OMB Control No. 3060-xxxx
Month 2023
Not Yet Approved by OMB

Estimated Time per Response
15 hours

Schools and Libraries Cybersecurity Pilot Program

Schools and Libraries Cybersecurity Pilot Program Application (FCC Form 484)

(Note: This is a representative description of the information to be collected via the online portal and is not intended to be a visual representation of what each applicant will see, the order in which they will see information, or the exact wording or directions used to collect the information. Where possible, information that was pre-filed in the system portal as part of the applicant's profile will be carried forward and pre-populated into the form.)

Item #	Field Description	Category	Purpose/Instructions
1	Applicant Name	Entity Information	This is the name of the applicant submitting this form—school, school district, library (outlet/branch or system) or a consortium of those entities (schools, libraries, or schools and libraries). If this information has already been entered into the applicant's profile, it will be pre-populated.
2	Entity Number	Entity Information	This is the Unique identifier assigned by the Administrator to the entity listed in Applicant Name. If this information has already been entered into the applicant's profile, it will be pre-populated.
3	Application Number	System Generated	Auto-generated by the system: This is an Administrator-assigned unique identifier for this application.
4	FCC Registration Number	Entity Information	This is the unique FCC identifier for the applicant. If this information has already been entered into the applicant's profile, it will be pre-populated.
5	Employer Identification Number (EIN)	Entity information	The EIN is also known as a Federal Tax Identification Number, and is used to identify a business or non-profit entity. If this information has already been entered into the applicant's profile, it will be pre-populated.
6	Mailing Address	Entity Information	This is the mailing address for the applicant. If this information has already been entered into the applicant's profile, it will be pre-populated.

Item #	Field Description	Category	Purpose/Instructions
7	Telephone Number	Entity Information	This is the main telephone number for the applicant which may/may not be the same as the telephone number for the person who should be contacted with questions about this application. If this information has already been entered into the applicant's profile, it will be pre-populated.
8	Contact Person's Name	Entity Information	Provide the name of the person who should be contacted with questions about this application. If this information has already been entered into the applicant's profile, it will be pre-populated.
9	Contact Person's Title or Position	Entity Information	Provide the title or position of the contact person. If this information has already been entered into the applicant's profile, it will be pre-populated.
10	Contact Person's Telephone Number	Entity Information	Telephone Number of the Contact Person. If this information has already been entered into the applicant's profile, it will be pre-populated n.
11	Contact Person's Mailing Address	Entity Information	Mailing Address of the Contact Person. If this information has already been entered into the applicant's profile, it will be pre-populated.
12	Contact Person's E-mail Address	Entity Information	E-mail Address of the Contact Person. If this information has already been entered into the applicant's profile, it will be pre-.
13	Type of Applicant	Entity Information	Options are: school, school district, library/library system, or consortium. If this information has already been entered into the applicant's profile, it will be pre-populated.
14	Applicant Attributes	Entity Information	Attributes for a School or School District include: Public, Private, Charter, and Educational Service Agency (ESA). Attributes for a Library System include: Public and Private. If this information has already been entered into the applicant's profile, it will be pre-populated.
15	Tribal Affiliation	Entity Information	If the applicant is a Tribal entity, the applicant will provide its Tribal affiliation. If this information has already been entered into the applicant's profile, it will be pre-populated.
16	E-Rate Status	Entity Information	This is to indicate whether the applicant participates in the E-Rate program. The applicant will select either "Yes" or "No".
17	E-Rate Discount Percentage	Entity Information	This is the E-Rate discount percentage for the applicant. If this information is in the applicant's profile, it will be pre-populated.

Item #	Field Description	Category	Purpose/Instructions
18	Urban/Rural Designation	Entity Information	This is the urban/rural designation for the applicant and will be system populated based on the applicant's physical address.
19	Lead Site Name	Entity Information	For consortia applications or applications with more than one site, this is the name of the site that will be the lead for the Schools and Libraries Cybersecurity Pilot Program project.
20	Number and Location of Participating Sites	Entity Information	For consortia applications or applications with more than one site, the applicant will provide information on the number and location of sites that will be participating in the Schools and Libraries Cybersecurity Pilot Program project. If this data is available in the applicant's profile, it will be pre-populated.
22	Executive Summary of Project	Project Information	Provide a summary of the proposed Pilot project for which Schools and Libraries Cybersecurity Pilot Program funding is being requested, including, but not limited to, information about the cybersecurity issues the applicant faces and the proposed cybersecurity action plan for the applicant and any other sites that included as part of the project.
23	Description of How Project Funding Will be Used	Project Information	Describe how the proposed Pilot project would use Schools and Libraries Cybersecurity Pilot Program funding to protect the applicant's broadband network and data, and address cybersecurity concerns, including, but not limited to, a discussion of the types of equipment and services the applicant plans to purchase and how it plans to use the equipment and services to protect its broadband network and data and manage and address its cybersecurity risks.
24	Previous Cybersecurity Experience	Project Information	Information on whether the applicant has previous experience implementing cybersecurity protections or has or is implementing a cybersecurity framework or program, including the length of the applicant's cybersecurity experience.
25	Current Cybersecurity Posture and Resources	Project Information	Information on the applicant's current cybersecurity posture and resources, including, but not limited to, how current cybersecurity risks are being managed and addressed and the cybersecurity equipment and services the applicant already has in place.

Item #	Field Description	Category	Purpose/Instructions
26	History of Cyber Threats and Attacks	Project Information	Information on whether the applicant has experienced a cybersecurity threat or attack, including, but not limited to, the timing and length of the threat or attack, information about the malicious cybersecurity actor(s), if known, the time it took to detect and respond to the threat or attack, the estimated cost of the threat or attack, and whether/how the cybersecurity threat or attack impacted the applicant's/participant's operations, network, or data.
27	Implementation of DOE or CISA Cybersecurity Recommendations	Project Information	Information on whether the applicant has implemented, or begun implementing, any of the U.S. Department of Education (DOE) or Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) recommended cybersecurity protections and which protections it will or has implemented.
28	Participation in Cybersecurity Collaboration and/or Information Sharing Groups	Project Information	Information on whether the applicant is a member of, or plans to join, any cybersecurity collaboration and information-sharing groups and a list of the applicable cybersecurity groups it has joined or plans to join.
29	Other Sources of Funding	Project Information	Information on whether the applicant has received, or expects to receive, cybersecurity funding from any other federal universal service program, or another federal, state, local, Tribal, or other program or source, including information about the source of the other funding, what the other funding will be used for, and whether funding from the Schools and Libraries Cybersecurity Pilot Program would be duplicative of the other funding received.
30	Cybersecurity Risks Proposed Pilot Project will Prevent or Address	Project Information	Information on the cybersecurity risks the proposed Schools and Libraries Cybersecurity Pilot Program project will prevent or address.
31	Pilot Project Implementation and Operation	Project Information	Description of the applicant's plan for implementing and operating the proposed Schools and Libraries Cybersecurity Pilot Program project.
32	Goals and Objectives	Project Information	Applicant's goals and objectives for the proposed Schools and Libraries Cybersecurity Pilot Program project.
33	Correction of Known Security Flaws and Routine Backups	Project Information	Information on whether the applicant plans to correct known security flaws and/or conduct routine backups as part of the proposed Schools and Libraries Cybersecurity Pilot Program project.

Item #	Field Description	Category	Purpose/Instructions
34	Recommended Cybersecurity Best Practices	Project Information	Information on whether the applicant plans to implement recommended best practices from highly-regarded cybersecurity organizations (e.g., the DOE, CISA, the National Institute of Standards and Technology (NIST), etc.) as part of the proposed Schools and Libraries Cybersecurity Pilot Program project.
35	Designated Cybersecurity Officer	Project Information	Information on the applicant's officer or other senior-level staff member that will be the designated cybersecurity officer and the tasks for which the officer will be responsible for.
36	Estimated Timeline for Ramping Up Proposed Pilot Project	Project Information	Estimated timeline for ramping up the proposed Schools and Libraries Cybersecurity Pilot program project.
37	Data and Metrics Collected by Applicant	Project Information	Description of the data the applicant will collect and the metrics it will use to assess the outcomes of the proposed Schools and Libraries Cybersecurity Pilot Program project, including, but not limited to, a description of how the project, will collect, track, and store such information.
38	Cost-Effectiveness Data and Metrics Collected by Service Provider	Project Information	Information on data the applicant will require its selected service providers to collect, track, and measure to determine the cost-effectiveness of Schools and Libraries Cybersecurity Pilot program-funded cybersecurity equipment and services.
39	Awareness and Readiness Data and Metrics Collected by Service Provider	Project Information	Information on the data the applicant will require its selected service providers to collect, track, and measure to determine the impact/effect on the applicant's current cybersecurity awareness and readiness.
40	Non-monetary Challenges	Project Information	Information on the non-monetary cybersecurity challenges faced by the applicant and if/how the Pilot project will address them.
41	Current Cybersecurity Measures	Project Information	Information on the current cybersecurity measures that are utilized by the applicant.
42	Cybersecurity Training	Project Information	Information about the applicant's cybersecurity training efforts, including, but not limited to the number/percentage of students, school and library staff, and/or library patrons who receive cybersecurity training, and training participation rates.

Item #	Field Description	Category	Purpose/Instructions
43	Free and Low-Cost Cybersecurity Resources	Project Information	Information on whether the applicant is utilizing or plans to utilize any of the free or low-cost cybersecurity resources identified/offered by the DOE or CISA, and which resources it is utilizing/plans to utilize. If an applicant has not started to utilize the available free and low-cost cybersecurity resources, they should explain what are the impediments that are preventing them from doing so.
44	Impediments to Developing a More Robust Cybersecurity Posture	Project Information	If applicable, information on why an applicant has not been able to take any preventative or mitigating actions to protect against cybersecurity threats and attacks and implement a more robust cybersecurity posture.
45	Ability of Proposed Pilot Project to be Self-sustaining	Project Information	Information on whether/how the applicant plans for the Schools and Libraries Cybersecurity Pilot Program project to be self-sustaining once established and after the Pilot program ends.
46	Network Equipment, Hardware and Software Services	Project Information	Information on any network equipment, hardware or software services the applicant plans to request as part of its Schools and Libraries Cybersecurity Pilot project, including, but not limited to, any cloud services or third-party managed cybersecurity services.
47	Cybersecurity Protections for Broadband Networks and Data Outside of the Pilot Program	Project Information	Information on whether the applicant plans to obtain or upgrade any of its cybersecurity protections for its broadband networks and data outside of the Schools and Libraries Cybersecurity Pilot program.
48	Implementation of Cybersecurity Recommendations or Framework Outside of Pilot Program	Project Information	If not selected to participate in the Schools and Libraries Cybersecurity Pilot Program, information on whether the applicant/participant has resources to begin implementation of the DOE's and/or CISA's cybersecurity recommendations and/or a cybersecurity program or framework.
49	Funding for Non-cybersecurity Equipment and Services That Support Cybersecurity Equipment and Services	Project Information	Information on whether the proposed Schools and Libraries Cybersecurity Pilot project has funding for any non-cybersecurity equipment or services that the applicant/participant will use to support cybersecurity equipment or services and protect against cybersecurity threats and attacks, including, but not limited to, whether the equipment/services facilitate capturing, transmitting, or storing data about cybersecurity threats, attacks, and/or incidents.

Item #	Field Description	Category	Purpose/Instructions
50	Will Service Provider be Required to Include any No Cost Cybersecurity Equipment and/or Services	Project Information	Information on whether the applicant will require its selected service provider(s) to provide any cybersecurity equipment and/or services at no cost to the applicant, including a description of the applicable equipment and services.
51	Required Free and Low Cost Cybersecurity Resources	Project Information	Information on any mandatory free and/or low cost cybersecurity resources the applicant expects the its selected service providers to implement and utilize.
52	Estimated Costs of Pilot-Eligible Services and Equipment	Project Information	Estimated cost information for the services and equipment that the applicant will seek funding through the Schools and Libraries Cybersecurity Pilot Program.
53	Total Estimated Funding Request	Project Information	Total estimated funding the applicant anticipates requesting from the Schools and Libraries Cybersecurity Pilot Program for eligible cybersecurity equipment and services.
54	Estimated Applicant/Participant Share of Cost for Eligible Items	Project Information	Applicant's estimated share of the costs for eligible equipment and services for which it requests funding under the Schools and Libraries Cybersecurity Pilot Program.
55	Estimated Applicant/Participant Cost for Ineligible Items	Project Information	Cost that the applicant expects to pay for equipment and services that ineligible for funding under the Schools and Libraries Cybersecurity Pilot Program.
56	Total Estimated Pilot Project Cost	Project Information	Total cost that the applicant estimates it will incur for participating in the Schools and Libraries Cybersecurity Pilot Program.
57	Sources of Support for Applicant's/Participant's Share of Cost for Eligible Items	Project Information	Information on the sources of financial support the applicant will use to pay its share of the cost for equipment and services that are eligible for funding under the Schools and Libraries Cybersecurity Pilot Program.
58	Plan to Cover Cost of Ineligible Items	Project Information	Information on the applicant's plan to pay the cost of equipment and services that are ineligible for funding under the Schools and Libraries Cybersecurity Pilot Program.
59	Supporting Documentation	Project Information	Provides an option for the user to upload and submit documents to support their proposed Pilot Program project.

Item #	Field Description	Category	Purpose/Instructions
60	I am authorized to submit this application on behalf of the above-named applicant 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 applicant 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).	Certifications	The Authorized Person is required to make all required certifications and provide all required signatures.

Item #	Field Description	Category	Purpose/Instructions
61	In addition to the foregoing, this applicant 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.	Certifications	See Item No. 60 above.

Item #	Field Description	Category	Purpose/Instructions
62	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, sections 1001, 286-287 and 1341 and Title 31, sections 3729–3730 and 3801–3812).	Certifications	See Item No. 60 above.

Item #	Field Description	Category	Purpose/Instructions
63	The applicant 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.	Certifications	See Item No. 60 above.
64	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.	Certifications	See Item No. 60 above.

Item #	Field Description	Category	Purpose/Instructions
65	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 for which I am seeking funding under the Schools and Libraries Cybersecurity Pilot Program.	Certifications	See Item No. 60 above.
66	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.	Certifications	See Item No. 60 above.
67	Name of Authorized Person	Signature	The Authorized Person is required to make all required certifications and provide all required signatures. This is the name of the Authorized Person certifying and submitting the form.
68	Title or Position of Authorized Person	Signature	This is the title or position of the Authorized Person certifying and submitting the form.
69	Date Submitted	Signature	Auto generated by system.
70	Date Signed	Signature	Auto generated by system.