U.S. DEPARTMENT OF
ENERGY

Office of
Cybersecurity, Energy Security,
and Emergency Response

Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) FOA

DE-FOA-0002986 FOA Webinar

Notice

- Welcome and thank you for attending!
- All attendee microphones and videos have been disabled.
- If you have any questions during this discussion, please send them to DE-FOA-0002986@netl.doe.gov. **Questions submitted via chat will not receive responses.**
- This webinar will focus solely on information provided in the FOA.
- Attendance at this webinar is not required. Your participation is **completely voluntary.** Participation does not affect your score in the evaluation process.
- **This webinar is being recorded.** Continued participation in this webinar will be considered your consent. If you do not consent to your name and/or image being recorded, please log off this webinar.

Agenda

1. Introductions
2. RMUC Program Overview
3. Registration Requirements
   - Infrastructure xCHANGE
   - SAM.gov
   - FedConnect
   - Key Submission Points
4. RMUC ACT FOA Overview
   - Award Information
   - Eligibility
   - Timeline
5. Application Process
   - Pre-Applications
   - Full Applications
   - Applications Not of Interest
6. Merit Review and Selection Process
7. Topic Areas
   - Topic Area 1: Eligible Utilities Only
   - Topic Area 2: All Eligible Entities
   - Topic Area 3: All Eligible Entities
8. Concluding Remarks

Rural and Municipal Utility Cybersecurity Program Funding Opportunity Webinar

December 19, 2023

1:00 p.m. ET

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Rural and Municipal Utility Cybersecurity Program

Charles Pruss
Federal Project Manager
Energy Delivery and Security Division
NETL

Cynthia Hsu
Cybersecurity Program Manager
RMUC Program
DOE CESER

Fania Barwick
Implementation Manager
RMUC Program
DOE CESER

Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program

Bipartisan Infrastructure Law (BIL) Section 40124: RMUC Program

Funding:

$250 million over 5 years (FY22-26) via grants, technical assistance, and cooperative agreements

Objectives:

1. Deploy cybersecurity technology, operational capability, or services that *enhance the security posture* of electric utilities through improvements in the ability to **protect** against, **detect**, **respond** to, or **recover** from a **cybersecurity threat.**

2. Increase the participation of eligible entities in cybersecurity **threat *information sharing* programs.**

RMUC Program

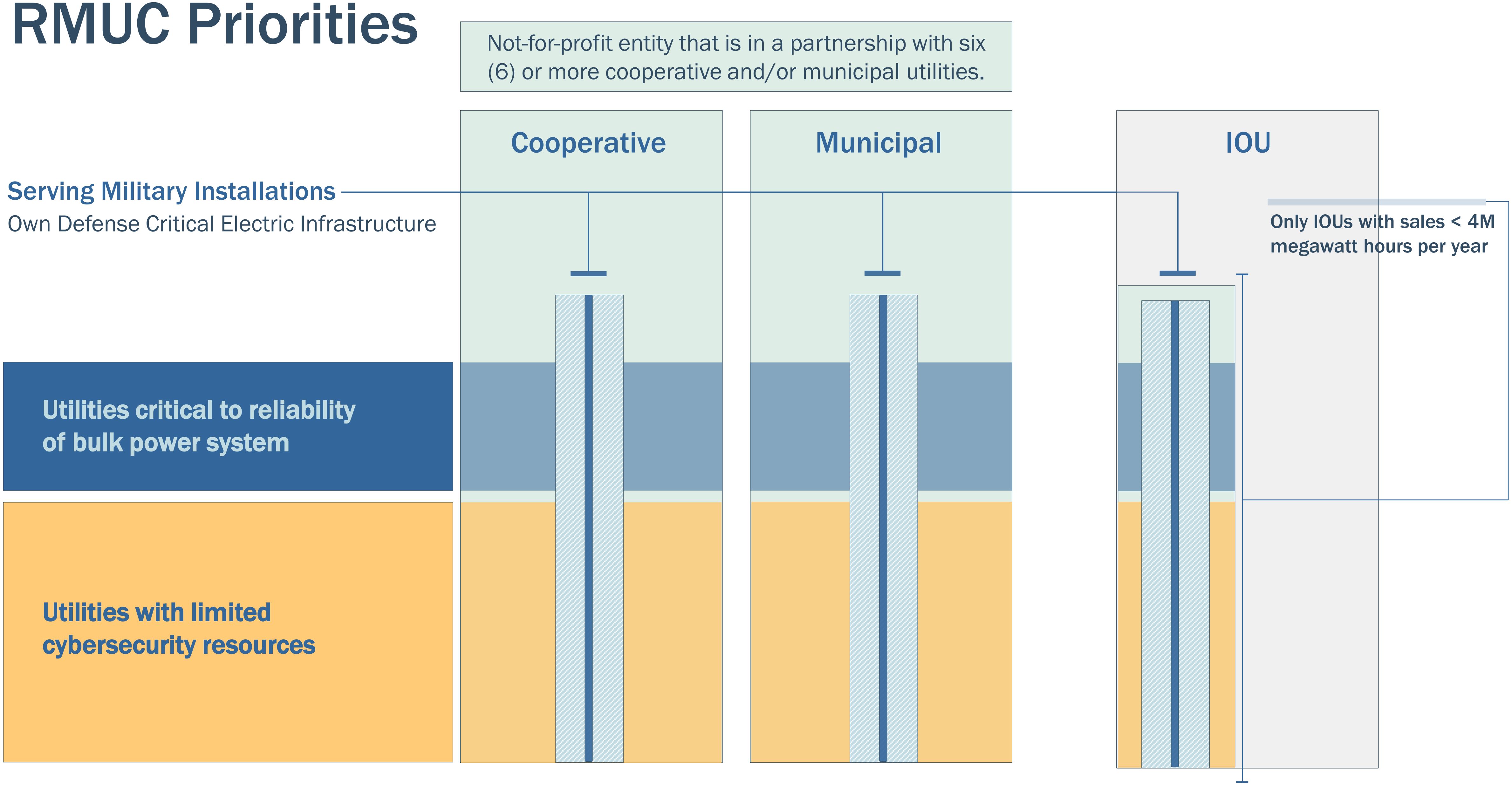
Eligibility:

- Rural electric cooperatives
- Municipal/Public Power electric utilities
  - a utility owned by a political subdivision of a State
  - a utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State
- Not-for-profits in partnership with rural or municipal electric utilities
- Investor-owned electric utilities that sell < 4,000,000 MWh/year

Priority Given to Eligible Entities:

- with limited cybersecurity resources;
- that own assets critical to the reliability of the bulk-power system (BPS); or,
- that own defense critical electric infrastructure (DCEI)

RMUC Priorities


Not-for-profit entity that is in a partnership with six (6) or more cooperative and/or municipal utilities.
Cooperative
Municipal
IOU
Serving Military Installations
Own Defense Critical Electric Infrastructure
Only IOUs with sales < 4M megawatt hours per year
Utilities critical to reliability of bulk power system
Utilities with limited cybersecurity resources

RMUC Advanced Cybersecurity Technology (ACT)

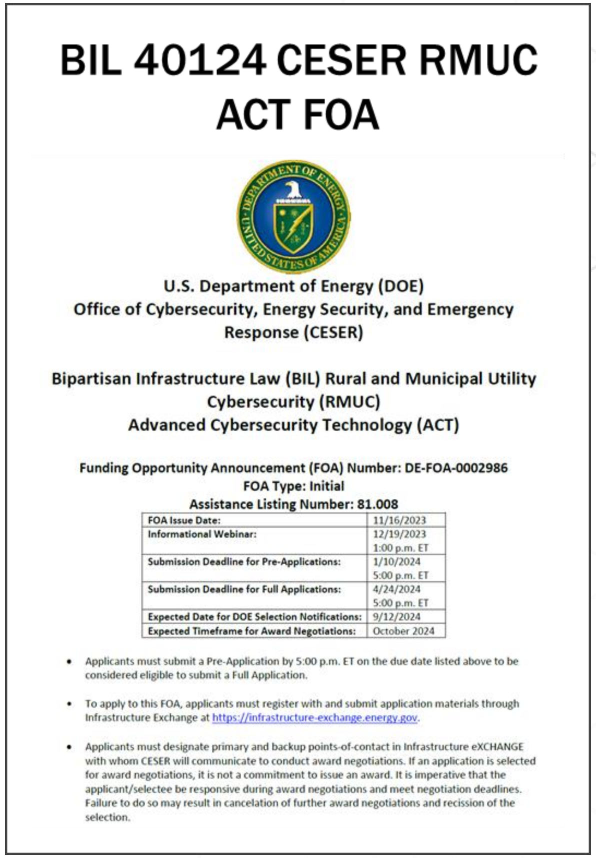
RMUC Program $70M Funding Opportunity Announcement

Downloading the ACT FOA – 2 Documents

- All applicants are required to read both the *BIL RMUC ACT Funding Opportunity Announcement DE-FOA-0002986* (FOA) and the accompanying *BIL RMUC ACT Administrative Requirements* (FOA Requirements) documents.

- Applicants are expected to understand and adhere to the submission requirements described in both documents.

- If there are any inconsistencies between the FOA and this presentation or statements from DOE personnel, applicants should rely on the language in FOA and FOA Requirements documents.



BIL 40124 CESER RMUC ACT FOA

U.S. Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC)
Advanced Cybersecurity Technology (ACT)

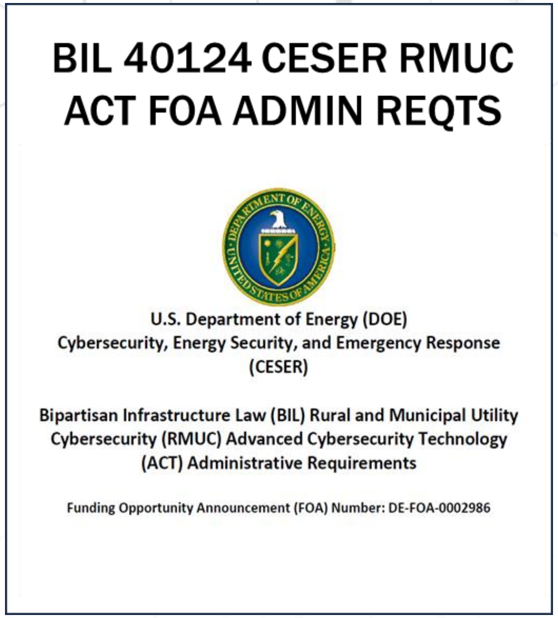
Funding Opportunity Announcement (FOA) Number: DE-FOA-0002986
FOA Type: Initial
Assistance Listing Number: 81.008

FOA Issue Date:	11/16/2023
Informational Webinar:	12/19/2023 1:00 p.m. ET
Submission Deadline for Pre-Applications:	1/10/2024 5:00 p.m. ET
Submission Deadline for Full Applications:	4/24/2024 5:00 p.m. ET
Expected Date for DOE Selection Notifications:	9/12/2024
Expected Timeframe for Award Negotiations:	October 2024

- Applicants must submit a Pre-Application by 5:00 p.m. ET on the due date listed above to be considered eligible to submit a Full Application.

- To apply to this FOA, applicants must register with and submit application materials through Infrastructure Exchange at https://infrastructure-exchange.energy.gov.

- Applicants must designate primary and backup points-of-contact in Infrastructure eXCHANGE with whom CESER will communicate to conduct award negotiations. If an application is selected for award negotiations, it is not a commitment to issue an award. It is imperative that the applicant/selectee be responsive during award negotiations and meet negotiation deadlines. Failure to do so may result in cancelation of further award negotiations and recission of the selection.



BIL 40124 CESER RMUC ACT FOA ADMIN REQTS

U.S. Department of Energy (DOE)
Cybersecurity, Energy Security, and Emergency Response (CESER)

Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) Administrative Requirements

Funding Opportunity Announcement (FOA) Number: DE-FOA-0002986

Both documents are available for download on Infrastructure eXCHANGE.

BIL RMUC ACT FOA (DE-FOA-0002986)

Anticipated Schedule

• FOA Issue Date	11/16/2023
• Submission Deadline for Pre-Applications	01/10/2024
• Expected Date for “Invited to Apply”	February 2024
• Submission Deadline for Full Applications	04/24/2024
• Expected Date for DOE Selection Notification	09/12/2024
• Expected Timeframe for Award Negotiations	Oct 2024 – Jan 2025
• Expected Date for Awards	Jan – Feb 2025

RMUC ACT FOA Issued	FOA Informational Webinar	**Pre-Applications Due** / DOE Review of Pre-Applications	Exchange Status Notification: Invited / Not Invited		**Full Applications DUE**	DOE Review of Full Applications				Estimated Date for Selection Notifications	DOE and Potential Recipient Award Negotiations			Estimated Date for Awards	
Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25

Registration Requirements

Application Success

- Want all potential applicants to understand the application process.
- There are several priority steps applicants must take before they can submit a Pre-application.
- Unfortunately, some of these steps are not "instantaneous" and may take several weeks to complete.
- START NOW!

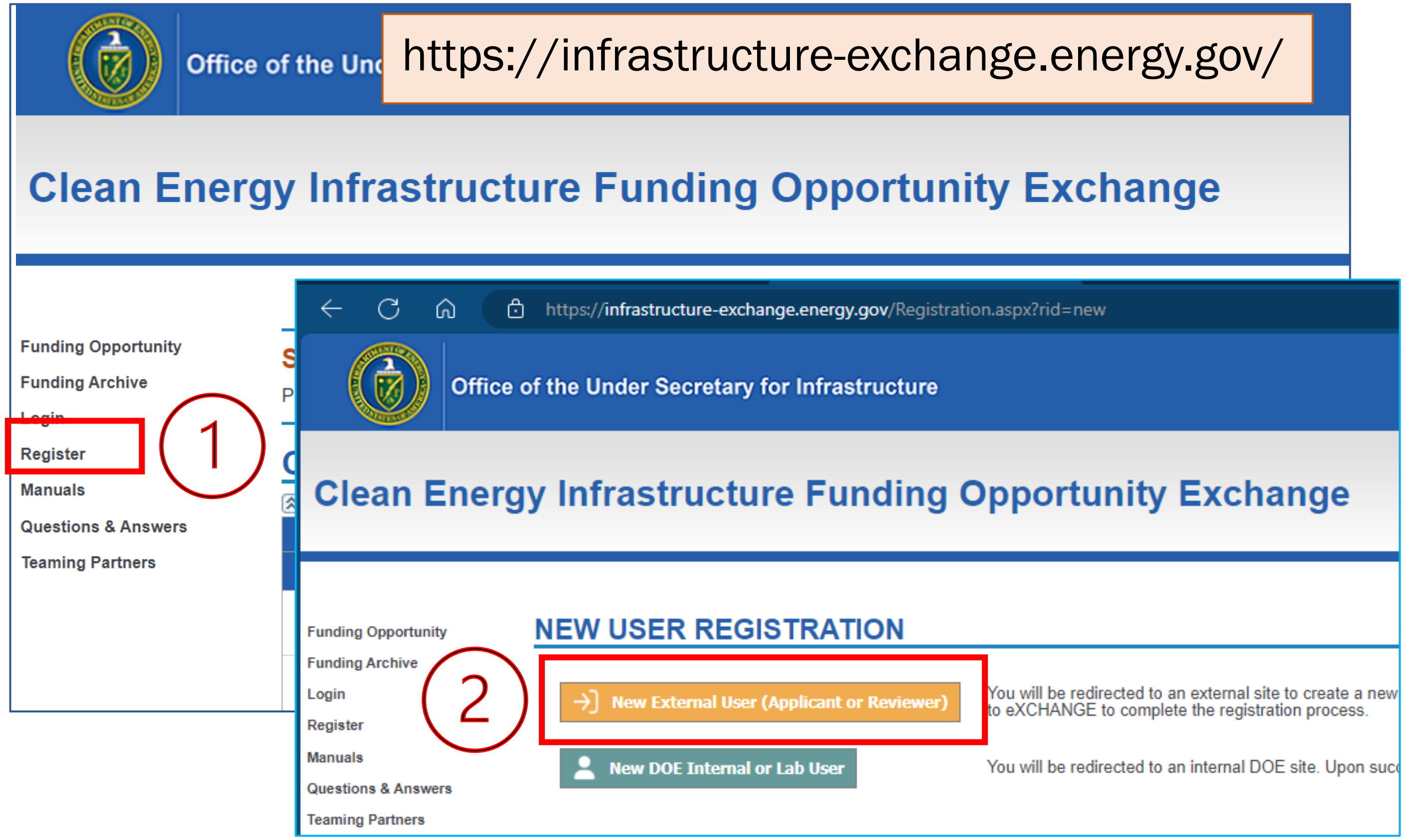
Registration Requirements

To apply to this FOA, Applicants must:

- ❑ Register with the Clean Energy Infrastructure eXCHANGE (https://infrastructure-exchange.energy.gov/)
- ❑ Register with the System for Award Management (SAM) (https://sam.gov/content/home);
- ❑ Obtain a Unique Entity Identifier (UEI) number;
- ❑ Register with Grants.gov (http://www.grants.gov); and
- ❑ Register in FedConnect (https://www.fedconnect.net).

Additional information on registration requirements can be found in Section V of the FOA.

FOA: Infrastructure xCHANGE



https://infrastructure-exchange.energy.gov/

Office of the Und

Clean Energy Infrastructure Funding Opportunity Exchange

- Funding Opportunity
- Funding Archive
- Login
- Register
- Manuals
- Questions & Answers
- Teaming Partners

1

https://infrastructure-exchange.energy.gov/Registration.aspx?rid=new

Office of the Under Secretary for Infrastructure

Clean Energy Infrastructure Funding Opportunity Exchange

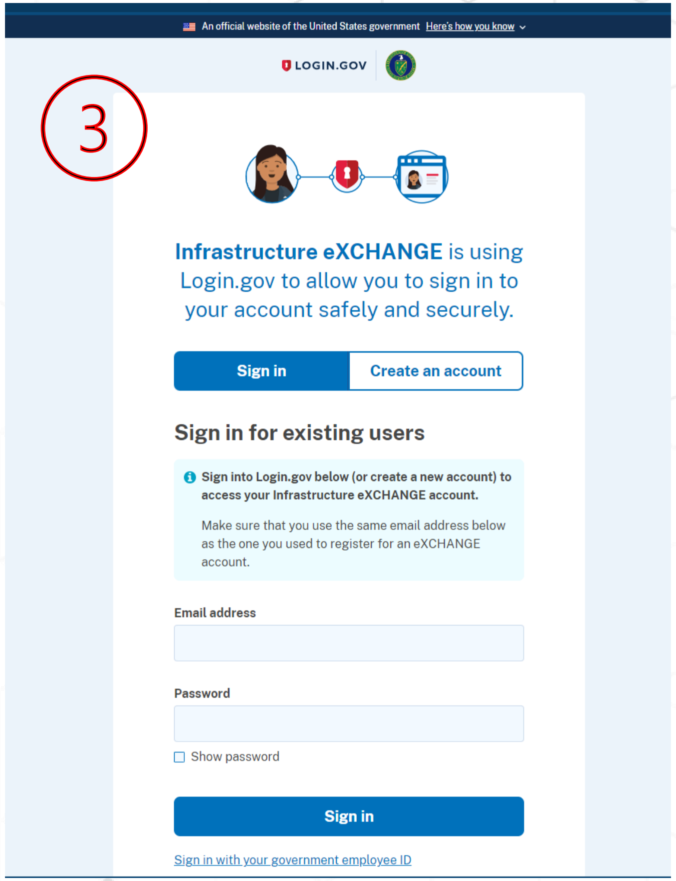
- Funding Opportunity
- Funding Archive
- Login
- Register
- Manuals
- Questions & Answers
- Teaming Partners

2

NEW USER REGISTRATION

New External User (Applicant or Reviewer) — You will be redirected to an external site to create a new to eXCHANGE to complete the registration process.

New DOE Internal or Lab User — You will be redirected to an internal DOE site. Upon suc



An official website of the United States government Here's how you know

LOGIN.GOV

3

Infrastructure eXCHANGE is using Login.gov to allow you to sign in to your account safely and securely.

Sign in | Create an account

Sign in for existing users

Sign into Login.gov below (or create a new account) to access your Infrastructure eXCHANGE account.

Make sure that you use the same email address below as the one you used to register for an eXCHANGE account.

Email address

Password

□ Show password

Sign in

Sign in with your government employee ID

The login that is created in (3) will be used every time you login to eXCHANGE

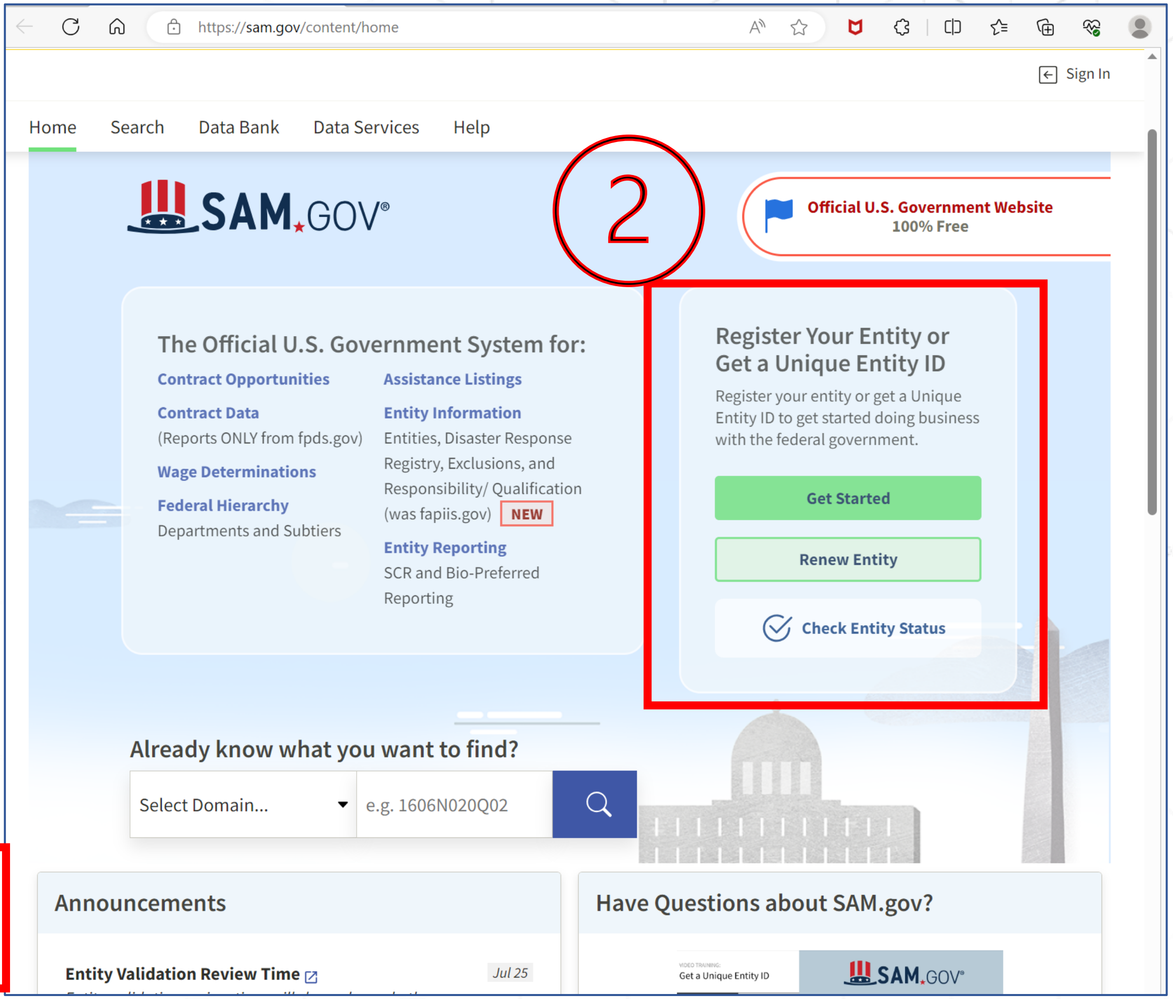
FOA: SAM.gov

What is SAM.gov?

The System for Award Management (SAM.gov) is an official website of the U.S. Government. There is no cost to use SAM.gov. You can use this site to:

- Register to do business with the U.S. Government
- Update, renew, or check the status of your entity registration
- Search for entity registration and exclusion records
- Search for assistance listings (formerly CFDA.gov), wage determinations (formerly WDOL.gov), contract opportunities (formerly FBO.gov), and contract data reports (formerly part of FPDS.gov).
- View and submit BioPreferred and Service Contract Reports
- Access publicly available award data via data extracts and system accounts

1 https://sam.gov/content/home


https://sam.gov/content/home
Sign In
Home
Search
Data Bank
Data Services
Help
SAM.GOV
2
Official U.S. Government Website
100% Free

The Official U.S. Government System for:

Contract Opportunities

Contract Data
(Reports ONLY from fpds.gov)

Wage Determinations

Federal Hierarchy
Departments and Subtiers

Assistance Listings

Entity Information
Entities, Disaster Response Registry, Exclusions, and Responsibility/ Qualification (was fapiis.gov) NEW

Entity Reporting
SCR and Bio-Preferred Reporting

Register Your Entity or Get a Unique Entity ID

Register your entity or get a Unique Entity ID to get started doing business with the federal government.

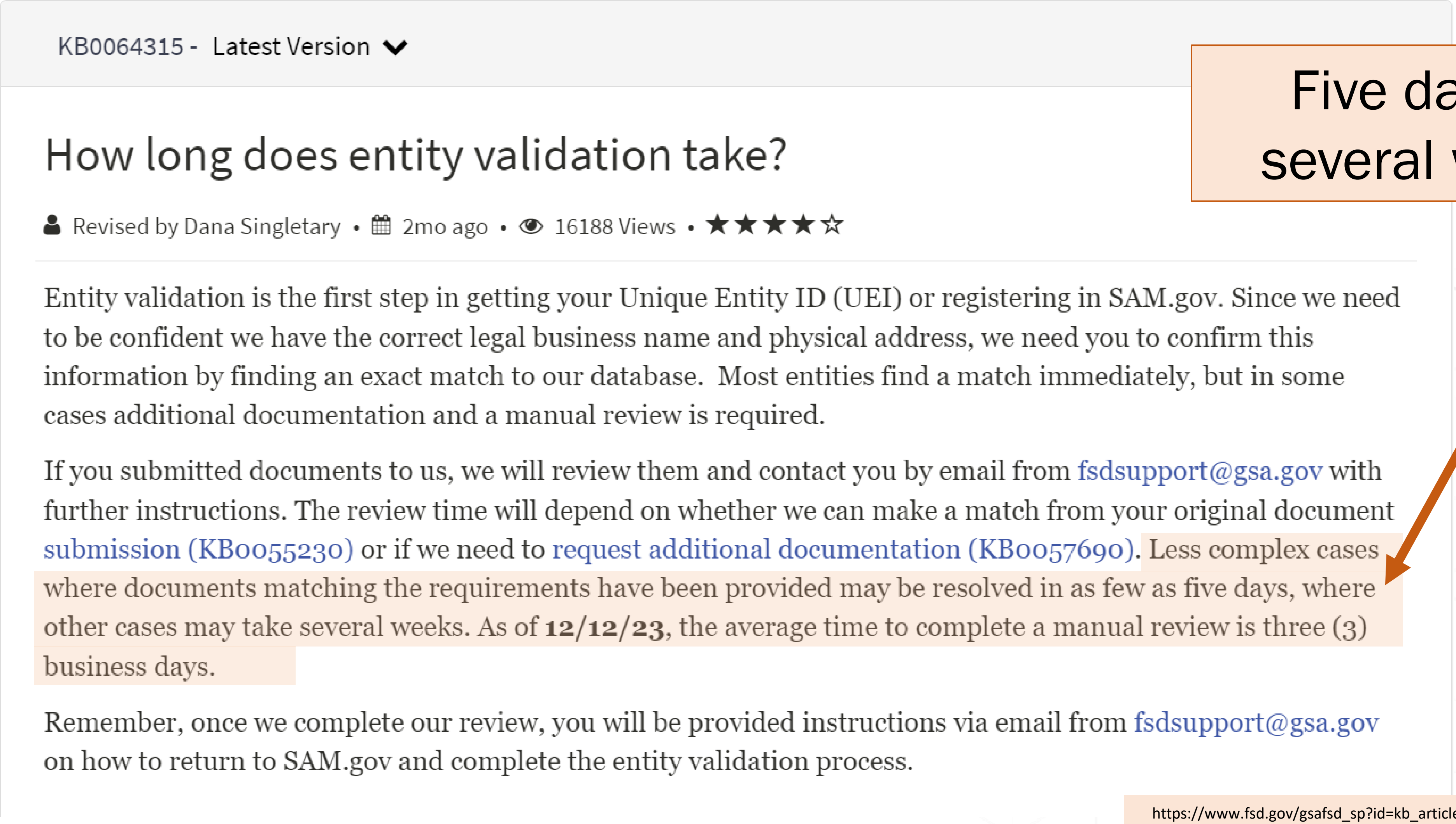
Already know what you want to find?

Announcements

Entity Validation Review Time Jul 25

Have Questions about SAM.gov?

How long does it take to get a UEI?



KB0064315 - Latest Version

How long does entity validation take?

Revised by Dana Singletary • 2mo ago • 16188 Views • ★★★★☆

Entity validation is the first step in getting your Unique Entity ID (UEI) or registering in SAM.gov. Since we need to be confident we have the correct legal business name and physical address, we need you to confirm this information by finding an exact match to our database. Most entities find a match immediately, but in some cases additional documentation and a manual review is required.

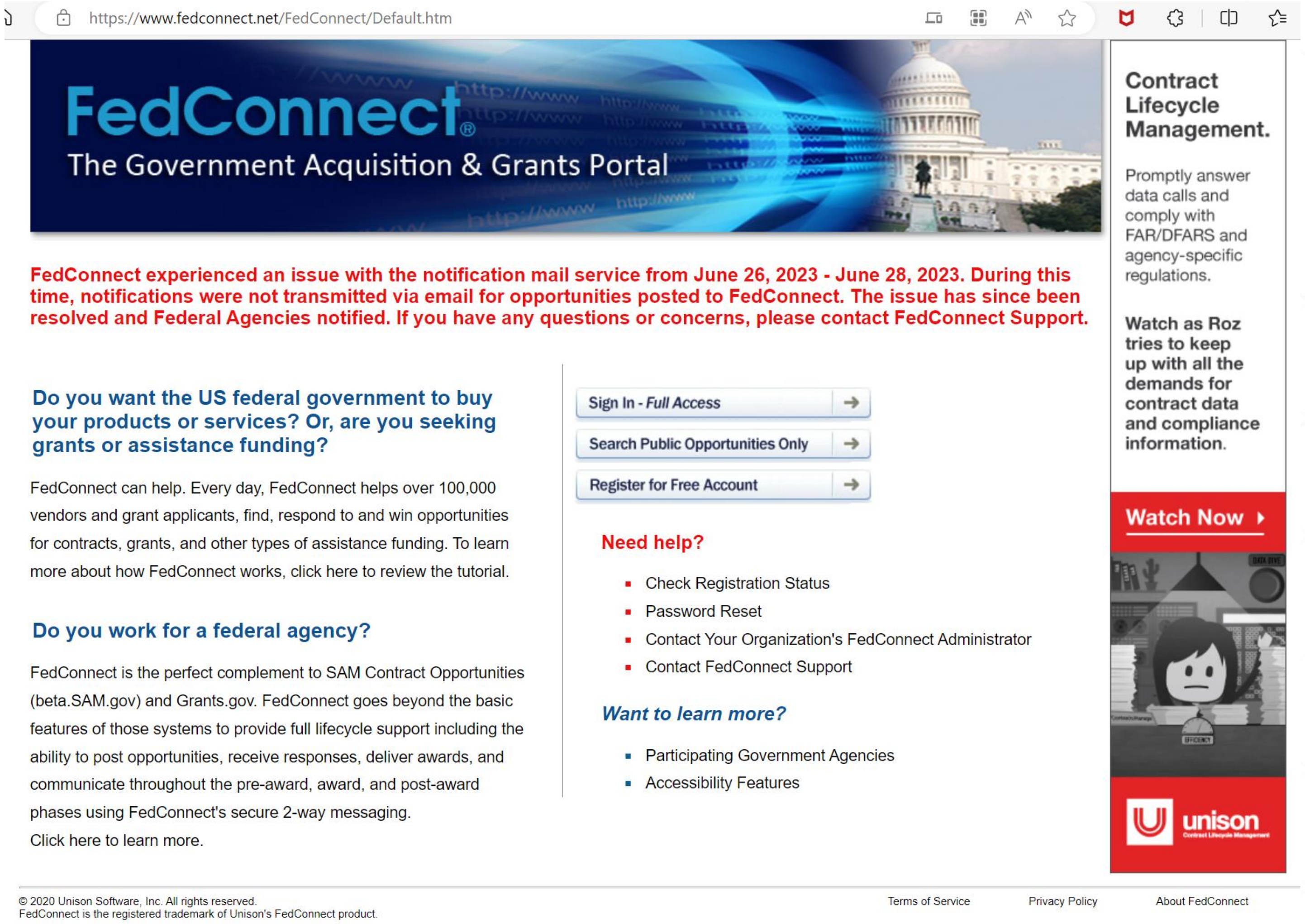
If you submitted documents to us, we will review them and contact you by email from fsdsupport@gsa.gov with further instructions. The review time will depend on whether we can make a match from your original document submission (KB0055230) or if we need to request additional documentation (KB0057690). Less complex cases where documents matching the requirements have been provided may be resolved in as few as five days, where other cases may take several weeks. As of **12/12/23**, the average time to complete a manual review is three (3) business days.

Remember, once we complete our review, you will be provided instructions via email from fsdsupport@gsa.gov on how to return to SAM.gov and complete the entity validation process.

Five days to several weeks

https://www.fsd.gov/gsafsd_sp?id=kb_article_view&sysparm_article=KB0064315

FOA: FedConnect



https://www.fedconnect.net/FedConnect/Default.htm
FedConnect®
The Government Acquisition & Grants Portal

FedConnect experienced an issue with the notification mail service from June 26, 2023 - June 28, 2023. During this time, notifications were not transmitted via email for opportunities posted to FedConnect. The issue has since been resolved and Federal Agencies notified. If you have any questions or concerns, please contact FedConnect Support.

Do you want the US federal government to buy your products or services? Or, are you seeking grants or assistance funding?

FedConnect can help. Every day, FedConnect helps over 100,000 vendors and grant applicants, find, respond to and win opportunities for contracts, grants, and other types of assistance funding. To learn more about how FedConnect works, click here to review the tutorial.

Do you work for a federal agency?

FedConnect is the perfect complement to SAM Contract Opportunities (beta.SAM.gov) and Grants.gov. FedConnect goes beyond the basic features of those systems to provide full lifecycle support including the ability to post opportunities, receive responses, deliver awards, and communicate throughout the pre-award, award, and post-award phases using FedConnect's secure 2-way messaging.
Click here to learn more.

Sign In - *Full Access* →
Search Public Opportunities Only →
Register for Free Account →

Need help?

- Check Registration Status
- Password Reset
- Contact Your Organization's FedConnect Administrator
- Contact FedConnect Support

Want to learn more?

- Participating Government Agencies
- Accessibility Features

Terms of Service Privacy Policy About FedConnect

https://www.fedconnect.net/FedConnect/Default.htm

Registration Things to Remember

- Register as early as possible as some of these systems, particularly SAM, can take several weeks to complete the process.

Do not wait until the day before the submission deadline to begin this registration process.

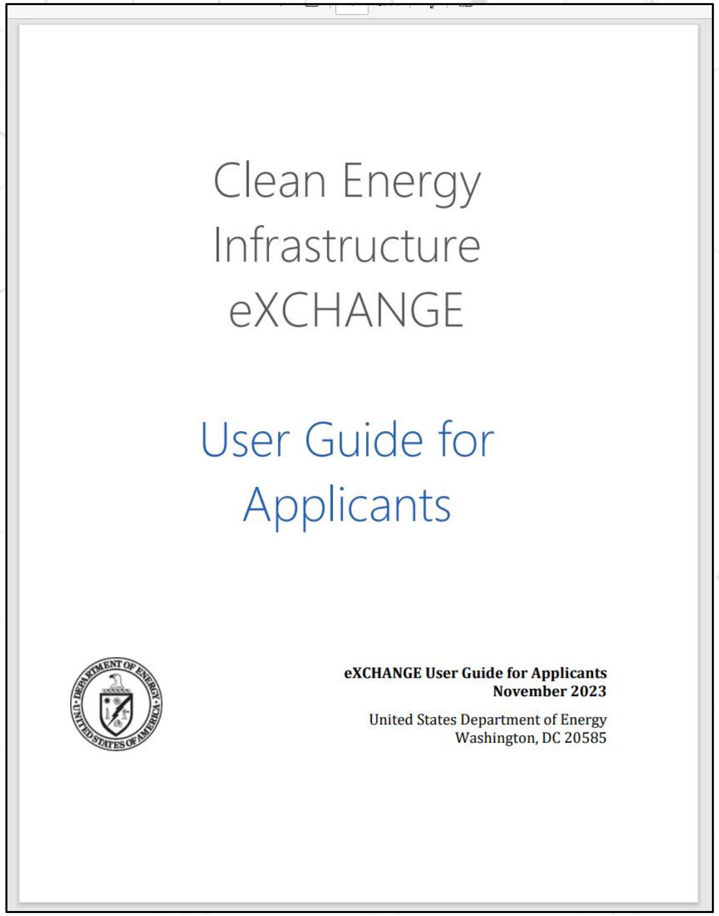
- Give yourself sufficient time to complete both the registration and application submission processes.

- Try to submit your application materials 1-2 days early. Technical issues can arise that could delay submittal upload.

- The application window on eXCHANGE will **close automatically** once the submission deadline window closes.

How to Submit Your Pre-Application

- Pre-Applications must be submitted through the Clean Energy Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/
  - DOE will not review or consider applications submitted through other means
- The Users' Guide for Applying to the Department of Energy Funding Opportunity Announcements can be found at https://infrastructure-exchange.energy.gove/Manuals.aspx



Clean Energy Infrastructure eXCHANGE

User Guide for Applicants

eXCHANGE User Guide for Applicants
November 2023

United States Department of Energy
Washington, DC 20585

Key Submission Points

❑ Verify data entry in eXCHANGE. Ensure data aligns with SAM.gov registration.

- Submissions could be deemed ineligible due to an incorrect entry.

❑ DOE strongly encourages Applicants to submit 1-2 days prior to the deadline to allow for full upload of application documents and to avoid potential technical glitches with eXCHANGE.

❑ **Make sure you hit the “submit” button**

- **Any change made after you hit submit will un-submit your application** and you will need to hit the submit button again.

❑ For your records, print out (or save as a PDF) the eXCHANGE page at each step, which contains the application’s Control Number.

Applicant Points-of-Contact

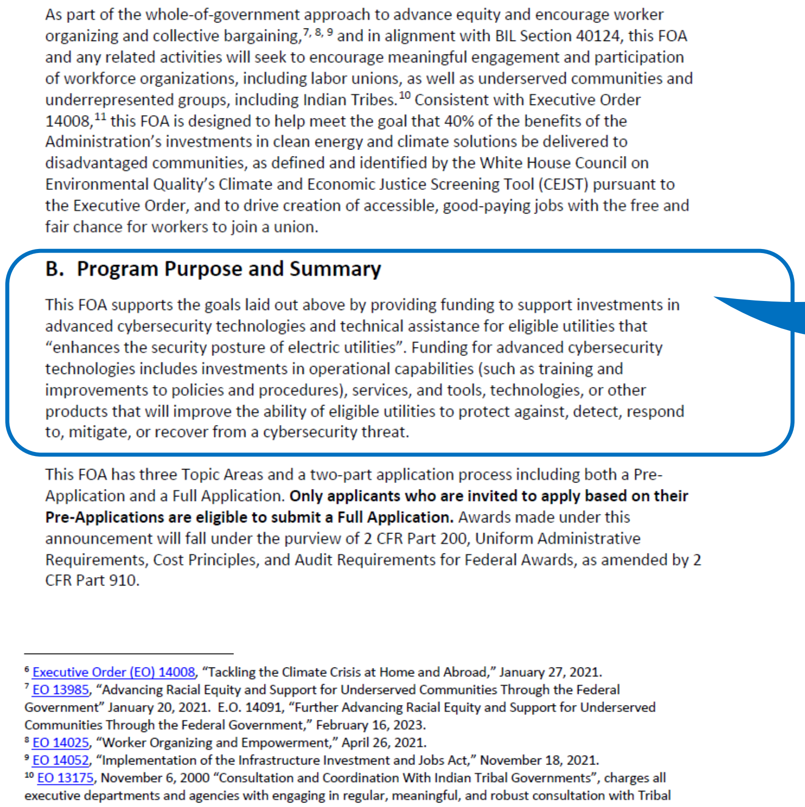
- Designate primary and backup point-of-contact in eXCHANGE with whom DOE will communicate award negotiations.

- **It is imperative that the Applicant/Selectee be responsive during award negotiations and meet negotiation deadlines.**
  - Failure to do so may result in cancellation of further award negotiations and rescission of the Selection.

RMUC ACT FOA Overview

FOA Description

FOA Section I.B (pg. 9)



As part of the whole-of-government approach to advance equity and encourage worker organizing and collective bargaining,[7, 8, 9] and in alignment with BIL Section 40124, this FOA and any related activities will seek to encourage meaningful engagement and participation of workforce organizations, including labor unions, as well as underserved communities and underrepresented groups, including Indian Tribes.[10] Consistent with Executive Order 14008,[11] this FOA is designed to help meet the goal that 40% of the benefits of the Administration's investments in clean energy and climate solutions be delivered to disadvantaged communities, as defined and identified by the White House Council on Environmental Quality's Climate and Economic Justice Screening Tool (CEJST) pursuant to the Executive Order, and to drive creation of accessible, good-paying jobs with the free and fair chance for workers to join a union.

B. Program Purpose and Summary

This FOA supports the goals laid out above by providing funding to support investments in advanced cybersecurity technologies and technical assistance for eligible utilities that "enhances the security posture of electric utilities". Funding for advanced cybersecurity technologies includes investments in operational capabilities (such as training and improvements to policies and procedures), services, and tools, technologies, or other products that will improve the ability of eligible utilities to protect against, detect, respond to, mitigate, or recover from a cybersecurity threat.

This FOA has three Topic Areas and a two-part application process including both a Pre-Application and a Full Application. **Only applicants who are invited to apply based on their Pre-Applications are eligible to submit a Full Application.** Awards made under this announcement will fall under the purview of 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, as amended by 2 CFR Part 910.

[6] Executive Order (EO) 14008, "Tackling the Climate Crisis at Home and Abroad," January 27, 2021.
[7] EO 13985, "Advancing Racial Equity and Support for Underserved Communities Through the Federal Government" January 20, 2021. E.O. 14091, "Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," February 16, 2023.
[8] EO 14025, "Worker Organizing and Empowerment," April 26, 2021.
[9] EO 14052, "Implementation of the Infrastructure Investment and Jobs Act," November 18, 2021.
[10] EO 13175, November 6, 2000 "Consultation and Coordination With Indian Tribal Governments", charges all executive departments and agencies with engaging in regular, meaningful, and robust consultation with Tribal

"This FOA supports Administration goals by providing funding to support investments in advanced cybersecurity technologies and technical assistance for eligible utilities that "enhances the security posture of electric utilities".

Advanced cybersecurity technologies includes **operational capabilities** (such as training and improvements to policies and procedures), **services**, and tools, technologies, or other products that will improve the ability of eligible utilities to protect against, detect, respond to, mitigate, or recover from a cybersecurity threat."

Award Information (FOA Section II.A. pg. 16)

Topic Area	Anticipated # of Awards	Anticipated Federal Share	Minimum Non-Federal Cost Share (%)	Anticipated Applicant Cost Share	Total Anticipated Award
Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities	10	Up to $2 Million	5%	Up to $105,263	Up to $20 Million
Topic Area 2: Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem	10	Up to $3 Million	5%	Up to $157,895	Up to $30 Million
Topic Area 3: Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources	10	Up to $2 Million	0%	n/a	Up to $20 Million
TOTALS	**30**				**Up to $70M**

Who is Eligible to Apply?

The proposed prime recipient and subrecipient(s) must be domestic entities.

Additionally, BIL Section 40124 directs who is eligible to apply for funding under this FOA.

Eligible Entities

(A) Rural electric cooperatives;

(B) Utilities owned by a political subdivision of a State, such as a municipally owned electric utility;

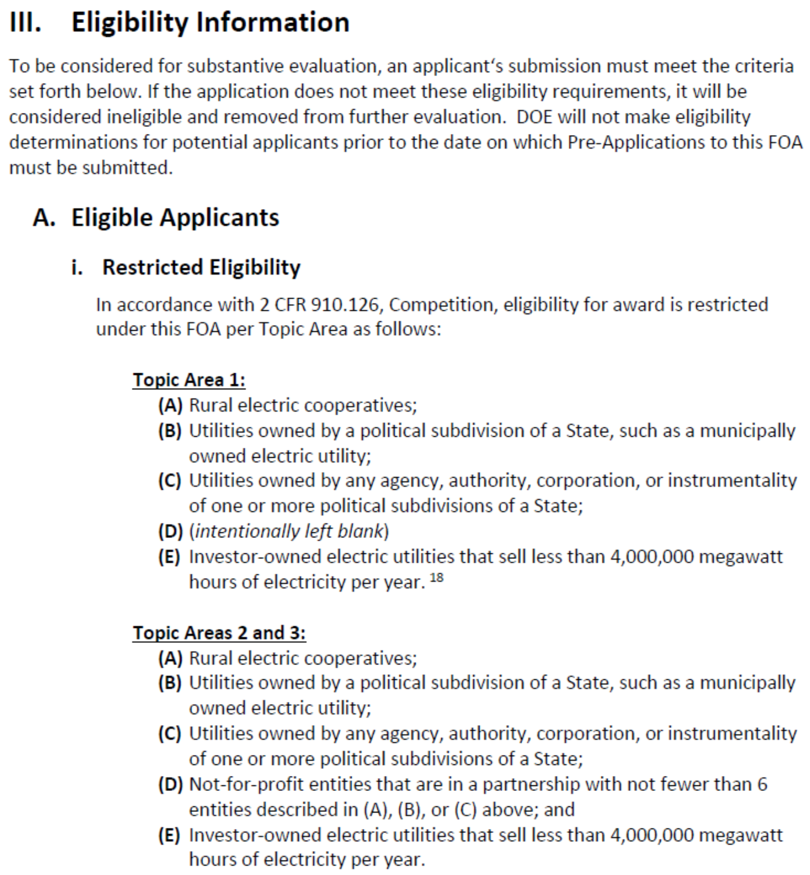
(C) Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State;

(D) Not-for-profit entities that are in a partnership with not fewer than 6 entities described in (A), (B), or (C) above; and

(E) Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year.

Who is Eligible to Apply?

FOA Section III.A.i (pg. 17)



III. Eligibility Information

To be considered for substantive evaluation, an applicant's submission must meet the criteria set forth below. If the application does not meet these eligibility requirements, it will be considered ineligible and removed from further evaluation. DOE will not make eligibility determinations for potential applicants prior to the date on which Pre-Applications to this FOA must be submitted.

A. Eligible Applicants

i. Restricted Eligibility

In accordance with 2 CFR 910.126, Competition, eligibility for award is restricted under this FOA per Topic Area as follows:

Topic Area 1:

(A) Rural electric cooperatives;
(B) Utilities owned by a political subdivision of a State, such as a municipally owned electric utility;
(C) Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State;
(D) (*intentionally left blank*)
(E) Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year. [18]

Topic Areas 2 and 3:

(A) Rural electric cooperatives;
(B) Utilities owned by a political subdivision of a State, such as a municipally owned electric utility;
(C) Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State;
(D) Not-for-profit entities that are in a partnership with not fewer than 6 entities described in (A), (B), or (C) above; and
(E) Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year.

Per the guidance provided under BIL Section 40124, eligibility for each Topic Area is as follows:

Topic Area 1 – Entities that fall under items (A), (B), (C), and (E) on the previous slide

Topic Areas 2 & 3 – All entities listed on the previous slide are eligible to apply

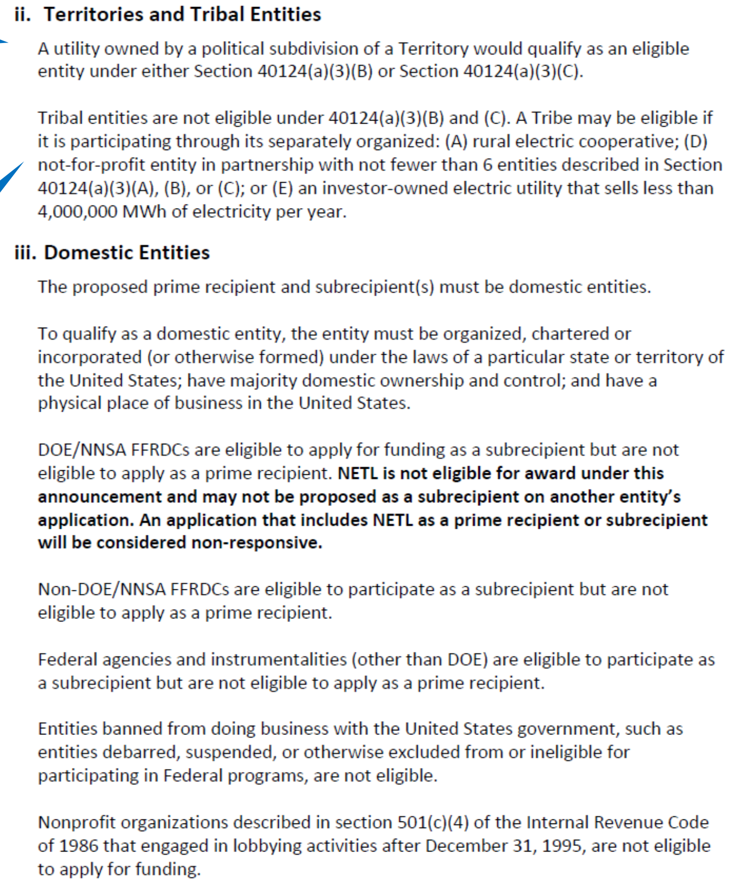
Additional Eligibility Information

Territories and Tribal Entities

- A utility owned by a political subdivision of a Territory would qualify as an eligible entity under items (B) or (C) on the previous slide.

- Tribal entities are not eligible under (B) and (C) on the previous slide. A Tribe may be eligible if it is participating through its separately organized: (A) rural electric cooperative; (D) not-for-profit entity in partnership with not fewer than 6 entities described in (A), (B), or (C) on the previous slide; or (E) an investor-owned electric utility that sells less than 4,000,000 MWh of electricity per year.

FOA Section III.A.ii (pg. 18)



ii. Territories and Tribal Entities

A utility owned by a political subdivision of a Territory would qualify as an eligible entity under either Section 40124(a)(3)(B) or Section 40124(a)(3)(C).

Tribal entities are not eligible under 40124(a)(3)(B) and (C). A Tribe may be eligible if it is participating through its separately organized: (A) rural electric cooperative; (D) not-for-profit entity in partnership with not fewer than 6 entities described in Section 40124(a)(3)(A), (B), or (C); or (E) an investor-owned electric utility that sells less than 4,000,000 MWh of electricity per year.

iii. Domestic Entities

The proposed prime recipient and subrecipient(s) must be domestic entities.

To qualify as a domestic entity, the entity must be organized, chartered or incorporated (or otherwise formed) under the laws of a particular state or territory of the United States; have majority domestic ownership and control; and have a physical place of business in the United States.

DOE/NNSA FFRDCs are eligible to apply for funding as a subrecipient but are not eligible to apply as a prime recipient. **NETL is not eligible for award under this announcement and may not be proposed as a subrecipient on another entity's application. An application that includes NETL as a prime recipient or subrecipient will be considered non-responsive.**

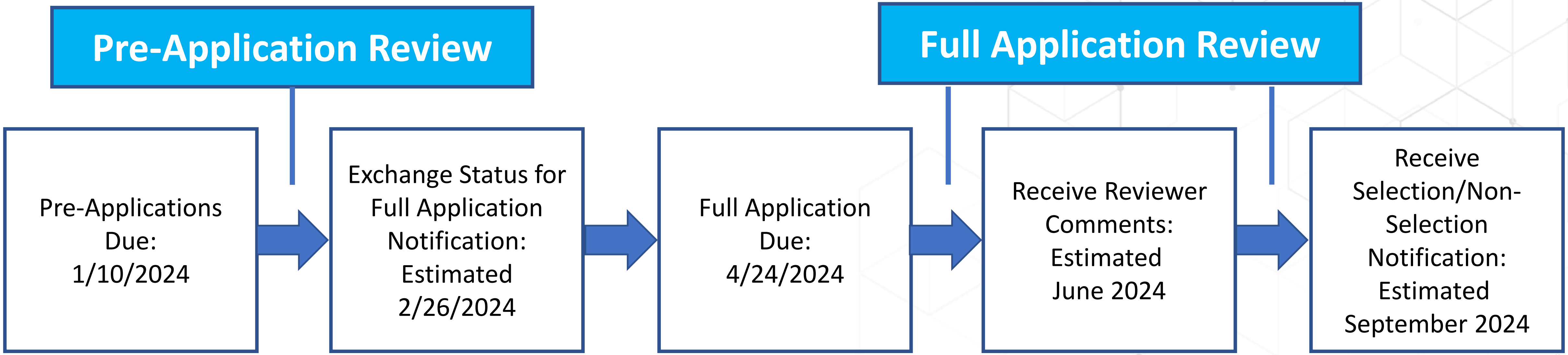
Non-DOE/NNSA FFRDCs are eligible to participate as a subrecipient but are not eligible to apply as a prime recipient.

Federal agencies and instrumentalities (other than DOE) are eligible to participate as a subrecipient but are not eligible to apply as a prime recipient.

Entities banned from doing business with the United States government, such as entities debarred, suspended, or otherwise excluded from or ineligible for participating in Federal programs, are not eligible.

Nonprofit organizations described in section 501(c)(4) of the Internal Revenue Code of 1986 that engaged in lobbying activities after December 31, 1995, are not eligible to apply for funding.

FOA Timeline



Pre-Application Review

Full Application Review

Pre-Applications Due: 1/10/2024

Exchange Status for Full Application Notification: Estimated 2/26/2024

Full Application Due: 4/24/2024

Receive Reviewer Comments: Estimated June 2024

Receive Selection/Non-Selection Notification: Estimated September 2024

DOE anticipates making awards by January 31, 2025

Application Process

Pre-Applications vs. Full Applications

This FOA consists of 2 steps – Pre-Applications and Full Applications

Pre-Applications

- See Topic Area specific eligible entity requirements
- May submit **multiple applications per topic area**
- Optional response template available on eXCHANGE for each Topic Area
- Need to only **submit one document** – completed Topic Area specific response
- Submissions **reviewed based on Topic Area criteria** outlined in the FOA
- Applications will **either be "invited"** to submit a full application or **"not invited"** to continue to the full application process

Full Applications

- Only Pre-applicants **"invited"** may submit
- May submit **only one per Topic Area**
- Must be an expansion of the Pre-Application idea – **should not be radically different**
- Submission package requires **multiple documents** – as many as 18
- Submissions **reviewed based on Topic Area criteria** outlined in the FOA
- Selections will be determined based on **review results** and **program policy factors**
- Applicants notified of selection/non-selection
- Project negotiations & award

Pre-Applications

Pre-Applications **must be submitted by**

1/10/2024 at 5:00 pm ET

through Clean Energy Infrastructure eXCHANGE

Pre-Application Review Criteria

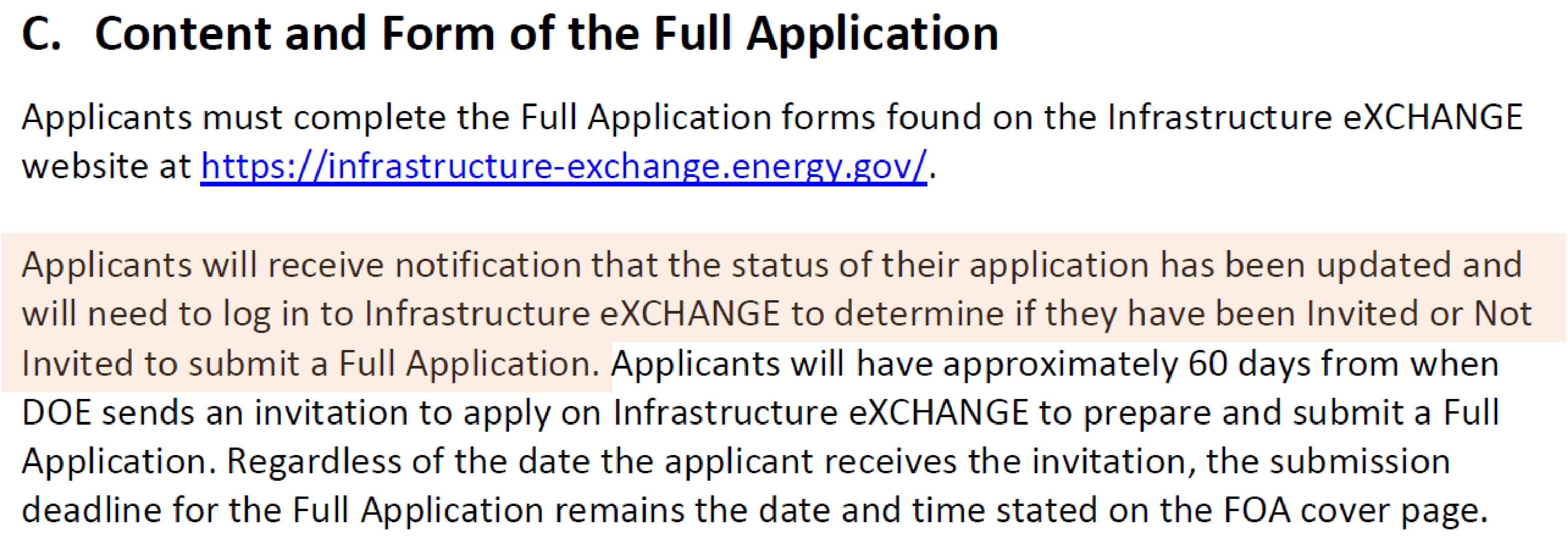
Each Topic Area has unique review criteria for each of the following categories:

- Applicant Profile (Topic Area 2 & 3 only)
- Project Overview
- Community Benefits
- Technical Approach
- Project Design and Management

Additional information on the Pre-Application Review Criteria can be found in FOA Sections VI.C, VII.C, and VIII.C.

How you will be notified if invited to submit a Full Application

FOA Section IV.C. (pg. 23)



C. Content and Form of the Full Application

Applicants must complete the Full Application forms found on the Infrastructure eXCHANGE website at https://infrastructure-exchange.energy.gov/.

Applicants will receive notification that the status of their application has been updated and will need to log in to Infrastructure eXCHANGE to determine if they have been Invited or Not Invited to submit a Full Application. Applicants will have approximately 60 days from when DOE sends an invitation to apply on Infrastructure eXCHANGE to prepare and submit a Full Application. Regardless of the date the applicant receives the invitation, the submission deadline for the Full Application remains the date and time stated on the FOA cover page.

Some Things to Consider

Applicants should anticipate the following if they are “invited” to submit a Full Application.

Some documents may take time to gather.

- Letters from Participating Utilities (Topics 2 & 3)
- Not-for-Profit Partnership Letters (Topics 2 & 3)
- Resumes (all Topic Areas)

The Full Application submission process is labor intensive and can be challenging if you are not familiar with the process.

Full Applications

- **Applicants must submit a Full Application by 4/24/2024 at 5:00 pm ET** through Clean Energy Infrastructure eXCHANGE

- Full Applications are eligible for review if:
  - The Applicant is an eligible entity according to Section III.A "Eligible Applicants";
  - The Applicant submitted a Pre-Application and was invited to submit a Full Application;
  - The proposed project is responsive to Section III.F "Responsiveness Criteria"; and
  - The Full Application is compliant with Section IV.C "Content and Form of the Full Application."

Full Application Review Criteria

Each Topic Area contains unique review criteria and consists of 5 categories

- Project Design and Management
- Assessment and Analysis Approach
- Implementation and Operations Plan
- Commitment, Team, and Resources
- Community Benefits Plan

Additional information on the Full Application Review Criteria can be found in Sections VI.E, VII.E, and VIII.E of the FOA

Multiple Applications – Utilities

Provided each application is a unique, distinct project:

- A utility may submit more than one Pre-Application to any of the 3 Topic Areas
- A utility may submit only one Full Application to each Topic Area; and
- A utility may participate as subrecipients or Participating Utilities in Topic Areas 2 or 3 on more than one application

If more than one Full Application is received from a utility within a Topic Area, then none of the Full Applications from that utility will be considered for that Topic Area.

Multiple Applications – Not-for-Profit Entities

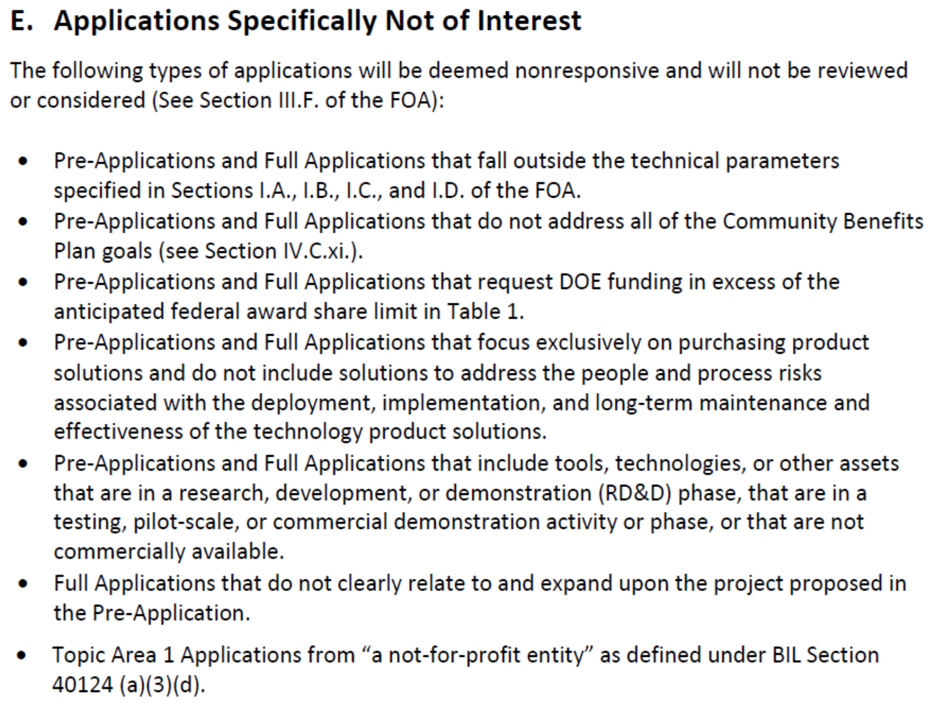
Provided each application is a unique, distinct project:

- Not-for-Profit entities may submit more than one Pre-Application to Topic Areas 2 and 3
- Not-for-Profit entities may submit only one Full Application per Topic Area

If more than one Full Application is received from a not-for profit entity within a Topic Area, then none of the Full Applications from that not-for-profit entity will be considered for that Topic Area.

Pre-Applications and Full Applications Not of Interest

FOA Section I.E (pgs. 13-14)



E. Applications Specifically Not of Interest

The following types of applications will be deemed nonresponsive and will not be reviewed or considered (See Section III.F. of the FOA):

- Pre-Applications and Full Applications that fall outside the technical parameters specified in Sections I.A., I.B., I.C., and I.D. of the FOA.
- Pre-Applications and Full Applications that do not address all of the Community Benefits Plan goals (see Section IV.C.xi.).
- Pre-Applications and Full Applications that request DOE funding in excess of the anticipated federal award share limit in Table 1.
- Pre-Applications and Full Applications that focus exclusively on purchasing product solutions and do not include solutions to address the people and process risks associated with the deployment, implementation, and long-term maintenance and effectiveness of the technology product solutions.
- Pre-Applications and Full Applications that include tools, technologies, or other assets that are in a research, development, or demonstration (RD&D) phase, that are in a testing, pilot-scale, or commercial demonstration activity or phase, or that are not commercially available.
- Full Applications that do not clearly relate to and expand upon the project proposed in the Pre-Application.
- Topic Area 1 Applications from "a not-for-profit entity" as defined under BIL Section 40124 (a)(3)(d).

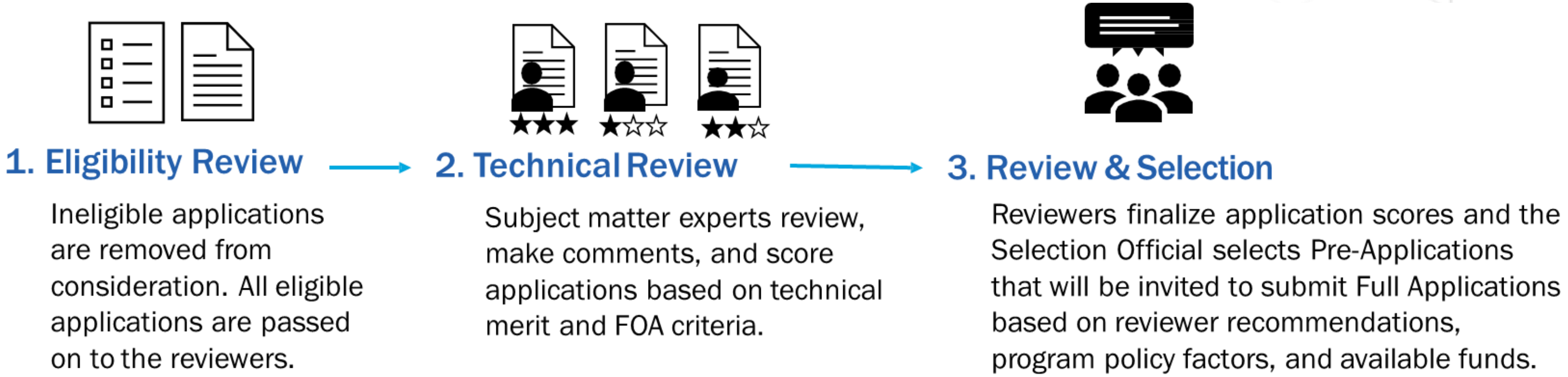
- Projects that focus exclusively on purchasing product solutions and do not include solutions to address the people and process risks associated with the deployment, implementation, and **long-term maintenance and effectiveness** of the technology product solutions.

- Full Applications **that do not clearly relate to and expand upon** the project proposed in the Pre-Application.

Merit Review and Selection Process

Merit Review & Selection Process

Pre-Applications



1. Eligibility Review →

Ineligible applications are removed from consideration. All eligible applications are passed on to the reviewers.

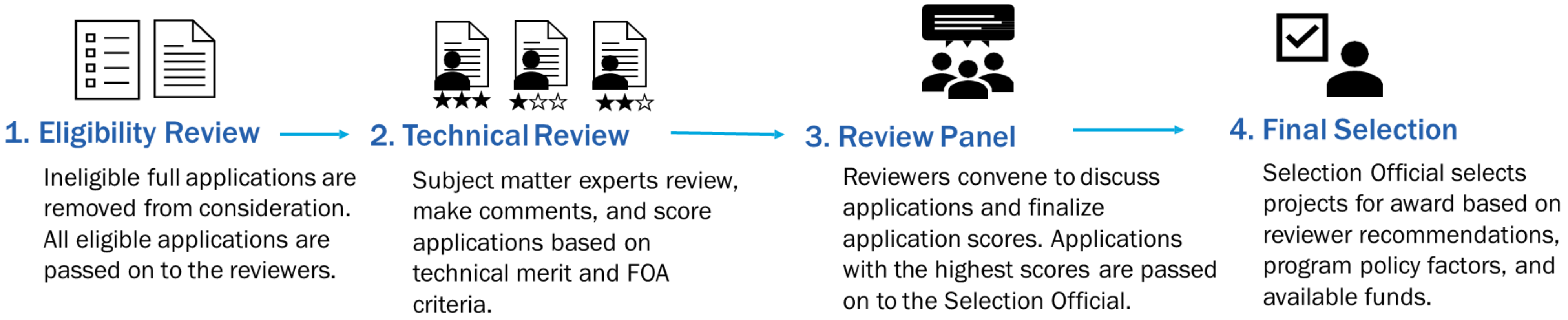
2. Technical Review →

Subject matter experts review, make comments, and score applications based on technical merit and FOA criteria.

3. Review & Selection

Reviewers finalize application scores and the Selection Official selects Pre-Applications that will be invited to submit Full Applications based on reviewer recommendations, program policy factors, and available funds.

Full Applications



1. Eligibility Review →

Ineligible full applications are removed from consideration. All eligible applications are passed on to the reviewers.

2. Technical Review →

Subject matter experts review, make comments, and score applications based on technical merit and FOA criteria.

3. Review Panel →

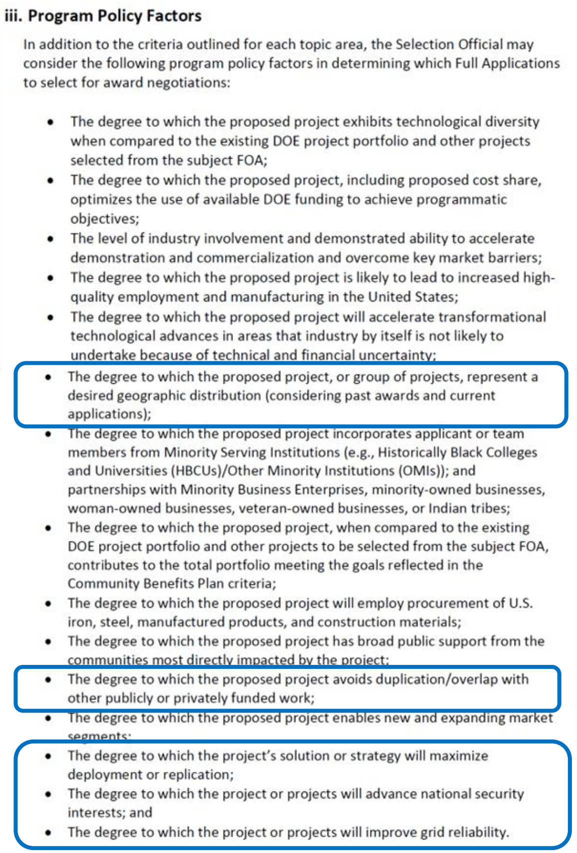
Reviewers convene to discuss applications and finalize application scores. Applications with the highest scores are passed on to the Selection Official.

4. Final Selection

Selection Official selects projects for award based on reviewer recommendations, program policy factors, and available funds.

Program Policy Factors

FOA Section IX.A.iii. (pgs. 88-89)



iii. Program Policy Factors

In addition to the criteria outlined for each topic area, the Selection Official may consider the following program policy factors in determining which Full Applications to select for award negotiations:

- The degree to which the proposed project exhibits technological diversity when compared to the existing DOE project portfolio and other projects selected from the subject FOA;
- The degree to which the proposed project, including proposed cost share, optimizes the use of available DOE funding to achieve programmatic objectives;
- The level of industry involvement and demonstrated ability to accelerate demonstration and commercialization and overcome key market barriers;
- The degree to which the proposed project is likely to lead to increased high-quality employment and manufacturing in the United States;
- The degree to which the proposed project will accelerate transformational technological advances in areas that industry by itself is not likely to undertake because of technical and financial uncertainty;
- The degree to which the proposed project, or group of projects, represent a desired geographic distribution (considering past awards and current applications);
- The degree to which the proposed project incorporates applicant or team members from Minority Serving Institutions (e.g., Historically Black Colleges and Universities (HBCUs)/Other Minority Institutions (OMIs)); and partnerships with Minority Business Enterprises, minority-owned businesses, woman-owned businesses, veteran-owned businesses, or Indian tribes;
- The degree to which the proposed project, when compared to the existing DOE project portfolio and other projects to be selected from the subject FOA, contributes to the total portfolio meeting the goals reflected in the Community Benefits Plan criteria;
- The degree to which the proposed project will employ procurement of U.S. iron, steel, manufactured products, and construction materials;
- The degree to which the proposed project has broad public support from the communities most directly impacted by the project;
- The degree to which the proposed project avoids duplication/overlap with other publicly or privately funded work;
- The degree to which the proposed project enables new and expanding market segments;
- The degree to which the project's solution or strategy will maximize deployment or replication;
- The degree to which the project or projects will advance national security interests; and
- The degree to which the project or projects will improve grid reliability.

The Selection Official may consider program policy factors in making a decision.

Program Policy Examples:

- The degree to which the proposed project, or group of projects, represent a desired geographic distribution (considering past award and current applications);
- The degree to which the proposed project avoids duplication/overlap with other publicly or privately funded work;
- The degree to which the project's solution or strategy will maximize deployment or replication;
- The degree to which the project or projects will advance national security interests;
- The degree to which the project or projects will improve grid reliability

Topic Areas

Topic Area Overview

This FOA consists of three (3) topic areas, each designed around a different aspect of helping eligible utilities improve their cybersecurity posture.

Topic Area 1 – Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities

Topic Area 2 – Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem

Topic Area 3 – Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources

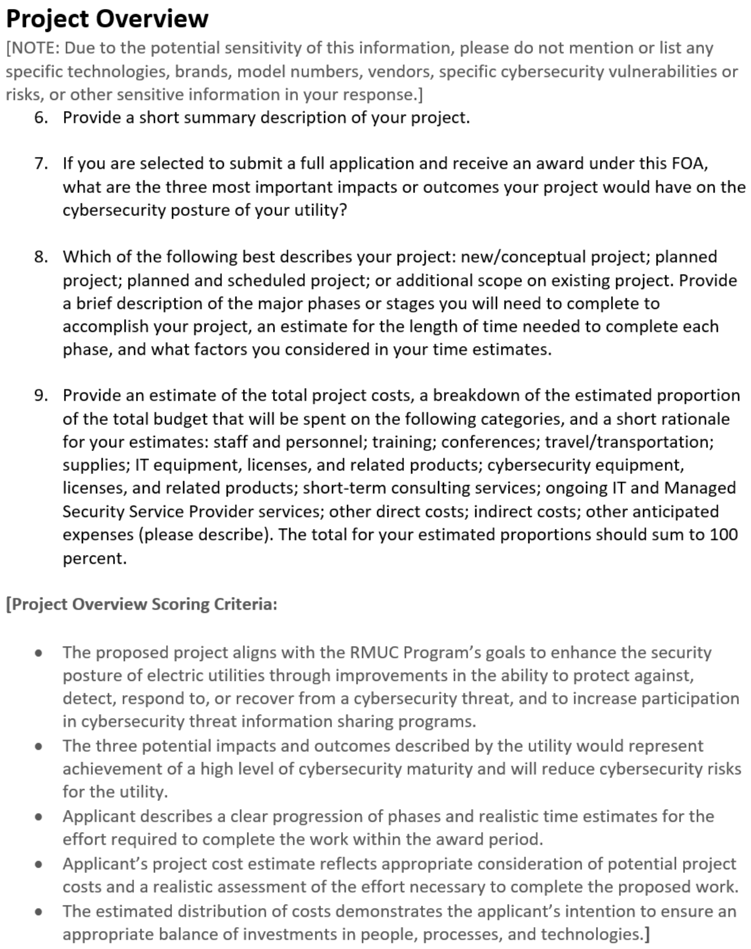
Optional Topic Area Pre-Application Templates

Pre-Application Categories

- Applicant Profile (Topic Area 2 & 3 only)
- Project Overview
- Community Benefits
- Technical Approach
- Project Design and Management

Optional Topic Area Pre-Application Templates

Pre-Application Content Requirements



Project Overview

[NOTE: Due to the potential sensitivity of this information, please do not mention or list any specific technologies, brands, model numbers, vendors, specific cybersecurity vulnerabilities or risks, or other sensitive information in your response.]

6. Provide a short summary description of your project.

7. If you are selected to submit a full application and receive an award under this FOA, what are the three most important impacts or outcomes your project would have on the cybersecurity posture of your utility?

8. Which of the following best describes your project: new/conceptual project; planned project; planned and scheduled project; or additional scope on existing project. Provide a brief description of the major phases or stages you will need to complete to accomplish your project, an estimate for the length of time needed to complete each phase, and what factors you considered in your time estimates.

9. Provide an estimate of the total project costs, a breakdown of the estimated proportion of the total budget that will be spent on the following categories, and a short rationale for your estimates: staff and personnel; training; conferences; travel/transportation; supplies; IT equipment, licenses, and related products; cybersecurity equipment, licenses, and related products; short-term consulting services; ongoing IT and Managed Security Service Provider services; other direct costs; indirect costs; other anticipated expenses (please describe). The total for your estimated proportions should sum to 100 percent.

Scoring Criteria

[Project Overview Scoring Criteria:

- The proposed project aligns with the RMUC Program's goals to enhance the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat, and to increase participation in cybersecurity threat information sharing programs.
- The three potential impacts and outcomes described by the utility would represent achievement of a high level of cybersecurity maturity and will reduce cybersecurity risks for the utility.
- Applicant describes a clear progression of phases and realistic time estimates for the effort required to complete the work within the award period.
- Applicant's project cost estimate reflects appropriate consideration of potential project costs and a realistic assessment of the effort necessary to complete the proposed work.
- The estimated distribution of costs demonstrates the applicant's intention to ensure an appropriate balance of investments in people, processes, and technologies.**]**

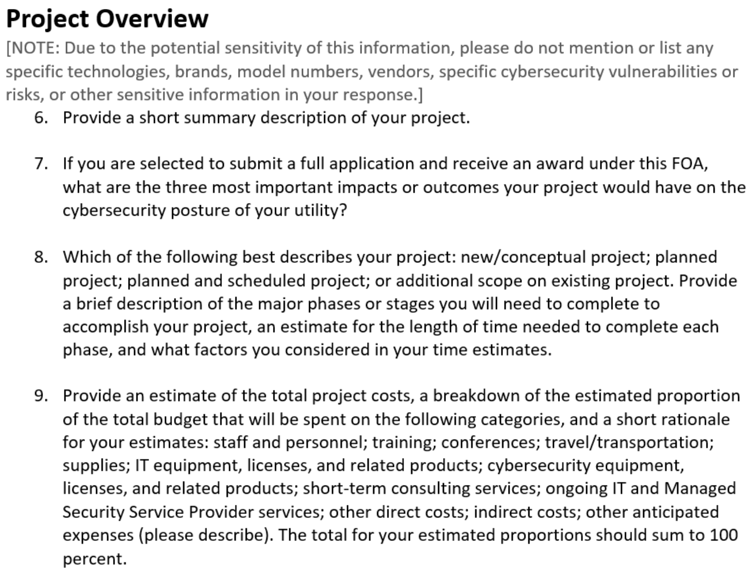
Pre-Application Categories

- Applicant Profile (Topic Area 2 & 3 only)
- Project Overview
- Community Benefits
- Technical Approach
- Project Design and Management

Topic Area templates are available for download on Infrastructure eXCHANGE.

Optional Topic Area Pre-Application Templates

Pre-Application Content Requirements



Project Overview

[NOTE: Due to the potential sensitivity of this information, please do not mention or list any specific technologies, brands, model numbers, vendors, specific cybersecurity vulnerabilities or risks, or other sensitive information in your response.]

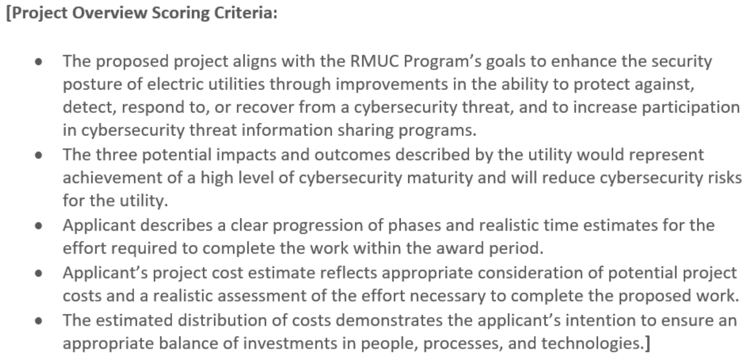
6. Provide a short summary description of your project.

7. If you are selected to submit a full application and receive an award under this FOA, what are the three most important impacts or outcomes your project would have on the cybersecurity posture of your utility?

8. Which of the following best describes your project: new/conceptual project; planned project; planned and scheduled project; or additional scope on existing project. Provide a brief description of the major phases or stages you will need to complete to accomplish your project, an estimate for the length of time needed to complete each phase, and what factors you considered in your time estimates.

9. Provide an estimate of the total project costs, a breakdown of the estimated proportion of the total budget that will be spent on the following categories, and a short rationale for your estimates: staff and personnel; training; conferences; travel/transportation; supplies; IT equipment, licenses, and related products; cybersecurity equipment, licenses, and related products; short-term consulting services; ongoing IT and Managed Security Service Provider services; other direct costs; indirect costs; other anticipated expenses (please describe). The total for your estimated proportions should sum to 100 percent.

Scoring Criteria

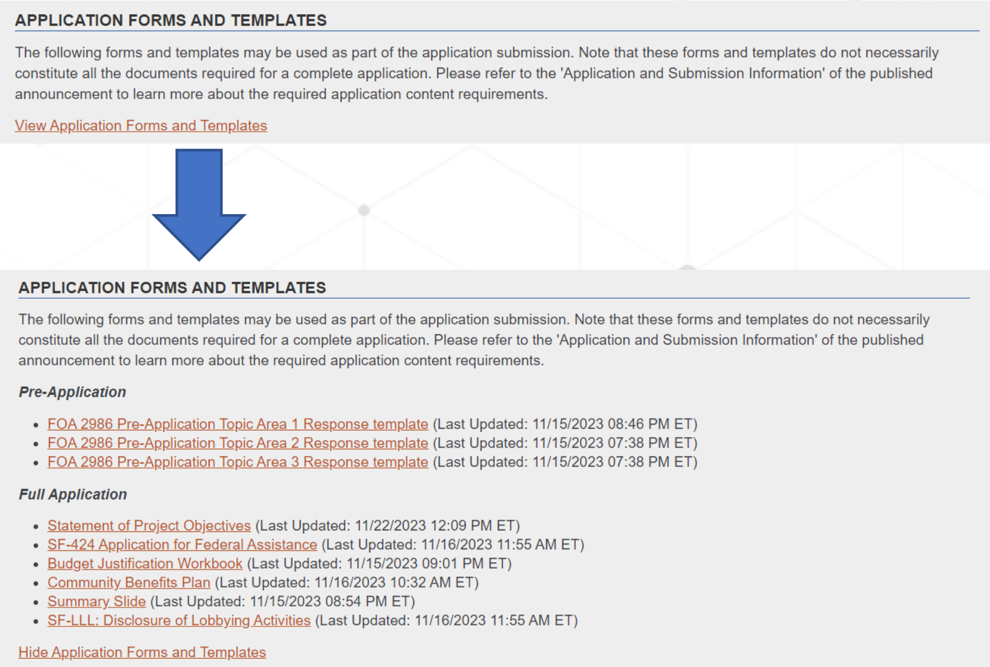


[Project Overview Scoring Criteria:

- The proposed project aligns with the RMUC Program's goals to enhance the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat, and to increase participation in cybersecurity threat information sharing programs.
- The three potential impacts and outcomes described by the utility would represent achievement of a high level of cybersecurity maturity and will reduce cybersecurity risks for the utility.
- Applicant describes a clear progression of phases and realistic time estimates for the effort required to complete the work within the award period.
- Applicant's project cost estimate reflects appropriate consideration of potential project costs and a realistic assessment of the effort necessary to complete the proposed work.
- The estimated distribution of costs demonstrates the applicant's intention to ensure an appropriate balance of investments in people, processes, and technologies.]

Pre-Application Categories

- Applicant Profile (Topic Area 2 & 3 only)
- Project Overview
- Community Benefits
- Technical Approach
- Project Design and Management



APPLICATION FORMS AND TEMPLATES

The following forms and templates may be used as part of the application submission. Note that these forms and templates do not necessarily constitute all the documents required for a complete application. Please refer to the 'Application and Submission Information' of the published announcement to learn more about the required application content requirements.

View Application Forms and Templates

APPLICATION FORMS AND TEMPLATES

The following forms and templates may be used as part of the application submission. Note that these forms and templates do not necessarily constitute all the documents required for a complete application. Please refer to the 'Application and Submission Information' of the published announcement to learn more about the required application content requirements.

Pre-Application

- FOA 2986 Pre-Application Topic Area 1 Response template (Last Updated: 11/15/2023 08:46 PM ET)
- FOA 2986 Pre-Application Topic Area 2 Response template (Last Updated: 11/15/2023 07:38 PM ET)
- FOA 2986 Pre-Application Topic Area 3 Response template (Last Updated: 11/15/2023 07:38 PM ET)

Full Application

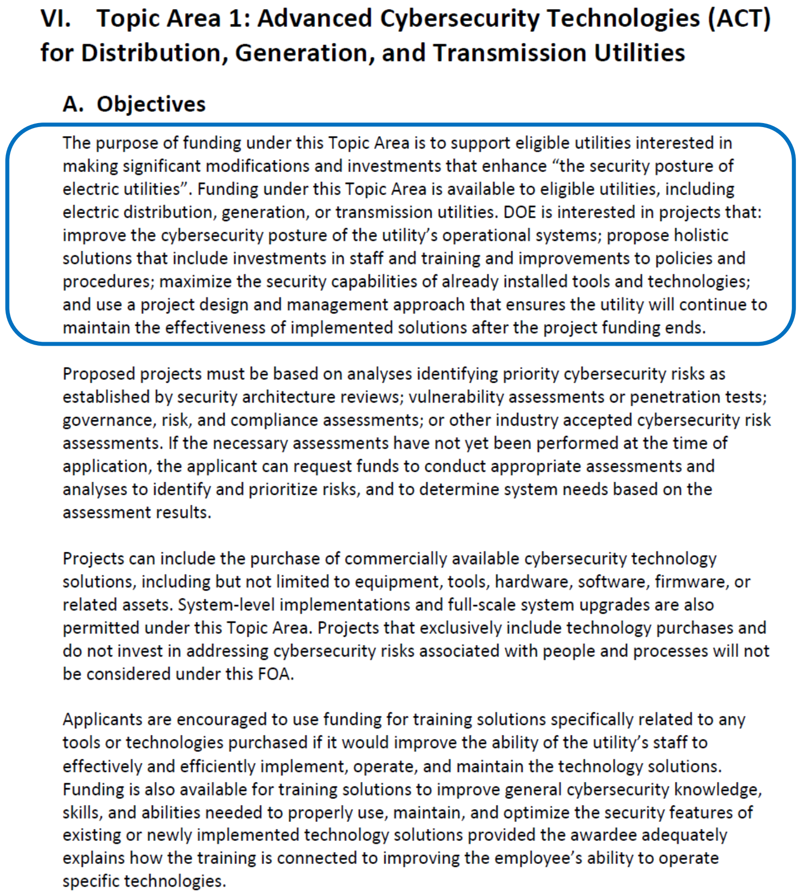
- Statement of Project Objectives (Last Updated: 11/22/2023 12:09 PM ET)
- SF-424 Application for Federal Assistance (Last Updated: 11/16/2023 11:55 AM ET)
- Budget Justification Workbook (Last Updated: 11/15/2023 09:01 PM ET)
- Community Benefits Plan (Last Updated: 11/16/2023 10:32 AM ET)
- Summary Slide (Last Updated: 11/15/2023 08:54 PM ET)
- SF-LLL: Disclosure of Lobbying Activities (Last Updated: 11/16/2023 11:55 AM ET)

Hide Application Forms and Templates

Topic Area 1 – Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities

Topic Area 1 – Objective and Goals

FOA Section VI.A (pgs. 42-43)



VI. Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities

A. Objectives

The purpose of funding under this Topic Area is to support eligible utilities interested in making significant modifications and investments that enhance "the security posture of electric utilities". Funding under this Topic Area is available to eligible utilities, including electric distribution, generation, or transmission utilities. DOE is interested in projects that: improve the cybersecurity posture of the utility's operational systems; propose holistic solutions that include investments in staff and training and improvements to policies and procedures; maximize the security capabilities of already installed tools and technologies; and use a project design and management approach that ensures the utility will continue to maintain the effectiveness of implemented solutions after the project funding ends.

Proposed projects must be based on analyses identifying priority cybersecurity risks as established by security architecture reviews; vulnerability assessments or penetration tests; governance, risk, and compliance assessments; or other industry accepted cybersecurity risk assessments. If the necessary assessments have not yet been performed at the time of application, the applicant can request funds to conduct appropriate assessments and analyses to identify and prioritize risks, and to determine system needs based on the assessment results.

Projects can include the purchase of commercially available cybersecurity technology solutions, including but not limited to equipment, tools, hardware, software, firmware, or related assets. System-level implementations and full-scale system upgrades are also permitted under this Topic Area. Projects that exclusively include technology purchases and do not invest in addressing cybersecurity risks associated with people and processes will not be considered under this FOA.

Applicants are encouraged to use funding for training solutions specifically related to any tools or technologies purchased if it would improve the ability of the utility's staff to effectively and efficiently implement, operate, and maintain the technology solutions. Funding is also available for training solutions to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions provided the awardee adequately explains how the training is connected to improving the employee's ability to operate specific technologies.

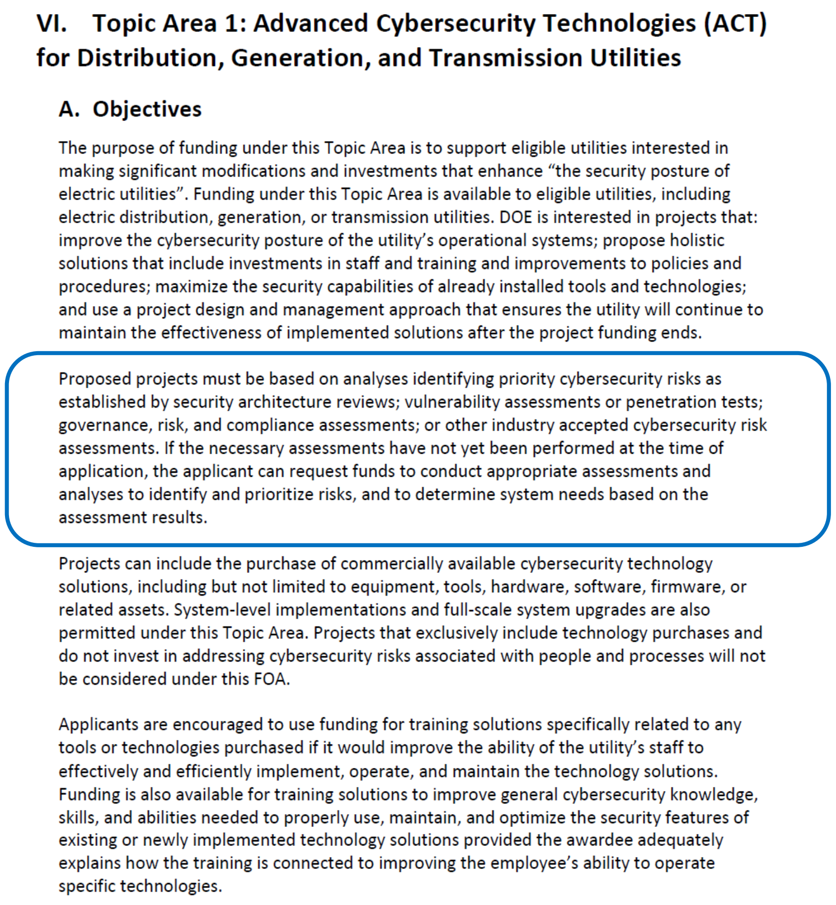
This Topic Area will provide direct support to eligible utilities interested in making significant modifications and investments that enhance "the security posture of electric utilities".

Goals

1) Improve the cybersecurity posture of the utility's operational systems;
2) Include appropriate balance of investments in staff, processes, and technologies;
3) Improve effective use of already installed tools and technologies when appropriate;
4) Increase participation and engagement of the utility in cybersecurity threat information sharing programs; and
5) Implement solutions that have a high likelihood of continued use and effectiveness after the project funding ends.

Topic Area 1 – Proposed Project Basis

FOA Section VI.A (pgs. 42-43)



VI. Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities

A. Objectives

The purpose of funding under this Topic Area is to support eligible utilities interested in making significant modifications and investments that enhance "the security posture of electric utilities". Funding under this Topic Area is available to eligible utilities, including electric distribution, generation, or transmission utilities. DOE is interested in projects that: improve the cybersecurity posture of the utility's operational systems; propose holistic solutions that include investments in staff and training and improvements to policies and procedures; maximize the security capabilities of already installed tools and technologies; and use a project design and management approach that ensures the utility will continue to maintain the effectiveness of implemented solutions after the project funding ends.

Proposed projects must be based on analyses identifying priority cybersecurity risks as established by security architecture reviews; vulnerability assessments or penetration tests; governance, risk, and compliance assessments; or other industry accepted cybersecurity risk assessments. If the necessary assessments have not yet been performed at the time of application, the applicant can request funds to conduct appropriate assessments and analyses to identify and prioritize risks, and to determine system needs based on the assessment results.

Projects can include the purchase of commercially available cybersecurity technology solutions, including but not limited to equipment, tools, hardware, software, firmware, or related assets. System-level implementations and full-scale system upgrades are also permitted under this Topic Area. Projects that exclusively include technology purchases and do not invest in addressing cybersecurity risks associated with people and processes will not be considered under this FOA.

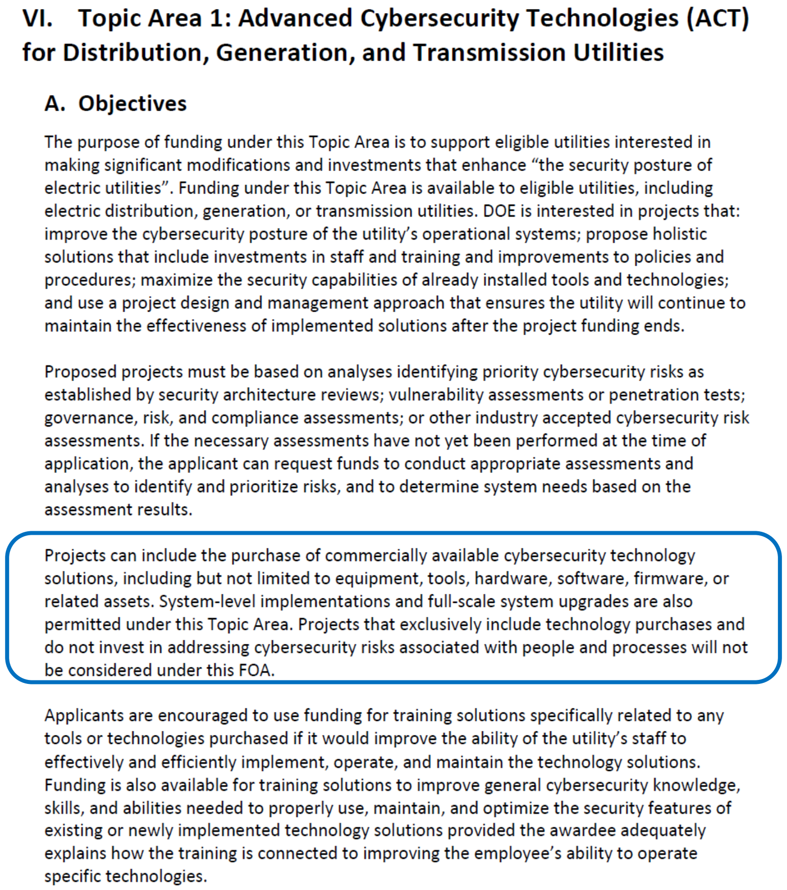
Applicants are encouraged to use funding for training solutions specifically related to any tools or technologies purchased if it would improve the ability of the utility's staff to effectively and efficiently implement, operate, and maintain the technology solutions. Funding is also available for training solutions to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions provided the awardee adequately explains how the training is connected to improving the employee's ability to operate specific technologies.

- Analyses identifying priority cybersecurity risks as established by security architecture reviews;
- Vulnerability assessments or penetration tests;
- Governance, risk, and compliance assessments; or
- Other industry accepted cybersecurity risk assessments.

If necessary assessments have not yet been performed at the time of application, applicants can request funds to conduct appropriate assessments and analyses to identify and prioritize risks, and to determine system needs based on the assessment results.

Topic Area 1 – What Could be Proposed

FOA Section VI.A (pgs. 42-43)



VI. Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities

A. Objectives

The purpose of funding under this Topic Area is to support eligible utilities interested in making significant modifications and investments that enhance "the security posture of electric utilities". Funding under this Topic Area is available to eligible utilities, including electric distribution, generation, or transmission utilities. DOE is interested in projects that: improve the cybersecurity posture of the utility's operational systems; propose holistic solutions that include investments in staff and training and improvements to policies and procedures; maximize the security capabilities of already installed tools and technologies; and use a project design and management approach that ensures the utility will continue to maintain the effectiveness of implemented solutions after the project funding ends.

Proposed projects must be based on analyses identifying priority cybersecurity risks as established by security architecture reviews; vulnerability assessments or penetration tests; governance, risk, and compliance assessments; or other industry accepted cybersecurity risk assessments. If the necessary assessments have not yet been performed at the time of application, the applicant can request funds to conduct appropriate assessments and analyses to identify and prioritize risks, and to determine system needs based on the assessment results.

Projects can include the purchase of commercially available cybersecurity technology solutions, including but not limited to equipment, tools, hardware, software, firmware, or related assets. System-level implementations and full-scale system upgrades are also permitted under this Topic Area. Projects that exclusively include technology purchases and do not invest in addressing cybersecurity risks associated with people and processes will not be considered under this FOA.

Applicants are encouraged to use funding for training solutions specifically related to any tools or technologies purchased if it would improve the ability of the utility's staff to effectively and efficiently implement, operate, and maintain the technology solutions. Funding is also available for training solutions to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions provided the awardee adequately explains how the training is connected to improving the employee's ability to operate specific technologies.

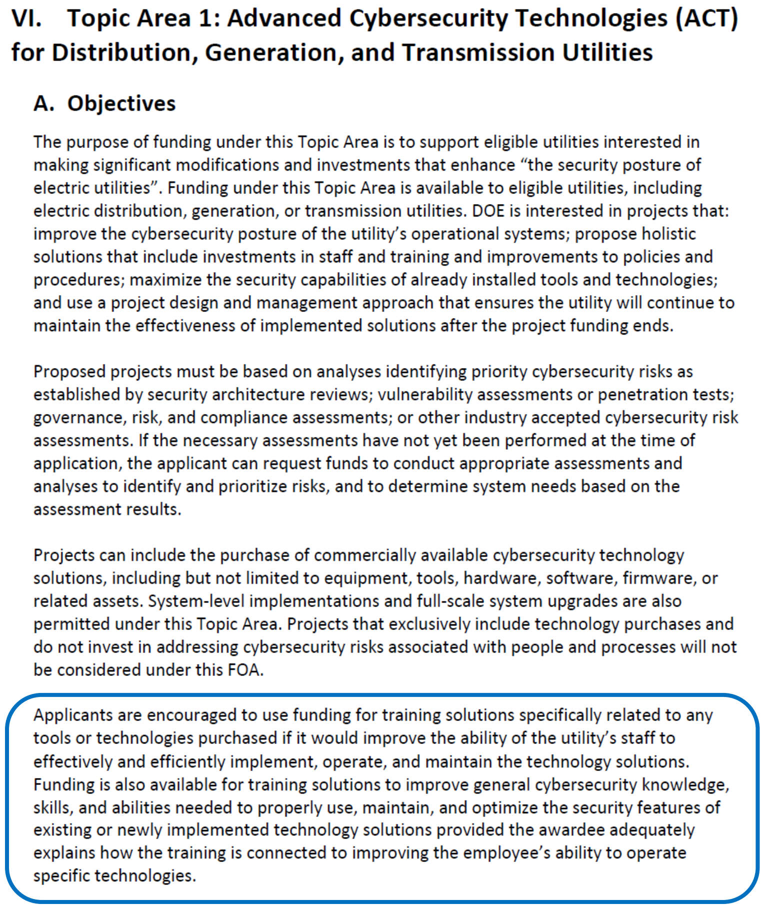
Projects could include:

1) Purchase of commercially available cybersecurity technology solutions, including but not limited to:
   - A. Equipment,
   - B. Tools,
   - C. Hardware,
   - D. Software,
   - E. Firmware, or
   - F. Related assets
2) System-level implementations and full-scale system upgrades.

Projects focused on technology purchases that do not address investments in cybersecurity risks associated with people and processes will not be considered under this FOA.

Topic Area 1 – How Can Funding be Used $

FOA Section VI.A (pgs. 42-43)



VI. Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities

A. Objectives

The purpose of funding under this Topic Area is to support eligible utilities interested in making significant modifications and investments that enhance "the security posture of electric utilities". Funding under this Topic Area is available to eligible utilities, including electric distribution, generation, or transmission utilities. DOE is interested in projects that: improve the cybersecurity posture of the utility's operational systems; propose holistic solutions that include investments in staff and training and improvements to policies and procedures; maximize the security capabilities of already installed tools and technologies; and use a project design and management approach that ensures the utility will continue to maintain the effectiveness of implemented solutions after the project funding ends.

Proposed projects must be based on analyses identifying priority cybersecurity risks as established by security architecture reviews; vulnerability assessments or penetration tests; governance, risk, and compliance assessments; or other industry accepted cybersecurity risk assessments. If the necessary assessments have not yet been performed at the time of application, the applicant can request funds to conduct appropriate assessments and analyses to identify and prioritize risks, and to determine system needs based on the assessment results.

Projects can include the purchase of commercially available cybersecurity technology solutions, including but not limited to equipment, tools, hardware, software, firmware, or related assets. System-level implementations and full-scale system upgrades are also permitted under this Topic Area. Projects that exclusively include technology purchases and do not invest in addressing cybersecurity risks associated with people and processes will not be considered under this FOA.

Applicants are encouraged to use funding for training solutions specifically related to any tools or technologies purchased if it would improve the ability of the utility's staff to effectively and efficiently implement, operate, and maintain the technology solutions. Funding is also available for training solutions to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions provided the awardee adequately explains how the training is connected to improving the employee's ability to operate specific technologies.

Training Examples:

1) Specific training solutions that would improve the ability of the utility's staff to implement, operate, and maintain the technology solution.

2) Training solutions to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions.

Topic Area 1 - Eligibility

Eligible applicants to Topic Area 1 fall into one of the following four categories based on language in BIL Section 40124:

(A) Rural electric cooperatives;

(B) Utilities owned by a political subdivision of a State, such as a municipally owned electric utility;

(C) Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State; and

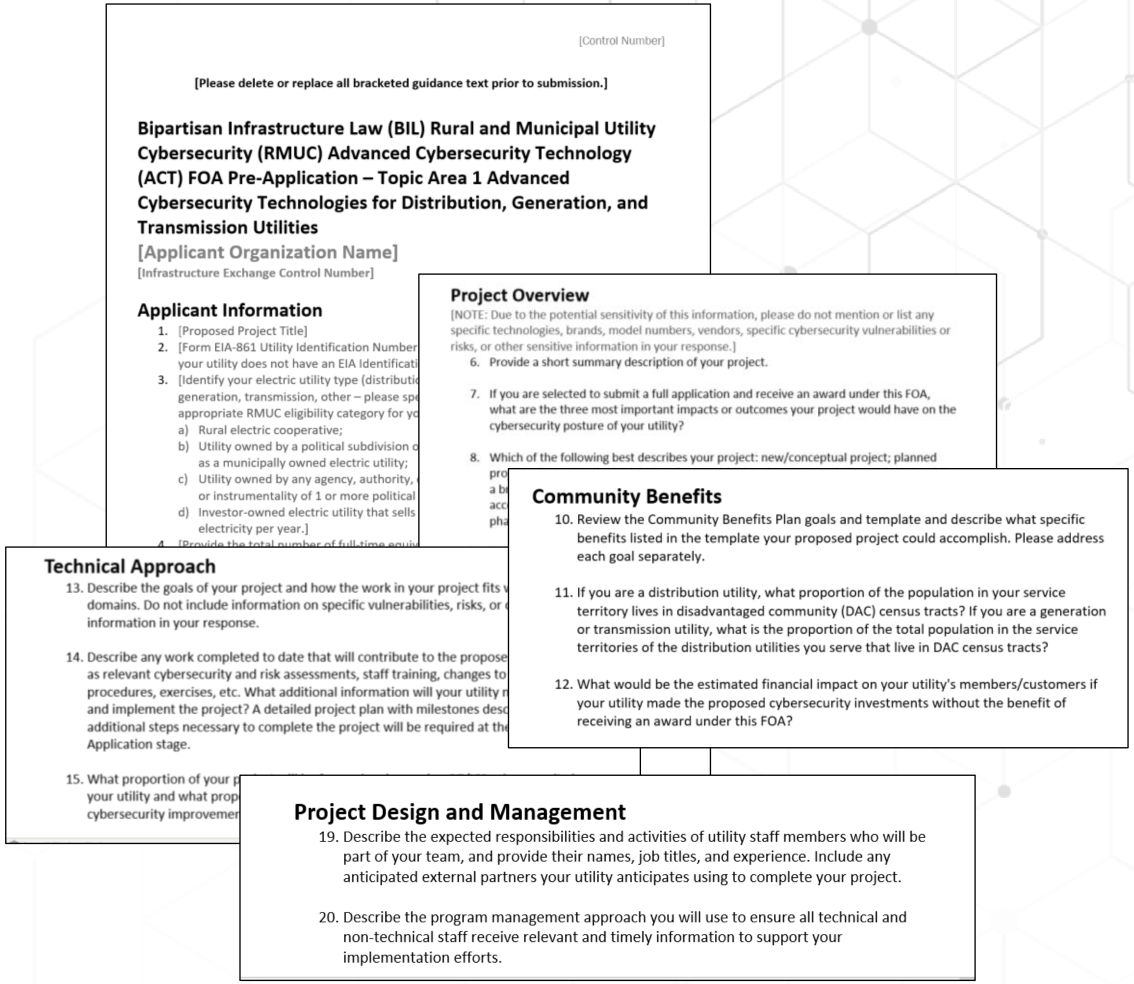
(D) (Intentionally left blank)

(E) Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year.

FOA Section III.A.i (pg. 17)

Topic Area 1 – Pre-Application Response Template

- Consists of 23 questions
- Optional Topic Area 1 Pre-Application Response Template found on eXCHANGE
- Answer completely and concisely
- Use review criteria to guide responses
- This document will be submitted for review to determine whether an applicant will be "invited" to submit a Full Application



[Control Number]

[Please delete or replace all bracketed guidance text prior to submission.]

Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) FOA Pre-Application – Topic Area 1 Advanced Cybersecurity Technologies for Distribution, Generation, and Transmission Utilities

[Applicant Organization Name]

[Infrastructure Exchange Control Number]

Applicant Information

1. [Proposed Project Title]
2. [Form EIA-861 Utility Identification Number
your utility does not have an EIA Identificati
3. [Identify your electric utility type (distributio
generation, transmission, other – please spe
appropriate RMUC eligibility category for yo
   a) Rural electric cooperative;
   b) Utility owned by a political subdivision o
   as a municipally owned electric utility;
   c) Utility owned by any agency, authority,
   or instrumentality of 1 or more political
   d) Investor-owned electric utility that sells
   electricity per year.]
4. [Provide the total number of full-time equiv

Project Overview

[NOTE: Due to the potential sensitivity of this information, please do not mention or list any specific technologies, brands, model numbers, vendors, specific cybersecurity vulnerabilities or risks, or other sensitive information in your response.]

6. Provide a short summary description of your project.

7. If you are selected to submit a full application and receive an award under this FOA, what are the three most important impacts or outcomes your project would have on the cybersecurity posture of your utility?

8. Which of the following best describes your project: new/conceptual project; planned
pro
a br
acc
pha

Community Benefits

10. Review the Community Benefits Plan goals and template and describe what specific benefits listed in the template your proposed project could accomplish. Please address each goal separately.

11. If you are a distribution utility, what proportion of the population in your service territory lives in disadvantaged community (DAC) census tracts? If you are a generation or transmission utility, what is the proportion of the total population in the service territories of the distribution utilities you serve that live in DAC census tracts?

12. What would be the estimated financial impact on your utility's members/customers if your utility made the proposed cybersecurity investments without the benefit of receiving an award under this FOA?

Technical Approach

13. Describe the goals of your project and how the work in your project fits
domains. Do not include information on specific vulnerabilities, risks, or
information in your response.

14. Describe any work completed to date that will contribute to the propose
as relevant cybersecurity and risk assessments, staff training, changes to
procedures, exercises, etc. What additional information will your utility
and implement the project? A detailed project plan with milestones desc
additional steps necessary to complete the project will be required at the
Application stage.

15. What proportion of your p
your utility and what prop
cybersecurity improvemen

Project Design and Management

19. Describe the expected responsibilities and activities of utility staff members who will be part of your team, and provide their names, job titles, and experience. Include any anticipated external partners your utility anticipates using to complete your project.

20. Describe the program management approach you will use to ensure all technical and non-technical staff receive relevant and timely information to support your implementation efforts.

Topic Area 1 Pre-Application Content Requirements

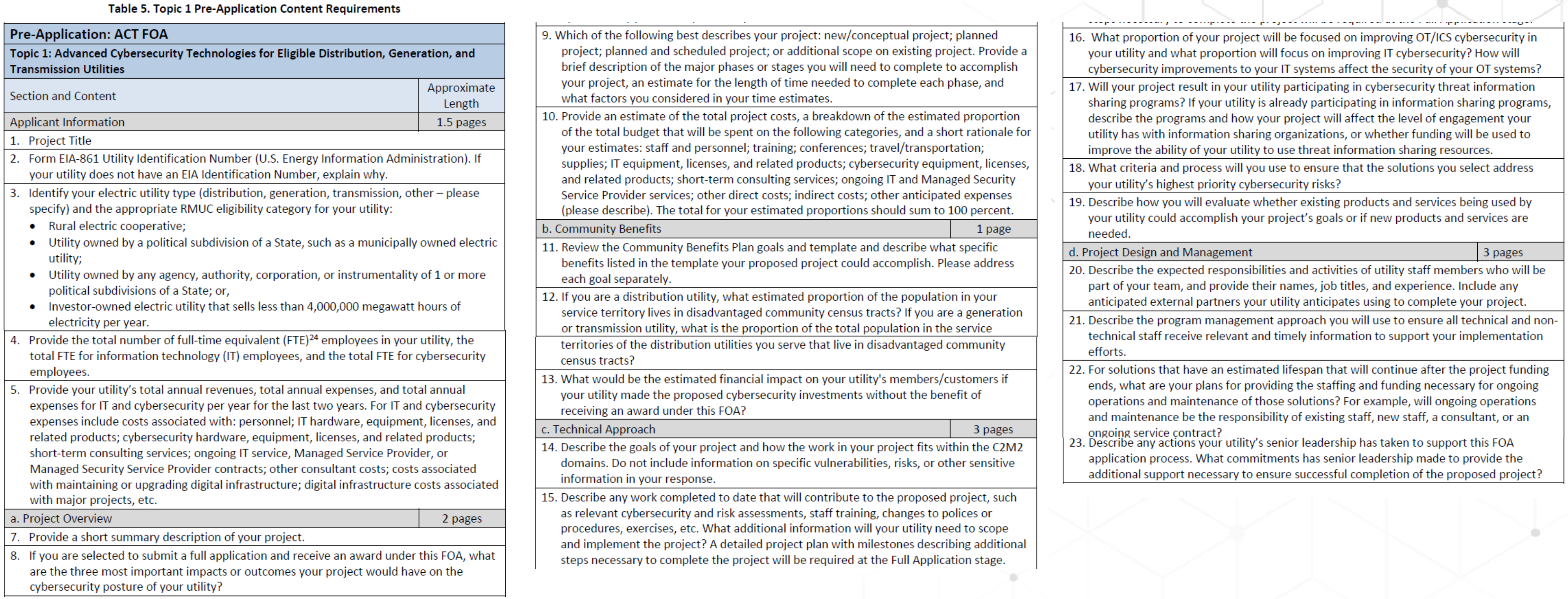


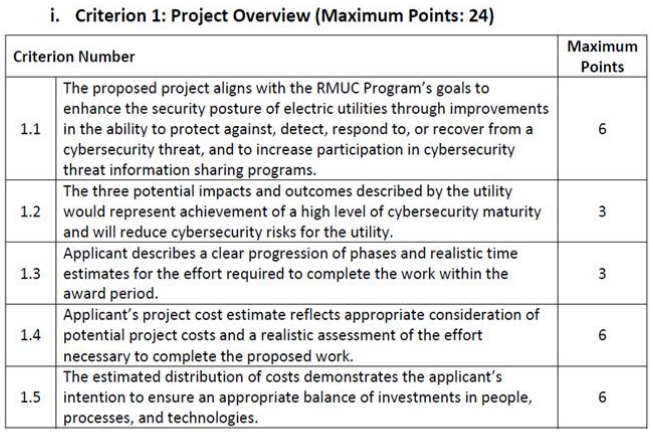
Table 5. Topic 1 Pre-Application Content Requirements

Pre-Application: ACT FOA	
Topic 1: Advanced Cybersecurity Technologies for Eligible Distribution, Generation, and Transmission Utilities	
Section and Content	Approximate Length
Applicant Information	1.5 pages
1. Project Title	
2. Form EIA-861 Utility Identification Number (U.S. Energy Information Administration). If your utility does not have an EIA Identification Number, explain why.	
3. Identify your electric utility type (distribution, generation, transmission, other – please specify) and the appropriate RMUC eligibility category for your utility: • Rural electric cooperative; • Utility owned by a political subdivision of a State, such as a municipally owned electric utility; • Utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State; or, • Investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year.	
4. Provide the total number of full-time equivalent (FTE)[24] employees in your utility, the total FTE for information technology (IT) employees, and the total FTE for cybersecurity employees.	
5. Provide your utility's total annual revenues, total annual expenses, and total annual expenses for IT and cybersecurity per year for the last two years. For IT and cybersecurity expenses include costs associated with: personnel; IT hardware, equipment, licenses, and related products; cybersecurity hardware, equipment, licenses, and related products; short-term consulting services; ongoing IT service, Managed Service Provider, or Managed Security Service Provider contracts; other consultant costs; costs associated with maintaining or upgrading digital infrastructure; digital infrastructure costs associated with major projects, etc.	
a. Project Overview	2 pages
7. Provide a short summary description of your project.	
8. If you are selected to submit a full application and receive an award under this FOA, what are the three most important impacts or outcomes your project would have on the cybersecurity posture of your utility?	
9. Which of the following best describes your project: new/conceptual project; planned project; planned and scheduled project; or additional scope on existing project. Provide a brief description of the major phases or stages you will need to complete to accomplish your project, an estimate for the length of time needed to complete each phase, and what factors you considered in your time estimates.	
10. Provide an estimate of the total project costs, a breakdown of the estimated proportion of the total budget that will be spent on the following categories, and a short rationale for your estimates: staff and personnel; training; conferences; travel/transportation; supplies; IT equipment, licenses, and related products; cybersecurity equipment, licenses, and related products; short-term consulting services; ongoing IT and Managed Security Service Provider services; other direct costs; indirect costs; other anticipated expenses (please describe). The total for your estimated proportions should sum to 100 percent.	
b. Community Benefits	1 page
11. Review the Community Benefits Plan goals and template and describe what specific benefits listed in the template your proposed project could accomplish. Please address each goal separately.	
12. If you are a distribution utility, what estimated proportion of the population in your service territory lives in disadvantaged community census tracts? If you are a generation or transmission utility, what is the proportion of the total population in the service territories of the distribution utilities you serve that live in disadvantaged community census tracts?	
13. What would be the estimated financial impact on your utility's members/customers if your utility made the proposed cybersecurity investments without the benefit of receiving an award under this FOA?	
c. Technical Approach	3 pages
14. Describe the goals of your project and how the work in your project fits within the C2M2 domains. Do not include information on specific vulnerabilities, risks, or other sensitive information in your response.	
15. Describe any work completed to date that will contribute to the proposed project, such as relevant cybersecurity and risk assessments, staff training, changes to polices or procedures, exercises, etc. What additional information will your utility need to scope and implement the project? A detailed project plan with milestones describing additional steps necessary to complete the project will be required at the Full Application stage.	
16. What proportion of your project will be focused on improving OT/ICS cybersecurity in your utility and what proportion will focus on improving IT cybersecurity? How will cybersecurity improvements to your IT systems affect the security of your OT systems?	
17. Will your project result in your utility participating in cybersecurity threat information sharing programs? If your utility is already participating in information sharing programs, describe the programs and how your project will affect the level of engagement your utility has with information sharing organizations, or whether funding will be used to improve the ability of your utility to use threat information sharing resources.	
18. What criteria and process will you use to ensure that the solutions you select address your utility's highest priority cybersecurity risks?	
19. Describe how you will evaluate whether existing products and services being used by your utility could accomplish your project's goals or if new products and services are needed.	
d. Project Design and Management	3 pages
20. Describe the expected responsibilities and activities of utility staff members who will be part of your team, and provide their names, job titles, and experience. Include any anticipated external partners your utility anticipates using to complete your project.	
21. Describe the program management approach you will use to ensure all technical and non-technical staff receive relevant and timely information to support your implementation efforts.	
22. For solutions that have an estimated lifespan that will continue after the project funding ends, what are your plans for providing the staffing and funding necessary for ongoing operations and maintenance of those solutions? For example, will ongoing operations and maintenance be the responsibility of existing staff, new staff, a consultant, or an ongoing service contract?	
23. Describe any actions your utility's senior leadership has taken to support this FOA application process. What commitments has senior leadership made to provide the additional support necessary to ensure successful completion of the proposed project?	

FOA Section VI.B (pgs. 43-46)

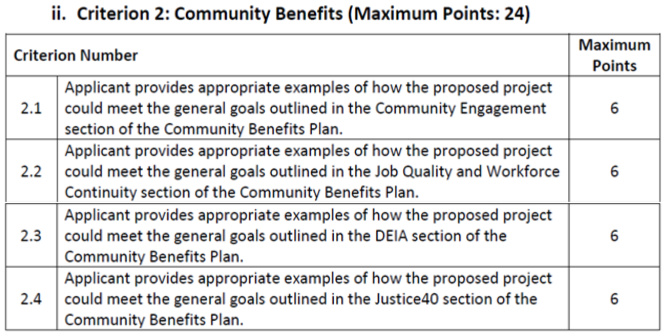
Topic Area 1 Pre-Application Review Criteria

Total Possible Score – 96 points



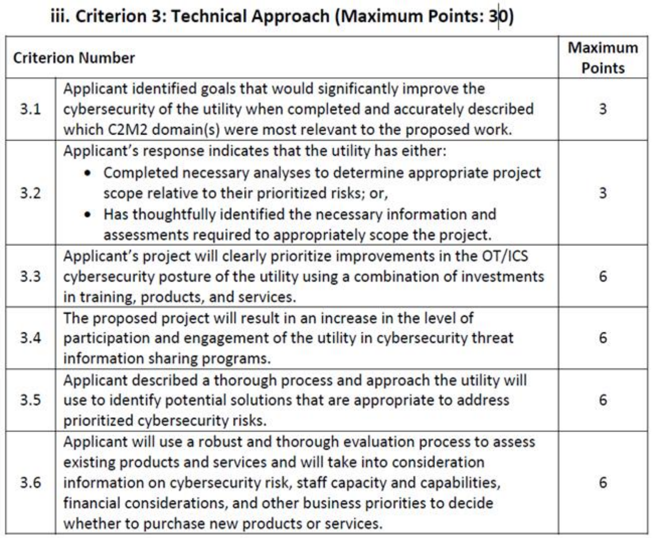
i. Criterion 1: Project Overview (Maximum Points: 24)

Criterion Number		Maximum Points
1.1	The proposed project aligns with the RMUC Program's goals to enhance the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat, and to increase participation in cybersecurity threat information sharing programs.	6
1.2	The three potential impacts and outcomes described by the utility would represent achievement of a high level of cybersecurity maturity and will reduce cybersecurity risks for the utility.	3
1.3	Applicant describes a clear progression of phases and realistic time estimates for the effort required to complete the work within the award period.	3
1.4	Applicant's project cost estimate reflects appropriate consideration of potential project costs and a realistic assessment of the effort necessary to complete the proposed work.	6
1.5	The estimated distribution of costs demonstrates the applicant's intention to ensure an appropriate balance of investments in people, processes, and technologies.	6



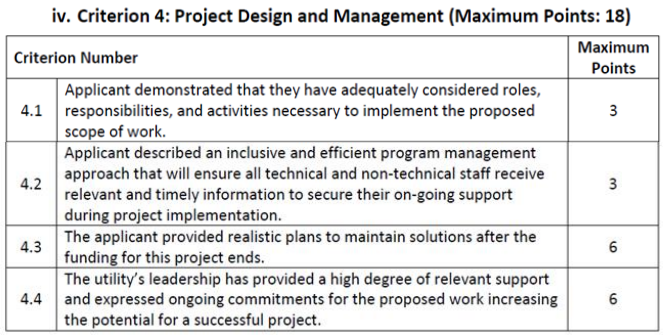
ii. Criterion 2: Community Benefits (Maximum Points: 24)

Criterion Number		Maximum Points
2.1	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Community Engagement section of the Community Benefits Plan.	6
2.2	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Job Quality and Workforce Continuity section of the Community Benefits Plan.	6
2.3	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the DEIA section of the Community Benefits Plan.	6
2.4	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Justice40 section of the Community Benefits Plan.	6



iii. Criterion 3: Technical Approach (Maximum Points: 30)

Criterion Number		Maximum Points
3.1	Applicant identified goals that would significantly improve the cybersecurity of the utility when completed and accurately described which C2M2 domain(s) were most relevant to the proposed work.	3
3.2	Applicant's response indicates that the utility has either: • Completed necessary analyses to determine appropriate project scope relative to their prioritized risks; or, • Has thoughtfully identified the necessary information and assessments required to appropriately scope the project.	3
3.3	Applicant's project will clearly prioritize improvements in the OT/ICS cybersecurity posture of the utility using a combination of investments in training, products, and services.	6
3.4	The proposed project will result in an increase in the level of participation and engagement of the utility in cybersecurity threat information sharing programs.	6
3.5	Applicant described a thorough process and approach the utility will use to identify potential solutions that are appropriate to address prioritized cybersecurity risks.	6
3.6	Applicant will use a robust and thorough evaluation process to assess existing products and services and will take into consideration information on cybersecurity risk, staff capacity and capabilities, financial considerations, and other business priorities to decide whether to purchase new products or services.	6



iv. Criterion 4: Project Design and Management (Maximum Points: 18)

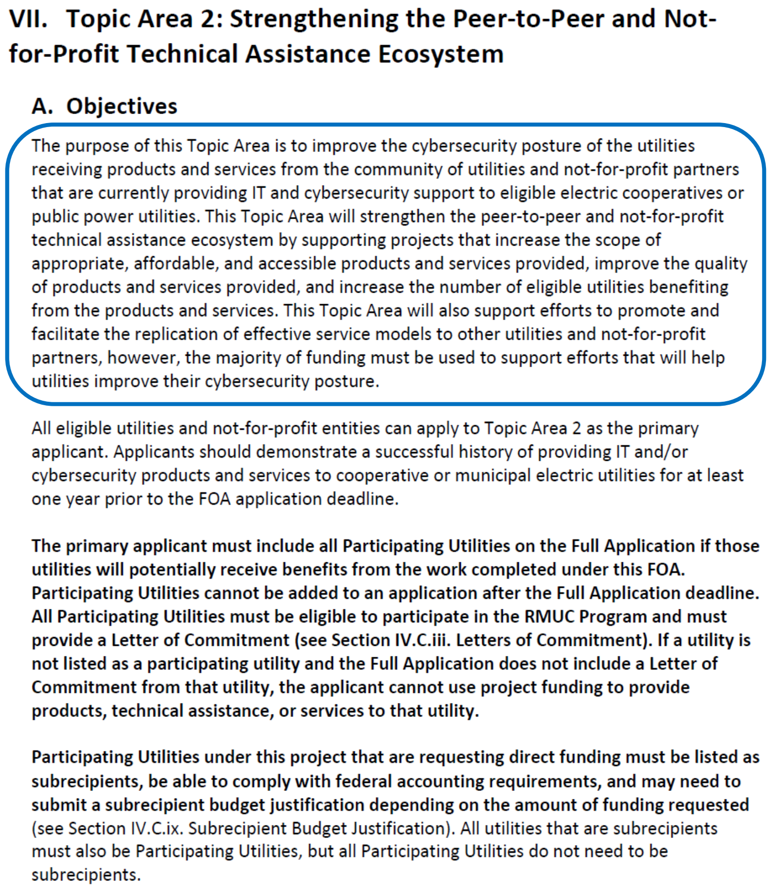
Criterion Number		Maximum Points
4.1	Applicant demonstrated that they have adequately considered roles, responsibilities, and activities necessary to implement the proposed scope of work.	3
4.2	Applicant described an inclusive and efficient program management approach that will ensure all technical and non-technical staff receive relevant and timely information to secure their on-going support during project implementation.	3
4.3	The applicant provided realistic plans to maintain solutions after the funding for this project ends.	6
4.4	The utility's leadership has provided a high degree of relevant support and expressed ongoing commitments for the proposed work increasing the potential for a successful project.	6

FOA Section VI.C (pgs. 46-48)

Topic Area 2 – Strengthening the Peer-to-Peer and Not-for-Profit Technical Ecosystem

Topic Area 2 – Objectives and Goals

FOA Section VI.A (pgs. 55-58)



VII. Topic Area 2: Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem

A. Objectives

The purpose of this Topic Area is to improve the cybersecurity posture of the utilities receiving products and services from the community of utilities and not-for-profit partners that are currently providing IT and cybersecurity support to eligible electric cooperatives or public power utilities. This Topic Area will strengthen the peer-to-peer and not-for-profit technical assistance ecosystem by supporting projects that increase the scope of appropriate, affordable, and accessible products and services provided, improve the quality of products and services provided, and increase the number of eligible utilities benefiting from the products and services. This Topic Area will also support efforts to promote and facilitate the replication of effective service models to other utilities and not-for-profit partners, however, the majority of funding must be used to support efforts that will help utilities improve their cybersecurity posture.

All eligible utilities and not-for-profit entities can apply to Topic Area 2 as the primary applicant. Applicants should demonstrate a successful history of providing IT and/or cybersecurity products and services to cooperative or municipal electric utilities for at least one year prior to the FOA application deadline.

The primary applicant must include all Participating Utilities on the Full Application if those utilities will potentially receive benefits from the work completed under this FOA. Participating Utilities cannot be added to an application after the Full Application deadline. All Participating Utilities must be eligible to participate in the RMUC Program and must provide a Letter of Commitment (see Section IV.C.iii. Letters of Commitment). If a utility is not listed as a participating utility and the Full Application does not include a Letter of Commitment from that utility, the applicant cannot use project funding to provide products, technical assistance, or services to that utility.

Participating Utilities under this project that are requesting direct funding must be listed as subrecipients, be able to comply with federal accounting requirements, and may need to submit a subrecipient budget justification depending on the amount of funding requested (see Section IV.C.ix. Subrecipient Budget Justification). All utilities that are subrecipients must also be Participating Utilities, but all Participating Utilities do not need to be subrecipients.

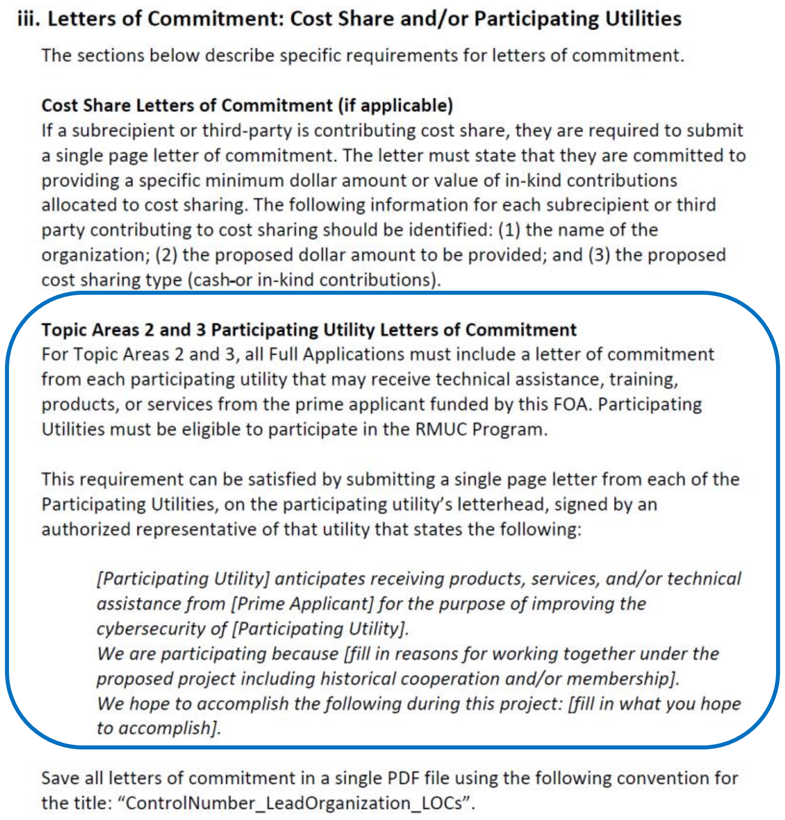
Improve the cybersecurity posture of Participating Utilities receiving products and services from the community of utilities and not-for-profit partners currently providing IT and cybersecurity support to eligible utilities.

Goals

1) Strengthen peer-to-peer and not-for-profit technical assistance ecosystem;
2) Increase scope of appropriate, affordable, and accessible product and services;
3) Improve quality of products and services provided;
4) Increase the number of eligible utilities benefiting from products and services; and
5) Create a replicable, scalable model for delivering cybersecurity services.

Topic Area 2 – Participating Utilities

FOA Section IV.C (pg. 29)



iii. Letters of Commitment: Cost Share and/or Participating Utilities

The sections below describe specific requirements for letters of commitment.

Cost Share Letters of Commitment (if applicable)
If a subrecipient or third-party is contributing cost share, they are required to submit a single page letter of commitment. The letter must state that they are committed to providing a specific minimum dollar amount or value of in-kind contributions allocated to cost sharing. The following information for each subrecipient or third party contributing to cost sharing should be identified: (1) the name of the organization; (2) the proposed dollar amount to be provided; and (3) the proposed cost sharing type (cash-or in-kind contributions).

Topic Areas 2 and 3 Participating Utility Letters of Commitment
For Topic Areas 2 and 3, all Full Applications must include a letter of commitment from each participating utility that may receive technical assistance, training, products, or services from the prime applicant funded by this FOA. Participating Utilities must be eligible to participate in the RMUC Program.

This requirement can be satisfied by submitting a single page letter from each of the Participating Utilities, on the participating utility's letterhead, signed by an authorized representative of that utility that states the following:

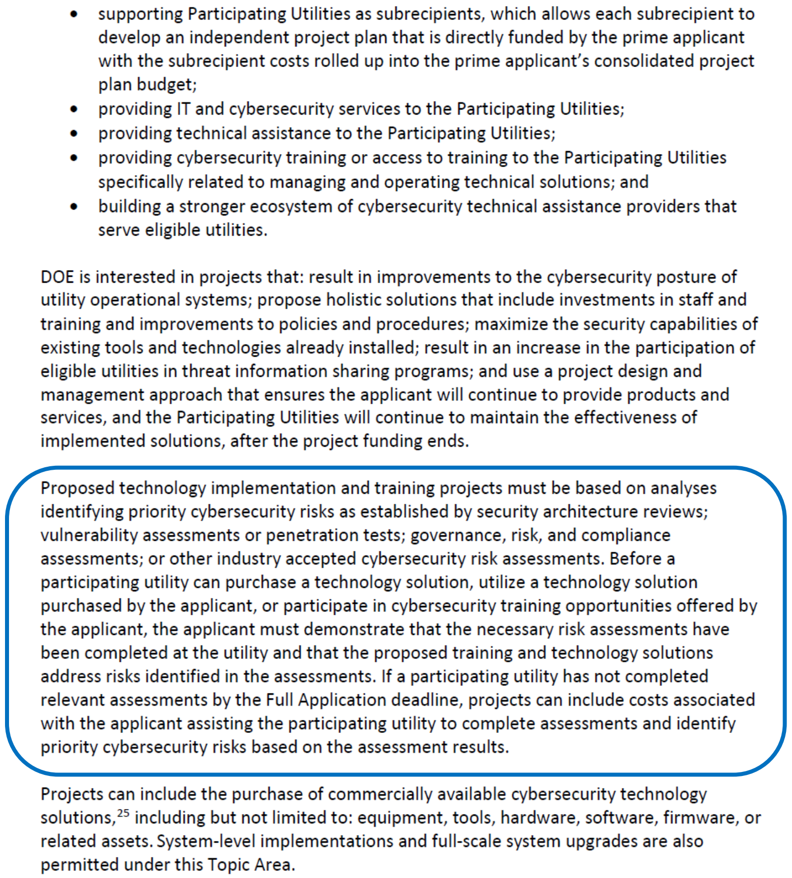
> *[Participating Utility] anticipates receiving products, services, and/or technical assistance from [Prime Applicant] for the purpose of improving the cybersecurity of [Participating Utility].*
> *We are participating because [fill in reasons for working together under the proposed project including historical cooperation and/or membership].*
> *We hope to accomplish the following during this project: [fill in what you hope to accomplish].*

Save all letters of commitment in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_LOCs".

Full Applications must include a letter of commitment from each Participating Utility that might receive technical assistance, training, products, or services from the prime applicant.

Topic Area 2 – Proposed Project Basis

FOA Section VI.A (pgs. 55-58)



- supporting Participating Utilities as subrecipients, which allows each subrecipient to develop an independent project plan that is directly funded by the prime applicant with the subrecipient costs rolled up into the prime applicant's consolidated project plan budget;
- providing IT and cybersecurity services to the Participating Utilities;
- providing technical assistance to the Participating Utilities;
- providing cybersecurity training or access to training to the Participating Utilities specifically related to managing and operating technical solutions; and
- building a stronger ecosystem of cybersecurity technical assistance providers that serve eligible utilities.

DOE is interested in projects that: result in improvements to the cybersecurity posture of utility operational systems; propose holistic solutions that include investments in staff and training and improvements to policies and procedures; maximize the security capabilities of existing tools and technologies already installed; result in an increase in the participation of eligible utilities in threat information sharing programs; and use a project design and management approach that ensures the applicant will continue to provide products and services, and the Participating Utilities will continue to maintain the effectiveness of implemented solutions, after the project funding ends.

Proposed technology implementation and training projects must be based on analyses identifying priority cybersecurity risks as established by security architecture reviews; vulnerability assessments or penetration tests; governance, risk, and compliance assessments; or other industry accepted cybersecurity risk assessments. Before a participating utility can purchase a technology solution, utilize a technology solution purchased by the applicant, or participate in cybersecurity training opportunities offered by the applicant, the applicant must demonstrate that the necessary risk assessments have been completed at the utility and that the proposed training and technology solutions address risks identified in the assessments. If a participating utility has not completed relevant assessments by the Full Application deadline, projects can include costs associated with the applicant assisting the participating utility to complete assessments and identify priority cybersecurity risks based on the assessment results.

Projects can include the purchase of commercially available cybersecurity technology solutions,[25] including but not limited to: equipment, tools, hardware, software, firmware, or related assets. System-level implementations and full-scale system upgrades are also permitted under this Topic Area.

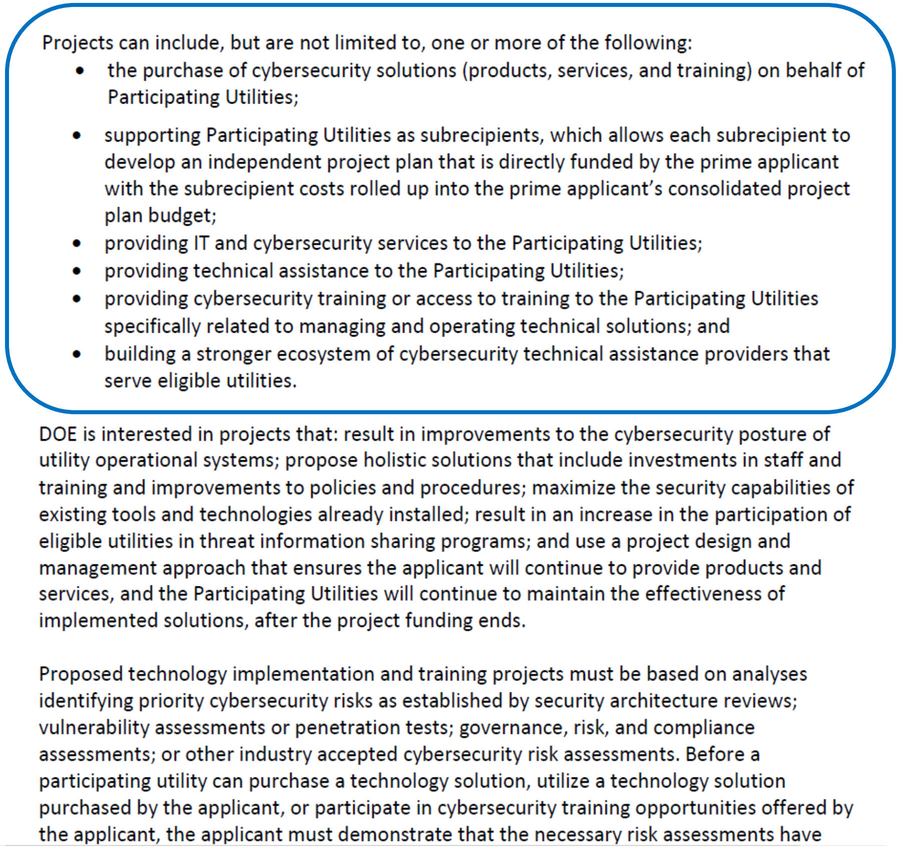
- Analyses identifying priority cybersecurity risks as established by security architecture reviews;
- Vulnerability assessments or penetration tests;
- Governance, risk, and compliance assessments; or
- Other industry accepted cybersecurity risk assessments.

The applicant must demonstrate that necessary risk assessments have been completed at the Participating Utilities and that the proposed training and technology solutions address risks identified in the assessments.

If assessments have not been completed, projects can include costs associated with assisting Participating Utilities to complete assessments and identify priority cybersecurity risks based on the assessment results.

Topic Area 2 – What Could be Proposed

FOA Section VI.A (pgs. 55-58)



Projects can include, but are not limited to, one or more of the following:

- the purchase of cybersecurity solutions (products, services, and training) on behalf of Participating Utilities;
- supporting Participating Utilities as subrecipients, which allows each subrecipient to develop an independent project plan that is directly funded by the prime applicant with the subrecipient costs rolled up into the prime applicant's consolidated project plan budget;
- providing IT and cybersecurity services to the Participating Utilities;
- providing technical assistance to the Participating Utilities;
- providing cybersecurity training or access to training to the Participating Utilities specifically related to managing and operating technical solutions; and
- building a stronger ecosystem of cybersecurity technical assistance providers that serve eligible utilities.

DOE is interested in projects that: result in improvements to the cybersecurity posture of utility operational systems; propose holistic solutions that include investments in staff and training and improvements to policies and procedures; maximize the security capabilities of existing tools and technologies already installed; result in an increase in the participation of eligible utilities in threat information sharing programs; and use a project design and management approach that ensures the applicant will continue to provide products and services, and the Participating Utilities will continue to maintain the effectiveness of implemented solutions, after the project funding ends.

Proposed technology implementation and training projects must be based on analyses identifying priority cybersecurity risks as established by security architecture reviews; vulnerability assessments or penetration tests; governance, risk, and compliance assessments; or other industry accepted cybersecurity risk assessments. Before a participating utility can purchase a technology solution, utilize a technology solution purchased by the applicant, or participate in cybersecurity training opportunities offered by the applicant, the applicant must demonstrate that the necessary risk assessments have

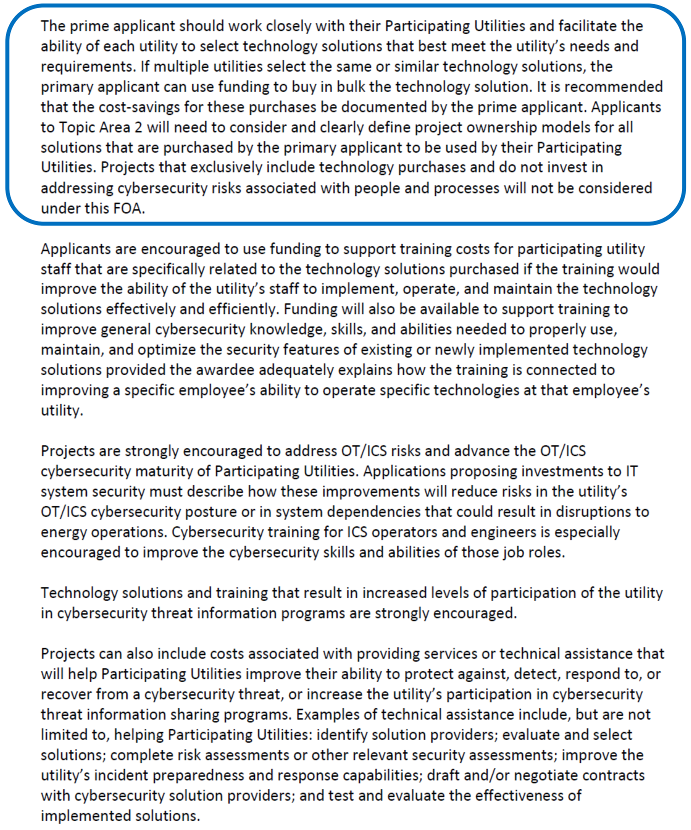
Projects could include but are not limited to:

1) Purchase of cybersecurity solutions on behalf of Participating Utilities
2) Providing IT and cybersecurity services to Participating Utilities
3) Providing technical assistance to Participating Utilities
4) Providing cybersecurity training or access to training to Participating Utilities
5) Building a stronger ecosystem of cybersecurity technical assistance providers

Projects including just technology purchases and not addressing investment in cybersecurity risks associated with people and processes will not be considered under this FOA.

Topic Area 2 – Working with Participating Utilities

FOA Section VI.A (pgs. 55-58)



The prime applicant should work closely with their Participating Utilities and facilitate the ability of each utility to select technology solutions that best meet the utility's needs and requirements. If multiple utilities select the same or similar technology solutions, the primary applicant can use funding to buy in bulk the technology solution. It is recommended that the cost-savings for these purchases be documented by the prime applicant. Applicants to Topic Area 2 will need to consider and clearly define project ownership models for all solutions that are purchased by the primary applicant to be used by their Participating Utilities. Projects that exclusively include technology purchases and do not invest in addressing cybersecurity risks associated with people and processes will not be considered under this FOA.

Applicants are encouraged to use funding to support training costs for participating utility staff that are specifically related to the technology solutions purchased if the training would improve the ability of the utility's staff to implement, operate, and maintain the technology solutions effectively and efficiently. Funding will also be available to support training to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions provided the awardee adequately explains how the training is connected to improving a specific employee's ability to operate specific technologies at that employee's utility.

Projects are strongly encouraged to address OT/ICS risks and advance the OT/ICS cybersecurity maturity of Participating Utilities. Applications proposing investments to IT system security must describe how these improvements will reduce risks in the utility's OT/ICS cybersecurity posture or in system dependencies that could result in disruptions to energy operations. Cybersecurity training for ICS operators and engineers is especially encouraged to improve the cybersecurity skills and abilities of those job roles.

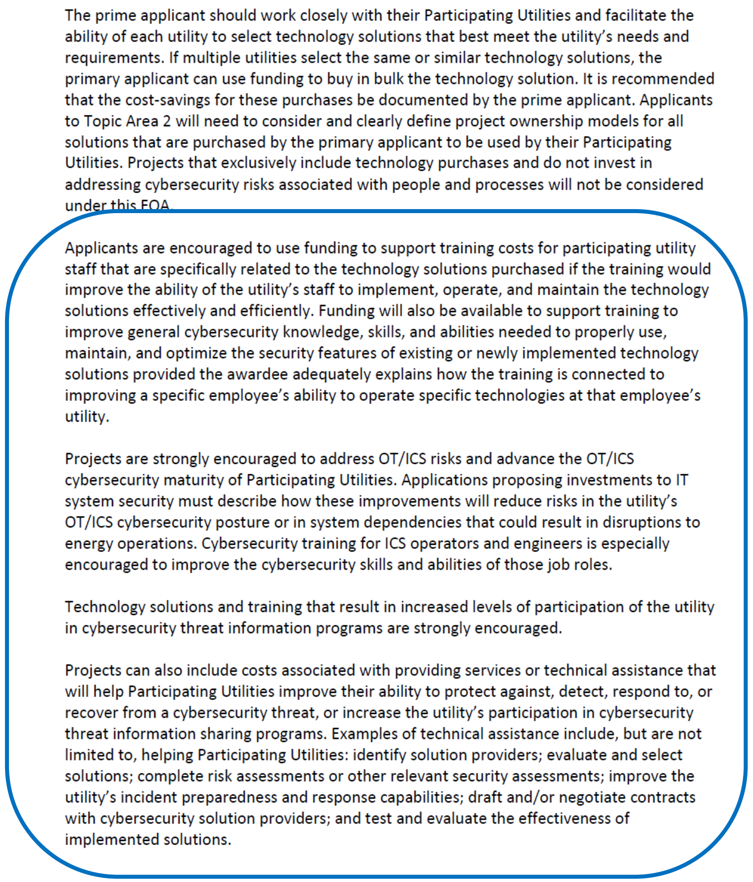
Technology solutions and training that result in increased levels of participation of the utility in cybersecurity threat information programs are strongly encouraged.

Projects can also include costs associated with providing services or technical assistance that will help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat, or increase the utility's participation in cybersecurity threat information sharing programs. Examples of technical assistance include, but are not limited to, helping Participating Utilities: identify solution providers; evaluate and select solutions; complete risk assessments or other relevant security assessments; improve the utility's incident preparedness and response capabilities; draft and/or negotiate contracts with cybersecurity solution providers; and test and evaluate the effectiveness of implemented solutions.

- Work closely together
- Select technology solutions that best meet utility needs and requirements.
- Bulk buy technology solutions if multiple utilities select the same or similar technology solutions.
- Document cost-savings for bulk buy purchases.
- Consider and clearly define project ownership models for all solutions purchased by the primary applicant to be used by their Participating Utilities.

Topic Area 2 – How Can Funding be Used

FOA Section VI.A (pgs. 55-58)



The prime applicant should work closely with their Participating Utilities and facilitate the ability of each utility to select technology solutions that best meet the utility's needs and requirements. If multiple utilities select the same or similar technology solutions, the primary applicant can use funding to buy in bulk the technology solution. It is recommended that the cost-savings for these purchases be documented by the prime applicant. Applicants to Topic Area 2 will need to consider and clearly define project ownership models for all solutions that are purchased by the primary applicant to be used by their Participating Utilities. Projects that exclusively include technology purchases and do not invest in addressing cybersecurity risks associated with people and processes will not be considered under this FOA.

Applicants are encouraged to use funding to support training costs for participating utility staff that are specifically related to the technology solutions purchased if the training would improve the ability of the utility's staff to implement, operate, and maintain the technology solutions effectively and efficiently. Funding will also be available to support training to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions provided the awardee adequately explains how the training is connected to improving a specific employee's ability to operate specific technologies at that employee's utility.

Projects are strongly encouraged to address OT/ICS risks and advance the OT/ICS cybersecurity maturity of Participating Utilities. Applications proposing investments to IT system security must describe how these improvements will reduce risks in the utility's OT/ICS cybersecurity posture or in system dependencies that could result in disruptions to energy operations. Cybersecurity training for ICS operators and engineers is especially encouraged to improve the cybersecurity skills and abilities of those job roles.

Technology solutions and training that result in increased levels of participation of the utility in cybersecurity threat information programs are strongly encouraged.

Projects can also include costs associated with providing services or technical assistance that will help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat, or increase the utility's participation in cybersecurity threat information sharing programs. Examples of technical assistance include, but are not limited to, helping Participating Utilities: identify solution providers; evaluate and select solutions; complete risk assessments or other relevant security assessments; improve the utility's incident preparedness and response capabilities; draft and/or negotiate contracts with cybersecurity solution providers; and test and evaluate the effectiveness of implemented solutions.

Training Examples:

1) Specific training solutions that would improve the ability of the utility's staff to implement, operate, and maintain the technology solution.
2) Training solutions to improve general cybersecurity knowledge, skills, and abilities needed to properly use, maintain, and optimize the security features of existing or newly implemented technology solutions.
3) Technology solutions and training resulting in increased levels of threat information sharing program participation.

Topic Area 2 - Eligibility

All RMUC Program eligible entities defined in BIL Section 40124 can apply to Topic 2:

(A) Rural electric cooperatives;

(B) Utilities owned by a political subdivision of a State, such as a municipally owned electric utility;

(C) Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State;

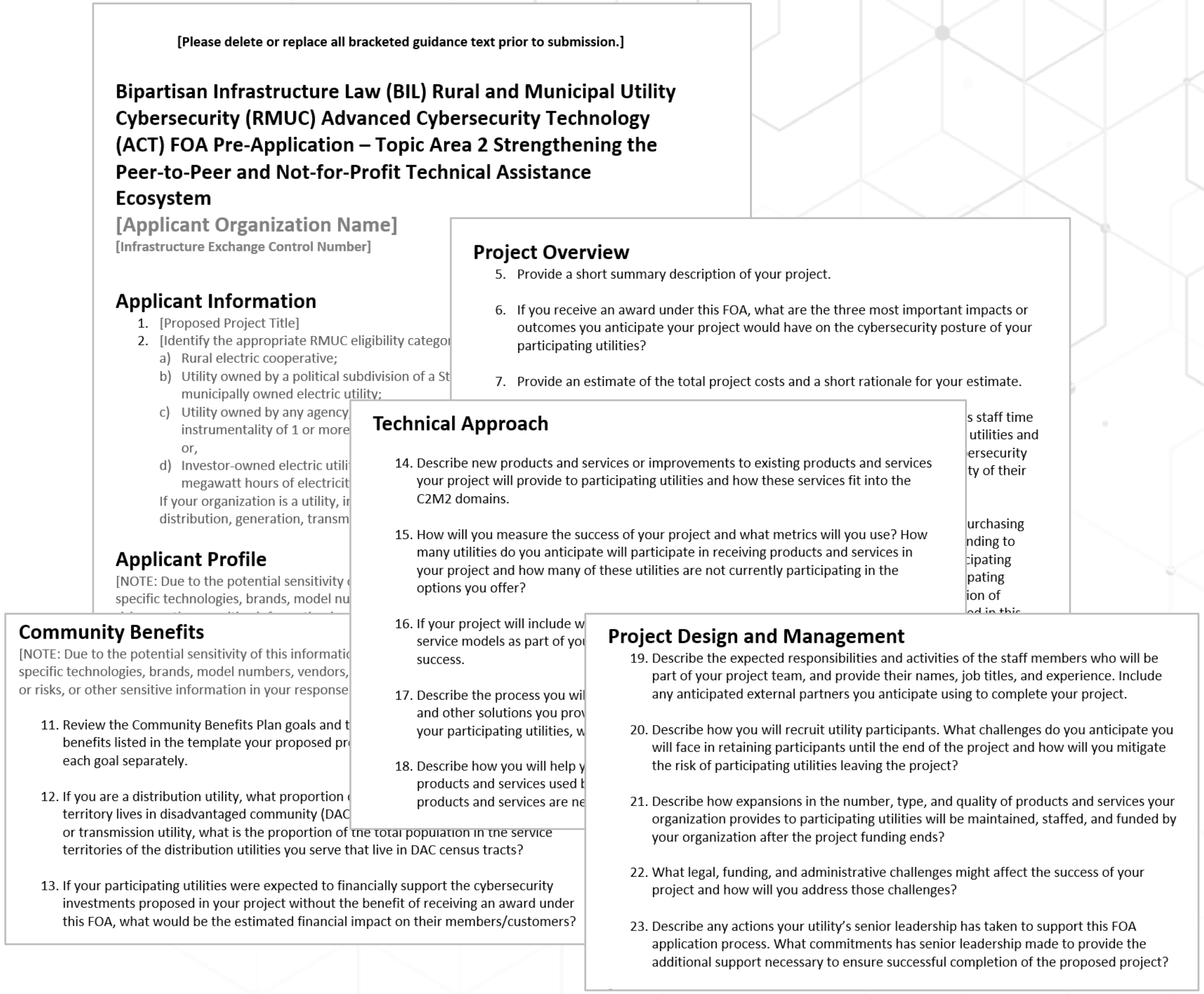
(D) Not-for-profit entities that are in a partnership with not fewer than 6 entities described in (A), (B), or (C) above; and

(E) Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year

FOA Section III.A.i (pg. 17)

Topic Area 2 – Pre-Application Response Template

- Consists of 23 questions
- Optional Topic Area 2 Pre-Application Response Template found on eXCHANGE
- Answer completely and concisely
- Use review criteria to guide responses
- This document is what will be submitted for review to determine whether an applicant will be “invited” to submit a Full Application



[Please delete or replace all bracketed guidance text prior to submission.]

Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) FOA Pre-Application – Topic Area 2 Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem

[Applicant Organization Name]

[Infrastructure Exchange Control Number]

Applicant Information

1. [Proposed Project Title]
2. [Identify the appropriate RMUC eligibility categor
   a) Rural electric cooperative;
   b) Utility owned by a political subdivision of a St
   municipally owned electric utility;
   c) Utility owned by any agency
   instrumentality of 1 or more
   or,
   d) Investor-owned electric utili
   megawatt hours of electricit

   If your organization is a utility, i
   distribution, generation, transm

Applicant Profile

[NOTE: Due to the potential sensitivity o
specific technologies, brands, model nu

Project Overview

5. Provide a short summary description of your project.
6. If you receive an award under this FOA, what are the three most important impacts or outcomes you anticipate your project would have on the cybersecurity posture of your participating utilities?
7. Provide an estimate of the total project costs and a short rationale for your estimate.

s staff time
utilities and
ersecurity
ty of their

urchasing
nding to
cipating
pating
ion of

Technical Approach

14. Describe new products and services or improvements to existing products and services your project will provide to participating utilities and how these services fit into the C2M2 domains.
15. How will you measure the success of your project and what metrics will you use? How many utilities do you anticipate will participate in receiving products and services in your project and how many of these utilities are not currently participating in the options you offer?
16. If your project will include w
service models as part of yo
success.
17. Describe the process you wi
and other solutions you prov
your participating utilities, w
18. Describe how you will help y
products and services used b
products and services are ne

Community Benefits

[NOTE: Due to the potential sensitivity of this informatio
specific technologies, brands, model numbers, vendors,
or risks, or other sensitive information in your response

11. Review the Community Benefits Plan goals and t
benefits listed in the template your proposed pr
each goal separately.
12. If you are a distribution utility, what proportion o
territory lives in disadvantaged community (DAC
or transmission utility, what is the proportion of the total population in the service territories of the distribution utilities you serve that live in DAC census tracts?
13. If your participating utilities were expected to financially support the cybersecurity investments proposed in your project without the benefit of receiving an award under this FOA, what would be the estimated financial impact on their members/customers?

Project Design and Management

19. Describe the expected responsibilities and activities of the staff members who will be part of your project team, and provide their names, job titles, and experience. Include any anticipated external partners you anticipate using to complete your project.
20. Describe how you will recruit utility participants. What challenges do you anticipate you will face in retaining participants until the end of the project and how will you mitigate the risk of participating utilities leaving the project?
21. Describe how expansions in the number, type, and quality of products and services your organization provides to participating utilities will be maintained, staffed, and funded by your organization after the project funding ends?
22. What legal, funding, and administrative challenges might affect the success of your project and how will you address those challenges?
23. Describe any actions your utility’s senior leadership has taken to support this FOA application process. What commitments has senior leadership made to provide the additional support necessary to ensure successful completion of the proposed project?

Topic Area 2 Pre-Application Questions

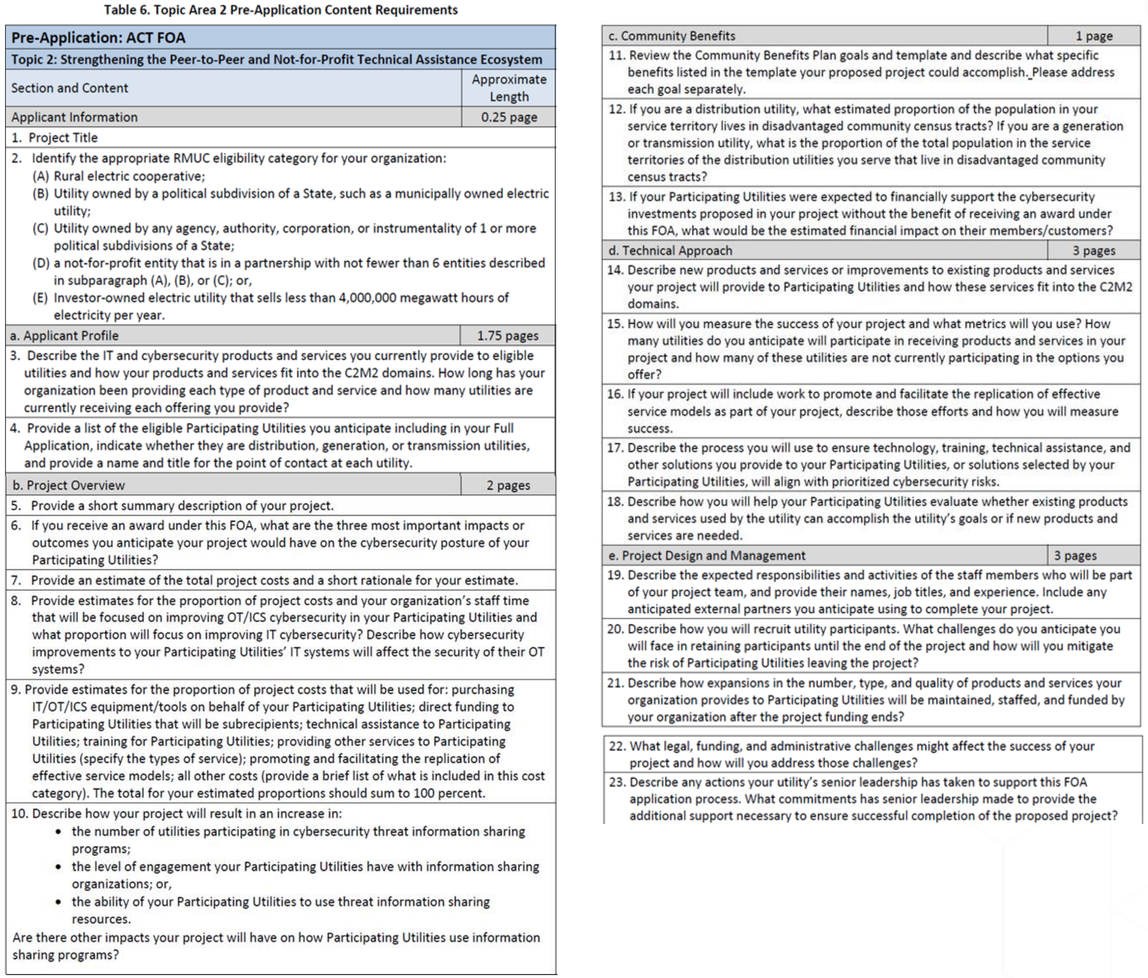


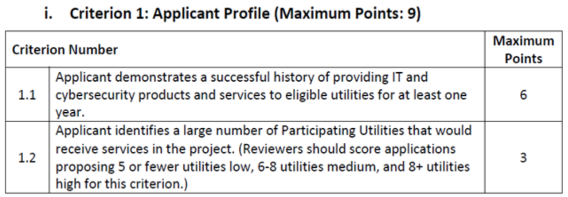
Table 6. Topic Area 2 Pre-Application Content Requirements

Pre-Application: ACT FOA	
Topic 2: Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem	
Section and Content	Approximate Length
Applicant Information	0.25 page
1. Project Title	
2. Identify the appropriate RMUC eligibility category for your organization: (A) Rural electric cooperative; (B) Utility owned by a political subdivision of a State, such as a municipally owned electric utility; (C) Utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State; (D) a not-for-profit entity that is in a partnership with not fewer than 6 entities described in subparagraph (A), (B), or (C); or, (E) Investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year.	
a. Applicant Profile	1.75 pages
3. Describe the IT and cybersecurity products and services you currently provide to eligible utilities and how your products and services fit into the C2M2 domains. How long has your organization been providing each type of product and service and how many utilities are currently receiving each offering you provide?	
4. Provide a list of the eligible Participating Utilities you anticipate including in your Full Application, indicate whether they are distribution, generation, or transmission utilities, and provide a name and title for the point of contact at each utility.	
b. Project Overview	2 pages
5. Provide a short summary description of your project.	
6. If you receive an award under this FOA, what are the three most important impacts or outcomes you anticipate your project would have on the cybersecurity posture of your Participating Utilities?	
7. Provide an estimate of the total project costs and a short rationale for your estimate.	
8. Provide estimates for the proportion of project costs and your organization's staff time that will be focused on improving OT/ICS cybersecurity in your Participating Utilities and what proportion will focus on improving IT cybersecurity? Describe how cybersecurity improvements to your Participating Utilities' IT systems will affect the security of their OT systems?	
9. Provide estimates for the proportion of project costs that will be used for: purchasing IT/OT/ICS equipment/tools on behalf of your Participating Utilities; direct funding to Participating Utilities that will be subrecipients; technical assistance to Participating Utilities; training for Participating Utilities; providing other services to Participating Utilities (specify the types of service); promoting and facilitating the replication of effective service models; all other costs (provide a brief list of what is included in this cost category). The total for your estimated proportions should sum to 100 percent.	
10. Describe how your project will result in an increase in: • the number of utilities participating in cybersecurity threat information sharing programs; • the level of engagement your Participating Utilities have with information sharing organizations; or, • the ability of your Participating Utilities to use threat information sharing resources. Are there other impacts your project will have on how Participating Utilities use information sharing programs?	
c. Community Benefits	1 page
11. Review the Community Benefits Plan goals and template and describe what specific benefits listed in the template your proposed project could accomplish. Please address each goal separately.	
12. If you are a distribution utility, what estimated proportion of the population in your service territory lives in disadvantaged community census tracts? If you are a generation or transmission utility, what is the proportion of the total population in the service territories of the distribution utilities you serve that live in disadvantaged community census tracts?	
13. If your Participating Utilities were expected to financially support the cybersecurity investments proposed in your project without the benefit of receiving an award under this FOA, what would be the estimated financial impact on their members/customers?	
d. Technical Approach	3 pages
14. Describe new products and services or improvements to existing products and services your project will provide to Participating Utilities and how these services fit into the C2M2 domains.	
15. How will you measure the success of your project and what metrics will you use? How many utilities do you anticipate will participate in receiving products and services in your project and how many of these utilities are not currently participating in the options you offer?	
16. If your project will include work to promote and facilitate the replication of effective service models as part of your project, describe those efforts and how you will measure success.	
17. Describe the process you will use to ensure technology, training, technical assistance, and other solutions you provide to your Participating Utilities, or solutions selected by your Participating Utilities, will align with prioritized cybersecurity risks.	
18. Describe how you will help your Participating Utilities evaluate whether existing products and services used by the utility can accomplish the utility's goals or if new products and services are needed.	
e. Project Design and Management	3 pages
19. Describe the expected responsibilities and activities of the staff members who will be part of your project team, and provide their names, job titles, and experience. Include any anticipated external partners you anticipate using to complete your project.	
20. Describe how you will recruit utility participants. What challenges do you anticipate you will face in retaining participants until the end of the project and how will you mitigate the risk of Participating Utilities leaving the project?	
21. Describe how expansions in the number, type, and quality of products and services your organization provides to Participating Utilities will be maintained, staffed, and funded by your organization after the project funding ends?	
22. What legal, funding, and administrative challenges might affect the success of your project and how will you address those challenges?	
23. Describe any actions your utility's senior leadership has taken to support this FOA application process. What commitments has senior leadership made to provide the additional support necessary to ensure successful completion of the proposed project?	

FOA Section VII.B (pgs. 58-61)

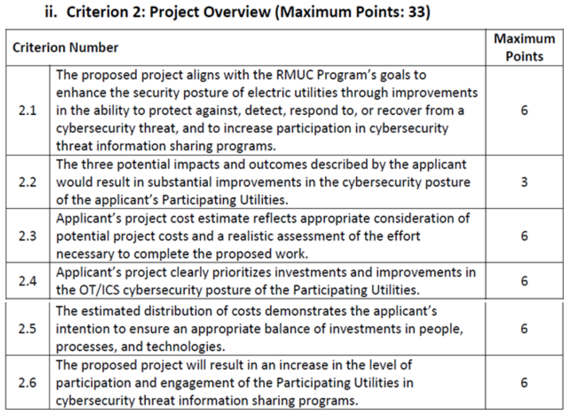
Topic Area 2 Pre-Application Review Criteria

Total Possible Score – 108 points



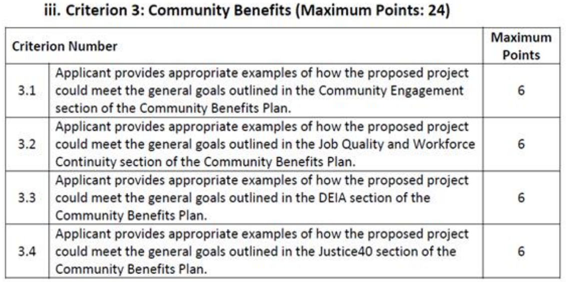
i. Criterion 1: Applicant Profile (Maximum Points: 9)

Criterion Number		Maximum Points
1.1	Applicant demonstrates a successful history of providing IT and cybersecurity products and services to eligible utilities for at least one year.	6
1.2	Applicant identifies a large number of Participating Utilities that would receive services in the project. (Reviewers should score applications proposing 5 or fewer utilities low, 6-8 utilities medium, and 8+ utilities high for this criterion.)	3



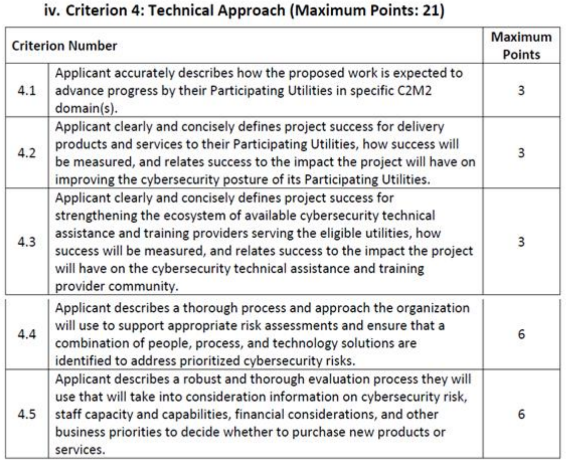
ii. Criterion 2: Project Overview (Maximum Points: 33)

Criterion Number		Maximum Points
2.1	The proposed project aligns with the RMUC Program's goals to enhance the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat, and to increase participation in cybersecurity threat information sharing programs.	6
2.2	The three potential impacts and outcomes described by the applicant would result in substantial improvements in the cybersecurity posture of the applicant's Participating Utilities.	3
2.3	Applicant's project cost estimate reflects appropriate consideration of potential project costs and a realistic assessment of the effort necessary to complete the proposed work.	6
2.4	Applicant's project clearly prioritizes investments and improvements in the OT/ICS cybersecurity posture of the Participating Utilities.	6
2.5	The estimated distribution of costs demonstrates the applicant's intention to ensure an appropriate balance of investments in people, processes, and technologies.	6
2.6	The proposed project will result in an increase in the level of participation and engagement of the Participating Utilities in cybersecurity threat information sharing programs.	6



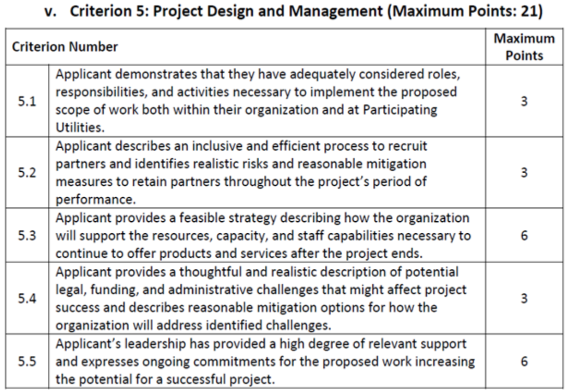
iii. Criterion 3: Community Benefits (Maximum Points: 24)

Criterion Number		Maximum Points
3.1	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Community Engagement section of the Community Benefits Plan.	6
3.2	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Job Quality and Workforce Continuity section of the Community Benefits Plan.	6
3.3	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the DEIA section of the Community Benefits Plan.	6
3.4	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Justice40 section of the Community Benefits Plan.	6



iv. Criterion 4: Technical Approach (Maximum Points: 21)

Criterion Number		Maximum Points
4.1	Applicant accurately describes how the proposed work is expected to advance progress by their Participating Utilities in specific C2M2 domain(s).	3
4.2	Applicant clearly and concisely defines project success for delivery products and services to their Participating Utilities, how success will be measured, and relates success to the impact the project will have on improving the cybersecurity posture of its Participating Utilities.	3
4.3	Applicant clearly and concisely defines project success for strengthening the ecosystem of available cybersecurity technical assistance and training providers serving the eligible utilities, how success will be measured, and relates success to the impact the project will have on the cybersecurity technical assistance and training provider community.	3
4.4	Applicant describes a thorough process and approach the organization will use to support appropriate risk assessments and ensure that a combination of people, process, and technology solutions are identified to address prioritized cybersecurity risks.	6
4.5	Applicant describes a robust and thorough evaluation process they will use that will take into consideration information on cybersecurity risk, staff capacity and capabilities, financial considerations, and other business priorities to decide whether to purchase new products or services.	6



v. Criterion 5: Project Design and Management (Maximum Points: 21)

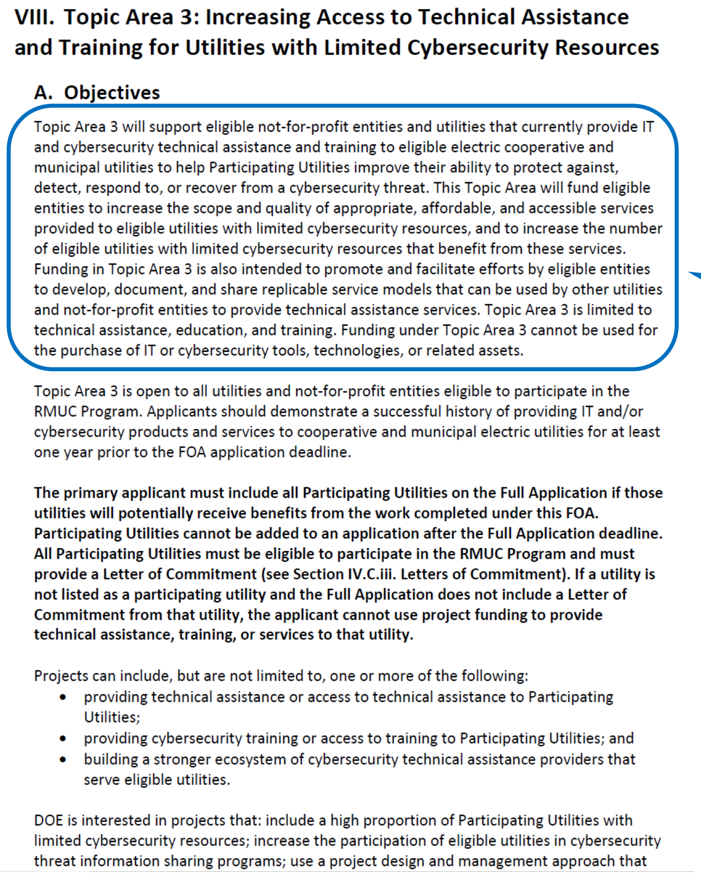
Criterion Number		Maximum Points
5.1	Applicant demonstrates that they have adequately considered roles, responsibilities, and activities necessary to implement the proposed scope of work both within their organization and at Participating Utilities.	3
5.2	Applicant describes an inclusive and efficient process to recruit partners and identifies realistic risks and reasonable mitigation measures to retain partners throughout the project's period of performance.	3
5.3	Applicant provides a feasible strategy describing how the organization will support the resources, capacity, and staff capabilities necessary to continue to offer products and services after the project ends.	6
5.4	Applicant provides a thoughtful and realistic description of potential legal, funding, and administrative challenges that might affect project success and describes reasonable mitigation options for how the organization will address identified challenges.	3
5.5	Applicant's leadership has provided a high degree of relevant support and expresses ongoing commitments for the proposed work increasing the potential for a successful project.	6

FOA Section VII.C (pgs. 61-63)

Topic Area 3 – Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources

Topic Area 3 – Goals and Objectives

FOA Section VIII.A (pgs. 72-74)



VIII. Topic Area 3: Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources

A. Objectives

Topic Area 3 will support eligible not-for-profit entities and utilities that currently provide IT and cybersecurity technical assistance and training to eligible electric cooperative and municipal utilities to help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat. This Topic Area will fund eligible entities to increase the scope and quality of appropriate, affordable, and accessible services provided to eligible utilities with limited cybersecurity resources, and to increase the number of eligible utilities with limited cybersecurity resources that benefit from these services. Funding in Topic Area 3 is also intended to promote and facilitate efforts by eligible entities to develop, document, and share replicable service models that can be used by other utilities and not-for-profit entities to provide technical assistance services. Topic Area 3 is limited to technical assistance, education, and training. Funding under Topic Area 3 cannot be used for the purchase of IT or cybersecurity tools, technologies, or related assets.

Topic Area 3 is open to all utilities and not-for-profit entities eligible to participate in the RMUC Program. Applicants should demonstrate a successful history of providing IT and/or cybersecurity products and services to cooperative and municipal electric utilities for at least one year prior to the FOA application deadline.

The primary applicant must include all Participating Utilities on the Full Application if those utilities will potentially receive benefits from the work completed under this FOA. Participating Utilities cannot be added to an application after the Full Application deadline. All Participating Utilities must be eligible to participate in the RMUC Program and must provide a Letter of Commitment (see Section IV.C.iii. Letters of Commitment). If a utility is not listed as a participating utility and the Full Application does not include a Letter of Commitment from that utility, the applicant cannot use project funding to provide technical assistance, training, or services to that utility.

Projects can include, but are not limited to, one or more of the following:

- providing technical assistance or access to technical assistance to Participating Utilities;
- providing cybersecurity training or access to training to Participating Utilities; and
- building a stronger ecosystem of cybersecurity technical assistance providers that serve eligible utilities.

DOE is interested in projects that: include a high proportion of Participating Utilities with limited cybersecurity resources; increase the participation of eligible utilities in cybersecurity threat information sharing programs; use a project design and management approach that

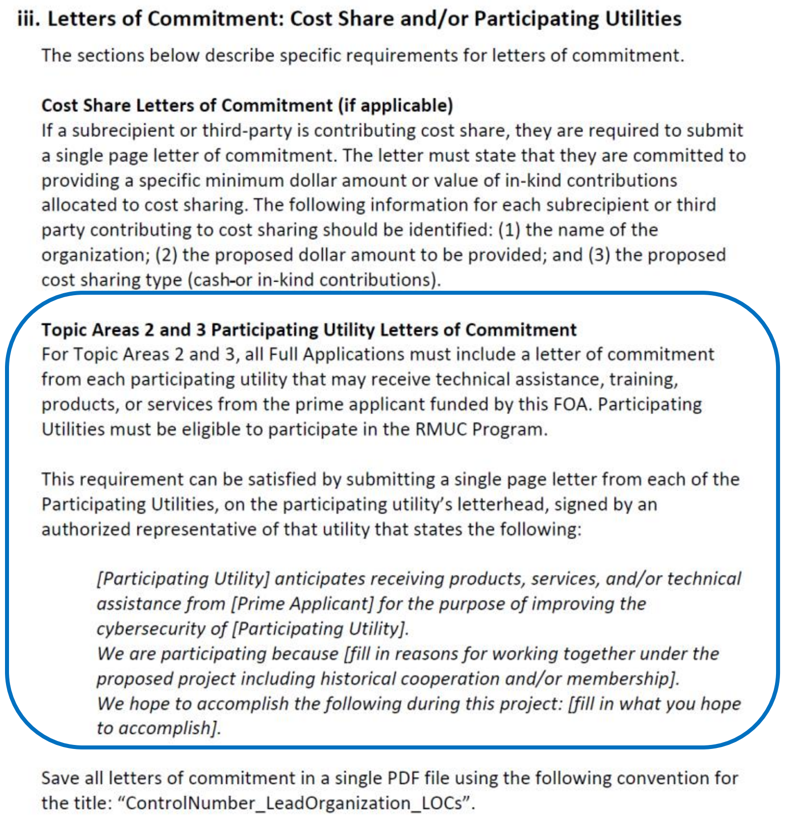
Support eligible not-for-profit entities and utilities currently providing IT and cybersecurity technical assistance and training to eligible utilities to help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat.

Goals

1) Increase the scope and quality of appropriate, affordable, and accessible services provided to eligible utilities with limited cybersecurity resources;
2) **Increase the number of eligible utilities with limited cybersecurity resources that benefit from these services;**
3) Promote and facilitate efforts to develop, document, and share replicable service models

Topic Area 3 – Participating Utilities

FOA Section IV.C (pg. 29)



iii. Letters of Commitment: Cost Share and/or Participating Utilities

The sections below describe specific requirements for letters of commitment.

Cost Share Letters of Commitment (if applicable)
If a subrecipient or third-party is contributing cost share, they are required to submit a single page letter of commitment. The letter must state that they are committed to providing a specific minimum dollar amount or value of in-kind contributions allocated to cost sharing. The following information for each subrecipient or third party contributing to cost sharing should be identified: (1) the name of the organization; (2) the proposed dollar amount to be provided; and (3) the proposed cost sharing type (cash-or in-kind contributions).

Topic Areas 2 and 3 Participating Utility Letters of Commitment
For Topic Areas 2 and 3, all Full Applications must include a letter of commitment from each participating utility that may receive technical assistance, training, products, or services from the prime applicant funded by this FOA. Participating Utilities must be eligible to participate in the RMUC Program.

This requirement can be satisfied by submitting a single page letter from each of the Participating Utilities, on the participating utility's letterhead, signed by an authorized representative of that utility that states the following:

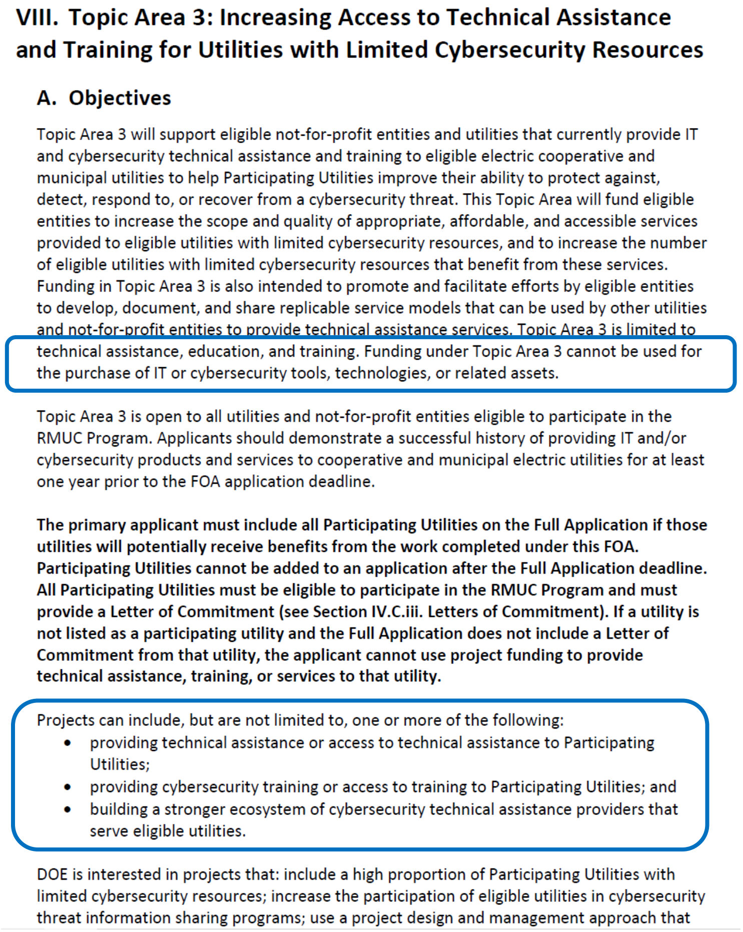
> *[Participating Utility] anticipates receiving products, services, and/or technical assistance from [Prime Applicant] for the purpose of improving the cybersecurity of [Participating Utility].*
> *We are participating because [fill in reasons for working together under the proposed project including historical cooperation and/or membership].*
> *We hope to accomplish the following during this project: [fill in what you hope to accomplish].*

Save all letters of commitment in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_LOCs".

Full Applications must include a letter of commitment from each Participating Utility that might receive technical assistance, training, products, or services from the prime applicant.

Topic Area 3 – What Could be Proposed

FOA Section VIII.A (pgs. 72-74)



VIII. Topic Area 3: Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources

A. Objectives

Topic Area 3 will support eligible not-for-profit entities and utilities that currently provide IT and cybersecurity technical assistance and training to eligible electric cooperative and municipal utilities to help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat. This Topic Area will fund eligible entities to increase the scope and quality of appropriate, affordable, and accessible services provided to eligible utilities with limited cybersecurity resources, and to increase the number of eligible utilities with limited cybersecurity resources that benefit from these services. Funding in Topic Area 3 is also intended to promote and facilitate efforts by eligible entities to develop, document, and share replicable service models that can be used by other utilities and not-for-profit entities to provide technical assistance services. Topic Area 3 is limited to technical assistance, education, and training. Funding under Topic Area 3 cannot be used for the purchase of IT or cybersecurity tools, technologies, or related assets.

Topic Area 3 is open to all utilities and not-for-profit entities eligible to participate in the RMUC Program. Applicants should demonstrate a successful history of providing IT and/or cybersecurity products and services to cooperative and municipal electric utilities for at least one year prior to the FOA application deadline.

The primary applicant must include all Participating Utilities on the Full Application if those utilities will potentially receive benefits from the work completed under this FOA. Participating Utilities cannot be added to an application after the Full Application deadline. All Participating Utilities must be eligible to participate in the RMUC Program and must provide a Letter of Commitment (see Section IV.C.iii. Letters of Commitment). If a utility is not listed as a participating utility and the Full Application does not include a Letter of Commitment from that utility, the applicant cannot use project funding to provide technical assistance, training, or services to that utility.

Projects can include, but are not limited to, one or more of the following:

- providing technical assistance or access to technical assistance to Participating Utilities;
- providing cybersecurity training or access to training to Participating Utilities; and
- building a stronger ecosystem of cybersecurity technical assistance providers that serve eligible utilities.

DOE is interested in projects that: include a high proportion of Participating Utilities with limited cybersecurity resources; increase the participation of eligible utilities in cybersecurity threat information sharing programs; use a project design and management approach that

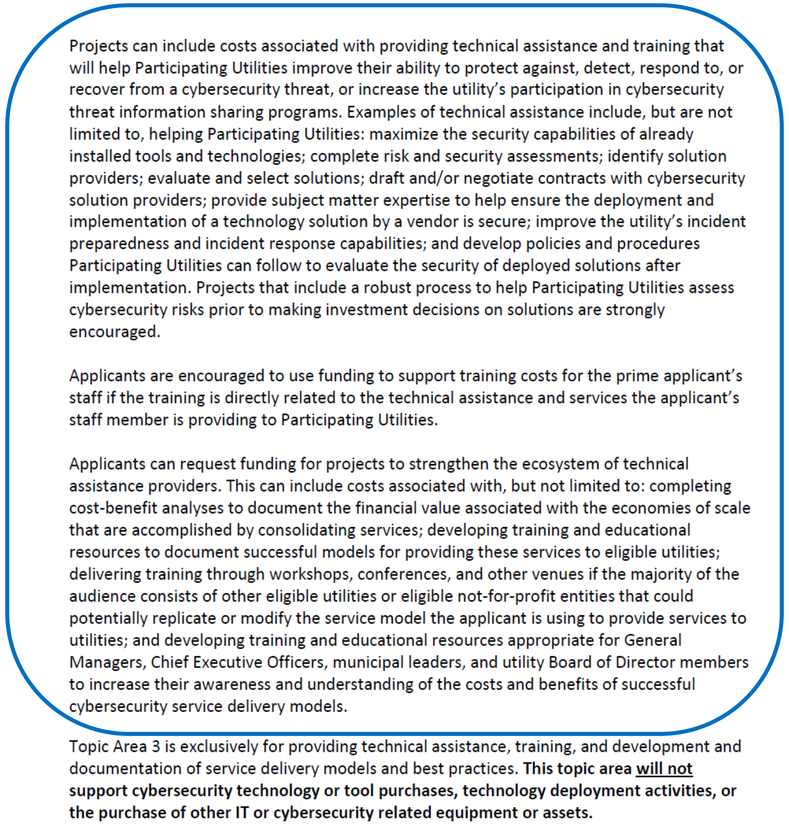
Projects could include, but are not limited to:

1) Providing technical assistance
2) Providing training
3) Building a stronger ecosystem of cybersecurity technical assistance providers

Funding ***cannot*** be used for the purchase of IT or cybersecurity tools, technologies, or related assets.

Topic Area 3 – How Can Funding be Used $

FOA Section VIII.A (pgs. 72-74)



Projects can include costs associated with providing technical assistance and training that will help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat, or increase the utility's participation in cybersecurity threat information sharing programs. Examples of technical assistance include, but are not limited to, helping Participating Utilities: maximize the security capabilities of already installed tools and technologies; complete risk and security assessments; identify solution providers; evaluate and select solutions; draft and/or negotiate contracts with cybersecurity solution providers; provide subject matter expertise to help ensure the deployment and implementation of a technology solution by a vendor is secure; improve the utility's incident preparedness and incident response capabilities; and develop policies and procedures Participating Utilities can follow to evaluate the security of deployed solutions after implementation. Projects that include a robust process to help Participating Utilities assess cybersecurity risks prior to making investment decisions on solutions are strongly encouraged.

Applicants are encouraged to use funding to support training costs for the prime applicant's staff if the training is directly related to the technical assistance and services the applicant's staff member is providing to Participating Utilities.

Applicants can request funding for projects to strengthen the ecosystem of technical assistance providers. This can include costs associated with, but not limited to: completing cost-benefit analyses to document the financial value associated with the economies of scale that are accomplished by consolidating services; developing training and educational resources to document successful models for providing these services to eligible utilities; delivering training through workshops, conferences, and other venues if the majority of the audience consists of other eligible utilities or eligible not-for-profit entities that could potentially replicate or modify the service model the applicant is using to provide services to utilities; and developing training and educational resources appropriate for General Managers, Chief Executive Officers, municipal leaders, and utility Board of Director members to increase their awareness and understanding of the costs and benefits of successful cybersecurity service delivery models.

Topic Area 3 is exclusively for providing technical assistance, training, and development and documentation of service delivery models and best practices. **This topic area will not support cybersecurity technology or tool purchases, technology deployment activities, or the purchase of other IT or cybersecurity related equipment or assets.**

Examples of what project funds could be used for:

1) Providing technical assistance and training that will help Participating Utilities improve their ability to protect against, detect, respond to, or recover from a cybersecurity threat, or
2) Provide technical assistance and training to increase the participation of Participating Utilities in cybersecurity threat information sharing programs
3) Support training costs for the prime applicant's staff if the training is directly related to technical assistance it provides to Participating Utilities
4) Strengthen ecosystem of technical assistance providers

Topic Area 3 - Eligibility

All RMUC Program eligible entities defined in BIL Section 40124 can apply to Topic Area 3.

(A) Rural electric cooperatives;

(B) Utilities owned by a political subdivision of a State, such as a municipally owned electric utility;

(C) Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a State;

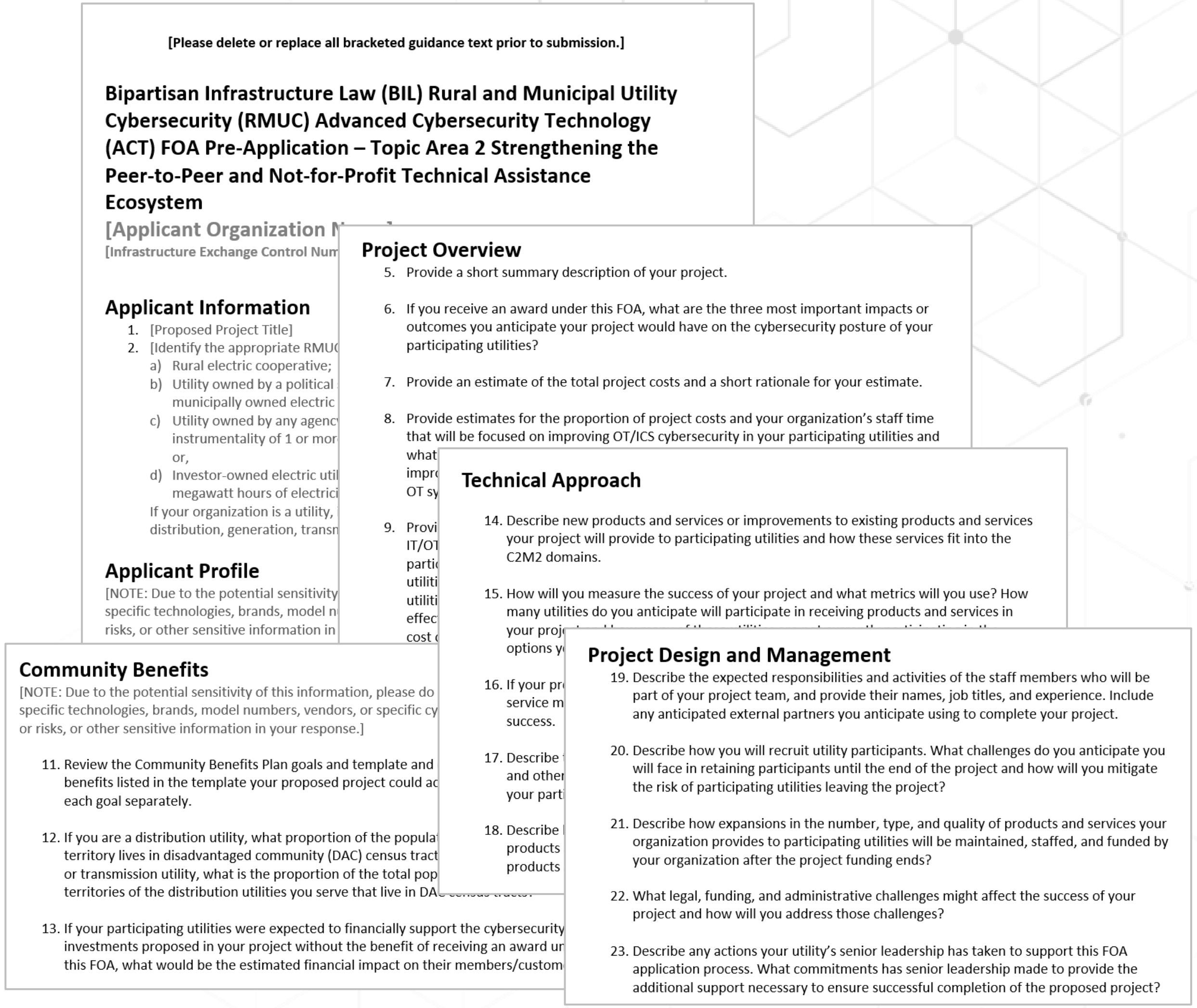
(D) Not-for-profit entities that are in a partnership with not fewer than 6 entities described in (A), (B), or (C) above; and

(E) Investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year

FOA Section III.A.i (pg. 17)

Topic Area 3 – Pre-Application Response Template

- Consists of 22 questions
- Optional Topic Area 3 Pre-Application Response Template found on eXCHANGE
- Answer completely and concisely
- Use review criteria to guide responses
- This document is what will be submitted for review to determine whether an applicant will be “invited” to submit a Full Application



[Please delete or replace all bracketed guidance text prior to submission.]

Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) FOA Pre-Application – Topic Area 2 Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem

[Applicant Organization N

[Infrastructure Exchange Control Num

Applicant Information

1. [Proposed Project Title]
2. [Identify the appropriate RMUC
   a) Rural electric cooperative;
   b) Utility owned by a political municipally owned electric
   c) Utility owned by any agency instrumentality of 1 or more or,
   d) Investor-owned electric util megawatt hours of electrici

   If your organization is a utility, distribution, generation, transm

Applicant Profile

[NOTE: Due to the potential sensitivity specific technologies, brands, model n risks, or other sensitive information in

Project Overview

5. Provide a short summary description of your project.
6. If you receive an award under this FOA, what are the three most important impacts or outcomes you anticipate your project would have on the cybersecurity posture of your participating utilities?
7. Provide an estimate of the total project costs and a short rationale for your estimate.
8. Provide estimates for the proportion of project costs and your organization’s staff time that will be focused on improving OT/ICS cybersecurity in your participating utilities and what impr OT sy
9. Provi IT/OT partic utiliti utiliti effec cost c

Community Benefits

[NOTE: Due to the potential sensitivity of this information, please do specific technologies, brands, model numbers, vendors, or specific cy or risks, or other sensitive information in your response.]

11. Review the Community Benefits Plan goals and template and benefits listed in the template your proposed project could ac each goal separately.
12. If you are a distribution utility, what proportion of the popula territory lives in disadvantaged community (DAC) census tract or transmission utility, what is the proportion of the total pop territories of the distribution utilities you serve that live in DA
13. If your participating utilities were expected to financially support the cybersecurity investments proposed in your project without the benefit of receiving an award ur this FOA, what would be the estimated financial impact on their members/custom

Technical Approach

14. Describe new products and services or improvements to existing products and services your project will provide to participating utilities and how these services fit into the C2M2 domains.
15. How will you measure the success of your project and what metrics will you use? How many utilities do you anticipate will participate in receiving products and services in your proj options y
16. If your pr service m success.
17. Describe and other your parti
18. Describe products products

Project Design and Management

19. Describe the expected responsibilities and activities of the staff members who will be part of your project team, and provide their names, job titles, and experience. Include any anticipated external partners you anticipate using to complete your project.
20. Describe how you will recruit utility participants. What challenges do you anticipate you will face in retaining participants until the end of the project and how will you mitigate the risk of participating utilities leaving the project?
21. Describe how expansions in the number, type, and quality of products and services your organization provides to participating utilities will be maintained, staffed, and funded by your organization after the project funding ends?
22. What legal, funding, and administrative challenges might affect the success of your project and how will you address those challenges?
23. Describe any actions your utility’s senior leadership has taken to support this FOA application process. What commitments has senior leadership made to provide the additional support necessary to ensure successful completion of the proposed project?

Topic Area 3 Pre-Application Questions

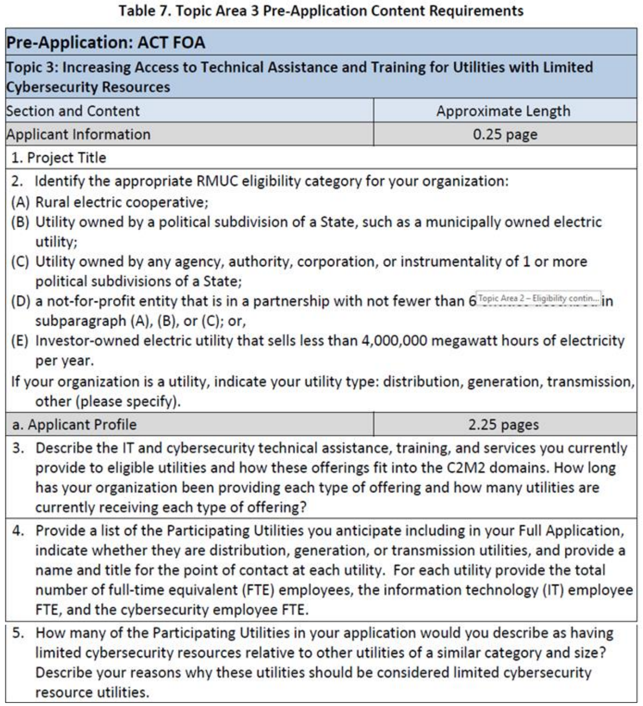
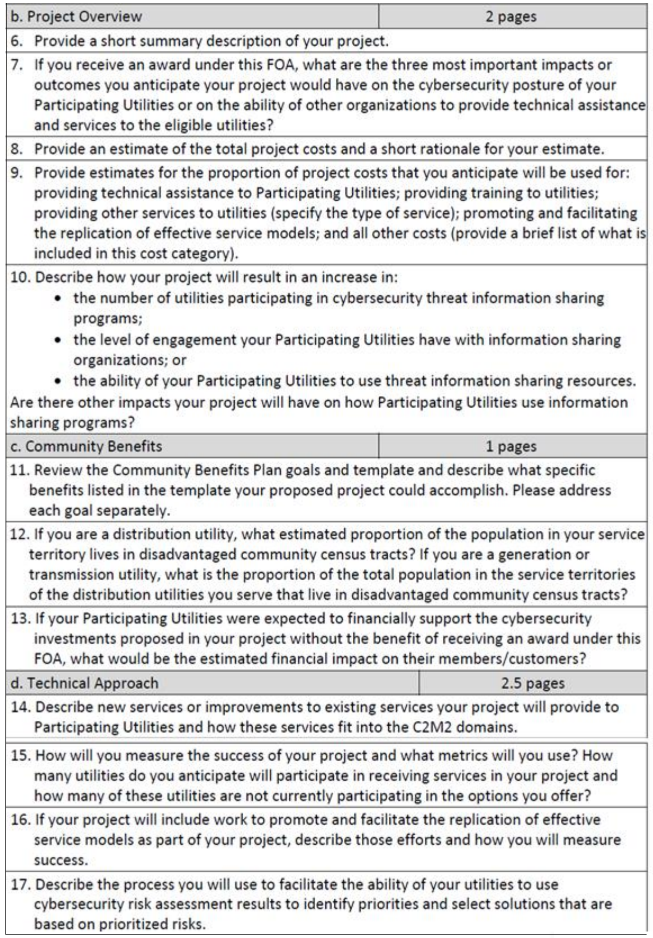
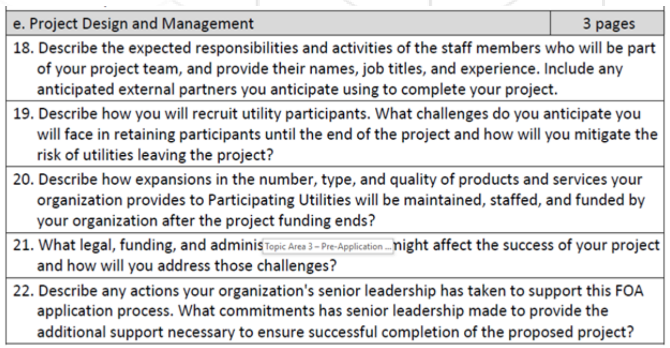


Table 7. Topic Area 3 Pre-Application Content Requirements

Pre-Application: ACT FOA	
Topic 3: Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources	
Section and Content	Approximate Length
Applicant Information	0.25 page
1. Project Title	
2. Identify the appropriate RMUC eligibility category for your organization: (A) Rural electric cooperative; (B) Utility owned by a political subdivision of a State, such as a municipally owned electric utility; (C) Utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State; (D) a not-for-profit entity that is in a partnership with not fewer than 6 Topic Area 2 – Eligibility contin... in subparagraph (A), (B), or (C); or, (E) Investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year. If your organization is a utility, indicate your utility type: distribution, generation, transmission, other (please specify).	
a. Applicant Profile	2.25 pages
3. Describe the IT and cybersecurity technical assistance, training, and services you currently provide to eligible utilities and how these offerings fit into the C2M2 domains. How long has your organization been providing each type of offering and how many utilities are currently receiving each type of offering?	
4. Provide a list of the Participating Utilities you anticipate including in your Full Application, indicate whether they are distribution, generation, or transmission utilities, and provide a name and title for the point of contact at each utility. For each utility provide the total number of full-time equivalent (FTE) employees, the information technology (IT) employee FTE, and the cybersecurity employee FTE.	
5. How many of the Participating Utilities in your application would you describe as having limited cybersecurity resources relative to other utilities of a similar category and size? Describe your reasons why these utilities should be considered limited cybersecurity resource utilities.	



b. Project Overview	2 pages
6. Provide a short summary description of your project.	
7. If you receive an award under this FOA, what are the three most important impacts or outcomes you anticipate your project would have on the cybersecurity posture of your Participating Utilities or on the ability of other organizations to provide technical assistance and services to the eligible utilities?	
8. Provide an estimate of the total project costs and a short rationale for your estimate.	
9. Provide estimates for the proportion of project costs that you anticipate will be used for: providing technical assistance to Participating Utilities; providing training to utilities; providing other services to utilities (specify the type of service); promoting and facilitating the replication of effective service models; and all other costs (provide a brief list of what is included in this cost category).	
10. Describe how your project will result in an increase in: • the number of utilities participating in cybersecurity threat information sharing programs; • the level of engagement your Participating Utilities have with information sharing organizations; or • the ability of your Participating Utilities to use threat information sharing resources. Are there other impacts your project will have on how Participating Utilities use information sharing programs?	
c. Community Benefits	1 pages
11. Review the Community Benefits Plan goals and template and describe what specific benefits listed in the template your proposed project could accomplish. Please address each goal separately.	
12. If you are a distribution utility, what estimated proportion of the population in your service territory lives in disadvantaged community census tracts? If you are a generation or transmission utility, what is the proportion of the total population in the service territories of the distribution utilities you serve that live in disadvantaged community census tracts?	
13. If your Participating Utilities were expected to financially support the cybersecurity investments proposed in your project without the benefit of receiving an award under this FOA, what would be the estimated financial impact on their members/customers?	
d. Technical Approach	2.5 pages
14. Describe new services or improvements to existing services your project will provide to Participating Utilities and how these services fit into the C2M2 domains.	
15. How will you measure the success of your project and what metrics will you use? How many utilities do you anticipate will participate in receiving services in your project and how many of these utilities are not currently participating in the options you offer?	
16. If your project will include work to promote and facilitate the replication of effective service models as part of your project, describe those efforts and how you will measure success.	
17. Describe the process you will use to facilitate the ability of your utilities to use cybersecurity risk assessment results to identify priorities and select solutions that are based on prioritized risks.	

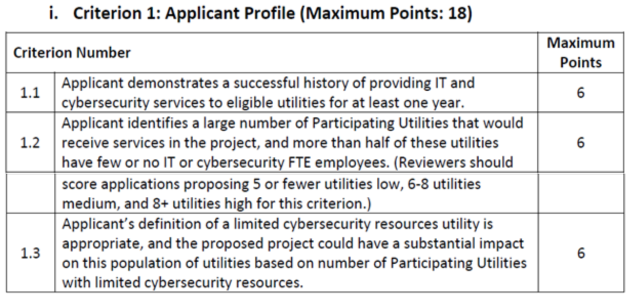


e. Project Design and Management	3 pages
18. Describe the expected responsibilities and activities of the staff members who will be part of your project team, and provide their names, job titles, and experience. Include any anticipated external partners you anticipate using to complete your project.	
19. Describe how you will recruit utility participants. What challenges do you anticipate you will face in retaining participants until the end of the project and how will you mitigate the risk of utilities leaving the project?	
20. Describe how expansions in the number, type, and quality of products and services your organization provides to Participating Utilities will be maintained, staffed, and funded by your organization after the project funding ends?	
21. What legal, funding, and adminis Topic Area 3 – Pre-Application ... night affect the success of your project and how will you address those challenges?	
22. Describe any actions your organization's senior leadership has taken to support this FOA application process. What commitments has senior leadership made to provide the additional support necessary to ensure successful completion of the proposed project?	

**FOA Section VIII.B
(pgs. 74-76)**

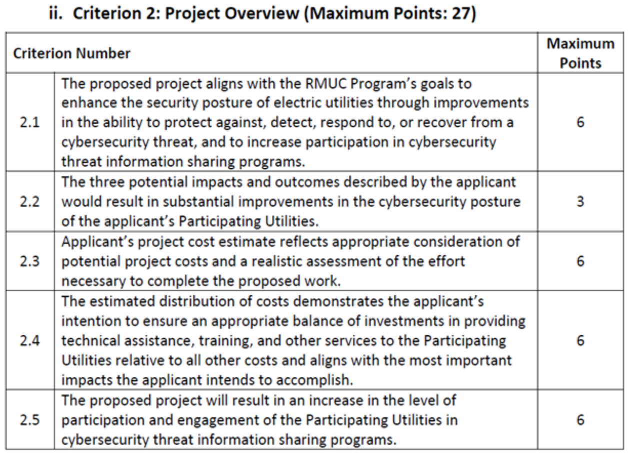
Topic Area 3 Pre-Application Review Criteria

Total Possible Score – 105 points



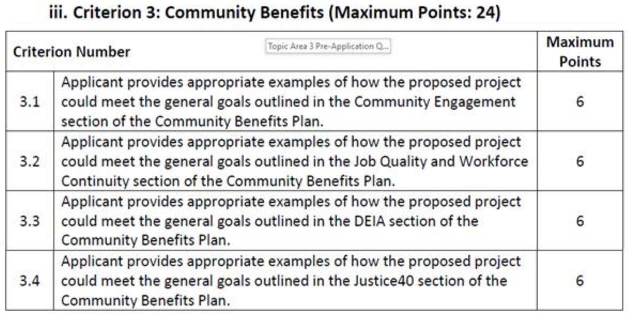
i. **Criterion 1: Applicant Profile (Maximum Points: 18)**

Criterion Number		Maximum Points
1.1	Applicant demonstrates a successful history of providing IT and cybersecurity services to eligible utilities for at least one year.	6
1.2	Applicant identifies a large number of Participating Utilities that would receive services in the project, and more than half of these utilities have few or no IT or cybersecurity FTE employees. (Reviewers should	6
	score applications proposing 5 or fewer utilities low, 6-8 utilities medium, and 8+ utilities high for this criterion.)	
1.3	Applicant's definition of a limited cybersecurity resources utility is appropriate, and the proposed project could have a substantial impact on this population of utilities based on number of Participating Utilities with limited cybersecurity resources.	6



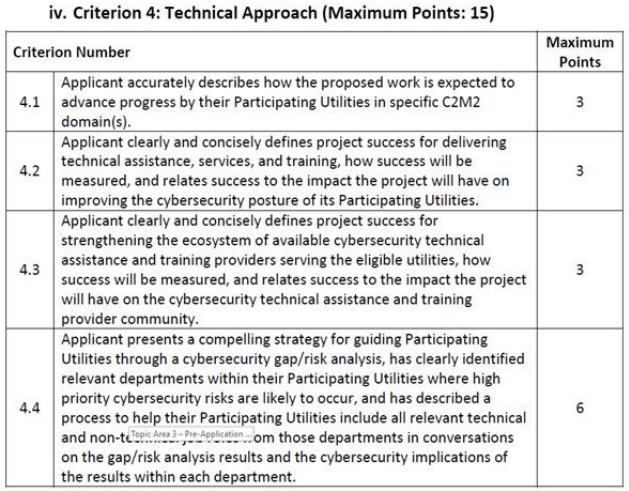
ii. **Criterion 2: Project Overview (Maximum Points: 27)**

Criterion Number		Maximum Points
2.1	The proposed project aligns with the RMUC Program's goals to enhance the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat, and to increase participation in cybersecurity threat information sharing programs.	6
2.2	The three potential impacts and outcomes described by the applicant would result in substantial improvements in the cybersecurity posture of the applicant's Participating Utilities.	3
2.3	Applicant's project cost estimate reflects appropriate consideration of potential project costs and a realistic assessment of the effort necessary to complete the proposed work.	6
2.4	The estimated distribution of costs demonstrates the applicant's intention to ensure an appropriate balance of investments in providing technical assistance, training, and other services to the Participating Utilities relative to all other costs and aligns with the most important impacts the applicant intends to accomplish.	6
2.5	The proposed project will result in an increase in the level of participation and engagement of the Participating Utilities in cybersecurity threat information sharing programs.	6



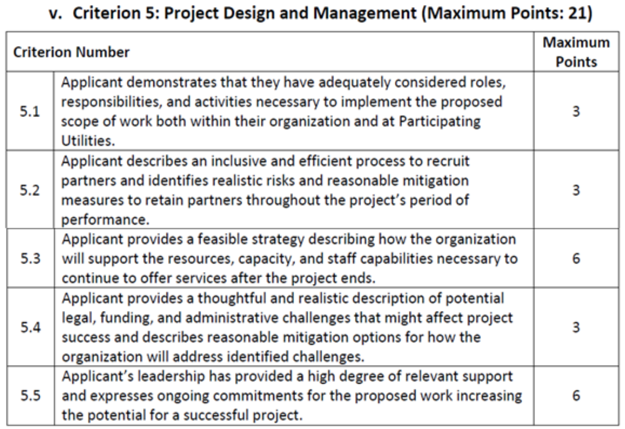
iii. **Criterion 3: Community Benefits (Maximum Points: 24)**

Criterion Number	Topic Area 3 Pre-Application Q...	Maximum Points
3.1	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Community Engagement section of the Community Benefits Plan.	6
3.2	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Job Quality and Workforce Continuity section of the Community Benefits Plan.	6
3.3	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the DEIA section of the Community Benefits Plan.	6
3.4	Applicant provides appropriate examples of how the proposed project could meet the general goals outlined in the Justice40 section of the Community Benefits Plan.	6



iv. **Criterion 4: Technical Approach (Maximum Points: 15)**

Criterion Number		Maximum Points
4.1	Applicant accurately describes how the proposed work is expected to advance progress by their Participating Utilities in specific C2M2 domain(s).	3
4.2	Applicant clearly and concisely defines project success for delivering technical assistance, services, and training, how success will be measured, and relates success to the impact the project will have on improving the cybersecurity posture of its Participating Utilities.	3
4.3	Applicant clearly and concisely defines project success for strengthening the ecosystem of available cybersecurity technical assistance and training providers serving the eligible utilities, how success will be measured, and relates success to the impact the project will have on the cybersecurity technical assistance and training provider community.	3
4.4	Applicant presents a compelling strategy for guiding Participating Utilities through a cybersecurity gap/risk analysis, has clearly identified relevant departments within their Participating Utilities where high priority cybersecurity risks are likely to occur, and has described a process to help their Participating Utilities include all relevant technical and non-te Topic Area 3 – Pre-Application ... om those departments in conversations on the gap/risk analysis results and the cybersecurity implications of the results within each department.	6



v. **Criterion 5: Project Design and Management (Maximum Points: 21)**

Criterion Number		Maximum Points
5.1	Applicant demonstrates that they have adequately considered roles, responsibilities, and activities necessary to implement the proposed scope of work both within their organization and at Participating Utilities.	3
5.2	Applicant describes an inclusive and efficient process to recruit partners and identifies realistic risks and reasonable mitigation measures to retain partners throughout the project's period of performance.	3
5.3	Applicant provides a feasible strategy describing how the organization will support the resources, capacity, and staff capabilities necessary to continue to offer services after the project ends.	6
5.4	Applicant provides a thoughtful and realistic description of potential legal, funding, and administrative challenges that might affect project success and describes reasonable mitigation options for how the organization will address identified challenges.	3
5.5	Applicant's leadership has provided a high degree of relevant support and expresses ongoing commitments for the proposed work increasing the potential for a successful project.	6

FOA Section VIII.C (pgs. 76-79)

Final Thoughts

Full Application Information

For applicants invited to submit a Full Application, an additional webinar will be held prior to the Full Application submission deadline. We will provide more information about the Full Application process and requirements in more detail in that webinar.

Feeling Overwhelmed?

- Completing the FOA process takes work and patience
- Applying and meeting all award requirements can seem overwhelming.
- We encourage you to work with your respective communities and partners to find assistance.
- In addition to the RMUC ACT FOA, the RMUC Program also offered the ACT 1 Prize Competition, which has fewer requirements. A second Prize, the ACT 2 Prize, is planned.

Questions about the ACT FOA or eXCHANGE

Questions about this FOA?

- Email DE-FOA-0002986@netl.doe.gov
- All Q&As related to this FOA will be posted on eXCHANGE
- You must select FOA Number DE-FOA-0002986 to view the Q&As
- DOE will attempt to respond to a question within 3 business days, unless a similar Q&A has already been posted to eXCHANGE

Problems logging into eXCHANGE or uploading and submitting application documents with eXCHANGE?

- Email InfrastructureExchangeSupport@hq.doe.gov
- Include the FOA title and number in the subject line (BIL RMUC ACT FOA: DE-FOA-0002986)

For Information About RMUC Program Announcements

- You can send a request to join the RMUC Program email list to: CESER.RMUC@hq.doe.gov

- Information about the RMUC Program is available at: https://www.energy.gov/ceser/rural-and-municipal-utility-advanced-cybersecurity-grant-and-technical-assistance-rmuc

Thank You for Attending!

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response