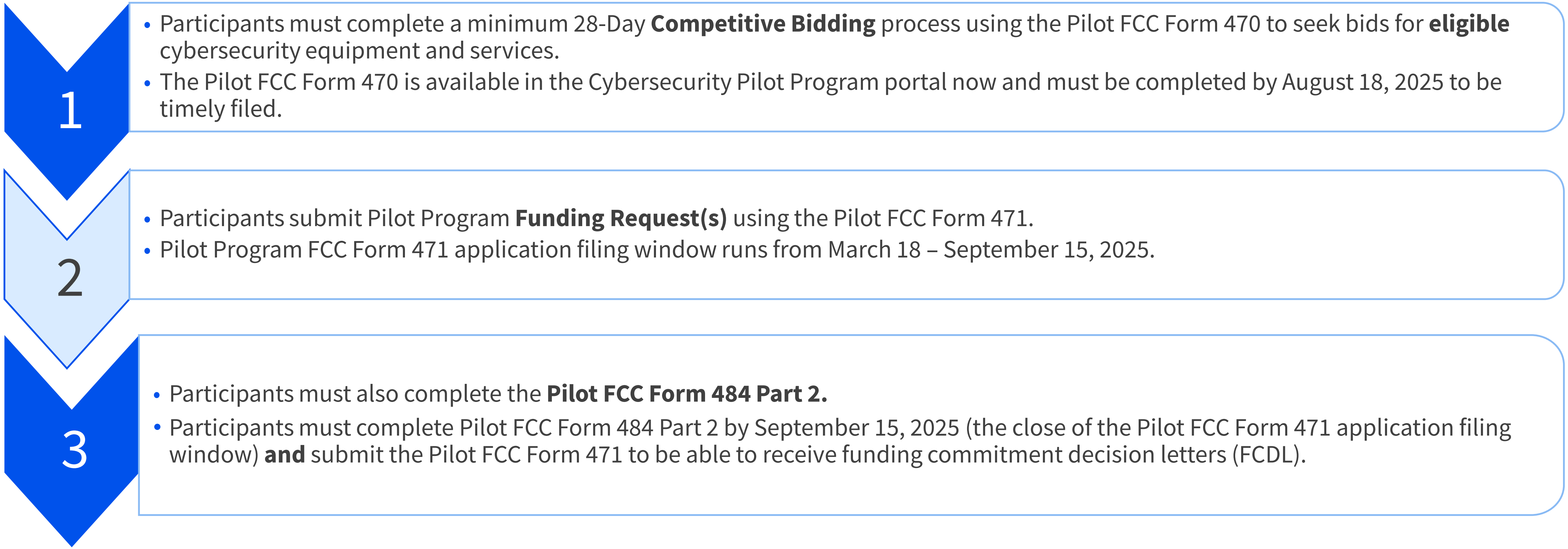
Universal Service
Administrative Co.

Housekeeping

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

Pilot Program: Process and Timeline

Pilot Program Participants: Timeline



1

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

2

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

3

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

Pilot Program:
FCC Form 484 Part 2 Overview

Pilot Program: FCC Form 484 Part 2 Overview

- In contrast to Part 1 of the 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 (USF) to support the cybersecurity needs of eligible schools and libraries going forward.

Pilot Program: FCC Form 484 Part 2 Overview

- Pilot participants must complete the Pilot FCC Form 484 Part 2 by the close of the Pilot FCC Form 471 window on **September 15, 2025, at 11:59 p.m. E.T.**
- Pilot participants who do not complete the Pilot FCC Form 484 Part 2 by the close of the window will be subject to removal from the Pilot and will not be eligible to receive Pilot Program funding.
- Pilot participants can access the Pilot FCC Form 484 Part 2 in the Cybersecurity Pilot Program portal. Detailed information about how to complete Part 2 of the form is provided in the FCC Form 484 Part 2 User Guide.
- For questions about, or help completing, Part 2 of the form, Pilot participants can contact the USAC Customer Service Center at (888) 203-8100 between 8 a.m. and 8 p.m. E.T. Monday through Friday.

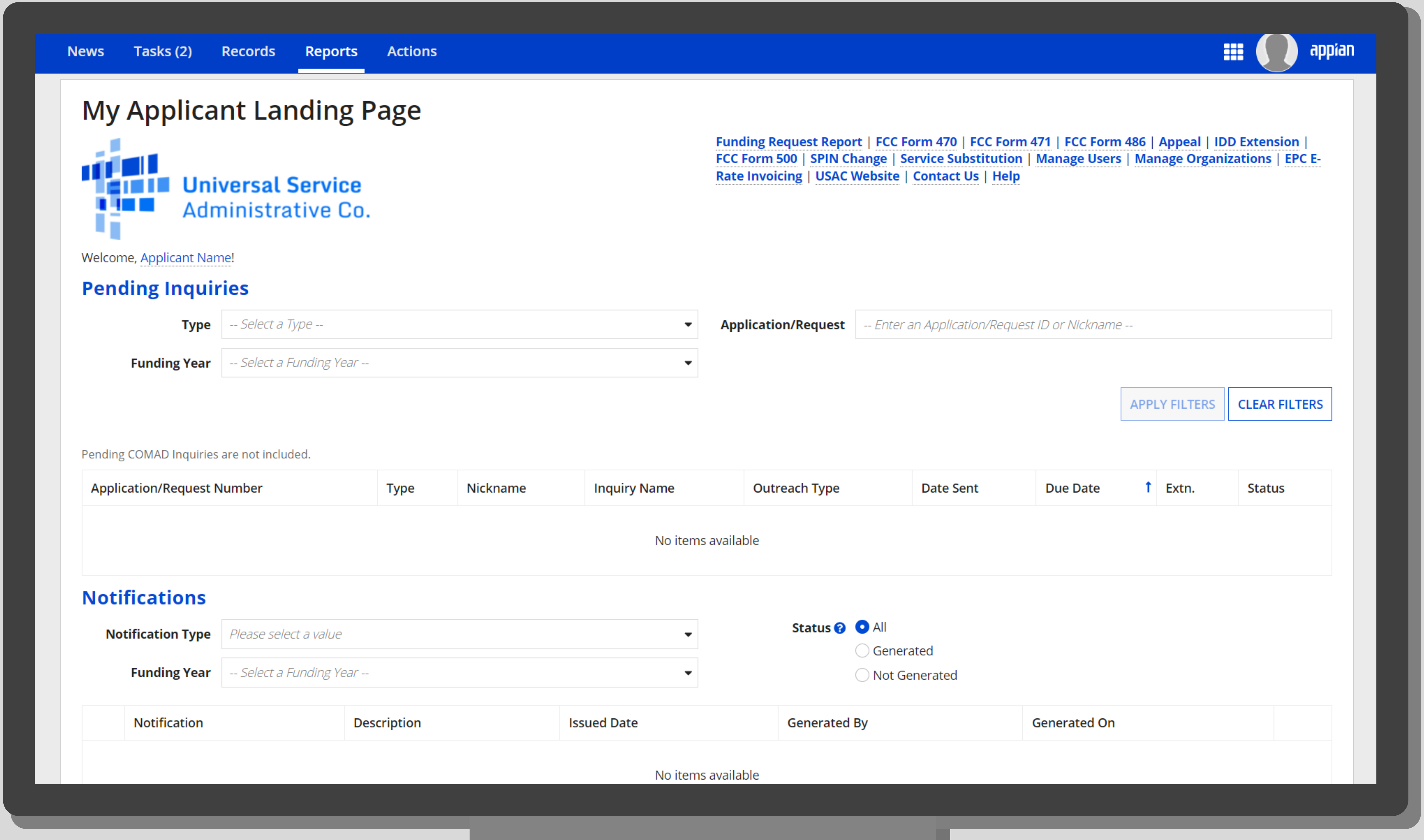
Pilot Program: FCC Form 484 Part 2 Overview

- Due to the sensitive nature of the data being collected in the Pilot FCC Form 484 Part 2, and the Pilot Program generally, consultant access to participants' forms, including the Pilot FCC Form 484 Part 2, is limited to **three consultants per form.**
- This means that, even if a Pilot participant's consultant information in its E-Rate Productivity Center (EPC) Account Profile lists more than three consultants, a participant must select and grant a consultant form-specific user rights for the consultant to have access a particular Pilot Program form.

Questions?

Pilot Program:
Pilot FCC Form 484 Part 2 Walkthrough

Pilot FCC Form 484 Part 2 Walkthrough: Getting Started



My Applicant Landing Page

Universal Service Administrative Co.

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

Welcome, Applicant Name!

Pending Inquiries

Type: -- Select a Type --

Application/Request: -- Enter an Application/Request ID or Nickname --

Funding Year: -- Select a Funding Year --

Pending COMAD Inquiries are not included.

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

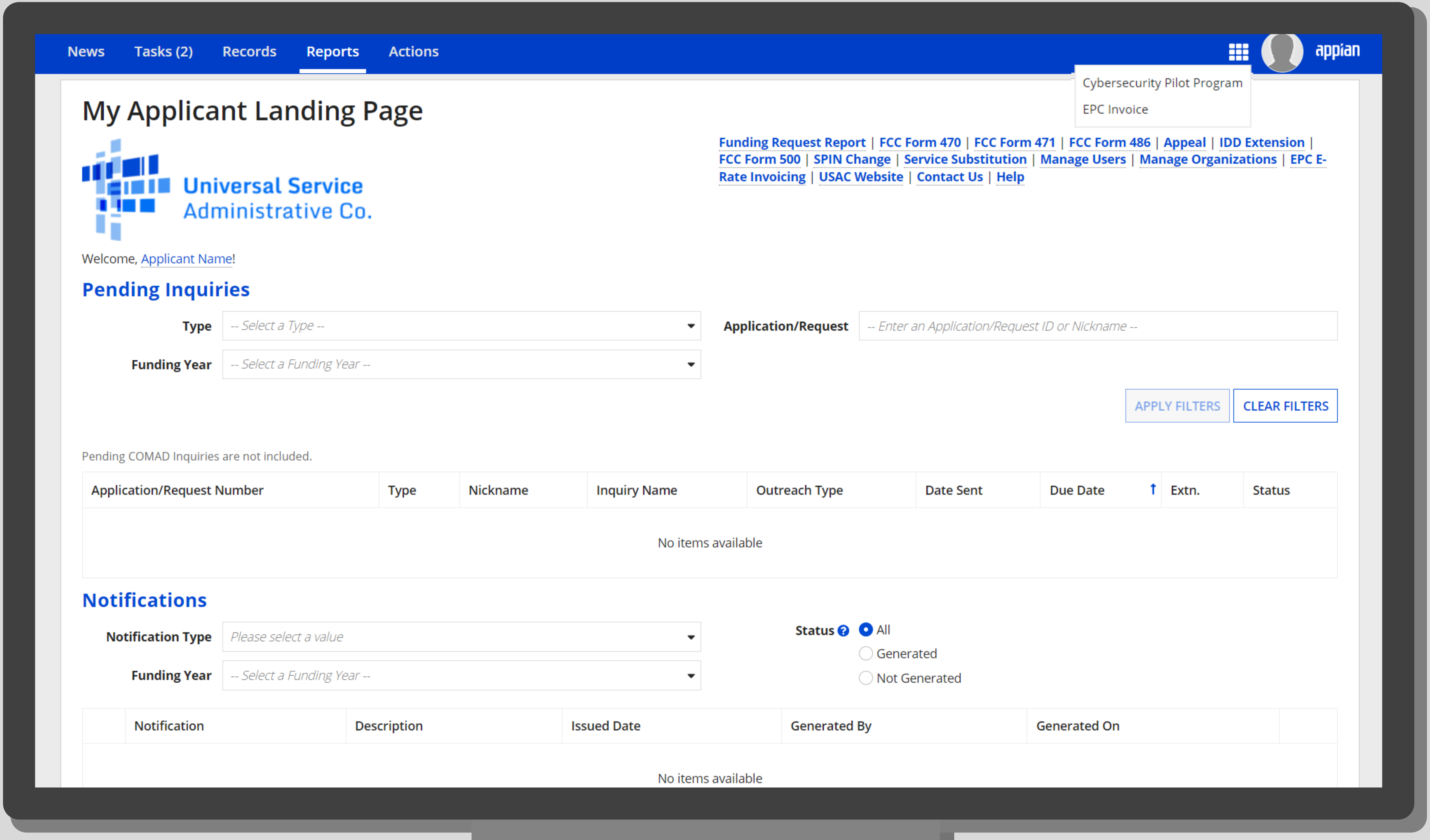
Notifications

Notification Type: Please select a value

Funding Year: -- Select a Funding Year --

Status ? ● All ○ Generated ○ Not Generated

	Notification	Description	Issued Date	Generated By	Generated On	
No items available						



My Applicant Landing Page

Universal Service Administrative Co.

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

Welcome, Applicant Name!

Pending Inquiries

Type: -- Select a Type --

Application/Request: -- Enter an Application/Request ID or Nickname --

Funding Year: -- Select a Funding Year --

APPLY FILTERS | CLEAR FILTERS

Pending COMAD Inquiries are not included.

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

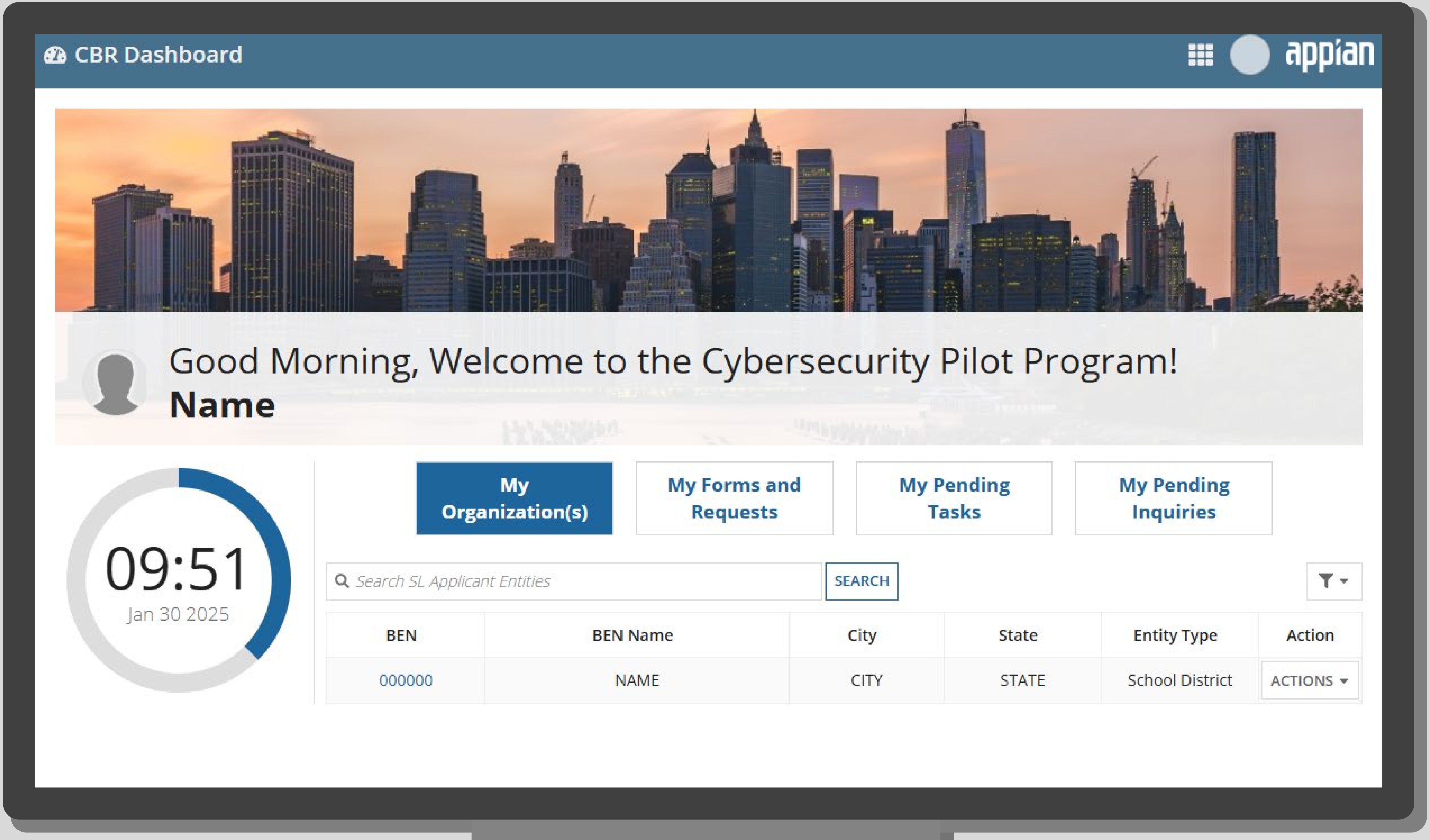
Notifications

Notification Type: Please select a value

Funding Year: -- Select a Funding Year --

Status ?
● All
○ Generated
○ Not Generated

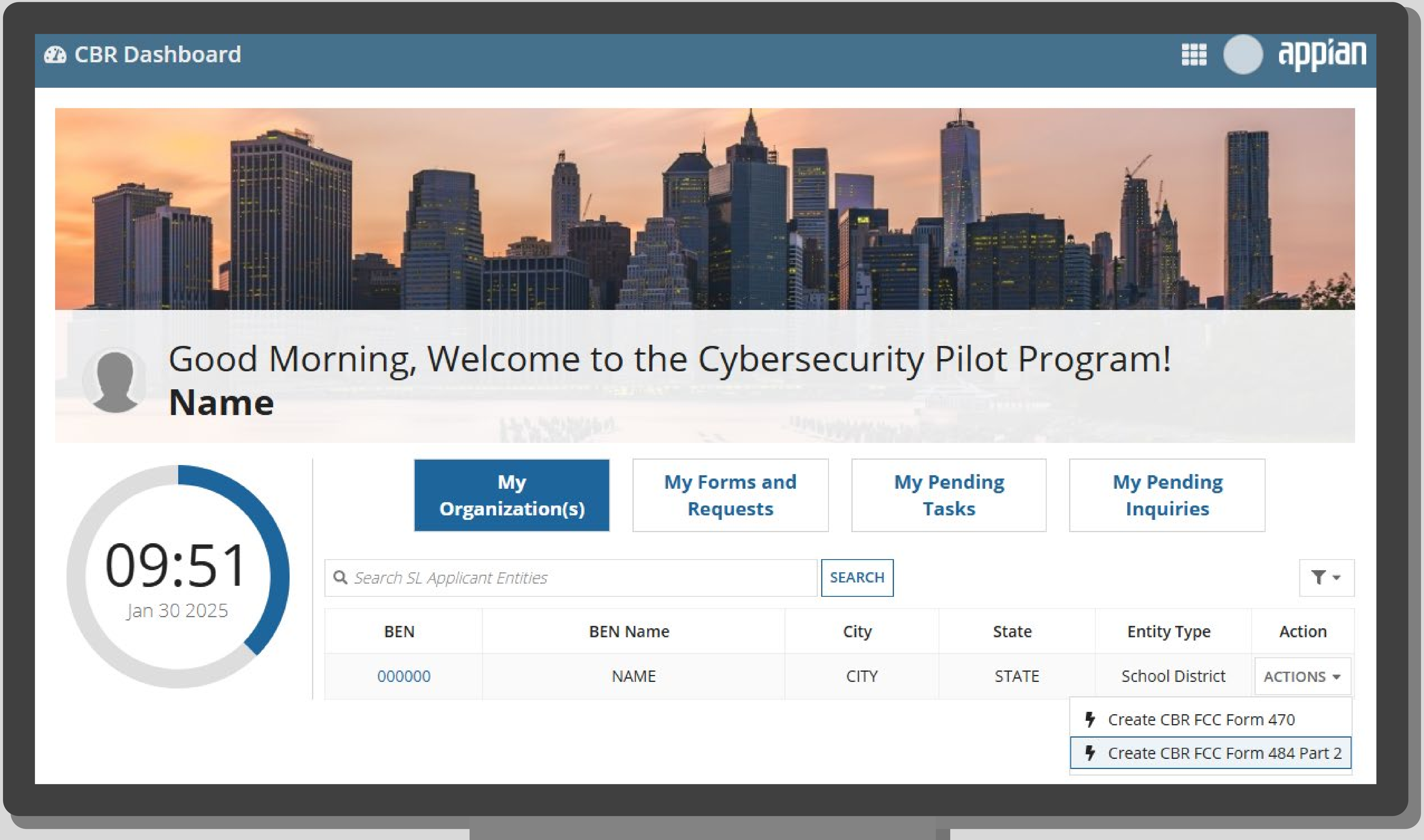
	Notification	Description	Issued Date	Generated By	Generated On	
No items available						



Good Morning, Welcome to the Cybersecurity Pilot Program!
Name

09:51
Jan 30 2025

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

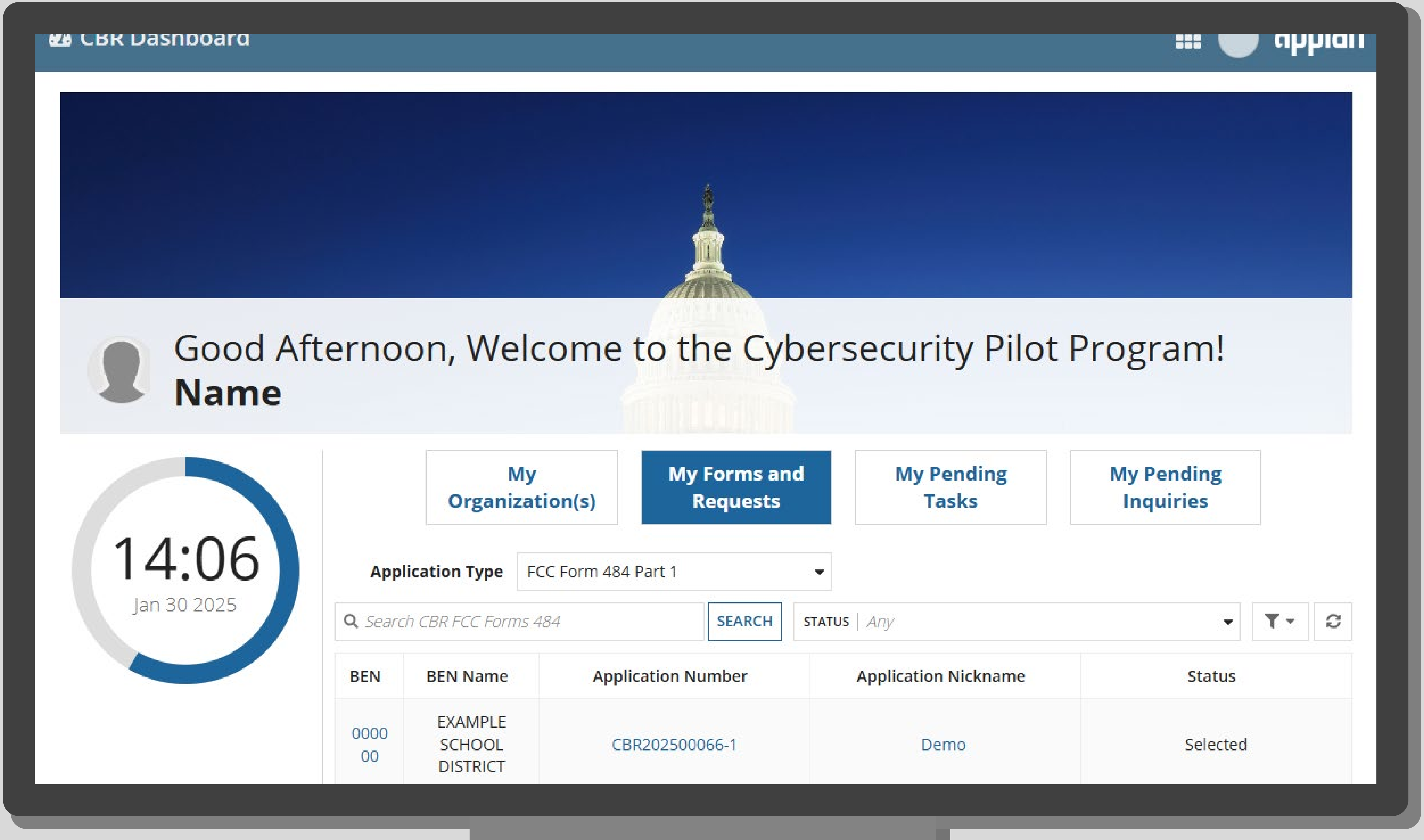


Good Morning, Welcome to the Cybersecurity Pilot Program!
Name

09:51
Jan 30 2025

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

Pilot FCC Form 484 Part 2 Walkthrough: Download FCC Form 484 Part 1



CBR Dashboard

appian

Good Afternoon, Welcome to the Cybersecurity Pilot Program!

Name

14:06

Jan 30 2025

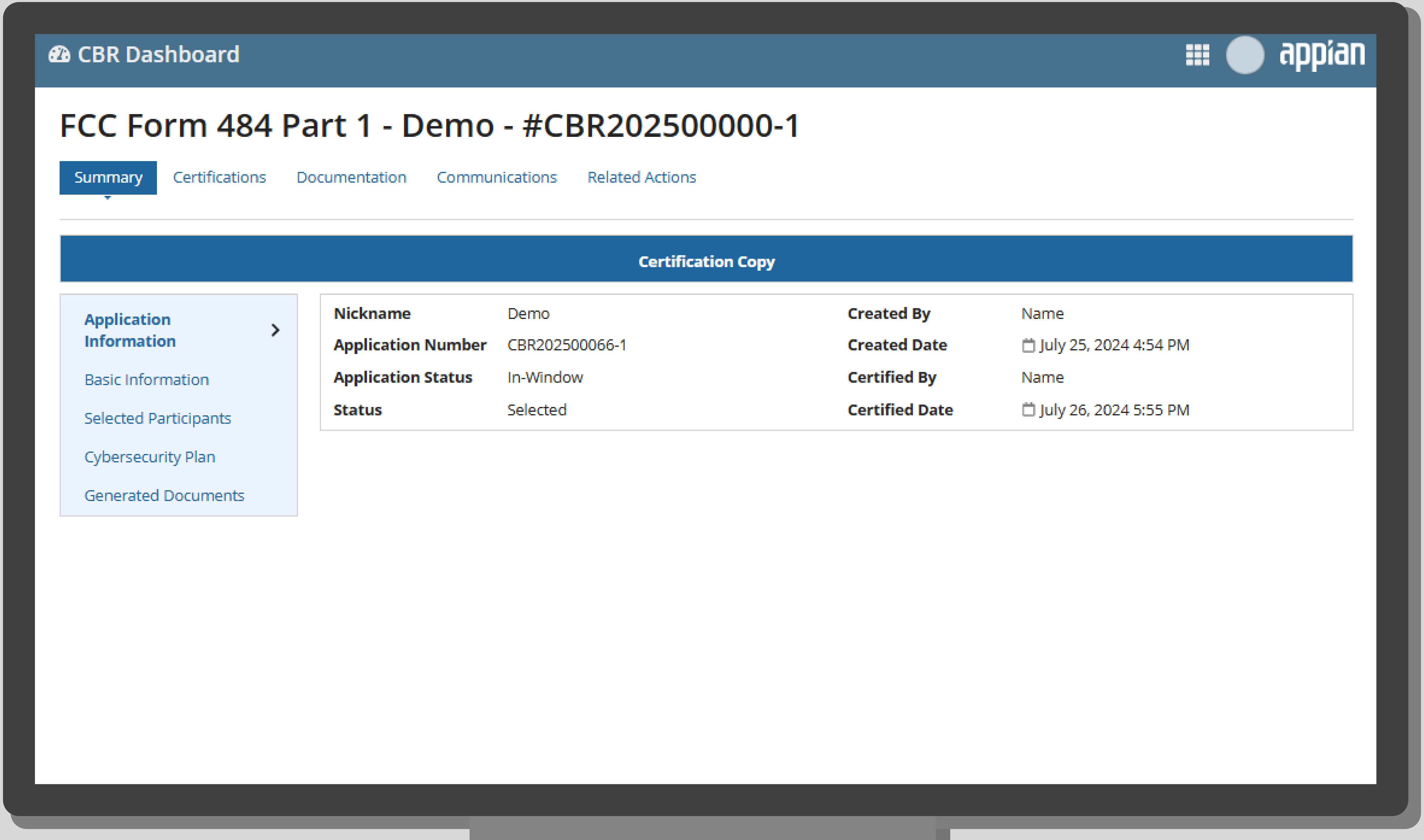
My Organization(s) | My Forms and Requests | My Pending Tasks | My Pending Inquiries

Application Type FCC Form 484 Part 1

Search CBR FCC Forms 484 SEARCH

STATUS Any

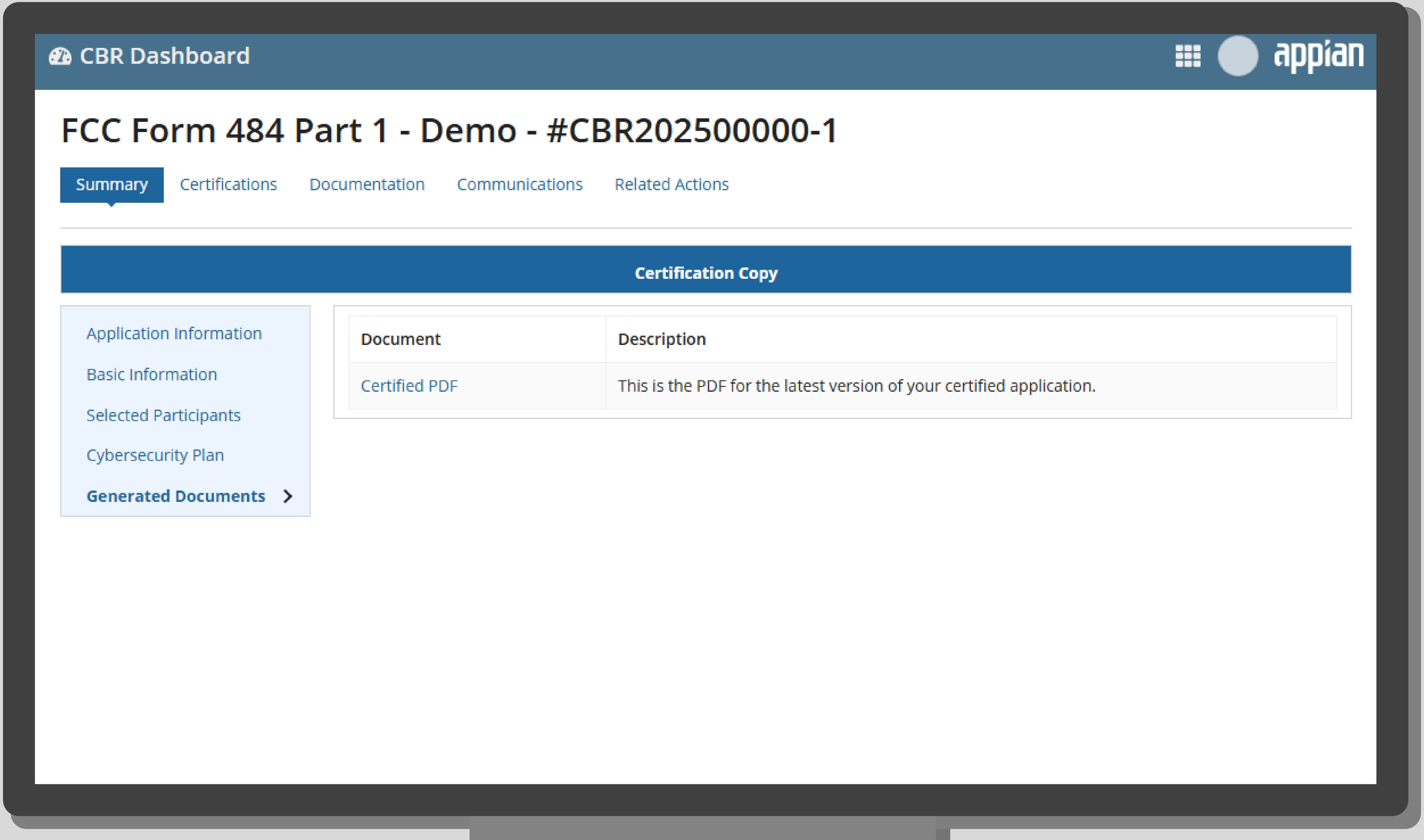
BEN	BEN Name	Application Number	Application Nickname	Status
000000	EXAMPLE SCHOOL DISTRICT	CBR202500066-1	Demo	Selected



FCC Form 484 Part 1 - Demo - #CBR202500000-1

Certification Copy

Nickname	Demo	**Created By**	Name
Application Number	CBR202500066-1	**Created Date**	July 25, 2024 4:54 PM
Application Status	In-Window	**Certified By**	Name
Status	Selected	**Certified Date**	July 26, 2024 5:55 PM

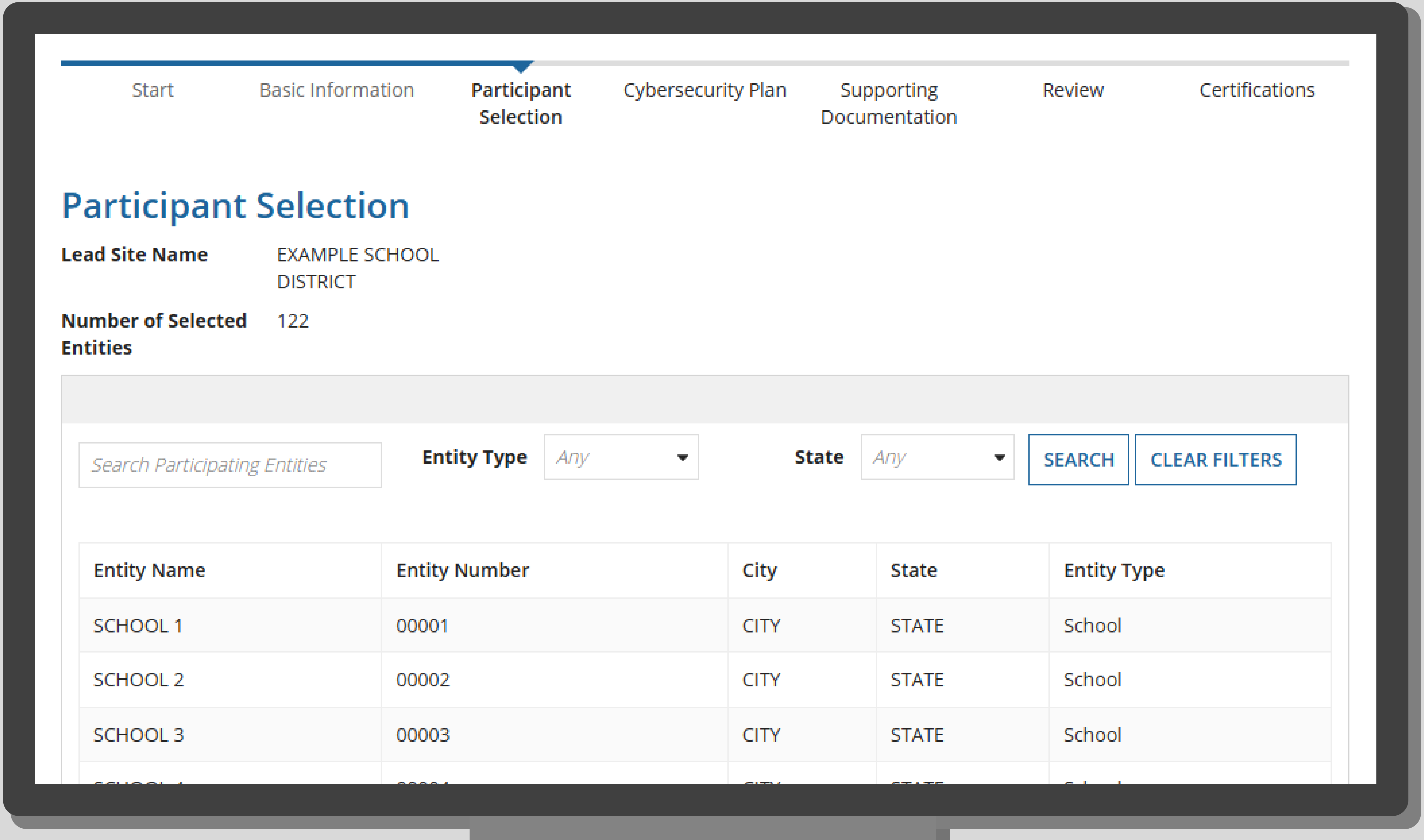


FCC Form 484 Part 1 - Demo - #CBR202500000-1

Certification Copy

Document	Description
Certified PDF	This is the PDF for the latest version of your certified application.

Pilot FCC Form 484 Part 2 Walkthrough: Participant Selection

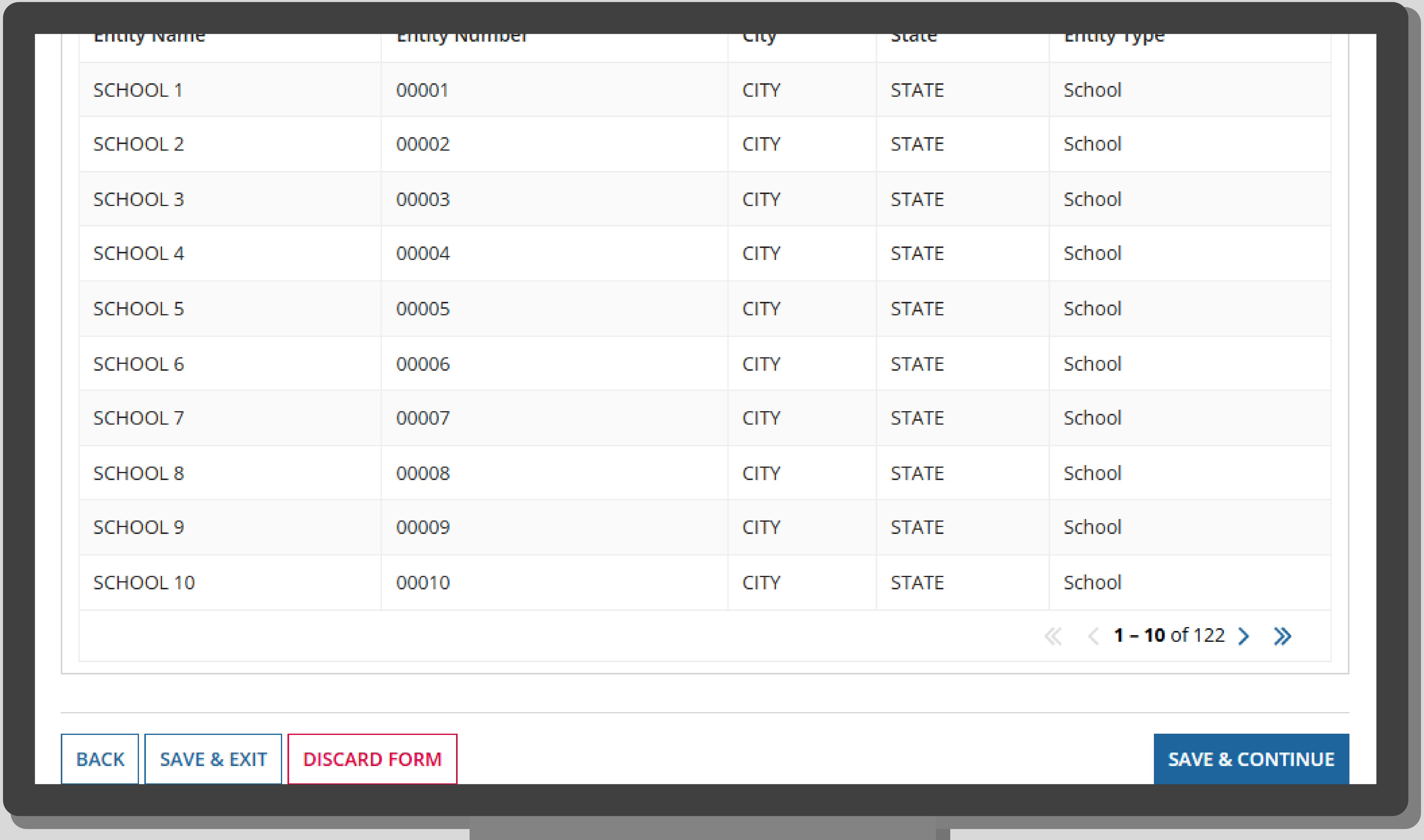


Participant Selection

Lead Site Name EXAMPLE SCHOOL DISTRICT

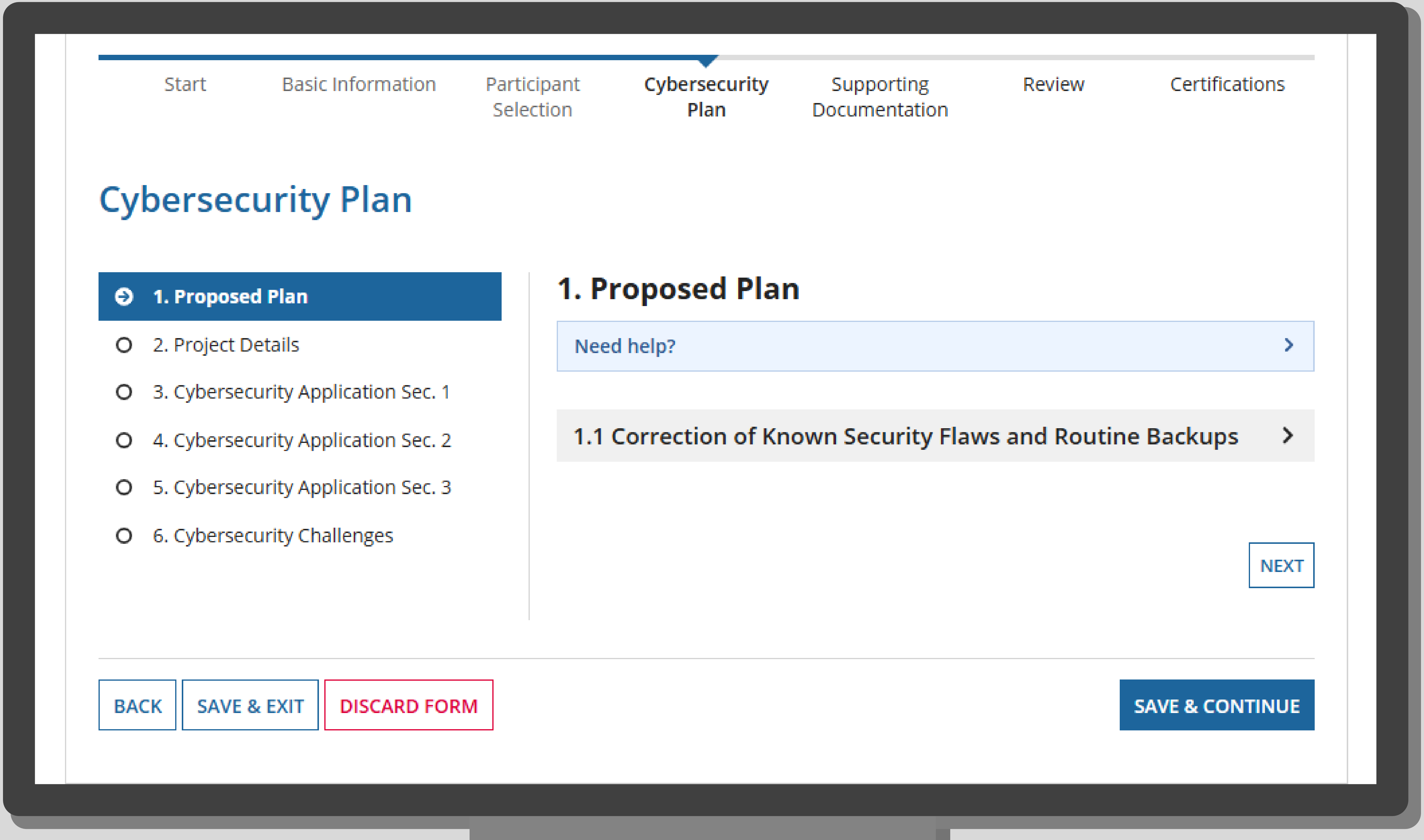
Number of Selected Entities 122

Entity Name	Entity Number	City	State	Entity Type
SCHOOL 1	00001	CITY	STATE	School
SCHOOL 2	00002	CITY	STATE	School
SCHOOL 3	00003	CITY	STATE	School
SCHOOL 4	00004	CITY	STATE	School



Entity Name	Entity Number	City	State	Entity Type
SCHOOL 1	00001	CITY	STATE	School
SCHOOL 2	00002	CITY	STATE	School
SCHOOL 3	00003	CITY	STATE	School
SCHOOL 4	00004	CITY	STATE	School
SCHOOL 5	00005	CITY	STATE	School
SCHOOL 6	00006	CITY	STATE	School
SCHOOL 7	00007	CITY	STATE	School
SCHOOL 8	00008	CITY	STATE	School
SCHOOL 9	00009	CITY	STATE	School
SCHOOL 10	00010	CITY	STATE	School

Pilot FCC Form 484 Part 2 Walkthrough: Cybersecurity Plan

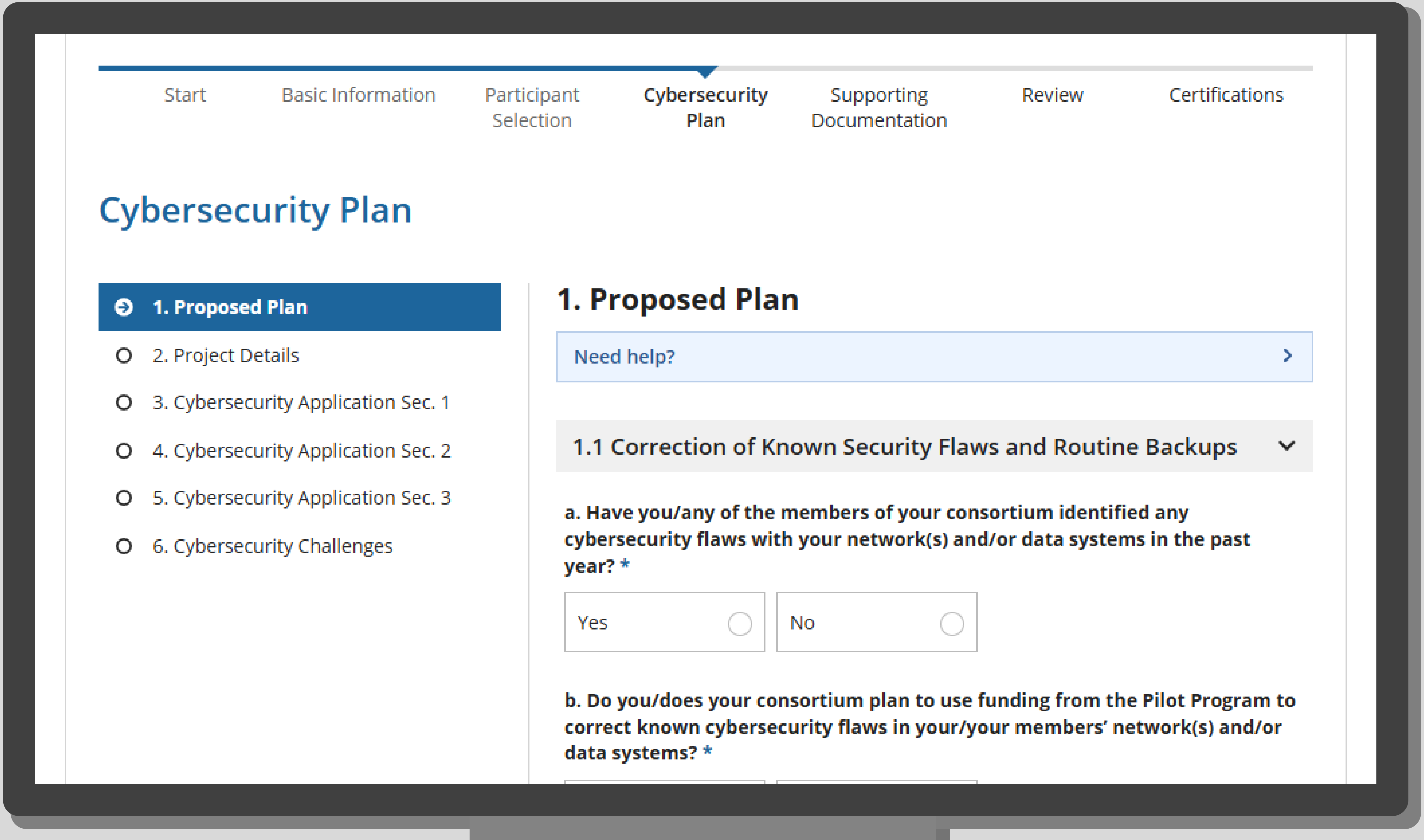


Cybersecurity Plan

1. Proposed Plan

Need help? >

1.1 Correction of Known Security Flaws and Routine Backups >



Cybersecurity Plan

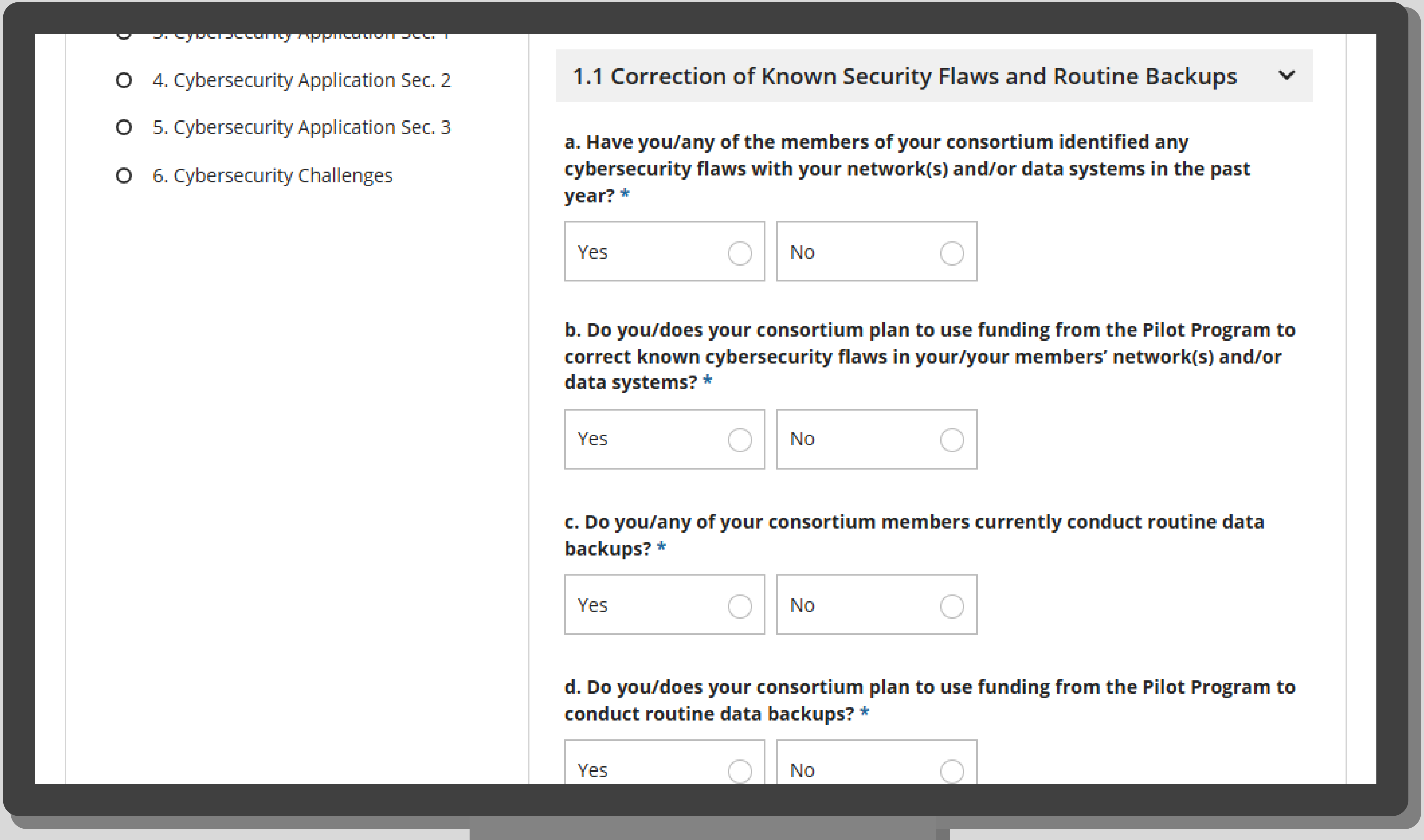
1. Proposed Plan

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? *

Yes ○ 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? *



○ 3. Cybersecurity Application Sec. 1

○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

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? *

Yes ○ 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? *

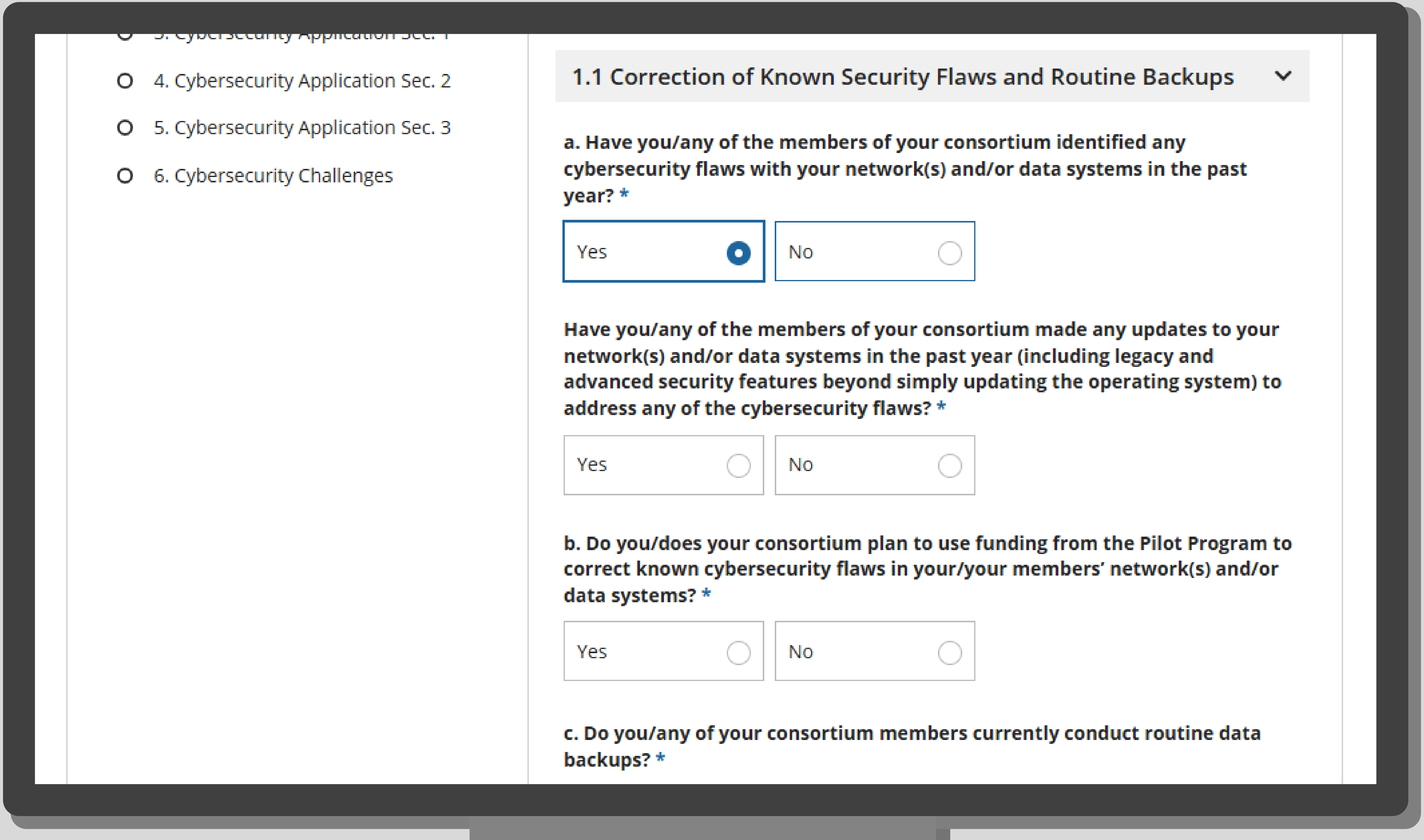
Yes ○ No ○

c. Do you/any of your consortium members currently conduct routine data backups? *

Yes ○ No ○

d. Do you/does your consortium plan to use funding from the Pilot Program to conduct routine data backups? *

Yes ○ No ○



○ 3. Cybersecurity Application Sec. 1

○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

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? *

Yes ● No ○

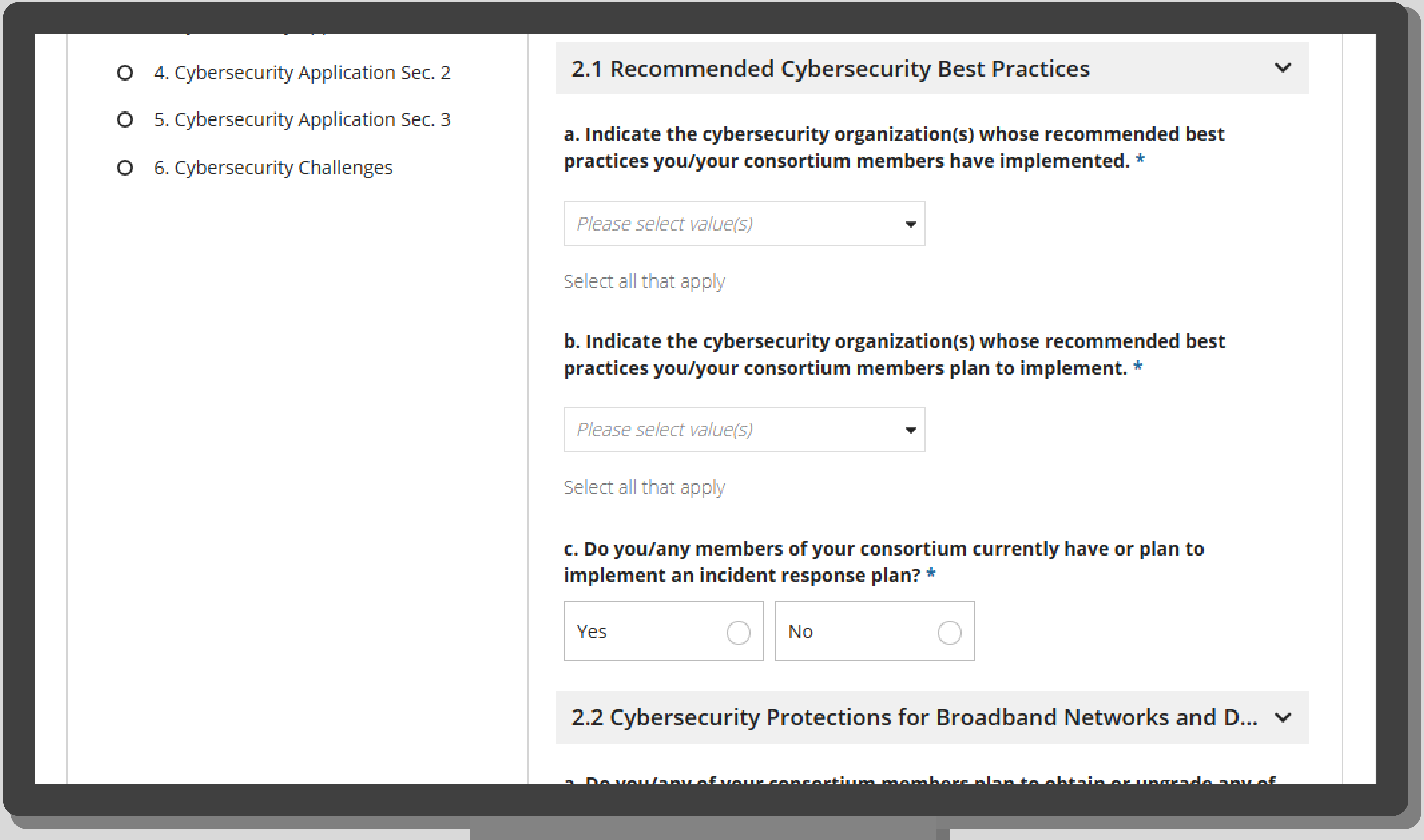
Have you/any of the members of your consortium made any updates to your network(s) and/or data systems in the past year (including legacy and advanced security features beyond simply updating the operating system) to address any of the cybersecurity flaws? *

Yes ○ 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? *

Yes ○ No ○

c. Do you/any of your consortium members currently conduct routine data backups? *



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

Please select value(s) ▾

Select all that apply

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. *

Please select value(s) ▾

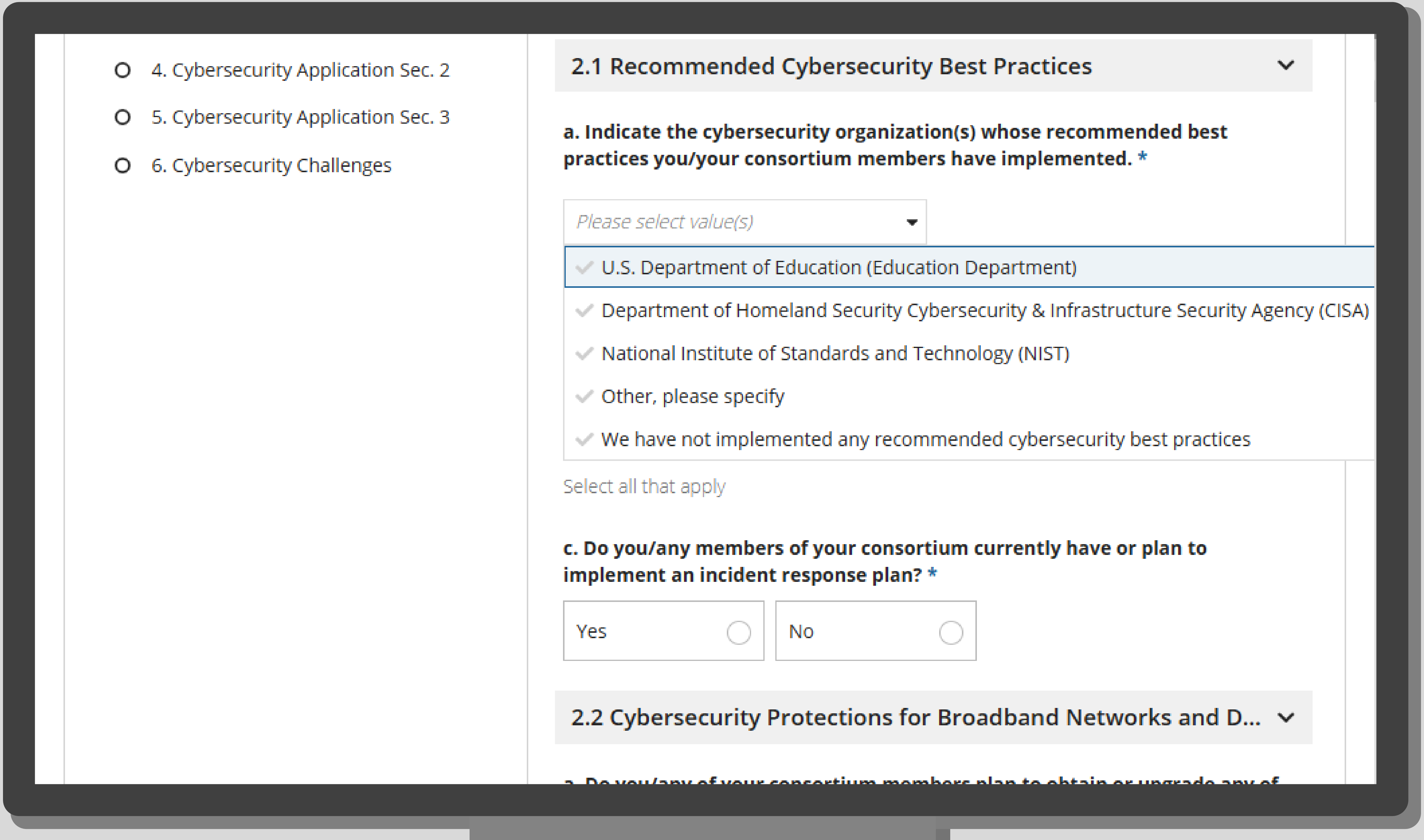
Select all that apply

c. Do you/any members of your consortium currently have or plan to implement an incident response plan? *

Yes ○ No ○

2.2 Cybersecurity Protections for Broadband Networks and D...

a. Do you/any of your consortium members plan to obtain or upgrade any of



2.1 Recommended Cybersecurity Best Practices

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

Please select value(s)

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

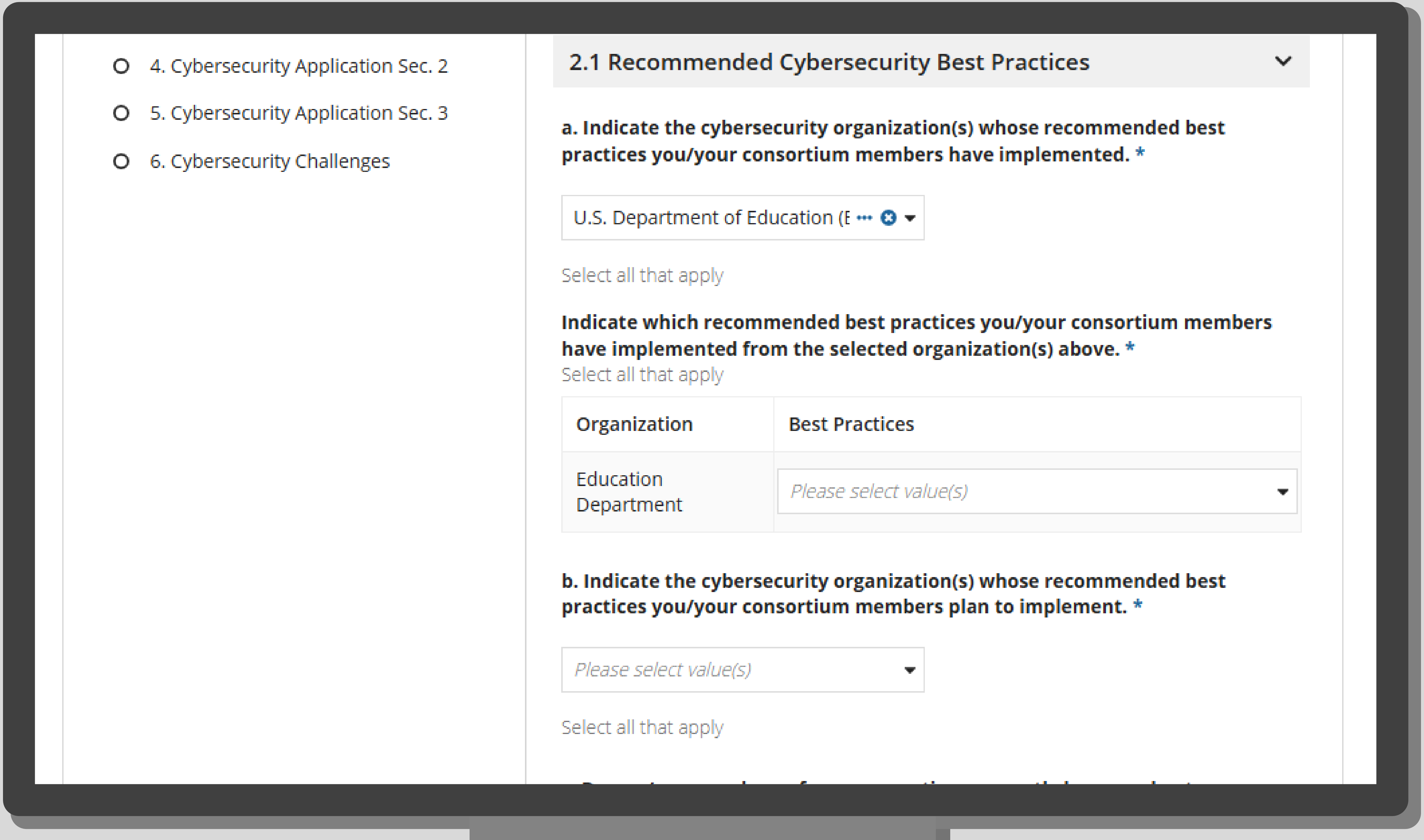
Select all that apply

c. Do you/any members of your consortium currently have or plan to implement an incident response plan? *

Yes ○ No ○

2.2 Cybersecurity Protections for Broadband Networks and D...

a. Do you/any of your consortium members plan to obtain or upgrade any of



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

Select all that apply

Indicate which recommended best practices you/your consortium members have implemented from the selected organization(s) above. *

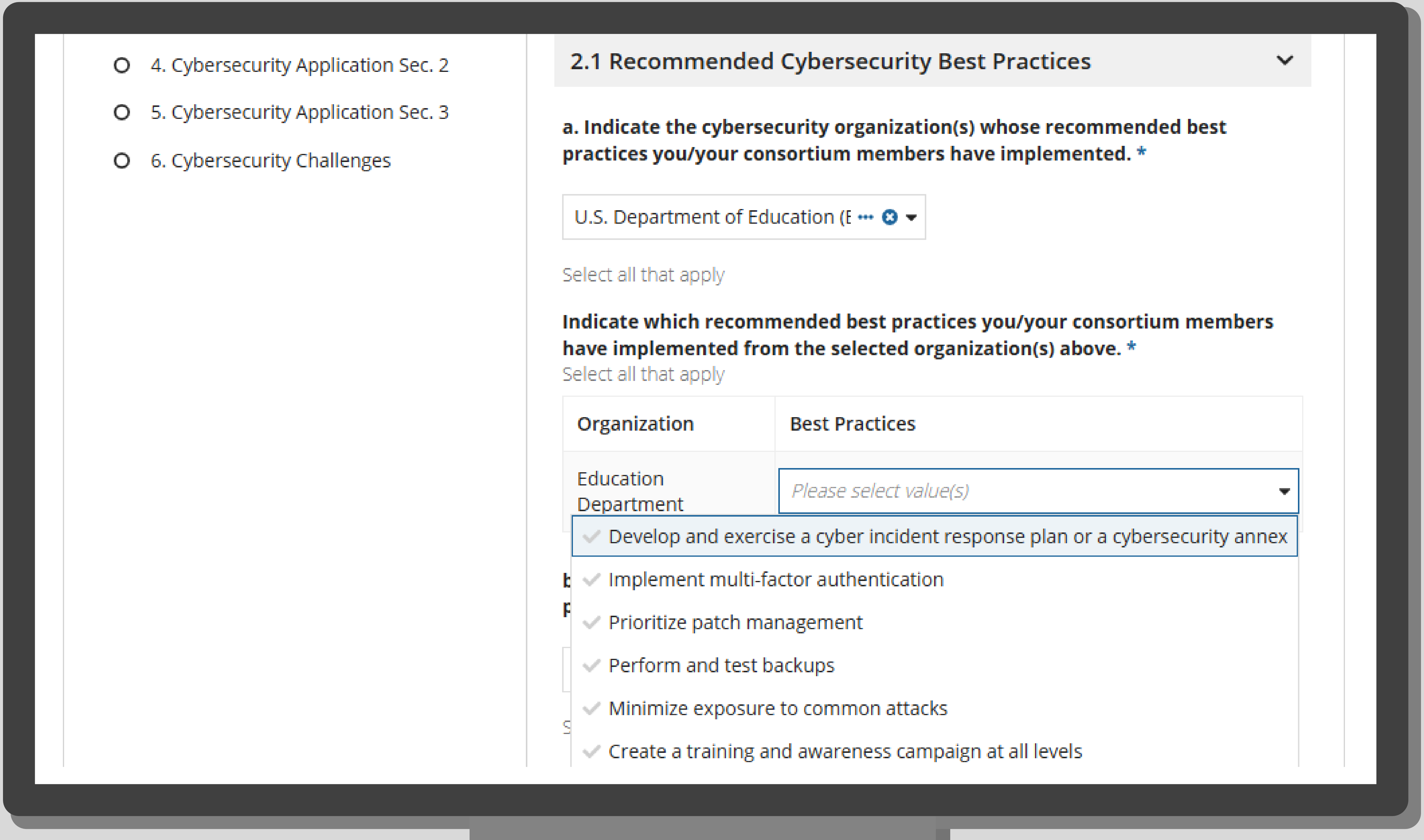
Select all that apply

Organization	Best Practices
Education Department	*Please select value(s)*

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. *

Please select value(s)

Select all that apply



○ 4. Cybersecurity Application Sec. 2
○ 5. Cybersecurity Application Sec. 3
○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

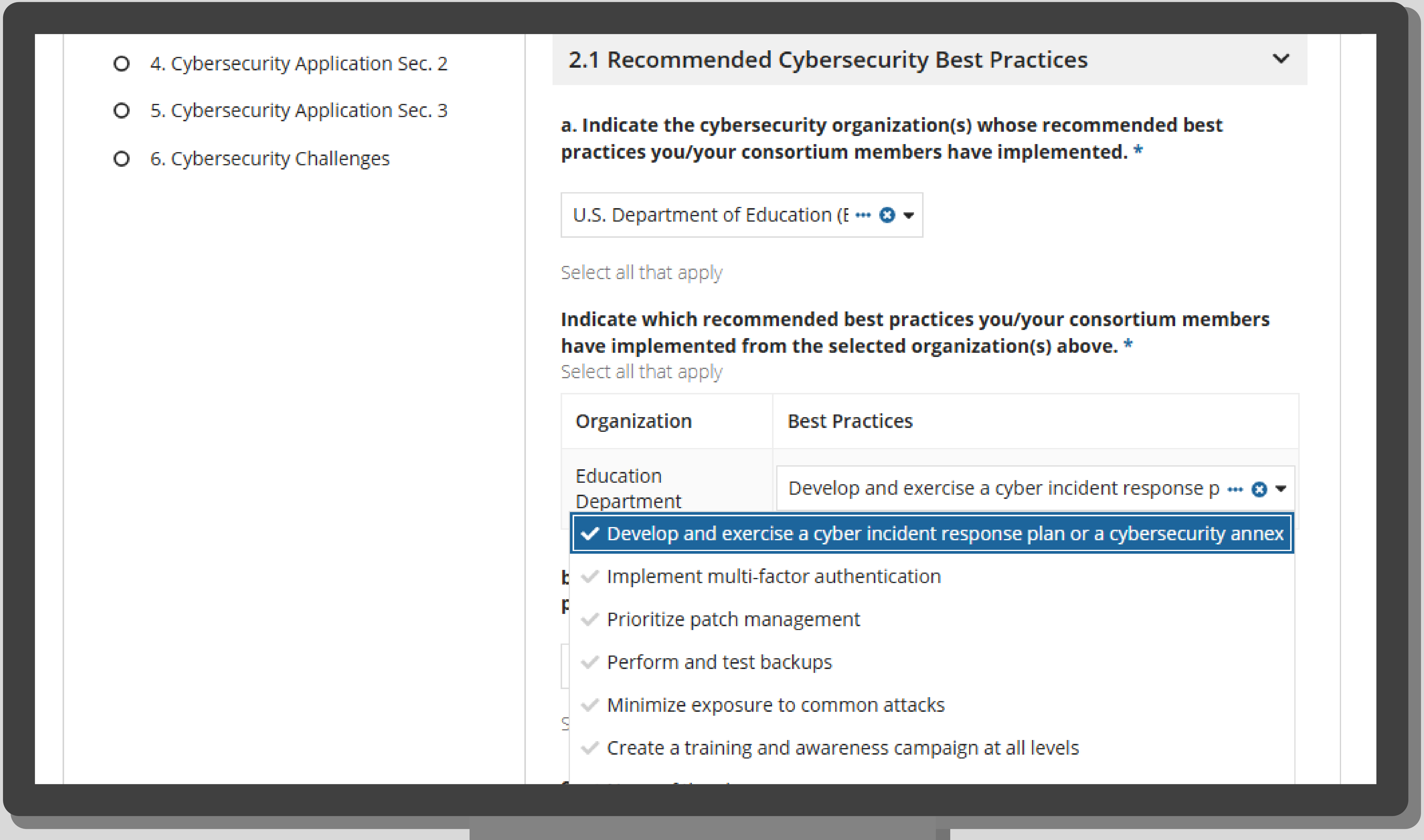
Select all that apply

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	*Please select value(s)*

- ✓ 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



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

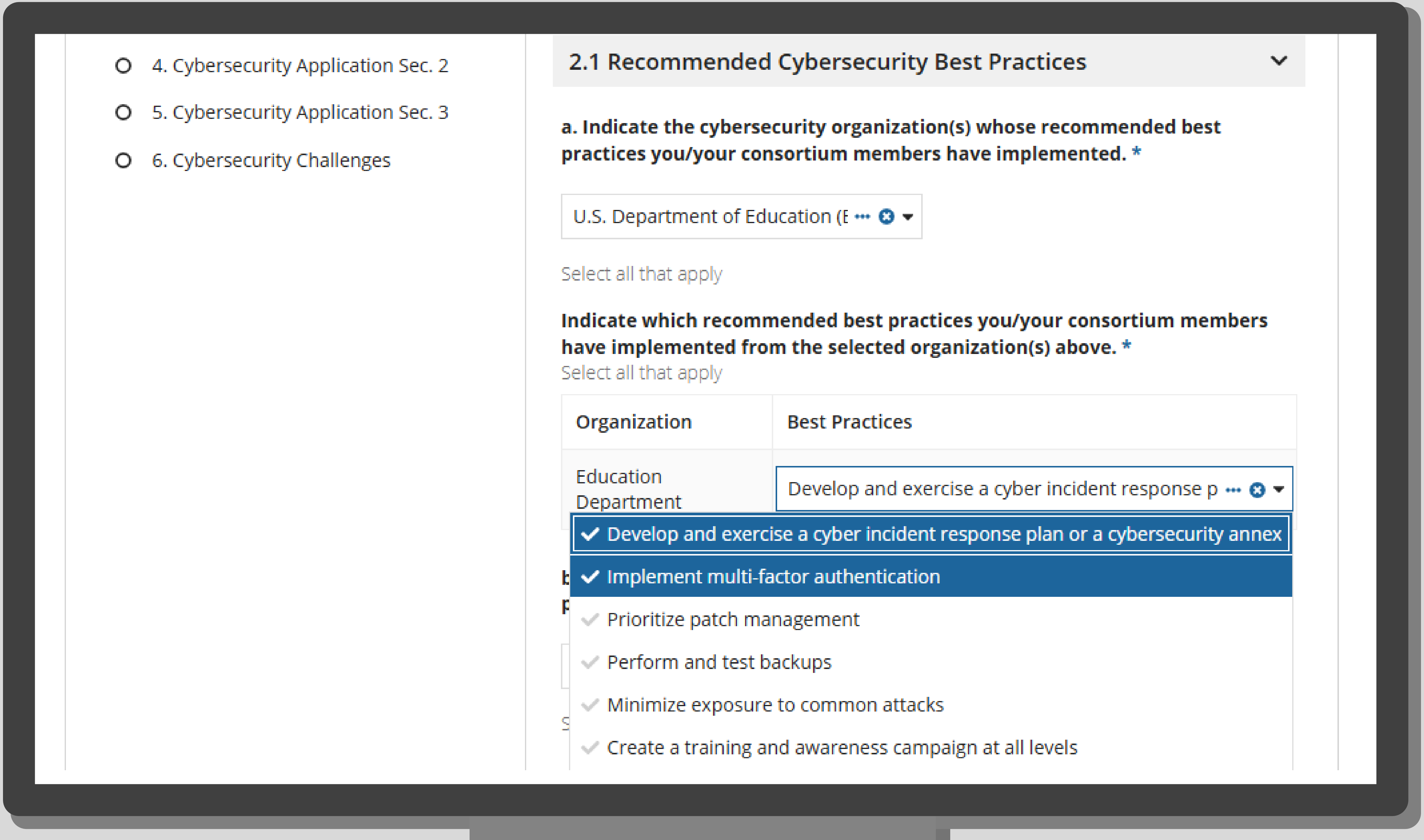
Select all that apply

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 p ···

- ✓ 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



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

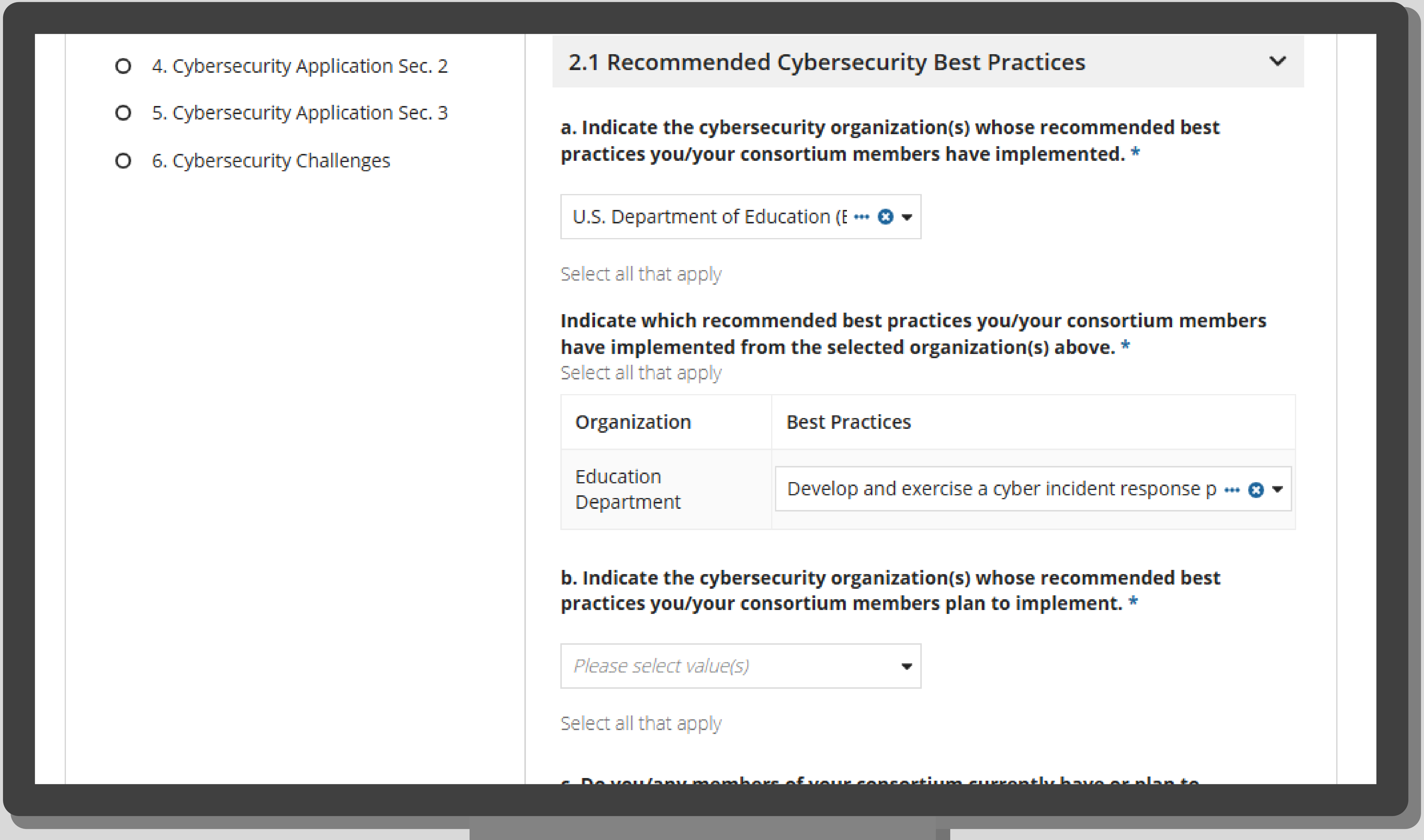
Select all that apply

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 p ···

- ✓ 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



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ••• ⊗ ▾

Select all that apply

Indicate which recommended best practices you/your consortium members have implemented from the selected organization(s) above. *

Select all that apply

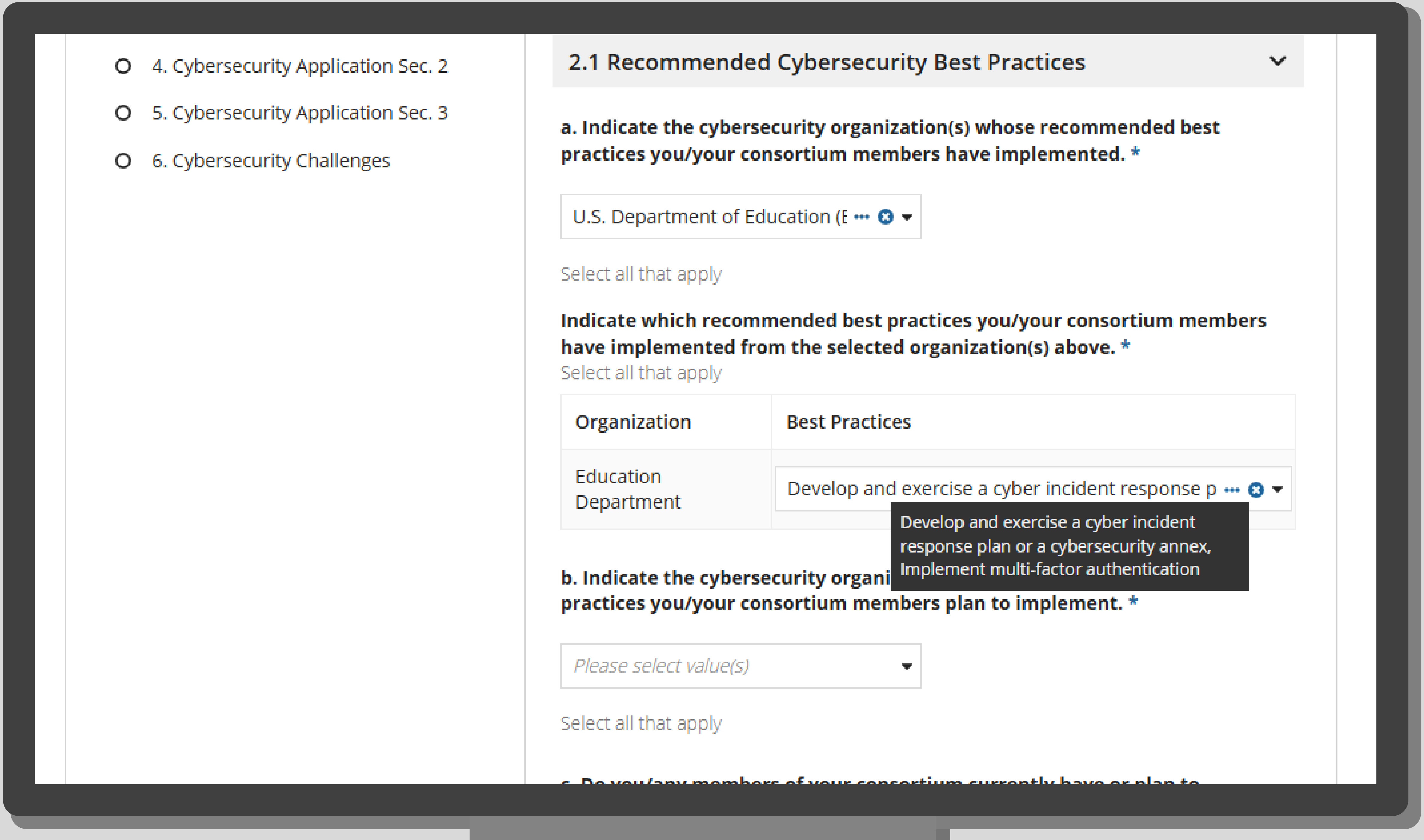
Organization	Best Practices
Education Department	Develop and exercise a cyber incident response p ••• ⊗ ▾

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. *

Please select value(s) ▾

Select all that apply

c. Do you/any members of your consortium currently have or plan to



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ••• ⊗ ▾

Select all that apply

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 p ••• ⊗ ▾

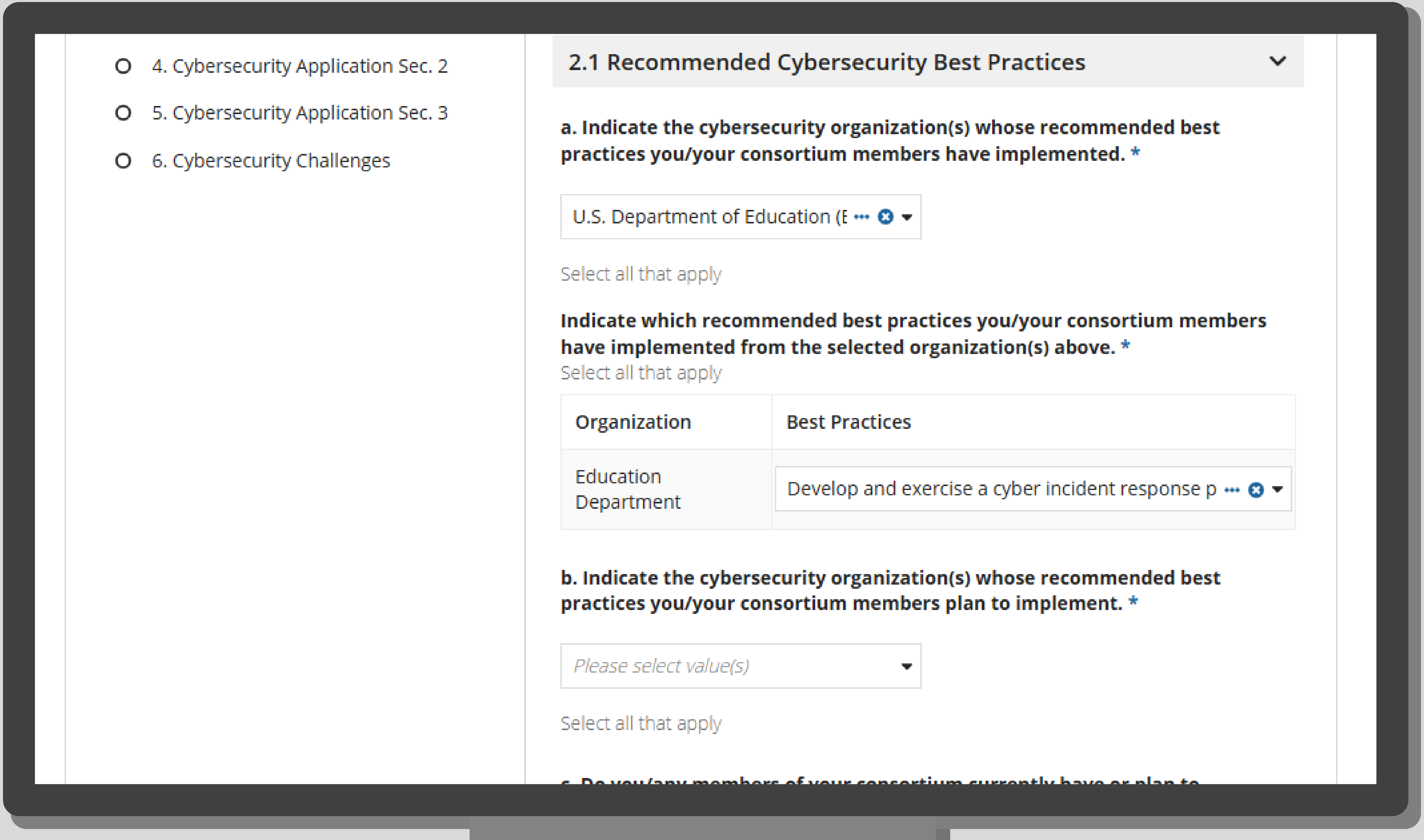
Develop and exercise a cyber incident response plan or a cybersecurity annex, Implement multi-factor authentication

b. Indicate the cybersecurity organi... practices you/your consortium members plan to implement. *

Please select value(s) ▾

Select all that apply

c. Do you/any members of your consortium currently have or plan to



○ 4. Cybersecurity Application Sec. 2
○ 5. Cybersecurity Application Sec. 3
○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

Select all that apply

Indicate which recommended best practices you/your consortium members have implemented from the selected organization(s) above. *

Select all that apply

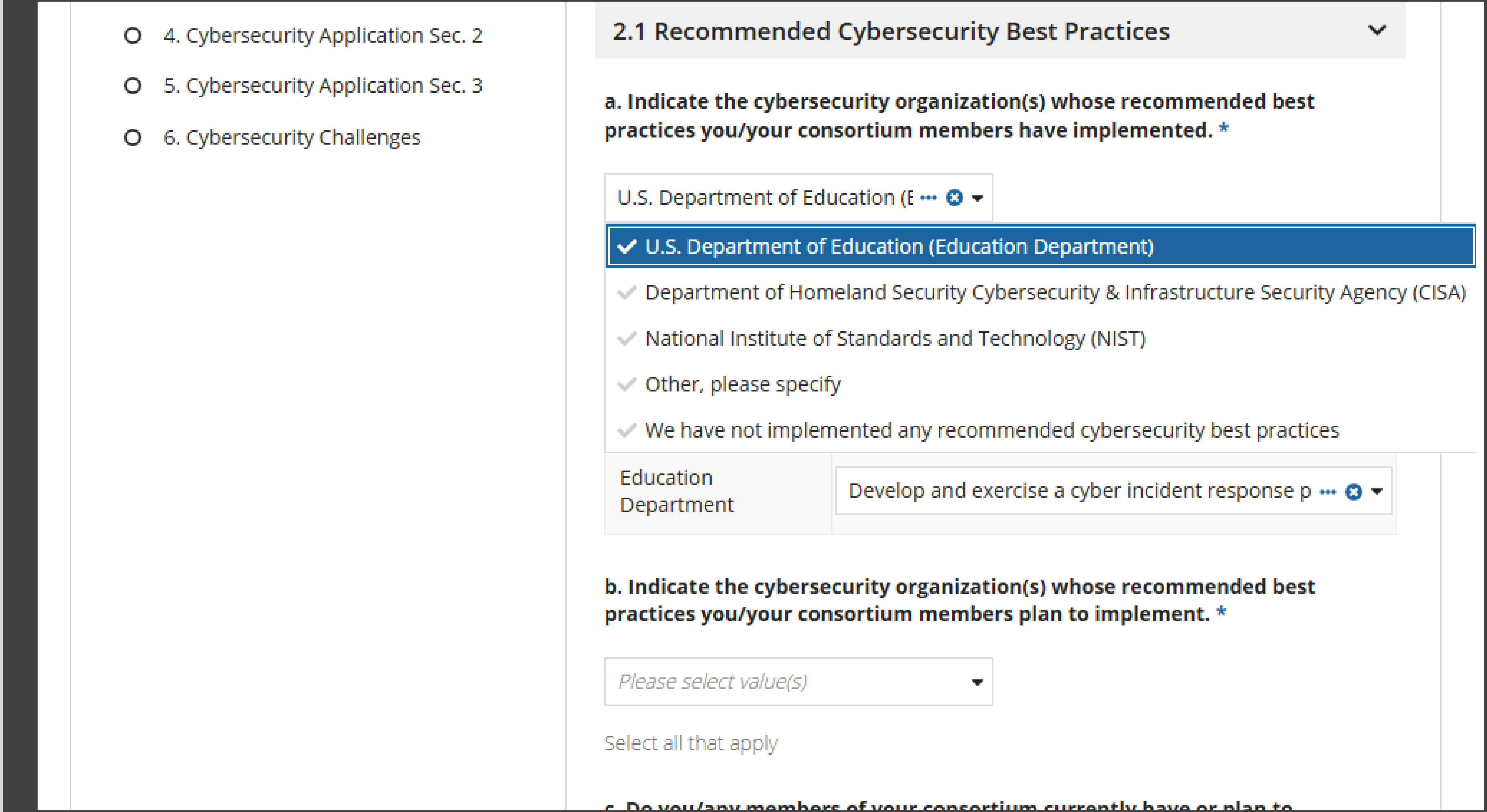
Organization	Best Practices
Education Department	Develop and exercise a cyber incident response p ···

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. *

Please select value(s)

Select all that apply

c. Do you/any members of your consortium currently have or plan to



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

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

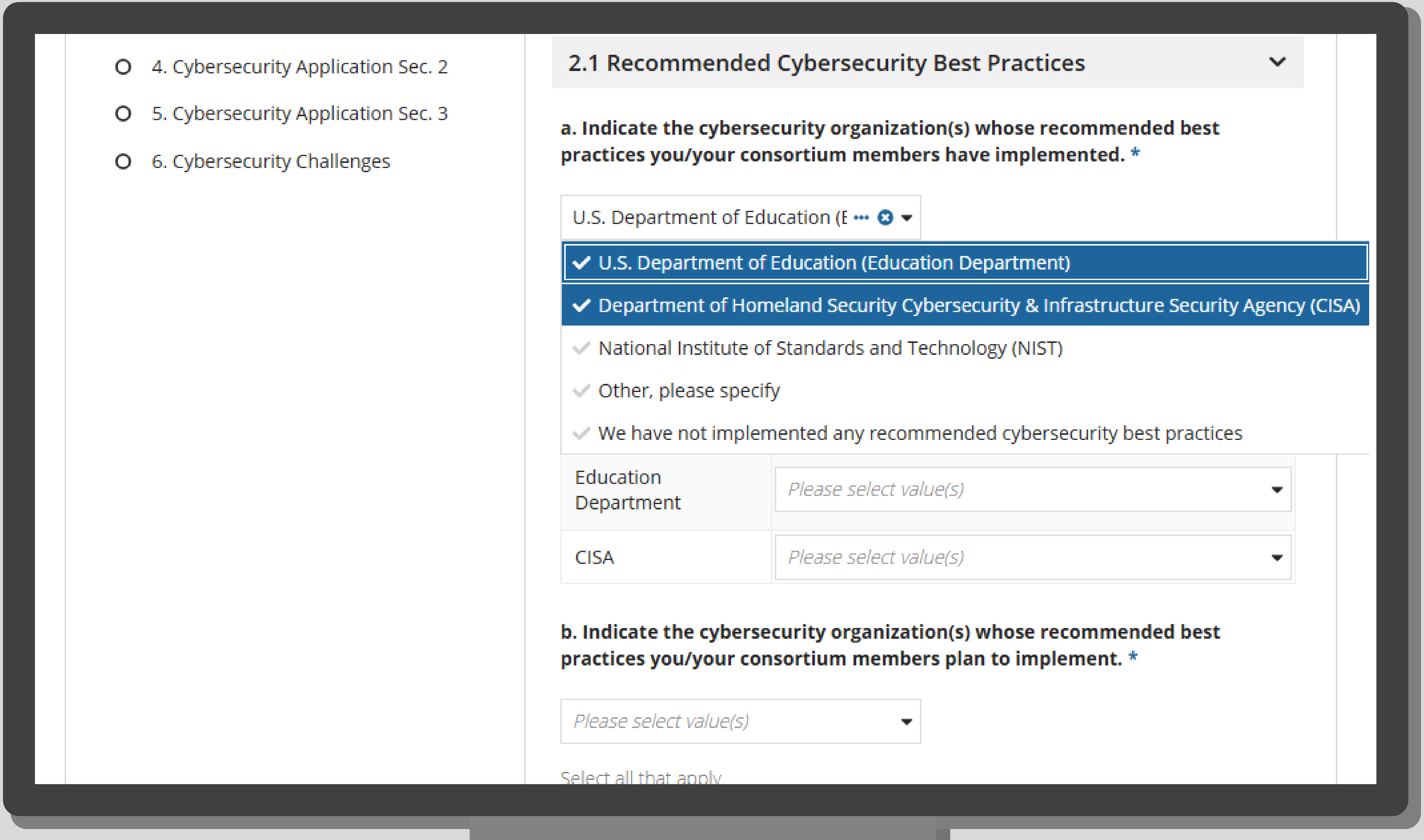
Education Department	Develop and exercise a cyber incident response p ···

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. *

Please select value(s)

Select all that apply

c. Do you/any members of your consortium currently have or plan to



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E •••

✓ U.S. Department of Education (Education Department)

✓ Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA)

✓ National Institute of Standards and Technology (NIST)

✓ Other, please specify

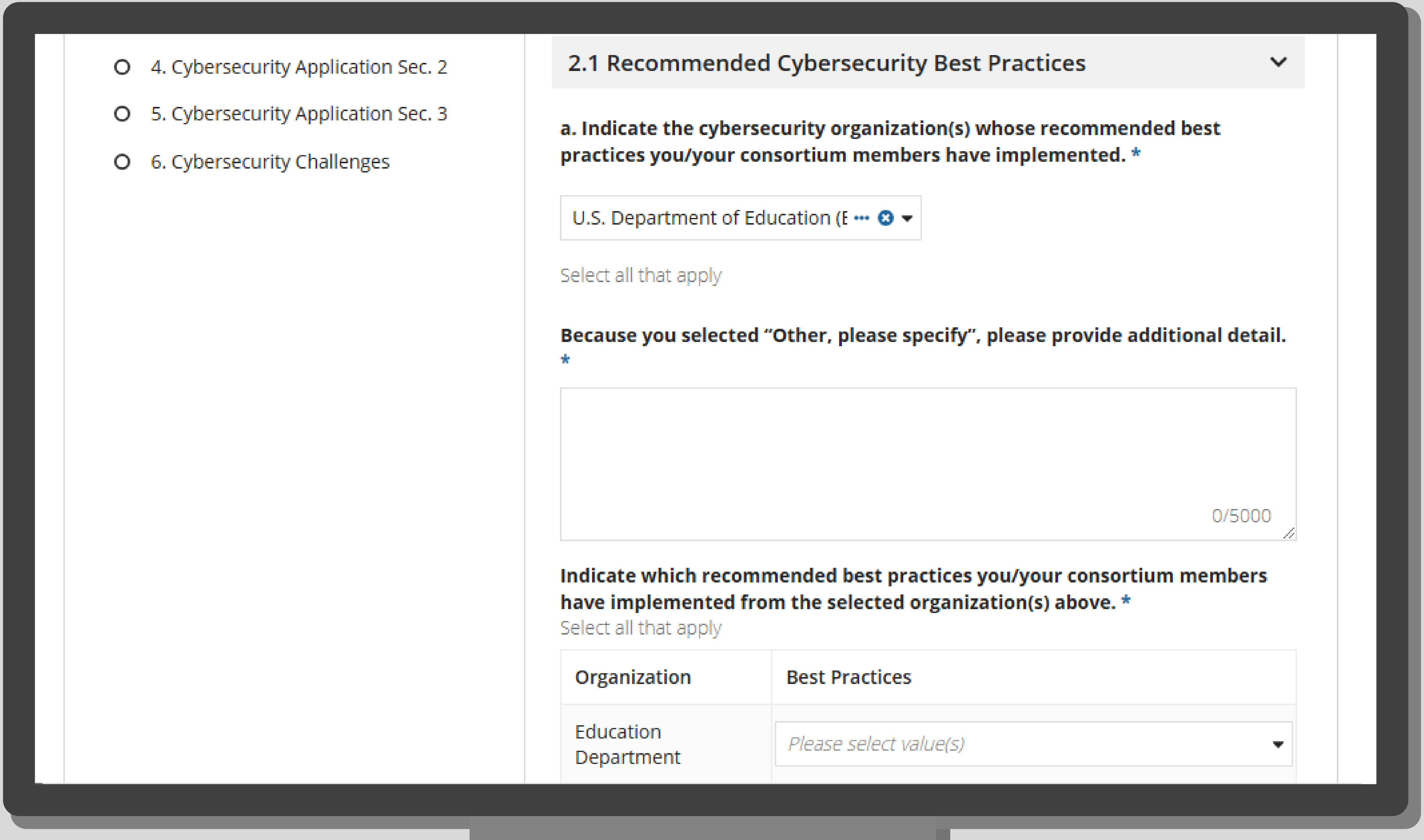
✓ We have not implemented any recommended cybersecurity best practices

Education Department	*Please select value(s)*
CISA	*Please select value(s)*

b. Indicate the cybersecurity organization(s) whose recommended best practices you/your consortium members plan to implement. *

Please select value(s)

Select all that apply



○ 4. Cybersecurity Application Sec. 2

○ 5. Cybersecurity Application Sec. 3

○ 6. Cybersecurity Challenges

2.1 Recommended Cybersecurity Best Practices

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

U.S. Department of Education (E ···

Select all that apply

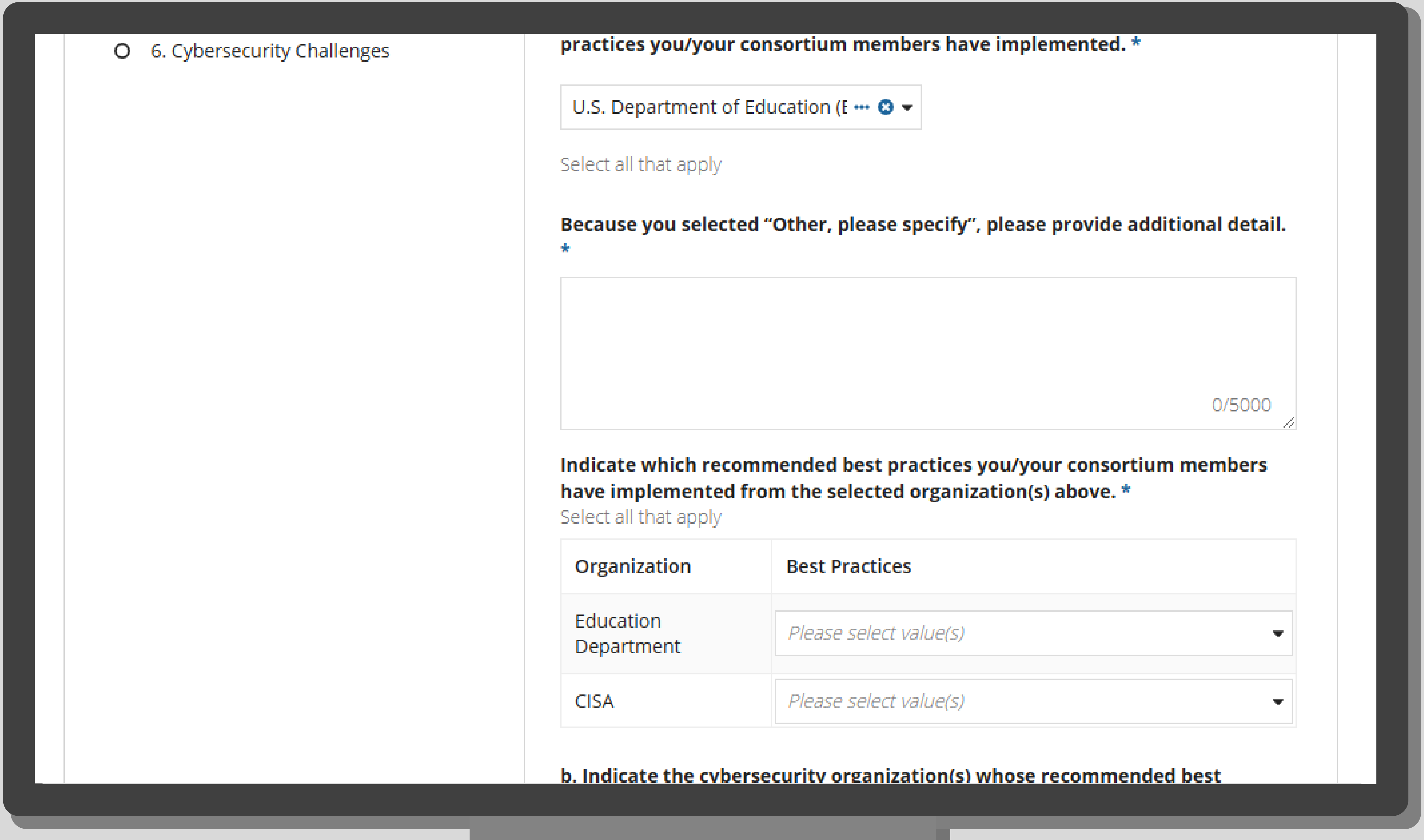
Because you selected “Other, please specify”, please provide additional detail. *

0/5000

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	*Please select value(s)*



○ 6. Cybersecurity Challenges

practices you/your consortium members have implemented. *

U.S. Department of Education (E ··· ⊗ ▾

Select all that apply

Because you selected “Other, please specify”, please provide additional detail. *

0/5000

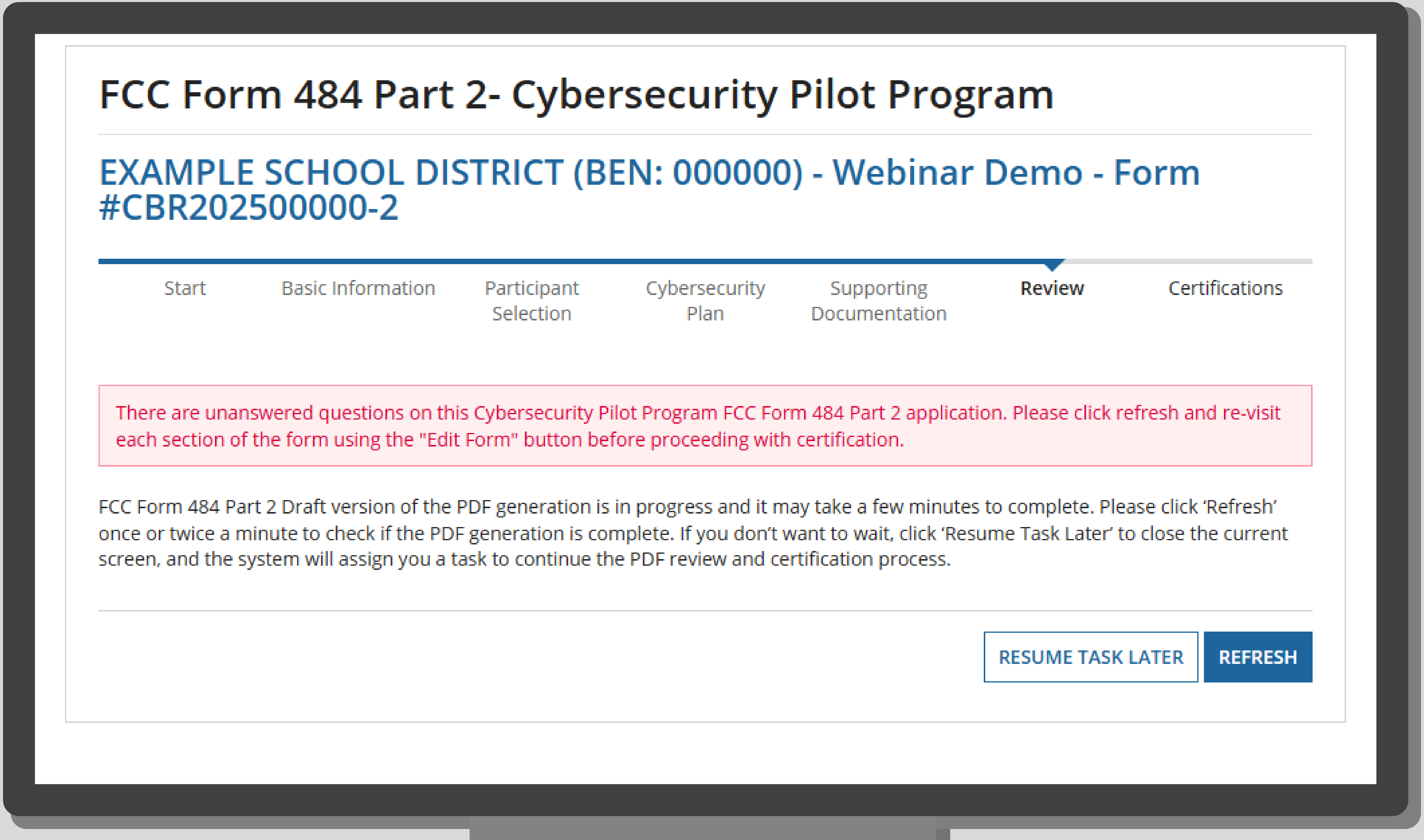
Indicate which recommended best practices you/your consortium members have implemented from the selected organization(s) above. *

Select all that apply

Organization	Best Practices
Education Department	*Please select value(s)* ▾
CISA	*Please select value(s)* ▾

b. Indicate the cybersecurity organization(s) whose recommended best

Pilot FCC Form 484 Part 2 Walkthrough: Certification

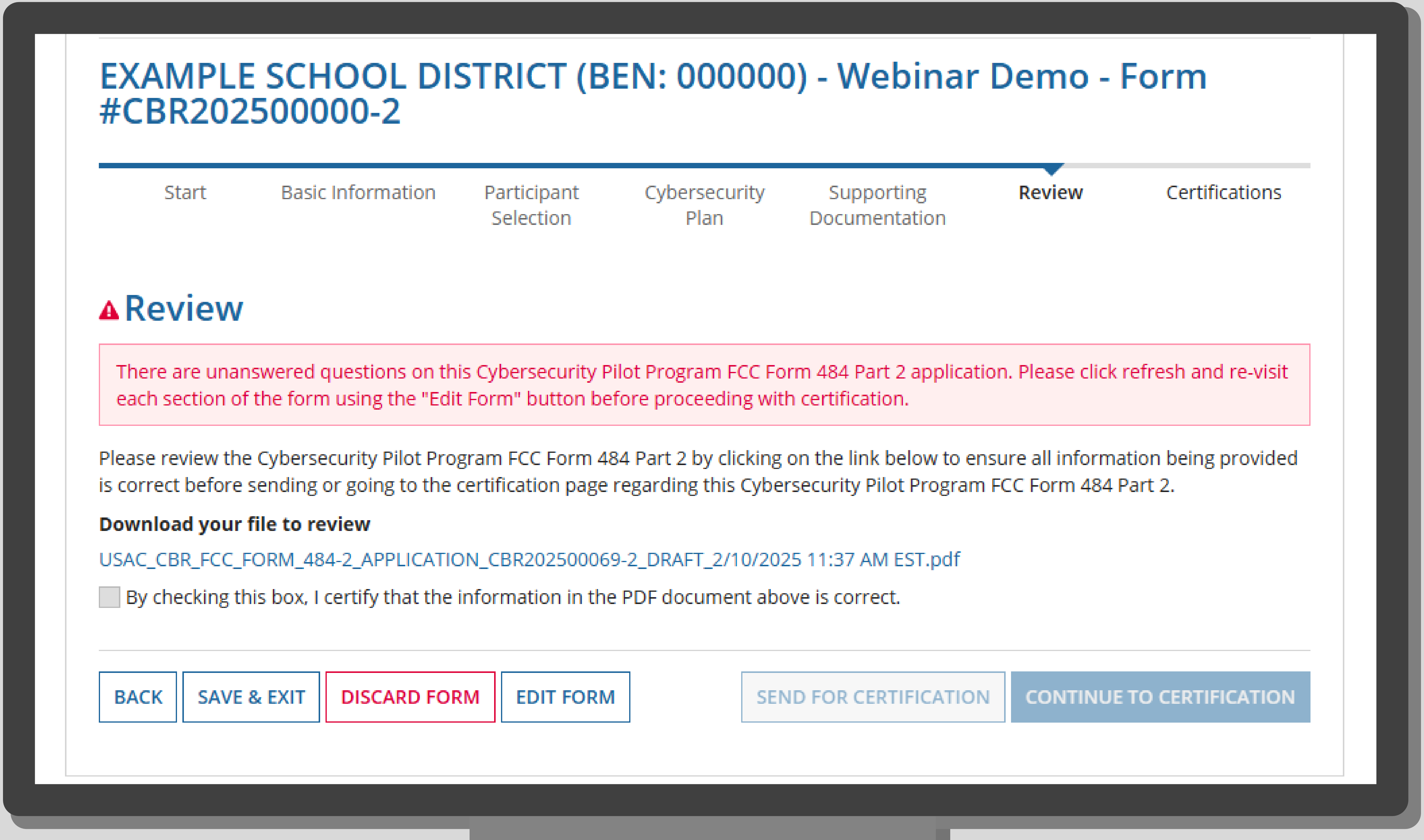


FCC Form 484 Part 2- Cybersecurity Pilot Program

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

There are unanswered questions on this Cybersecurity Pilot Program FCC Form 484 Part 2 application. Please click refresh and re-visit each section of the form using the "Edit Form" button before proceeding with certification.

FCC Form 484 Part 2 Draft version of the PDF generation is in progress and it may take a few minutes to complete. Please click ‘Refresh’ once or twice a minute to check if the PDF generation is complete. If you don’t want to wait, click ‘Resume Task Later’ to close the current screen, and the system will assign you a task to continue the PDF review and certification process.



EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

Review

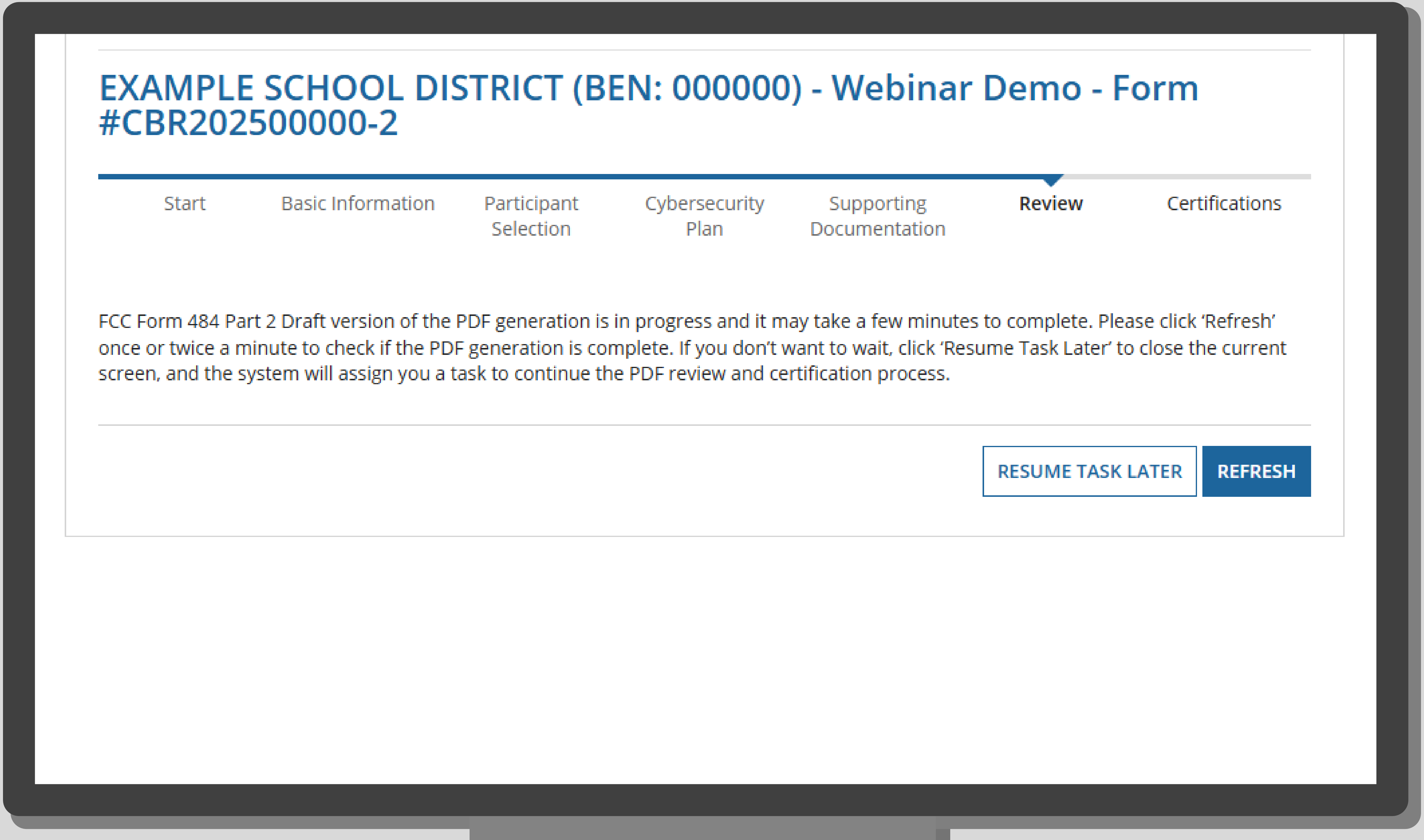
There are unanswered questions on this Cybersecurity Pilot Program FCC Form 484 Part 2 application. Please click refresh and re-visit each section of the form using the "Edit Form" button before proceeding with certification.

Please review the Cybersecurity Pilot Program FCC Form 484 Part 2 by clicking on the link below to ensure all information being provided is correct before sending or going to the certification page regarding this Cybersecurity Pilot Program FCC Form 484 Part 2.

Download your file to review

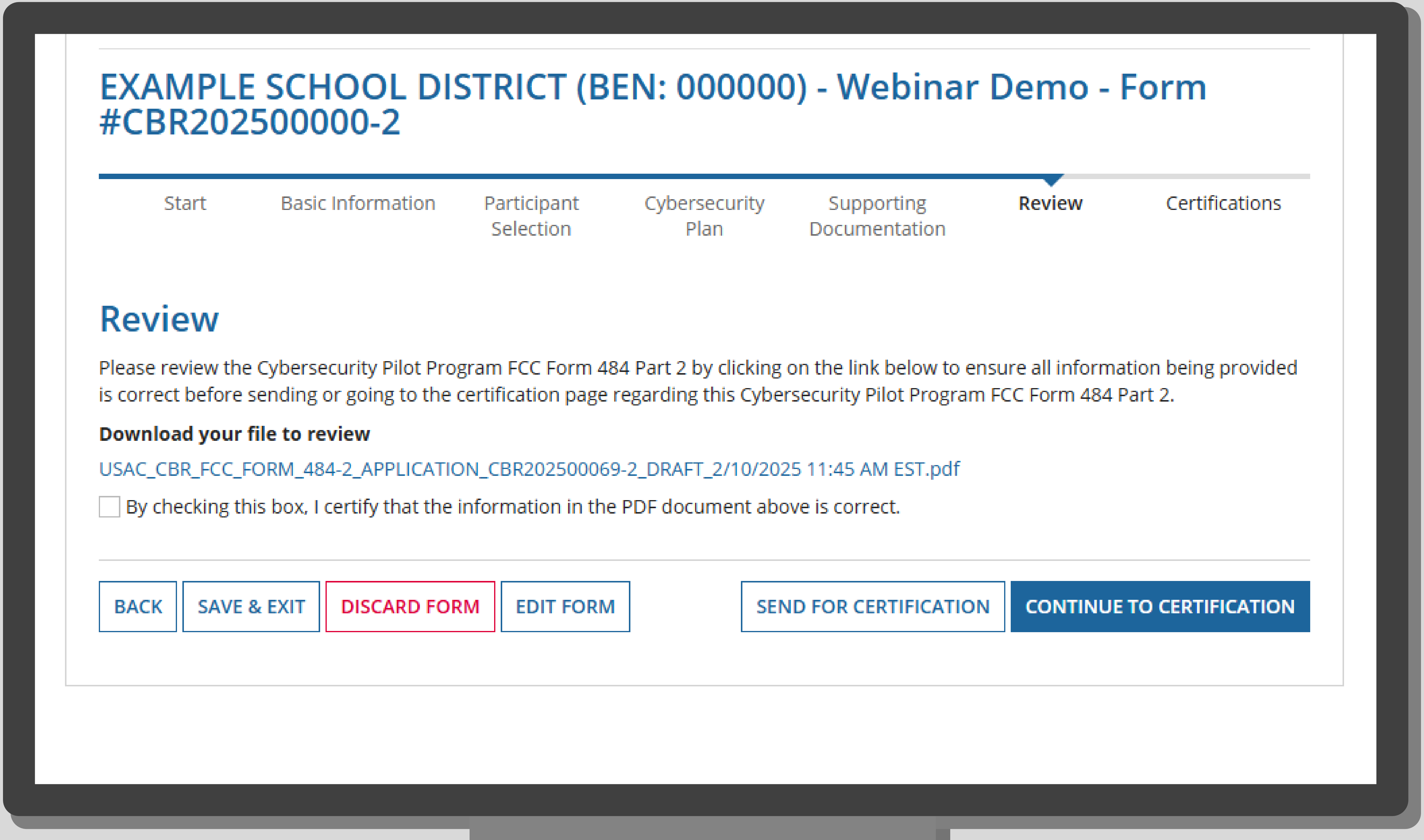
USAC_CBR_FCC_FORM_484-2_APPLICATION_CBR202500069-2_DRAFT_2/10/2025 11:37 AM EST.pdf

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



EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

FCC Form 484 Part 2 Draft version of the PDF generation is in progress and it may take a few minutes to complete. Please click ‘Refresh’ once or twice a minute to check if the PDF generation is complete. If you don’t want to wait, click ‘Resume Task Later’ to close the current screen, and the system will assign you a task to continue the PDF review and certification process.



EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

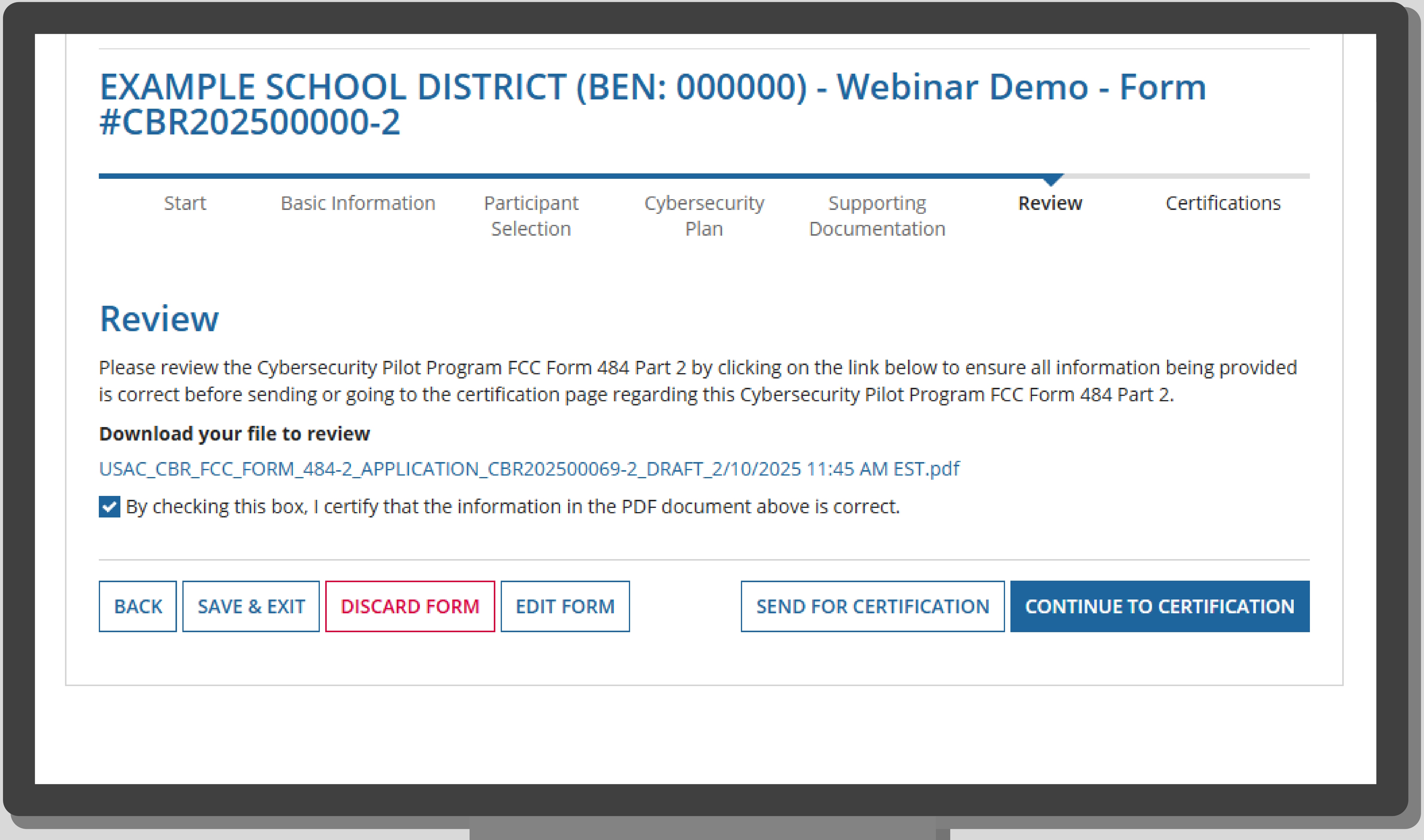
Review

Please review the Cybersecurity Pilot Program FCC Form 484 Part 2 by clicking on the link below to ensure all information being provided is correct before sending or going to the certification page regarding this Cybersecurity Pilot Program FCC Form 484 Part 2.

Download your file to review

USAC_CBR_FCC_FORM_484-2_APPLICATION_CBR202500069-2_DRAFT_2/10/2025 11:45 AM EST.pdf

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



EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

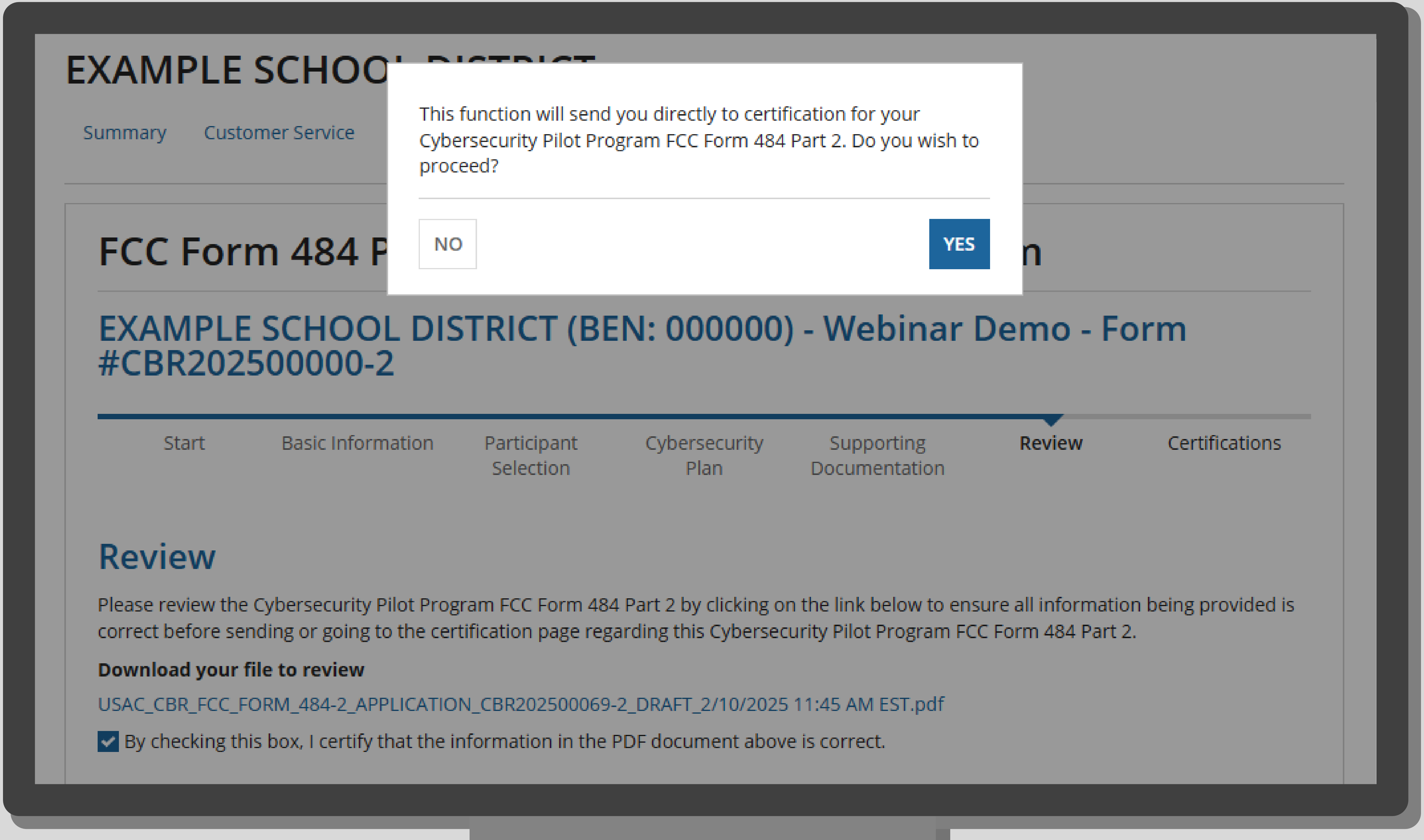
Review

Please review the Cybersecurity Pilot Program FCC Form 484 Part 2 by clicking on the link below to ensure all information being provided is correct before sending or going to the certification page regarding this Cybersecurity Pilot Program FCC Form 484 Part 2.

Download your file to review

USAC_CBR_FCC_FORM_484-2_APPLICATION_CBR202500069-2_DRAFT_2/10/2025 11:45 AM EST.pdf

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



EXAMPLE SCHOO

This function will send you directly to certification for your Cybersecurity Pilot Program FCC Form 484 Part 2. Do you wish to proceed?

FCC Form 484 P n

EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

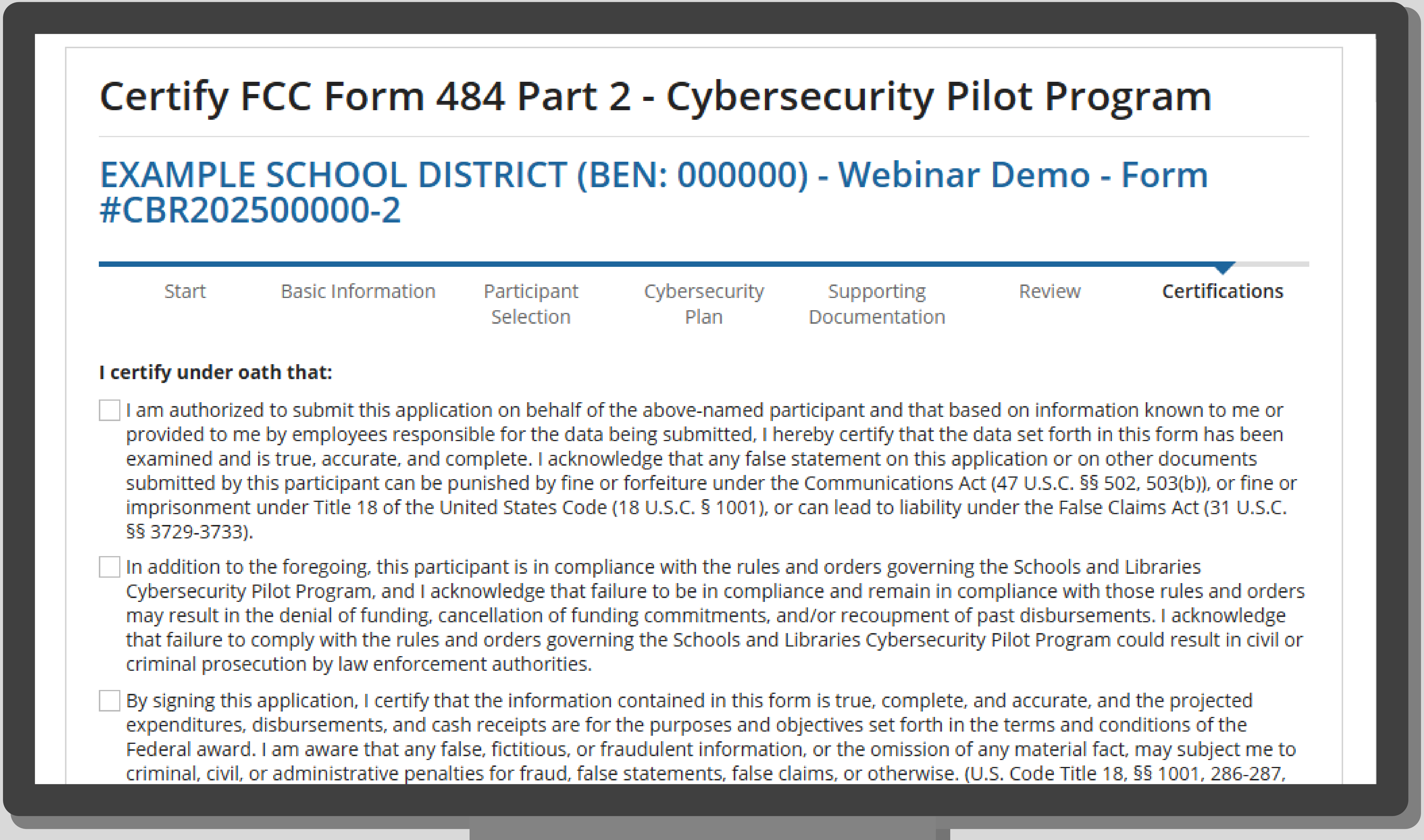
Review

Please review the Cybersecurity Pilot Program FCC Form 484 Part 2 by clicking on the link below to ensure all information being provided is correct before sending or going to the certification page regarding this Cybersecurity Pilot Program FCC Form 484 Part 2.

Download your file to review

USAC_CBR_FCC_FORM_484-2_APPLICATION_CBR202500069-2_DRAFT_2/10/2025 11:45 AM EST.pdf

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



Certify FCC Form 484 Part 2 - Cybersecurity Pilot Program

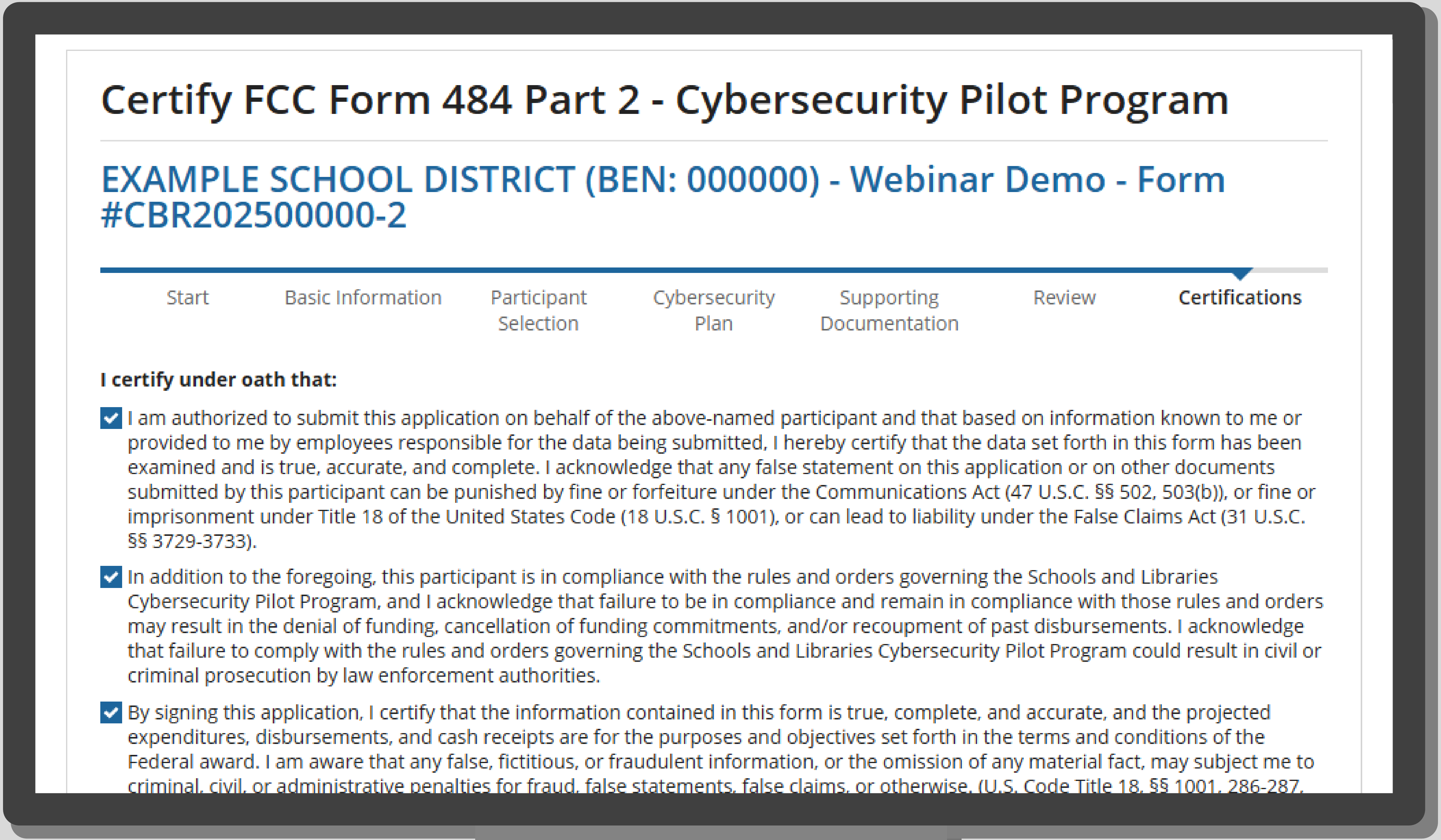
EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

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,



Certify FCC Form 484 Part 2 - Cybersecurity Pilot Program

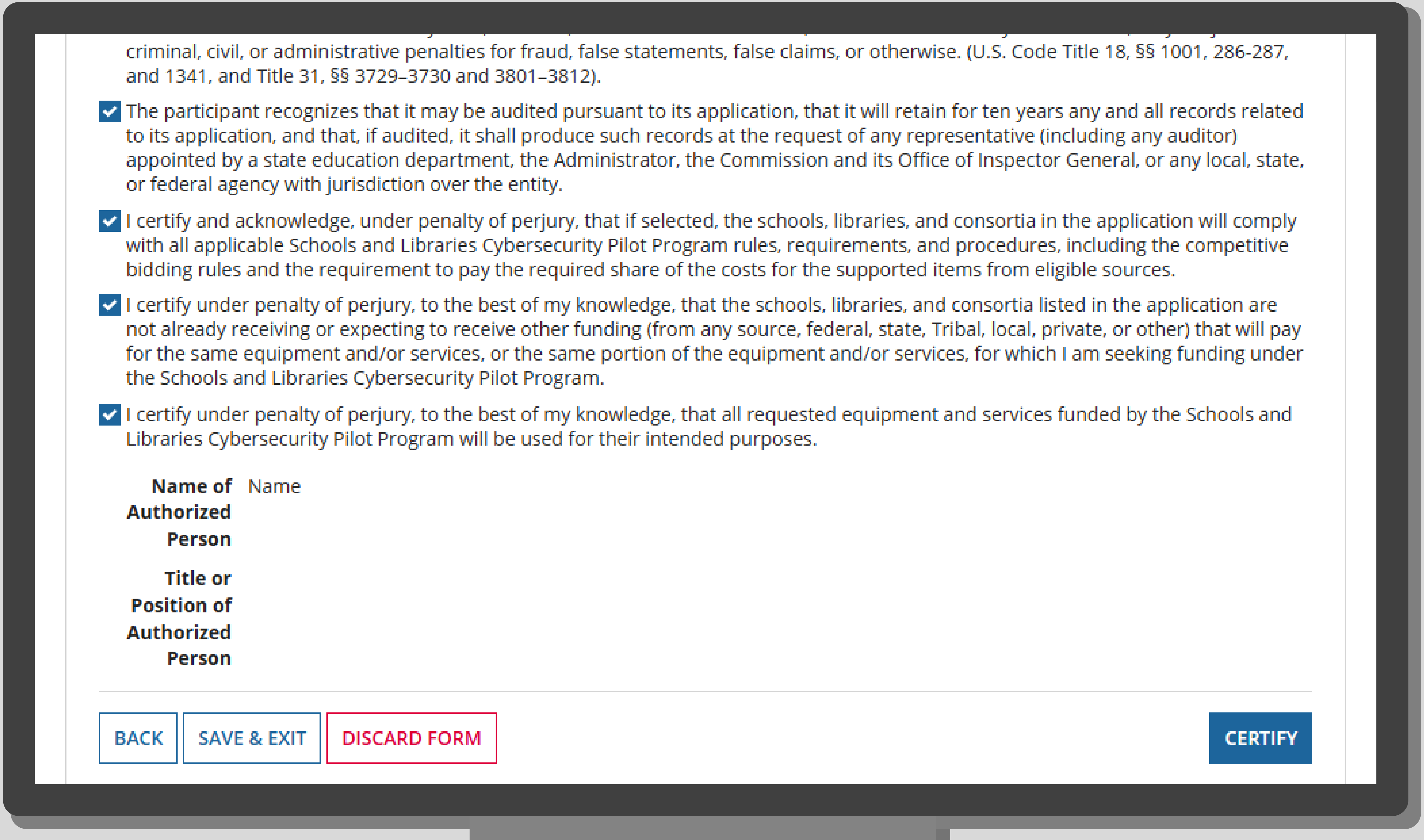
EXAMPLE SCHOOL DISTRICT (BEN: 000000) - Webinar Demo - Form #CBR202500000-2

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,



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 if selected, the schools, libraries, and consortia in the application 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 consortia listed in the application 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.

Name of Authorized Person Name

Title or Position of Authorized Person

Questions?

Pilot Program: Resources and Training

Pilot Program: Resources

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

Pilot Program: Upcoming Trainings

- **Pilot FCC Form 471 Webinar**
  March 18 @ 3 p.m. E.T.
  Register

Thank You!

Universal Service Administrative Co.