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: Modification 000002
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:	6/6/2024 5:00 p.m. ET
Expected Date for DOE Selection Notifications:	9/18/2024
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.

Modifications

All modifications to the FOA are HIGHLIGHTED in the body of the FOA.

Mod. No.	Date	Description of Modification
000001	2/1/2024	- Submission deadline for full applications changed to 5/16/2024 at 5pm ET. - Expected Date for DOE Selection Notifications changed to 9/18/2024. - Template language for Not-for-Profit Partner Documentation in Section IV.C.v updated.
000002	4/10/2024	- Submission deadline for full applications changed to 6/6/2024 at 5pm ET. - Added language to clarify a not-for-profit

Registration Requirements

There are several one-time actions that must be completed before submitting an application in response to this Funding Opportunity Announcement (FOA) (e.g., register with the System for Award Management (SAM), obtain a Unique Entity Identifier (UEI) number, register with Grants.gov, and register with the Clean Energy Infrastructure Funding Opportunity Exchange (INFRASTRUCTURE eXCHANGE). It is vital that applicants address these items as soon as possible. Some may take several weeks, and failure to complete them could interfere with an applicant's ability to apply to this FOA.

- **System for Award Management**
  Applicants must register in SAM at https://www.sam.gov/ prior to submitting an application in response to this FOA. Designating an Electronic Business Point of Contact and obtaining a special password called an MPIN are important steps in SAM registration. The applicant must maintain an active SAM registration with current information at all times during which it has an active Federal award or application under consideration. More information about SAM registration for applicants is found at: https://www.fsd.gov/gsafsd_sp?id=gsafsd_kb_articles&sys_id=650d493e1bab7c105465eaccac4bcbcb.

  NOTE: If clicking the SAM links do not work, please copy and paste the link into your browser.

  Due to the high demand of SAM registrations and UEI requests, entity legal business name and address validations are taking longer than expected to process. Entities should start the SAM and UEI registration process as soon as possible. If entities have technical difficulties with the SAM registration or UEI validation process they should utilize the HELP feature on SAM.gov. SAM.gov will work entity service tickets in the order in which they are received and asks that entities not create multiple service tickets for the same request or technical issue. Additional entity validation resources can be found here: GSAFSD Tier 0 Knowledge Base - Validating your Entity.

- **UEI**
  Applicants must obtain an UEI from the SAM to uniquely identify the entity. The UEI is available in the SAM entity registration record. Due to extended wait-times, if an applicant is unable to secure a UEI by the deadline for submittal of a concept paper, the applicant may provisionally mark the UEI "N/A."

  NOTE: Subawardees/subrecipients at all tiers must also obtain an UEI from the SAM and provide the UEI to the Prime Recipient before the subaward can be issued. Full registration in SAM is not required to obtain an UEI for subaward reporting.

- **INFRASTRUCTURE FUNDING OPPORTUNITY EXCHANGE (INFRASTRUCTURE eXCHANGE)**
  Register and create an account on INFRASTRUCTURE eXCHANGE at https://infrastructure-exchange.energy.gov . This account will allow the user to apply to any open FOAs that are currently in INFRASTRUCTURE eXCHANGE.

  It is recommended that each organization or business unit, whether acting as a team or a single entity, use only one account as the contact point for each submission. Applicants should also designate backup points of contact so they may be easily contacted if deemed necessary. **This step is required to apply to this FOA.** The INFRASTRUCTURE eXCHANGE registration does not have a delay; however, **the remaining registration requirements below could take several weeks to process and are necessary for a potential applicant to receive an award under this FOA.** Questions related to the registration process and use of the INFRASTRUCTURE eXCHANGE website should be submitted to: InfrastructureExchangeSupport@hq.doe.gov

- **Grants.gov**
  Applicants must register with Grants.gov (http://www.grants.gov) to receive automatic updates when Amendments to this FOA are posted. **Please note that Pre-Applications and Full Applications will not be accepted through Grants.gov.** Modifications to this FOA will be posted on both the Infrastructure eXCHANGE website and the Grants.gov system, however, you will only receive an email notification when a modification is posted if you register for email notifications for this FOA in Grants.gov. The RMUC Program recommends that you register as soon after the release of this FOA as possible to ensure you receive timely notice of any amendments or other funding announcements.

- **FedConnect.net**
  Register in FedConnect (https://www.fedconnect.net). To create an organization account, your organization's SAM MPIN is required. For more information about the SAM MPIN or other registration requirements, review the FedConnect Ready, Set, Go! Guide at https://www.fedconnect.net/FedConnect/Marketing/Documents/FedConnect_Ready_Set_Go.pdf.

- **Electronic Authorization of Applications and Award Documents**
  Submission of an application and supplemental information under this FOA through electronic systems used by the DOE, including INFRASTRUCTURE eXCHANGE and FedConnect, constitutes the authorized representative's approval and electronic signature.

Table of Contents

I. Funding Opportunity Description 8

A. Background 8
B. Program Purpose and Summary 10
C. Summary Description of Topic Areas 11
i. Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities 11
ii. Topic Area 2: Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem 11
iii. Topic Area 3: Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources 12
D. Project Scope 13
E. Applications Specifically Not of Interest 14
F. Community Benefits Plan: Job Quality and Equity 15
G. Cybersecurity Plan: BIL Section 40126 15
H. Informational Webinar 16

II. Award Information 17

A. Estimated Funding and Period of Performance 17

III. Eligibility Information 18

A. Eligible Applicants 18
i. Restricted Eligibility 18
ii. Territories and Tribal Entities 19
iii. Domestic Entities 19
B. Cost Sharing 20
C. Limitation on Number of Pre-Applications and Full Applications for Review 21
i. Utilities: 21
ii. Not-for-Profit Entities: 21
D. Pre-Application and Full Application Compliance Criteria 22
E. Questions Regarding Eligibility 22
F. Responsiveness Criteria 22
G. Deadlines Enforced through Infrastructure eXCHANGE 22

IV. Pre-Application and Full Application Submission Information 24

A. Application Process 24
i. Forms 24
ii. Format Requirements 24
B. Content and Form of the Pre-Application 25
C. Content and Form of the Full Application 26
i. Project Plan 27
ii. Resumes 29
iii. Letters of Commitment: Cost Share and/or Participating Utilities 30
iv. Organizational Commitment to Long-Term Success – All Topic Areas 30
v. Not-for-Profit Partner Documentation (if applicable) 31
vi. Statement of Project Objectives (SOPO) 32
vii. SF-424: Application for Federal Assistance 32
viii. Budget Justification Workbook 32
ix. Subrecipient Budget Justification 33

x. Potentially Duplicate Funding Notice 33
xi. Community Benefits Plan: Job Quality and Equity 33
xii. Community Benefits Plan Budget Justification 37
xiii. Summary for Public Release 37
xiv. Summary Slide 37
xv. Transparency of Foreign Connections 38
xvi. Budget for DOE/NNSA FFRDC (if applicable) 39
xvii. Authorization for Non-DOE/NNSA or DOE/NNSA FFRDCs (if applicable) 39
xviii. SF-LLL: Disclosure of Lobbying Activities (required) 39
D. Submission Dates and Times 40
E. Post Selection Information Requests 40

V. Registration Requirements 41

A. System for Award Management 41
B. FedConnect 41
C. Grants.gov 41
D. Electronic Authorization of Applications and Award Documents 41
E. Infrastructure eXCHANGE Portal 41

VI. Topic Area 1: Advanced Cybersecurity Technologies (ACT) for Distribution, Generation, and Transmission Utilities 43

A. Objectives 43
B. Topic Area 1 Pre-Application Content Requirements 44
C. Topic Area 1 Pre-Application Review Criteria 47
i. Criterion 1: Project Overview (Maximum Points: 24) 47
ii. Criterion 2: Community Benefits (Maximum Points: 24) 47
iii. Criterion 3: Technical Approach (Maximum Points: 30) 48
iv. Criterion 4: Project Design and Management (Maximum Points: 18) 48
D. Topic Area 1 Full Application Project Plan Content Requirements 49
i. Project Design and Management 49
ii. Assessment and Analysis Approach 50
iii. Implementation and Operations Plan 50
iv. Commitment, Team, and Resources 50
E. Topic Area 1 Full Application Review Criteria 51
i. Criterion 1: Project Design and Management (Maximum Points: 33) 51
ii. Criterion 2: Assessment and Analysis Approach (Maximum Points: 18) 52
iii. Criterion 3: Implementation and Operations Plan (Maximum Points: 24) 52
iv. Criterion 4: Commitment, Team, and Resources (Maximum Points: 24) 53
v. Criterion 5: Community Benefits Plan (Maximum Points: 36) 54

VII. Topic Area 2: Strengthening the Peer-to-Peer and Not-for-Profit Technical Assistance Ecosystem 56

A. Objectives 56
B. Topic Area 2 Pre-Application Content Requirements 59
C. Topic Area 2 Pre-Application Review Criteria 62
i. Criterion 1: Applicant Profile (Maximum Points: 9) 62
ii. Criterion 2: Project Overview (Maximum Points: 33) 62
iii. Criterion 3: Community Benefits (Maximum Points: 24) 63
iv. Criterion 4: Technical Approach (Maximum Points: 21) 63
v. Criterion 5: Project Design and Management (Maximum Points: 21) 64
D. Topic Area 2 Full Application Project Plan Content Requirements 64
i. Project Design and Management 64

ii. Assessment and Analysis Approach 65
iii. Implementation and Operations Plan 66
iv. Commitment, Team, and Resources 67
E. Topic Area 2 Full Application Review Criteria 68
i. Criterion 1: Project Design and Management (Maximum Points: 39)....68
ii. Criterion 2: Assessment and Analysis Approach (Maximum Points: 24) 69
iii. Criterion 3: Implementation and Operations Plan (Maximum Points: 30)....69
iv. Criterion 4: Commitment, Team, and Resources (Maximum Points: 33)....70
v. Criterion 5: Community Benefits Plan (Maximum Points: 36)....71

VIII. Topic Area 3: Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources 73

A. Objectives....73
B. Topic Area 3 Pre-Application Content Requirements 75
C. Topic Area 3 Pre-Application Review Criteria 77
i. Criterion 1: Applicant Profile (Maximum Points: 18)....77
ii. Criterion 2: Project Overview (Maximum Points: 27)....78
iii. Criterion 3: Community Benefits (Maximum Points: 24) 78
iv. Criterion 4: Technical Approach (Maximum Points: 15)....79
v. Criterion 5: Project Design and Management (Maximum Points: 21)....79
D. Topic Area 3: Full Application Project Plan Content Requirements 80
i. Project Design and Management 80
ii. Assessment and Analysis Approach 81
iii. Implementation and Operations Plan 82
iv. Commitment, Team, and Resources 82
E. Topic Area 3 Full Application Review Criteria 83
i. Criterion 1: Project Design and Management (Maximum Points: 48)....83
ii. Criterion 2: Assessment and Analysis Approach (Maximum Points: 27) 84
iii. Criterion 3: Implementation and Operations Plan (Maximum Points: 24)....85
iv. Criterion 4: Commitment, Team, and Resources (Maximum Points: 27)....86
v. Criterion 5: Community Benefits Plan (Maximum Points: 36)....87

IX. Evaluation and Selection Process.... 89

A. Overview 89
i. Standards for Application Evaluation 89
ii. Selection 89
iii. Program Policy Factors 89
iv. Recipient Responsibility and Qualifications....90
B. Anticipated Notice of Selection and Award Negotiation Dates 91

I. Funding Opportunity Description

A. Background

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is issuing this Funding Opportunity Announcement (FOA). Awards made under this FOA will be funded, in whole or in part, with funds appropriated by the Infrastructure Investment and Jobs Act (IIJA),[1] more commonly known as the Bipartisan Infrastructure Law (BIL).

The BIL is a once-in-a-generation investment in American infrastructure. The BIL appropriates more than $62 billion to the U.S. Department of Energy (DOE)[2] to invest in American manufacturing and workers; expand access to energy efficiency and clean energy; deliver secure, reliable, clean, and affordable power to more Americans; and demonstrate and deploy the technologies of tomorrow through clean energy demonstrations.

Section 40124 of the BIL directs DOE to invest $250 million to create a new program, the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program, to provide eligible entities (defined in Section III.A.) with financial and technical assistance support to improve their cybersecurity posture. This FOA provides $70 million in federal funding to support the RMUC Program's goals.

The activities to be funded under this FOA support BIL Section 40124 and the broader government-wide efforts to increase the security, reliability, and resiliency of our energy infrastructure. Investments to improve the cybersecurity resilience of electric utilities eligible to participate in the RMUC Program will improve energy resilience in rural communities, decrease energy burdens on utility members and customers, and increase the cybersecurity knowledge, skills, and abilities of utility employees in rural communities. These investments will help maximize the benefits of the clean energy transition by facilitating secure grid modernization deployments as the nation works to curb the climate crisis, empower workers, and advance environmental justice.

BIL Section 40124 is focused on:

1) Deploying advanced cybersecurity technologies for electric utility systems, where the term ''advanced cybersecurity technology'' means "any technology, operational capability, or service, including computer hardware, software, or a related asset, that

[1] Infrastructure Investment and Jobs Act, Public Law 117-58 (November 15, 2021). This FOA uses the more common name Bipartisan Infrastructure Law. https://www.congress.gov/bill/117th-congress/house-bill/3684.
[2] U.S. Department of Energy. November 2021. "DOE Fact Sheet: The Bipartisan Infrastructure Deal Will Deliver for American Workers, Families and Usher in the Clean Energy Future." https://www.energy.gov/articles/doe-fact-sheet-bipartisan-infrastructure-deal-will-deliver-american-workers-families-and-0

enhances the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat"[3]; and
2) Increasing the participation of eligible entities in cybersecurity threat information sharing programs.

Section 40124 specifies that the RMUC Program shall give priority for grants and technical assistance to an eligible entity that, as determined by DOE:

(A) has limited cybersecurity resources;
(B) owns assets critical to the reliability of the bulk power system; or
(C) owns defense critical electric infrastructure.[4]

Within the three priority categories outlined in the BIL Section 40124, the majority of the RMUC Program's eligible entities fall into the limited cybersecurity resources category. DOE also expects that, in general, limited cybersecurity resource utilities also have limited experience and staffing resources to participate in competitive federal funding opportunities. To make this FOA more accessible, the information is divided into two documents:

1) RMUC ACT FOA: The FOA contains information that will help potential applicants decide whether or not to apply, requirements for the application process, and specific requirements for the three Topic Areas (Sections VI, VII, and VII); and
2) ACT FOA Administrative Requirements: This is a separate document that contains additional details on requirements associated with applying for and accepting a federal financial assistance award.

Applicants are required to read and comply with the language in both this *RMUC ACT FOA* document and the *ACT FOA Administrative Requirements* document.

DOE's BIL investments will support efforts to enhance U.S. competitiveness, drive the creation of good-paying union jobs, tackle the climate crisis, and ensure strong access to economic, environmental, and other benefits for disadvantaged communities.[5] These investments will build a clean and equitable energy economy that achieves a zero-carbon

[3] Section 40124 of the Bipartisan Infrastructure Law. https://www.congress.gov/bill/117th-congress/house-bill/3684.

[4]The term "defense critical electric infrastructure" means any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary pursuant to subsection (c), but is not owned or operated by the owner or operator of such facility. 16 USC 824o-1: Critical electric infrastructure security (house.gov)

[5] Pursuant to E.O. 14008, "Tackling the Climate Crisis at Home and Abroad," January 27, 2021, and the Office of Management and Budget's Interim Justice40 Implementation Guidance M-21-28 and M23-09 (https://www.whitehouse.gov/wp-content/uploads/2023/01/M-23-09_Signed_CEQ_CPO.pdf), DOE recognizes disadvantaged communities as defined and identified by the White House Council on Environmental Quality's Climate and Economic Justice Screening Tool (CEJST), located at https://screeningtool.geoplatform.gov/. DOE's Justice40 Implementation Guidance is located at https://www.energy.gov/sites/default/files/2022-07/Final%20DOE%20Justice40%20General%20Guidance%20072522.pdf.

electricity system by 2035, and put the United States on a path to achieve net-zero emissions economy-wide by no later than 2050[6] to benefit all Americans.

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 officials in the development of Federal policies that have Tribal implications. Memorandum on Tribal Consultation and Strengthening Nation-to-Nation Relationships | The White House.
[11] EO 14008, "Tackling the Climate Crisis at Home and Abroad," January 27, 2021.

All Projects Specifically Not of Interest, as described in Section I.E. of this FOA, are deemed nonresponsive and will not be reviewed or considered.

C. Summary Description of Topic Areas

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

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" (See Section III.A. Eligible Applicants). Funding under this Topic Area is available to utilities eligible to participate in the RMUC Program. Not-for-profit entities who are not utilities as defined by BIL Section 40124 are not eligible to apply for this Topic Area. This Topic Area is intended for individual utilities that will apply as the prime recipient. Utilities interested in applying as a group must apply under Topic Area 2 or 3 and will not be eligible under Topic Area 1.

Applications must address the following objectives: 1) improve the cybersecurity posture of the utility's operational systems; 2) include an appropriate balance of investments in staff, processes, and technologies; 3) improve the 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.

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

This Topic Area will support investments that strengthen the community of eligible entities that are currently providing information technology (IT) and cybersecurity support to eligible electric cooperative and municipal utilities and meet the legislative intent to enhance "the security posture of electric utilities". Funding can be requested for activities that will improve the cybersecurity posture of utilities by increasing the scope of appropriate, affordable, and accessible products and services provided, including but not limited to purchases of IT and cybersecurity tools and services, technical assistance, and training. Funding can also be requested to enhance the ability of entities to provide products and services and increasing the number of eligible utilities benefiting from the products and services provided. This Topic Area will also provide funding to promote and facilitate the replication of effective service models to other utilities and not-for-profit partners interested in providing products and services to eligible cooperative and municipal utilities.

Funding under this topic area is available 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 technical assistance and services to cooperative or municipal electric utilities for at least one year prior to the FOA Full Application deadline.

All utilities that could receive technical assistance or funding that is funded through the primary applicant's proposed work under Topic Area 2 must be listed in the application as Participating Utilities in the project (see Section IV.C.iii). Participating Utilities cannot be added to an application after the Full Application deadline. All utilities that are subrecipients must also be Participating Utilities, but all Participating Utilities do not need to be subrecipients.

Applications must address the following objectives: 1) improve the Operational Technology and Industrial Control Systems (OT/ICS) cybersecurity posture of the Participating Utilities receiving products and services; 2) include an appropriate balance of investments in staff, processes, and technologies; 3) result in an increase in the participation of eligible utilities in cybersecurity threat information sharing programs; 4) have a high likelihood of continuing to provide cybersecurity products and services after the project funding ends; and 5) create a replicable, scalable model for delivering cybersecurity services.

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

This Topic Area will support investments that can strengthen the community of eligible entities that are currently providing IT and cybersecurity support to eligible cooperative and municipal utilities. Applications under Topic Area 3 must focus on improving the knowledge, skills, and abilities of utility participants and cannot include the purchase of cybersecurity tools, technologies, or related assets.

The intent of this Topic Area is to improve the cybersecurity posture of utilities with limited cybersecurity resources by:

- Increasing the scope of appropriate, affordable, and accessible technical assistance and training services provided by eligible entities;
- Enhancing the ability of eligible entities to provide services; and
- Increasing the number of utilities benefiting from the services.

This Topic Area is also focused on supporting efforts to promote and facilitate the replication of effective service models in other eligible entities interested in providing services to electric cooperative and municipal utilities.

This Topic Area 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 technical assistance and services to cooperative or municipal electric utilities for at least one year prior to the FOA application deadline.

All utilities that could receive technical assistance that is funded through the primary applicant's proposed work under Topic Area 3 must be listed in the application as Participating Utilities in the project (see Section IV.C.iii). Participating Utilities cannot be added to an application after the Full Application deadline. This Topic Area is limited to providing only technical assistance and training. No technology or tool deployment activities will be funded. There are no cost share requirements for this Topic Area.

Applications under this Topic Area must address the following objectives: 1) include a high percentage of Participating Utilities with limited cybersecurity resources; 2) result in an increase in the participation of eligible utilities in cybersecurity threat information sharing programs; 3) have a high likelihood of continuing to provide services after the project funding ends; and 4) create a replicable, scalable model for delivering cybersecurity services.

D. Project Scope

Projects that include the purchase of tools, technologies, or training must be based on the results of cybersecurity risk assessments. Applicants must clearly justify how the proposed projects will reduce identified cybersecurity risks. Applicants that have not completed assessments at the time of application may request funding to complete cybersecurity risk assessments as part of their applications.

Proposed solutions must address prioritized cybersecurity risks using an approach that includes investments in people and process solutions as well as the technology component of the solution. All projects must describe and demonstrate an ability of the utility to appropriately maintain and manage solutions after the project funding ends. Applications must show that tool and technology solutions are commercially available.[12]

Projects that improve the cybersecurity of the utility's (or utilities') operational technology (OT) or industrial control systems (ICS), and/or increase the participation of eligible utilities in cybersecurity threat information sharing programs are strongly encouraged.

Applicants should assemble a project team with diverse expertise and experience and applications must demonstrate the team has the experience and capacity to execute the proposed project and manage a federal grant.

[12] For the purposes of this FOA, commercially available solutions are defined as solutions that have been offered for sale, lease, or license to the public. Documentation that a technology is commercially available could include showing the solution can be warrantied or that it can be purchased from a commercial vendor for the intended purpose.

Applicants will be asked to refer to the DOE's Cybersecurity Capability Maturity Model Version 2.1 (C2M2)[13] domains listed below and to describe how the proposed solutions will advance progress in these domains. Projects that are comprehensive and address more than one C2M2 domain are preferred.

1. Asset, Change, and Configuration Management (ASSET)
2. Threat and Vulnerability Management (THREAT)
3. Risk Management (RISK)
4. Identity and Access Management (ACCESS)
5. Situational Awareness (SITUATION)
6. Event and Incident Response, Continuity of Operations (RESPONSE)
7. Third-Party Risk Management (THIRD-PARTIES)
8. Workforce Management (WORKFORCE)
9. Cybersecurity Architecture (ARCHITECTURE)
10. Cybersecurity Program Management (PROGRAM)

Applicants are not required to complete a C2M2 assessment as part of their proposed projects.

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.

[13] The DOE C2M2 is available on the DOE website at this location: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

- Topic Area 1 Applications from "a not-for-profit entity" as defined under BIL Section 40124 (a)(3)(d).

F. Community Benefits Plan: Job Quality and Equity

To support the goal of building a clean and equitable energy economy, BIL-funded projects are expected to (1) support meaningful community and labor engagement; (2) invest in America's workforce; (3) advance diversity, equity, inclusion, and accessibility (DEIA); and (4) contribute to the President's goal that 40% of the overall benefits of certain federal investments flow to disadvantaged communities (the Justice40 Initiative).[14] To ensure these goals are met, applications must include a Community Benefits Plan that describes how the proposed project would incorporate the four objectives stated above. Section IV.C.xi. provides more details on the Community Benefits Plan goals and requirements.

G. Cybersecurity Plan: BIL Section 40126

In accordance with BIL Section 40126, applicants selected for award negotiations must submit a cybersecurity plan to DOE prior to receiving funding.[15] These plans are intended to foster a cybersecurity-by-design approach for BIL efforts. The Department will use these plans to ensure effective integration and coordination across its research, development, and demonstration programs. **A cybersecurity plan is not required as part of the application submission for this FOA, but all applications selected under this FOA will be required to submit a cybersecurity plan during the award negotiation phase.**

DOE recommends using open guidance and standards, such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) and the DOE Cybersecurity Capability Maturity Model (C2M2).[16] The cybersecurity plan created pursuant to BIL Section 40126 should document any deviation from open standards, as well as the utilization of proprietary standards where the awardee determines that such deviation is necessary.

[14] The Justice40 initiative, established by E.O. 14008, sets a goal that 40% of the overall benefits of certain federal investments flow to disadvantaged communities. The Justice40 Interim Guidance provides a broad definition of disadvantaged communities (page 2): https://www.whitehouse.gov/wp-content/uploads/2021/07/M-21-28.pdf.

[15] 42 U.S.C. § 18725

[16] NERC critical infrastructure protection (CIP) standards for entities responsible for the availability and reliability of the bulk electric system. NIST IR 7628: 2 Smart grid cyber security strategy and requirements. NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations: Catalog of security controls in 18 categories, along with profiles for low-, moderate-, and high-impact systems. NIST SP800-82, Guide to Industrial Control Systems (ICS) Security. NIST SP800-39, Integrated Enterprise-Wide Risk Management: Organization, mission, and information system view. AMI System Security Requirements: Security requirements for advanced metering infrastructure. ISO (International Organization for Standardization) 27001, Information Security Management Systems: Guidance on establishing governance and control over security activities (this document must be purchased). IEEE (Institute of Electrical and Electronics Engineers) 1686-2007, Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (this document must be purchased). DOE Cybersecurity Capability Maturity Model (C2M2).

- Cybersecurity plans should be commensurate to the threats and vulnerabilities associated with the proposed efforts and demonstrate the cybersecurity maturity of the project.
- Cybersecurity plans may cover a range of topics relevant to the proposed project—e.g., software development lifecycle, third-party risks, and incident reporting.
- At a minimum, cybersecurity plans should address questions noted in BIL Section 40126 (b), Contents of Cybersecurity Plan.[17]

Supplementary guidance on the cybersecurity plan requirement is available at https://www.energy.gov/ceser/bipartisan-infrastructure-law-implementation.

H. Informational Webinar

DOE will conduct at least one informational webinar during the FOA process. Webinars will be held after the initial FOA release is announced. Webinars will be held before the due date for Pre-Applications.

Attendance is not mandatory and will not positively or negatively impact the overall review of any applicant submissions. The webinars will be open to all applicants who wish to participate. Applicants should refrain from asking questions during the webinars or communicating information that would reveal confidential and/or proprietary information specific to their project. The anticipated webinar dates are listed on the cover page of the FOA.

[17] 42 U.S.C. § 18725

II. Award Information

A. Estimated Funding and Period of Performance

DOE expects to make a total of approximately $70 million of federal funding available for new cooperative agreements under this FOA, subject to the availability of appropriated funds. Project periods are expected to run 24-48 months comprised of one or more budget periods. Project continuation will be contingent upon several elements, including satisfactory performance and DOE's Go/No-Go decision. See the *ACT FOA Administrative Requirements* available on Infrastructure eXCHANGE under the FOA's posting for additional award guidance.

DOE may issue awards in one, multiple, or none of the following topic areas:

Table 1: Awards for the ACT FOA

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

*Applicants may propose cost share in excess of 5% which could result in higher total award values.
**The DOE share listed under the award size is the maximum DOE funding that can be proposed for each Topic Area. Applications that propose a DOE share in excess of this limit will not be evaluated.
*** Example calculation provided in Section III.B.

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[19] 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.

[18] If an eligible entity under IIJA Section 40124(1)(3)(E) is owned by a holding company, the eligible entity, and not the holding company, must submit the FOA application as the prime applicant. If the cybersecurity resources of the eligible entity are part of a shared services agreement with a holding company, the holding company may participate in the program; however, the application must be submitted by the eligible entity and funds awarded to the eligible entity may only be for the benefit of the eligible entity and may not be used for the benefit of non-eligible subsidiaries of the holding company.

[19] For the purposes of Section 40124, 'not-for-profit entity' includes nonprofit organizations and institutions of higher education under 2 CFR Part 200, provided that the entity is legally obligated to operate on a not-for-profit basis.

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.

B. Cost Sharing

Applicants are bound by the cost share proposed in their Full Applications if selected for award negotiations. Cost share requirements under this FOA are as follows:

Topic Areas 1 and 2: Cost share must be at least 5% of the total project costs. Total project costs are the sum of the government share, including FFRDC costs if applicable, and the recipient share of the project costs. The cost share must come from non-Federal sources unless otherwise allowed by law. (See 2 CFR 200.306 and 2 CFR 910.130 for the applicable cost sharing requirements.)

The following formula can be used to calculate cost share.

$$\frac{\$\ Federal\ Share}{100\ -Cost\ Share\ (\%)} * Cost\ Share\ (\%) = \$\ Recipient\ Cost\ Share$$

For example, if the federal share is $1,500,000 and the required cost share is 5%, the cost share dollar amount can be calculated as follows:

$$\frac{\$1{,}500{,}000}{100\ -5} * 5 = \$78{,}947.37$$

Total project costs are the sum of the recipient cost share and federal share.

$$\$1{,}500{,}000 + \$78{,}947.37 = \$1{,}578{,}947.37$$

Topic Area 3: Cost sharing is not required for this Topic Area.

Please see Appendix A of the *ACT FOA Administrative Requirements* document for additional information.

C. Limitation on Number of Pre-Applications and Full Applications for Review

i. Utilities[20]:

- may submit more than one Pre-Application to any of the three Topic Areas provided that each Pre-Application describes a unique, distinct project;
- may submit only one Full Application to each Topic Area provided that each Application describes a unique, distinct project; and
- may participate as subrecipients or as Participating Utilities in Topic Areas 2 or 3 on more than one application, provided that each application describes a unique, distinct project.

If a utility has more than one successful Pre-Application within a single Topic Area as the prime applicant, the utility may submit only one Full Application for that Topic Area. If more than one Full Application is received from the same utility within a Topic Area none of the Full Applications from that utility will be considered for that Topic Area. Only Full Applications associated with successful Pre-Applications will be considered.

ii. Not-for-Profit Entities[21]:

- may submit more than one Pre-Application to Topic Areas 2 and 3 of this FOA provided that each Pre-Application describes a unique, distinct project; and
- may only submit one Full Application per Topic Area.

If a not-for-profit entity has more than one successful Pre-Application within a single Topic Area, they may only submit one Full Application to that Topic Area. If more than one Full Application is received from the same not-for-profit entity within a Topic Area none of the Full Applications from that not-for-profit entity will be considered for that Topic Area. Only Full Applications associated with successful Pre-Applications will be considered.

[20] Utilities refers to utilities that are eligible entities as outlined in BIL Section 40124(a)(3)(A)-(C), (E) where funds under this award will enhance, "the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat." This includes: rural electric cooperatives; utilities owned by a political subdivision of a state; utilities owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a state; and investor-owned electric utilities that sell less than 4,000,000 megawatt hours of electricity per year.

[21] Not-for-Profit Entities refers to not-for-profits that are eligible entities as outlined in BIL Section 40124(a)(3)(D), "a not-for-profit entity that is in a partnership with not fewer than 6 entities described in subparagraph (A), (B), or (C)." Not-for-profit entities must present signed evidence of these partnerships in their Full Applications. Evidence of a partnership relationship can be demonstrated by following the instructions contained in Section IV.C.v Not-for-profit Partnership Documentation.

D. Pre-Application and Full Application Compliance Criteria

To be considered compliant, applicant submissions must:

- Comply with the applicable content and form requirements listed in Section IV. of the FOA;
- Include all required documents;
- Be successfully uploaded and submitted to Infrastructure eXCHANGE https://infrastructure-exchange.energy.gov/; and
- Be submitted by the deadline stated in the FOA.

DOE will not review or consider submissions submitted through means other than Infrastructure eXCHANGE, submissions submitted after the applicable deadline, or incomplete submissions.

E. Questions Regarding Eligibility

DOE will not make eligibility determinations for potential applicants prior to the date on which Pre-Applications to this FOA must be submitted. The decision whether to submit an application in response to this FOA lies solely with the applicant.

F. Responsiveness Criteria

All Applications Specifically Not of Interest, as described in Section I.E. of the FOA, are deemed nonresponsive and are not reviewed or considered.

G. Deadlines Enforced through Infrastructure eXCHANGE

Infrastructure eXCHANGE is designed to enforce the deadlines specified in this FOA. The "Apply" and "Submit" buttons will automatically disable at the defined submission deadlines.

Applicants who experience technical difficulties with submission PRIOR to the FOA deadline should contact the Infrastructure eXCHANGE helpdesk for assistance (InfrastructureExchangeSupport@hq.doe.gov).

Applicants are strongly encouraged to submit their Pre-Applications and Full Applications, and at least 48 hours in advance of the submission deadlines. DOE will not extend the submission deadline for applicants that fail to submit required information by the applicable deadline due to server/connection congestion.

Under normal conditions (i.e., at least 48 hours before the submission deadline) applicants should allow at least one hour to upload and submit all of the documents associated with their Pre-Application or Full Application. Applicants must ensure they have submitted their documents into the system after they are uploaded. Once the documents are uploaded and

submitted in Infrastructure eXCHANGE, applicants may replace documents with revised or updated versions until the expiration of the applicable deadline. *If revised documents are uploaded, the application package will not be updated until the applicant hits the submit button.*

IV. Pre-Application and Full Application Submission Information

A. Application Process

The application process includes two phases. First applicants will submit a Pre-Application consisting of short-answer questions to solicit targeted information on the proposed project and how it will address the requirements of the topic area. DOE will review Pre-Applications, and based on the results of the review, DOE will invite selected applicants to submit a Full Application. **Only applicants who are invited to apply based on their Pre-Applications are eligible to submit a Full Application.** If an applicant is invited to submit a Full Application, the responses in the Full Application must expand upon and substantiate the applicant's Pre-Application with supplementary information.

Applicants who are not invited to submit Full Applications will not be eligible for funding under this FOA.

i. Forms

Both the Pre-Application and Full Application forms and instructions are available on Infrastructure eXCHANGE. To access these materials, go to https://infrastructure-exchange.energy.gov/Default.aspx and select the funding opportunity number associated with this FOA: DE-FOA-0002986.

ii. Format Requirements

Pre-Application and Full Application submissions must conform to the form and content requirements described below, including maximum page lengths. Submissions must meet the following requirements:

- Each Pre-Application and Full Application must be submitted in PDF format unless stated otherwise;
- Each must be written in English;
- All pages must be formatted to fit on 8.5 x 11-inch paper with margins not less than one inch on every side. Use Calibri typeface, a black font color, and a font size of 12 point or larger (except in figures or tables, which may be 10 point font). References must be included as footnotes or endnotes in a font size of 10 or larger. Footnotes and endnotes are counted toward the maximum page requirement;
- A **control number** will be issued when an applicant begins the Infrastructure eXCHANGE application process. The control number must be included with all application documents. Specifically, the control number must be prominently

displayed on the upper right corner of the header of every page and included in the file name (i.e., *Control Number_Applicant Name_Application*);
- Page numbers must be included in the footer of every page; and
- Each submission must not exceed the specified maximum page limit, including cover page, charts, graphs, maps, and photographs when printed using the formatting requirements set forth above and single spaced. If applicants exceed the maximum page lengths indicated below, DOE will review only the authorized number of pages and disregard any additional pages.

Note: The maximum file size that can be uploaded to the Infrastructure eXCHANGE website is 50MB. Files larger than 50MB cannot be uploaded and hence cannot be submitted for review. If a file is larger than 50MB but is still within the maximum page limit specified in the FOA, it must be broken into parts, file names must indicate the part number, and each part must be uploaded separately. For example:
ProjectPlan_Part_1
ProjectPlan_Part_2

DOE will not accept late submissions that resulted from technical difficulties due to uploading files that exceed 50MB.

B. Content and Form of the Pre-Application

Each Pre-Application must describe a single project, not exceed 12 pages, and address all the Topic Area specific requirements listed. Each Topic Area has unique Pre-Application requirements that are explained in the Sections VI.B, VII.B, and VIII.B. Each Pre-Application must be submitted separately on Infrastructure eXCHANGE.

Templates are provided to assist applicants in preparing their Pre-Applications and may be found on Infrastructure eXCHANGE. Use of the template is not mandatory but is highly encouraged. Each Topic Area template includes all of questions for that Topic Area, and recommended page limits for each Section of the Pre-Application. Applicants are not required to follow recommended pages for each Section, but the total page count of the Pre-Application must not exceed 12 pages.

DOE will review only the information provided to support the Topic Area Pre-Application questions. Additional information will not be considered. Note that responses provided in the Pre-Application must be verified and/or substantiated in the Full Application.

DOE will review each Pre-Application based on the criteria specific to that Topic Area. **Based on the results of the review, DOE will invite a subset of applicants to submit a Full Application. DOE will only accept Full Applications from those applicants who have been invited to submit a Full Application.**

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.

All Full Application documents must be marked with the control number that will be issued to the applicant when the applicant begins the Infrastructure eXCHANGE application process. Full Applications must conform to the requirements listed in Table 3 and must not exceed the stated page limits. Reviewers of the Full Application should be able to clearly understand how the Full Application Project Plan relates to and expands upon information provided in the applicant's Pre-Application.

Table 3. Required Documents for Full Application

Document Number	Component	File Format	Page Limit	File Name
i.	Project Plan	PDF	25 page limit	ControlNumber_LeadOrganization_ProjectPlan
ii.	Resumes	PDF	2 pages each	ControlNumber_LeadOrganization_Resumes
iii.	Letters of Commitment	PDF	1 page each	ControlNumber_LeadOrganization_LOCs
iv.	Organizational Commitment to Long-Term Success	PDF	n/a	ControlNumber_LeadOrganization_OrgCom
v.	Not-for-profit Partner Documentation	PDF	n/a	ControlNumber_LeadOrganization_PartnershipDocumentation
vi.	Statement of Project Objectives	MS Word	5 page limit	ControlNumber_LeadOrganization_SOPO
vii.	SF-424: Application for Federal Assistance	PDF	n/a	ControlNumber_LeadOrganization_App424
viii.	Budget Justification Workbook	MS Excel	n/a	ControlNumber_LeadOrganization_Budget_Justification
ix.	Subrecipient Budget Justification (if applicable)	MS Excel	n/a	ControlNumber_LeadOrganization_Subrecipient_Budget_Justification
x.	Potentially Duplicative Funding Notice	PDF	n/a	ControlNumber_LeadOrganization_PDFN
xi.	Community Benefits Plan: Job Quality and Equity	PDF	12 page limit	ControlNumber_LeadOrganization_CBP

xii.	Community Benefits Plan Budget Justification	MS Excel	n/a	ControlNumber_CBP_Budget_Justification
xiii.	Summary for Public Release	PDF	1 page limit	ControlNumber_LeadOrganization_Summary
xiv.	Summary Slide	MS PowerPoint	1	ControlNumber_LeadOrganization_Slide
xv.	Transparency of Foreign Connections	PDF	n/a	BusinessSensitive_ControlNumber_LeadOrganization_TFC
xvi.	Budget for DOE/NNSA FFRDC, if applicable (see DOE O 412.1A, Attachment 2)	PDF	n/a	ControlNumber_LeadOrganization_WP
xvii.	Authorization for Non-DOE/NNSA or DOE/NNSA FFRDCs (if applicable) from cognizant Contracting Officer	PDF	n/a	ControlNumber_LeadOrganization_FFRDCAuth
xviii.	SF-LLL Disclosure of Lobbying Activities	PDF	n/a	ControlNumber_LeadOrganization_SF-LLL

Warning: The maximum file size that can be uploaded to the Infrastructure eXCHANGE website is 50MB. See Section V.E for instructions on how to upload application materials that exceed 50MB.

The following sections provide guidance on the content and form of each component of the Full Application that is listed in Table 3. Specific guidance on the information that should be included in the Project Plan for a specific Topic Area is provided under each Topic Area (Sections VI-VIII). All Full Applications must conform to the content and form guidance in this section and the Topic Specific guidance under the appropriate Topic Area.

i. Project Plan

The Project Plan for the Full Application may not be more than 25 pages, including the cover page, table of contents, and all citations, charts, graphs, maps, photos, or other graphics. The Project Plan must include all of the sections and information listed in Table 4 below.

Save the Project Plan in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_ProjectPlan".

Specific content requirements for the four sections of the Project Plan (Project Design and Management; Assessment and Analysis Approach; Implementation and Operation Plan; and Commitment, Team, and Resources) are provided for each Topic Area in Sections VI-VIII.

Table 4. Project Plan Required Information

Full Application Project Plan		
SECTION	**DESCRIPTION**	**PAGE LIMIT**
Cover Page	The cover page should include the project title, the FOA Topic Area, the project location(s), and any statements regarding confidentiality. Provide the names and contact information for both the technical and business points of contact for the primary applicant and the names of all organizations that are part of the project team. For each organization provide the names of project managers and of the senior/key personnel.	1 page maximum, included in the 25-page limit
Table of Contents	The Table of Contents must include, at a minimum, all of the required sections identified in this table.	1 page maximum, included in the 25-page limit
1. Project Design and Management	This section describes how the project will be performed, timelines, tasks, milestones, budgets, and anticipated outcomes. Buy America Requirements for Infrastructure Projects: Within the first two pages of the Project Plan, include a short statement on whether the project will involve the construction, alteration, and/or repair of infrastructure in the United States. See ACT FOA Administrative Requirements Section III.B.vii and Appendix D for applicable definitions and other information to inform this statement.	
2. Assessment and Analysis Approach	This section describes the evaluation process used to identify utility needs and how cybersecurity risks and challenges might be addressed through technical assistance, services, and implemented solutions.	
3. Implementation and Operation Plan	This section describes how technical assistance, services, or chosen technology solutions will be implemented or provided to improve a utility's cybersecurity posture and how solutions focused on people and processes will be holistically incorporated into the project's implementation.	

4. Commitment, Team, and Resources	The section defines how the applicant and any utility participants will effectively participate in the project; appropriate technical and non-technical staff expertise, roles, and responsibilities for each entity; allocated time commitments; and sustainability of the solutions.	
The information above is not all-inclusive. Applicants should refer to Sections VI-VIII for additional information and a detailed description of what must be included in the Project Plan for each Topic Area.		

ii. Resumes

Applicants must submit a resume (limited to two pages) for each project manager and senior/key personnel[22] that will be involved in the project. A resume provides information reviewers can use to evaluate the relevant skills and experience of the key project personnel, and to meet federal due diligence security requirements. The resumes should cover the last 10 years and include, but are not limited to, the following:

1. Contact information;
2. Education: All academic institutions attended, major/area, degree, and start and end dates of attendance;
3. Training: Relevant certifications or credentials, including any certifications or credentials from a Registered Apprenticeship or Labor Management Partnership;
4. Professional experience: Beginning with the current position, list professional/academic positions in chronological order with start and end dates of the engagement and a brief description; and
5. List all current academic, professional, or institutional appointments, foreign or domestic, at any academic, government, non-profit institution or elsewhere, whether or not remuneration is received, and include whether the appointment was full-time, part-time, or voluntary.

Please justify any lapses in employment as it is required that each resume covers the past 10 years or since age 18, whichever period is shorter.

Save all of the resumes in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_Resumes".

[22] Senior/key personnel – An individual who contributes in a substantive, meaningful way to the project proposed to be carried out with a DOE award.

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".

iv. Organizational Commitment to Long-Term Success – All Topic Areas

All applicants to this FOA will need to demonstrate that the applicant has the necessary support and commitment from the organization's leadership for the project to be successful. At a minimum, every Full Application must include a one-page letter of support, intent, and commitment signed by the applicant's authorizing official. This letter must:

1. State that the official supports your organization's Full Application;

2. Provide specific examples of what commitments the authorizing official will make in terms of staff time, funding, paid on-the-job training, and other resources to ensure the success of the proposed project over the duration of the project, and the continued success of the project after federal funding ends. For example, commitments to support budgets over a specified period of years that will cover the annual post-implementation costs for any on-going training and technology solution license fees or consulting services necessary after federal funding ends, and a commitment that this funding will be included in your organization's annual budget request; and
3. Include a statement that the official signing the letter is authorized to make these commitments.

Additional demonstrations of commitment are recommended for applicants in all Topic Areas and can include but are not limited to:

1. A utility Board or local government resolution describing the governing body's commitment to fully support the organization's staff time, funding resources, and continued investments to maintain the effectiveness of the solutions implemented;
2. A letter of intent from the City Manager, Mayor, or County Commissioner, if applicable, to support the organization's staff time, efforts, and support for future funding allocations to maintain the effectiveness of the solutions implemented;
3. Other documents demonstrating a long-term commitment.

Save your organizational commitment letter and any additional documents in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_OrgCom".

v. Not-for-Profit Partner Documentation (if applicable)

In addition to the Letters of Commitment, not-for-profit entities applying to this FOA under Topic Areas 2 or 3 must present evidence of a partnership with not fewer than six (6) rural electric cooperatives, utilities owned by a political subdivision of a State, such as a municipally owned electric utility, or utilities owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State. This requirement can be satisfied by submitting a single page letter from each of the six partner utilities, on the partner utility's letterhead, signed by an authorized representative of the utility and by the prime applicant organization that states the following:

> *[Partner Organization] is entering into a partnership with [prime applicant] to accomplish potential work associated with the Department of Energy's (DOE) Rural and Municipal Utility Cybersecurity (RMUC) Program.*

vi. Statement of Project Objectives (SOPO)

Applicants must complete a SOPO. A SOPO template is available on Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/. The SOPO, including the Milestone Table, must not exceed 5 pages when printed using standard 8.5" x 11" paper with 1" margins (top, bottom, left, and right) with Calibri font not smaller than 12-point (except in figures or tables, which may be 10-point font).

Save the SOPO in a single Microsoft Word file using the following convention for the title: "ControlNumber_LeadOrganization_SOPO".

vii. SF-424: Application for Federal Assistance

Applicants must complete the SF-424: Application for Federal Assistance, which is available on Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/. The dates and dollar amounts on the SF-424 are for the complete project period and not just the first project year, first phase, or other subset of the project period. The list of certifications and assurances referenced in Field 21 can be found at http://energy.gov/management/office-management/operational-management/financial-assistance/financial-assistance-forms, under Certifications and Assurances.

Save the SF-424 in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_424".

viii. Budget Justification Workbook

Applicants must complete the Budget Justification Workbook, available on Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/. Applicants must complete each tab of the Budget Justification Workbook for the project, including all work to be performed by the prime recipient and its subrecipients and contractors. Applicants should include costs associated with implementing the various BIL-specific requirements (e.g., Buy America requirements for infrastructure projects, Davis-Bacon, Community Benefits Plan, reporting, oversight) and with required annual audits and incurred cost proposals in their proposed budget documents. Such costs may be reimbursed as a direct or indirect cost. The "Instructions and Summary" included with the Budget Justification Workbook will auto-populate as the applicant enters information into the Workbook. Applicants must carefully read the "Instructions and Summary" tab provided within the Budget Justification Workbook.
Save the Budget Justification Workbook in a single Microsoft Excel file using the following convention for the title:
"ControlNumber_LeadOrganization_Budget_Justification".

ix. Subrecipient Budget Justification

Applicants must provide a separate budget justification for each subrecipient that is expected to perform work estimated to be more than $250,000 or 25% of the total work effort, whichever is less. The budget justification must include the same justification information described in the "Budget Justification" section above.

Save each subrecipient budget justification in a Microsoft Excel file using the following convention for the title: "ControlNumber_LeadOrganization_Subrecipient_Budget_Justification".

x. Potentially Duplicate Funding Notice

If the applicant or project team member has other active awards of federal funds, the applicant must determine whether the activities of those awards potentially overlap with the activities set forth in its application to this FOA. If there is a potential overlap, the applicant must notify DOE in writing of the potential overlap and state how it will ensure any project funds (i.e., recipient cost share and federal funds) will not be used for identical cost items under multiple awards. Likewise, for projects that receive funding under this FOA, if a recipient or project team member receives any other award of federal funds for activities that potentially overlap with the activities funded under the DOE award, the recipient must promptly notify DOE in writing of the potential overlap and state whether project funds from any of those other federal awards have been, are being, or are to be used (in whole or in part) for one or more of the identical cost items under the DOE award. If there are identical cost items, the recipient must promptly notify the DOE Contracting Officer in writing of the potential duplication and eliminate any inappropriate duplication of funding.

Save the Potentially Duplicative Funding Notice in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_PDFN."

xi. Community Benefits Plan: Job Quality and Equity

The Community Benefits Plan: Job Quality and Equity (Community Benefits Plan or Plan) must set forth the applicant's approach to ensuring that federal investments advance four goals: 1) community engagement; 2) investing in job quality and workforce continuity 3) advancing Diversity, Equity, Inclusion, and Accessibility (DEIA); and 4) contributing to the Justice40[23] Initiative. The below sections include the requirements for each goal.

[23] Pursuant to Executive Order 14008 and the Office of Management and Budget's Interim Justice40 Implementation Guidance M-21-28, DOE has developed a definition and tools to locate and identify disadvantaged communities. These resources can be located at https://energyjustice.egs.anl.gov/. Pursuant to Office of Management and Budget's Memorandum M-23-09, DOE recognizes disadvantaged communities as defined and

For your convenience, a Community Benefits Plan template is available on Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/. Applicants are strongly encouraged to use the template to complete their specific Plan. If the template is not used, the Plan must address all of the elements described below, and as outlined in the template.

The applicant's Community Benefits Plan must include at least one Specific, Measurable, Achievable, Relevant and Timely (SMART) milestone per budget period to measure progress on the proposed actions. The Plan will be evaluated as part of the technical review process. If DOE selects a project, DOE will incorporate the Community Benefits Plan into the award and the recipient must implement its Community Benefits Plan when carrying out its project. Public transparency around the plan and SMART commitments ensure accountability. In addition, DOE will evaluate the recipient's progress during the award period of performance, including as part of the Go/No-Go review process.

The Community Benefits Plan must not exceed 12 pages. It must be submitted in PDF format using the following convention name for the title: "Control Number_LeadOrganization_CBP."

This Plan must address the technical review criterion titled "Community Benefits Plan: Job Quality & Equity." See Section VI.E.v, VII.E.v, VIII.E.v of the FOA.

See below for additional information on the Community Benefits Plan content requirements.

The Community Benefits Plan must address the following:

1. Community Engagement: The Community Benefits Plan must describe the applicant's actions to date and plans to engage with community partners, such as local and/or Tribal governments, labor unions, and community-based organizations that support or work with underserved communities, including disadvantaged communities as defined for purposes of the Justice40 Initiative.

2. Investing in Job Quality and Workforce Continuity: A well-qualified, skilled, and trained workforce is necessary to ensure project stability, continuity, and

identified by the White House Council on Environmental Quality's Climate and Economic Justice Screening Tool (CEJST) Version 1.0, which can be located at https://screeningtool.geoplatform.gov/. DOE's Justice40 Implementation Guidance is located at https://www.energy.gov/sites/default/files/2022-07/Final%20DOE%20Justice40%20General%20Guidance%20072522.pdf.

success, and to meet program goals. High-quality jobs are critical to attracting and retaining the qualified workforce required.

The Plan must describe the applicant's approach to investing in workforce education and training of both new and incumbent workers and ensuring jobs are of sufficient quality to attract and retain skilled workers in the industry.

As the 1935 National Labor Relations Act states, employees' ability to organize, bargain collectively, and participate, through labor organizations of their choosing, in decisions that affect them contributes to the effective conduct of business and facilitates amicable settlements of any potential disputes between employees and employers, providing assurances of project efficiency, continuity, and multiple public benefits.

The Plan must include:

A) A description of:
    i. Wages, benefits, and other worker supports to be provided, benchmarking against local median wages;
    ii. Commitments to invest in workforce education and training; and
    iii. Efforts to engage employees in the design and execution of workplace safety and health plans.

B) It is the policy of the United States to eliminate the causes of certain substantial obstructions to the free flow of commerce by encouraging the practice and procedure of collective bargaining and by protecting the exercise by workers of full freedom of association. Applicant should provide a description of how and if they plan to affirmatively support worker organizing and collective bargaining. This might include a pledge to remain neutral during any union organizing campaigns, intention or willingness to permit union recognition through card check (as opposed to requiring union elections), intention or willingness to enter into binding arbitration to settle first contracts, a pledge to allow union organizers access to appropriate onsite non-work places (e.g., lunch rooms), a pledge to refrain from holding captive audience meetings, and other supportive commitments or pledges.

3. DEIA: The Community Benefits Plan must include a section describing how DEIA objectives will be incorporated into the project. The section should detail how the applicant will partner with underrepresented businesses and/or other project partners to help address DEIA.

The following is a list of potential DEIA actions that could be included in a Plan. This list is offered to provide guidance to applicants and is not intended to be comprehensive:

A) Commit to partnering with Minority Business Enterprises, minority-owned businesses, women-owned businesses, and veteran-owned businesses;

B) Provide workers with comprehensive support services, such as childcare and transportation, to increase representation and access in project's construction and operations jobs.

4. Justice40 Initiative: Applicants must provide an overview of benefits to disadvantaged communities that the project can deliver, supported by measurable milestones. The Justice40 Initiative section must include:

A. Identification of applicable disadvantaged communities to which the anticipated project benefits will flow.

B. Identification of applicable benefits that are quantifiable, measurable, and trackable, including, at a minimum, a discussion of the relevance of each of four DOE Justice40 Initiative benefits outlined below.

   Benefits include (but are not limited to) measurable direct or indirect investments or positive project outcomes that achieve or contribute to the following in disadvantaged communities: (1) a decrease in energy burden; (2) increases in clean energy enterprise creation and contracting (e.g., minority-owned or disadvantaged business enterprises); (3) increased parity in clean energy technology access and adoption; and (4) an increase in energy resilience.

C. A description of how and when anticipated benefits are expected to flow to disadvantaged communities or other communities. For example, whether the benefits will be provided directly within the disadvantaged communities identified in the Justice40 Initiative section or in another way; whether the benefits will flow during project development or after project completion; and how the applicant will track benefits delivered.

For projects funded under this FOA, DOE will provide specific reporting guidance for the benefits described above.

xii. Community Benefits Plan Budget Justification

Applicants must provide a separate budget justification identifying the Community Benefit Plan costs included in the "Budget Justification Workbook." This Community Benefits Plan Budget Justification must include the same justification information described in the "Budget Justification Workbook" section above but should only include Community Benefits Plan costs.

Save the Community Benefits Plan Budget Justification in a Microsoft Excel file using the following convention for the title: "ControlNumber_CBP_Budget_Justification".

xiii. Summary for Public Release

Applicants must submit a one-page summary of their project that is suitable for dissemination to the public. It should be a self-contained document that identifies the name of the applicant, the lead project manager/principal investigator(s), the project title, the objectives of the project, a description of the project, including methods to be employed, the potential impact of the project (e.g., benefits, outcomes), major participants (for collaborative projects), and the project's commitments and goals described in the Community Benefits Plan. This document must not include any proprietary or business-sensitive information, as DOE may make it available to the public after selections are made. The summary must not exceed one page when printed, using standard 8.5" x 11" paper with 1" margins (top, bottom, left, and right) with font not smaller than 12-point.

Save the Summary for Public Release in a single PDF file using the following naming convention: "ControlNumber_LeadOrganization_Summary".

xiv. Summary Slide

Applicants must provide a single slide summarizing the proposed project. The Summary Slide template is available on Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/ and must include the following information:

- A summary of the proposed project;
- A description of the projects anticipated impact;
- Proposed project goals;
- Any key graphics (illustrations, charts and/or tables);
- The project's high-level intended impacts/outcomes;
- Topline community benefits;
- Project title, prime recipient, PI/LPM, and Senior/Key Personnel information; and
- Requested DOE funds and proposed applicant cost share.

Save the Summary Slide in a single Microsoft PowerPoint file using the following convention for the title: "ControlNumber_LeadOrganization_Slide".

xv. Transparency of Foreign Connections

Applicants must provide the following as it relates to the proposed recipient and subrecipients. **Include a separate disclosure for the applicant and each proposed subrecipient.** U.S. National Laboratories, domestic government entities, and institutions of higher education are only required to respond to items 1, 2 and 9, and if applying to serve as the prime recipient, must provide complete responses for project team members that are not U.S. National Laboratories, domestic government entities, or institutions of higher education.

1. Entity name, website address, and mailing address;
2. The identity of all owners, principal investigators, project managers, and senior/key personnel who are a party to any *Foreign Government-Sponsored Talent Recruitment Program* of a foreign country of risk[24];
3. The existence of any joint venture or subsidiary that is based in, funded by, or has a foreign affiliation with any foreign country of risk;
4. Any current or pending contractual or financial obligation or other agreement specific to a business arrangement, or joint venture-like arrangement with an enterprise owned by a foreign state or any foreign entity;
5. Percentage, if any, that the proposed recipient or subrecipient has foreign ownership or control;
6. Percentage, if any, that the proposed recipient or subrecipient is wholly or partially owned by an entity in a foreign country of risk;
7. Percentage, if any, of venture capital or institutional investment by an entity that has a general partner or individual holding a leadership role in such entity who has a foreign affiliation with any foreign country of risk;
8. Any technology licensing or intellectual property sales to a foreign country of risk, during the 5-year period preceding submission of the proposal;
9. Any foreign business entity, offshore entity, or entity outside the United States related to the proposed recipient or subrecipient;
10. Complete list of all directors (and board observers), including their full name, citizenship and shareholder affiliation, date of appointment, duration of term, as well as a description of observer rights as applicable;
11. Complete capitalization table for your entity, including all equity interests (including LLC and partnership interests, as well as derivative securities). Include both the number of shares issued to each equity holder, as well as the percentage of that series and all equity on a fully diluted basis. Identify the principal place of incorporation (or organization) for each equity holder. If the

[24] DOE defines Country of Risk to include China, Russia, North Korea, and Iran. This list is subject to change.

equity holder is a natural person, identify the citizenship(s). If the recipient or subrecipient is a publicly traded company, provide the above information for shareholders with an interest greater than 5%;

12. A summary table identifying all rounds of financing, the purchase dates, the investors for each round, and all the associated governance and information rights obtained by investors during each round of financing; and
13. An organization chart to illustrate the relationship between your entity and the immediate parent, ultimate parent, and any intermediate parent, as well as any subsidiary or affiliates. Identify where each entity is incorporated.

DOE reserves the right to request additional or clarifying information based on the information submitted.

Save the Transparency of Foreign Connections information in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_TFC."

xvi. Budget for DOE/NNSA FFRDC (if applicable)

If a DOE/NNSA FFRDC is to perform a portion of the work, the applicant must provide a DOE work proposal (WP) in accordance with the requirements in DOE Order 412.1A, Work Authorization System, Attachment 2, available at: https://www.directives.doe.gov/directives-documents/400-series/0412.1-BOrder-a-chg1-AdmChg.

Save the WP in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_WP".

xvii. Authorization for Non-DOE/NNSA or DOE/NNSA FFRDCs (if applicable)

The federal agency sponsoring the FFRDC must authorize in writing the use of the FFRDC on the proposed project and this authorization must be submitted with the application. The use of a FFRDC must be consistent with the contractor's authority under its award.

Save the Authorization in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_FFRDCAuth".

xviii. SF-LLL: Disclosure of Lobbying Activities (required)

Recipients and subrecipients may not use any federal funds to influence or attempt to influence, directly or indirectly, congressional action on any legislative or appropriation matters.

Recipients and subrecipients are required to complete and submit SF-LLL, "Disclosure of Lobbying Activities" (https://grants.gov/forms/forms-repository/sf-424-individual-family) to ensure that non-federal funds have not been paid and will not be paid to any person for influencing or attempting to influence any of the following in connection with the application:

- An officer or employee of any federal agency;
- A member of Congress;
- An officer or employee of Congress; or
- An employee of a member of Congress.

Save the SF-LLL in a single PDF file using the following convention for the title: "ControlNumber_LeadOrganization_SF-LLL".

D. Submission Dates and Times

All required submissions must be submitted in Infrastructure eXCHANGE no later than 5 p.m. ET on the dates provided on the cover page of this FOA.

E. Post Selection Information Requests

If selected for award negotiations, DOE reserves the right to require that selected applicants provide additional or clarifying information regarding the application submissions, the project, the project team, the award requirements, and any other matters related to anticipated award. The following is a list of examples of information that may be required:

- Personnel proposed to work on the project and collaborating organizations (See Section IV.B.xviii. Participants and Collaborating Organizations in the *ACT FOA Administrative Requirements*);
- Indirect cost information;
- Other budget information;
- Letters of Commitment from third parties contributing to cost share, if applicable;
- Name and phone number of the Designated Responsible Employee for complying with national policies prohibiting discrimination (See 10 CFR 1040.5);
- Information for the DOE Office of Civil Rights to process assurance reviews under 10 CFR 1040;
- Representation of Limited Rights Data and Restricted Software, if applicable;
- Information related to Davis-Bacon Act requirements;
- Information related to any proposed Workforce and Community Agreement, as defined above in "Community Benefits Plan: Job Quality and Equity," that applicants may have made with the relevant community;
- Any proposed or required Project Labor Agreements; and
- Environmental Questionnaire.

V. Registration Requirements

There are several one-time actions before submitting an application in response to this FOA, and it is vital that applicants address these items as soon as possible. Some may take several weeks, and failure to complete them could interfere with an applicant's ability to apply to this FOA, or to meet the negotiation deadlines and receive an award if the application is selected. These requirements are described in detail at the front of this document, and as follows:

A. System for Award Management

Register with the SAM at https://www.sam.gov. Designating an Electronic Business Point of Contact (EBiz POC) and obtaining a special password called a Marketing Partner ID Number (MPIN) are important steps in SAM registration. Please update your SAM registration annually.

B. FedConnect

Register in FedConnect at https://www.fedconnect.net. To create an organization account, your organization's SAM MPIN is required. For more information about the SAM MPIN or other registration requirements, review the FedConnect Ready, Set, Go! Guide at https://www.fedconnect.net/FedConnect/Marketing/Documents/FedConnect_Ready_Set_Go.pdf.

C. Grants.gov

Register in Grants.gov (https://www.grants.gov/) to receive automatic updates when Amendments to this FOA are posted. However, **please note that Pre-Applications and Full Applications will not be accepted through Grants.gov.**

D. Electronic Authorization of Applications and Award Documents

Submission of an application and supplemental information under this FOA through electronic systems used by the DOE, including Grants.gov and FedConnect.net, constitutes the authorized representative's approval and electronic signature.

E. Infrastructure eXCHANGE Portal

To apply to this FOA, applicants must register with and submit application materials through Infrastructure eXCHANGE at https://infrastructure-exchange.energy.gov/, the Clean Energy Infrastructure online application portal.

To access application forms and instructions available for this FOA go to the portal and search for the funding opportunity number associated with this FOA: DE-FOA-0002986.

Infrastructure eXCHANGE is designed to enforce the deadlines specified in this FOA. The "Apply" and "Submit" buttons will automatically disable at the defined submission deadlines.

Note: The maximum file size that can be uploaded to the Infrastructure eXCHANGE website is 50MB. Files in excess of 50MB cannot be uploaded, and hence cannot be submitted for review. If a file exceeds 50MB but is still within the maximum page limit specified in the FOA it must be broken into parts and denoted to that effect. For example, FileName_Part_1 and FileName_Part_2.

DOE will not accept late submissions that resulted from technical difficulties due to uploading files that exceed 50MB.

Applicants who experience technical difficulties with submission PRIOR to the FOA deadline should contact the Infrastructure eXCHANGE helpdesk for assistance (InfrastructureExchangeSupport@hq.doe.gov).

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 must address OT/ICS risks and advance the OT/ICS cybersecurity maturity of eligible 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, governance/policy, and training solutions that result in increased levels of participation of the utility in cybersecurity threat information programs are strongly encouraged.

Projects can include costs associated with hiring subject matter experts or consulting services to help the utility accomplish the goals of this Topic Area.

B. Topic Area 1 Pre-Application Content Requirements

All applicants for Topic Area 1 must submit a Pre-Application that addresses the information requested in Table 5. It is recommended that applicants review *Section VI.C. Pre-Application Review Criteria* to help guide responses to the Pre-Application questions. Pre-Applications must not exceed 12 pages. Do not describe specific cybersecurity vulnerabilities, risks, or other sensitive information in your responses.

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)[25] 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	

[25] The United States Government Accountability Office (GAO) defines Full-Time Equivalent (FTE) as the total number of regular straight-time hours (i.e., not including overtime or holiday hours) worked by employees divided by the number of compensable hours applicable to each fiscal year. Annual leave, sick leave, and compensatory time off and other approved leave categories are considered to be "hours worked" for purposes of defining FTE employment. https://www.gao.gov/assets/gao-05-734sp.pdf

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?

C. Topic Area 1 Pre-Application Review Criteria

This section describes the criteria reviewers will use to score the applicant's Pre-Application. It is recommended that applicants review these criteria and consider the weighting of each of the criterion as they complete their Pre-Applications. An applicant can receive a maximum of 96 total 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

D. Topic Area 1 Full Application Project Plan Content Requirements

The applicant should review and consider the weighting of each of the review criteria (see Section VI.E) when preparing the Project Plan. The Full Application Project Plan must clearly relate to and expand upon the information provided in the applicant's Pre-Application.

i. Project Design and Management

1. Describe your project including the overall project objectives and the desired impacts and outcomes of the proposed work.
2. Describe the current status of the proposed project (new/conceptual project; planned project; planned and scheduled project; or, additional scope on existing project), and the objectives for the high-level phases or stages of the proposed work, including the timeline required to accomplish each phase of work. What are the tasks your utility will need to complete to advance each phase of work and the measurable milestones you will use to document your progress? Consider milestones that are specific, measurable, achievable, relevant, and timely (SMART), and that are appropriate, verifiable, and show a critical path toward achievement of project goals.
3. Describe the steps your utility took to generate the Budget Justification provided with your application and describe the rationale for your estimated personnel requirements and training needs. What proportion of the budget will be spent on solutions focused on people, on process, and on technology (Note the proportions should sum to 100%)?
4. Describe any potential project or organizational risks that may impact your ability to successfully complete the proposed work and how you will manage those risks.
5. Within the first two pages of the Project Plan, include a short statement on whether the project will involve the construction, alteration, and/or repair of infrastructure in the United States. See ACT FOA Administrative Requirements Section III.B.vii and Appendix D for applicable definitions and other information to inform this statement.

ii. Assessment and Analysis Approach

1. What cybersecurity assessments has your utility already performed and what additional assessments are planned as part of this project? If you have not already performed any cybersecurity assessments, what assessments are you planning to complete as part of this project? Describe the purpose of each assessment and how the results will be used in your project.
2. Describe the sources of information you will use, including assessments, to identify gaps in your utility's cybersecurity posture and the processes you will use to analyze the results.
3. Describe the process you will use to prioritize identified cybersecurity risks. What criteria will you use, which job roles will be involved in the conversations to prioritize risks, and why are these perspectives considered critical to the prioritization process?

iii. Implementation and Operations Plan

1. Describe the process you will use to engage with utility staff to help select solutions. How will you determine funding allocations between investments in people, process, and technology? How will you evaluate whether existing products and services being used by your utility can accomplish your project's goals? How will your utility evaluate and select new solutions to mitigate the risks you've prioritized?
2. What steps will your organization need to take prior to implementing any new solutions and how will you mitigate business and/or operational risks associated with the implementation of new solutions?
3. Describe how you will achieve buy-in and active participation from technical and non-technical staff to ensure a selected solution is successful after its implementation. What solutions are proposed in your project that will require a rollout strategy to engage non-technical staff?
4. What challenges will your utility face integrating new tools and technologies into your existing technology stack and how will you address them?
5. Describe the testing processes you will use after technical solutions are implemented to identify residual security risks and to confirm security controls work as expected after implementation.
6. How will your organization minimize third-party risks associated with purchasing and implementing the selected solutions?

iv. Commitment, Team, and Resources

1. Describe the responsibilities and activities of all staff members who will be part of your project team, their job titles and experience, and why they are appropriately equipped to handle the requirements of this project and of a federal award. Identify who on your project team will be the primary point of

contact (POC) responsible for ensuring project coordination and describe the expected responsibilities for your POC?

2. Describe the additional or ongoing training your staff will need to continue to maintain and update the policy and technical solutions implemented during your project after the funding ends? How will your utility continue to support this training?
3. Describe the changes that will be made to written documentation, policies, processes, and procedures to institutionalize and support the continued effectiveness of the solutions, to ensure periodic reassessments of your cybersecurity posture and risks, and to support continuous learning for your staff?
4. What commitment has your utility's leadership made to meet the ongoing costs associated with the implemented technical solutions, licenses, and contracts, and to ensure adequate ongoing training for your staff after the project funding ends?

E. Topic Area 1 Full Application Review Criteria

Review Criteria will be evaluated against the entirety of your full application package including your narrative Project Plan and the other documents listed in Section IV.C. An applicant can receive a maximum of 135 total points.

i. Criterion 1: Project Design and Management (Maximum Points: 33)

Criterion Number		**Maximum Points**
FA-1.1	The overall objectives and desired impacts of the proposed work will result in improvements in the cybersecurity posture of the electric utility's operational systems and increase the participation and engagement of the utility in cybersecurity threat information sharing programs.	6
FA-1.2	The objectives for each phase of work (if applicable), are clearly described and responsive to the objectives of Topic Area 1.	3
FA-1.3	Applicant has developed a realistic project schedule taking into consideration the committed internal capacity, availability of materials or hardware, and technical assistance needs.	3
FA-1.4	Applicant includes relevant tasks in a logical sequence that increases the likelihood of achieving the objectives of the proposed project including assessment and risk prioritization, selection and implementation of solutions, testing of solutions after implementation, timing of relevant training, and modifications to processes and procedures.	6
FA-1.5	Applicant identifies meaningful milestones that are specific, measurable, achievable, relevant, and timely (SMART), and that are	6

	appropriate, verifiable and show a critical path toward achievement of project goals.	
FA-1.6	Applicant's budget reflects realistic costs to accomplish the proposed scope of work and an appropriate balance of investments in people, processes, and technologies. (Reviewers will consider both Applicant's Project Plan and the Budget Justification.)	6
FA-1.7	Applicant provides a thorough assessment of potential risks that may impact project success and describes a reasonable approach to manage identified risks, and to continue to assess and address risks throughout the project.	3

ii. Criterion 2: Assessment and Analysis Approach (Maximum Points: 18)

Criterion Number		**Maximum Points**
FA-2.1	Applicant clearly describes cybersecurity assessment(s) that have been performed or are planned and demonstrates a meaningful understanding of how to use the different assessments and the results to better understand the utility's cybersecurity posture and risks.	6
FA-2.2	Applicant presents a compelling strategy for conducting a cybersecurity gap/risk analysis, has clearly identified relevant departments within the utility where high priority cybersecurity risks are likely to occur, and has included all relevant technical and non-technical job roles from those departments in conversations on the cybersecurity implications of the results within each department.	6
FA-2.3	Applicant has described a robust process to prioritize the cybersecurity risks identified in the assessments and demonstrates an appropriate level of project management communication to ensure a shared understanding across all departments on the implications of the risks, and why certain risks will be prioritized to receive funding in the proposed project.	6

iii. Criterion 3: Implementation and Operations Plan (Maximum Points: 24)

Criterion Number		**Maximum Points**
FA-3.1	Applicant demonstrates an understanding of the key considerations in selecting cybersecurity solutions based on prioritized risks and describes a strategy for evaluating existing solutions and alternative	6

	solutions and ensuring that funding is invested in solutions focused on people, process, and technology.	
FA-3.2	Applicant demonstrates an understanding of business and/or operational risks associated with implementing new cybersecurity solutions and has described an appropriate approach to managing the risks.	3
FA-3.3	Applicant has accurately identified solutions that will require participation from other utility staff to be successful, and describes a thoughtful, appropriate, and comprehensive approach for rollout plans that are highly likely to achieve buy-in from the relevant utility staff necessary for the success of the solutions.	3
FA-3.4	Applicant demonstrates a clear understanding of the potential challenges of integrating cybersecurity solutions into legacy systems and describes a realistic plan to overcome these challenges.	3
FA-3.5	Applicant describes a range of appropriate testing methods that will be used to identify cybersecurity risks that exist after the solutions are implemented, and to test that the solutions successfully provide the cybersecurity control that was expected.	6
FA-3.6	Applicant describes actions that will minimize third-party cybersecurity risks including negotiating contracts that include appropriate service level agreements and distribute risk and liability equitably between the parties.	3

iv. Criterion 4: Commitment, Team, and Resources (Maximum Points: 24)

Criterion Number		**Maximum Points**
FA-4.1	Applicant has committed an adequate level of qualified staff resources who are dedicated to the project team. (Reviewers will consider the Applicant's Program Plan, Budget Justification, resumes, and the Leadership Letter of Commitment to Long-Term Success.)	3
FA-4.2	The qualifications, expertise, and experience of key personnel and team members are appropriate for the proposed project and for managing a federal award.	3
FA-4.3	Applicant demonstrates a realistic understanding of the additional and ongoing staff training necessary to maintain the effectiveness of policy and technical solutions as the threat landscape changes and describes how the utility will continue to support this training.	6
FA-4.4	Applicant has a clear plan to update or develop written policies, processes, and procedures to institutionalize and support the continued effectiveness of solutions, including periodically	6

	reassessing the utility's cybersecurity posture and risks, and ensuring support for continuous learning and improvement.	
FA-4.5	Applicant's leadership has provided specific verifiable commitments to provide the funding necessary to meet the ongoing costs associated with the selected solutions. (Reviewers will consider the Applicant's Program Plan and the Leadership Letter of Commitment to Long-Term Success.)	6

v. Criterion 5: Community Benefits Plan (Maximum Points: 36)

Criterion Number		**Maximum Points**
FA-5.1	Community Engagement • Extent to which the applicant demonstrates community engagement to date that results in support for the proposed project; and • Extent to which Applicant plans to communicate benefits of the project to service members/customers.	6
FA-5.2	• Extent to which the applicant thoughtfully demonstrates how they will benefit their local communities. This could include engaging with local communities to increase cybersecurity awareness or sharing knowledge and skills attained through this project with local communities.	3
FA-5.3	Job Quality and Workforce Continuity • Quality and manner in which the proposed project will create and/or retain high quality, good-paying jobs with employer-sponsored benefits for both Applicant and sub-contractors; • Extent to which the project provides employees with the ability to organize, bargain collectively, and participate, through labor organizations of their choosing, in decisions that affect them and that contribute to the effective conduct of business and facilitates amicable settlements of any potential disputes between employees and employers, providing assurances of project efficiency, continuity, and multiple public benefits; and • Extent to which applicant demonstrates that they are a responsible employer.	6
FA-5.4	• Extent to which the applicant demonstrates a strong commitment to providing paid on-the-job training that will enable employees to improve their cybersecurity knowledge, skills, and abilities.	3
FA-5.5	Diversity, Equity, Inclusion, and Accessibility • Extent to which the Community Benefits Plan includes specific and high-quality actions to meet DEIA goals, which may include DEIA	9

	recruitment procedures, supplier diversity plans, and other DEIA initiatives; and • Quality of any partnerships and agreements with apprenticeship readiness programs, or community-based workforce training and support organizations serving workers facing systematic barriers to employment to facilitate participation in the project's construction and operations.	
FA-5.6	<u>Justice40 Initiative</u> • Extent to which the Community Benefits Plan identifies: specific, measurable benefits for disadvantaged communities and how the benefits will flow to disadvantaged communities; and • Extent to which the project would contribute to meeting the objective that 40% of the benefits of climate and clean energy investments will flow to disadvantaged communities.	9

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.

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 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,[26] 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.

[26] For the purposes of this FOA, commercially available solutions are defined as solutions that have been offered for sale, lease, or license to the public. Documentation that a technology is commercially available could include showing the solution can be warrantied or that it can be purchased from a commercial vendor for the intended purpose.

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.

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 and bulk purchases of products and services; developing training and educational resources to document successful models for providing these services to eligible utilities; delivering training on how to implement successful service models using workshops, conferences, and other venues if the majority of the audience consists of other eligible RMUC Program entities that could potentially replicate or modify the program model the applicant is using to serve eligible 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 the cybersecurity delivery program models that are successful.

Projects can include costs associated with hiring subject matter experts or consulting services to help the applicant accomplish the goals of this Topic Area.

B. Topic Area 2 Pre-Application Content Requirements

All applicants for Topic Area 2 must submit a Pre-Application that addresses the information requested in Table 6. It is recommended that applicants review *Section VII.C. Pre-Application Review Criteria* to help guide responses to the Pre-Application questions. Pre-Applications must not exceed 12 pages. Do not describe specific cybersecurity vulnerabilities, risks, or other sensitive information in your responses.

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.	

If your organization is a utility, indicate your utility type: distribution, generation, transmission, other (please specify).	
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?

C. Topic Area 2 Pre-Application Review Criteria

This section describes the criteria reviewers will use to score the applicant's Pre-Application. It is recommended that applicants review these criteria and consider the weighting of each of the criterion as they complete their Pre-Applications. An applicant can receive a maximum of 108 total 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

D. Topic Area 2 Full Application Project Plan Content Requirements

The applicant should review and consider the weighting of each of the review criteria (see Section VII.E) when preparing the Project Plan. The Full Application Project Plan must clearly relate to and expand upon the information provided in the applicant's Pre-Application.

i. Project Design and Management

1. Describe your project including the overall project objectives and the desired impacts and outcomes of the proposed work. Identify those project goals that

you anticipate will have a substantial impact on improving the cybersecurity posture of your Participating Utilities.

2. Describe the objectives for high-level phases or stages of the proposed work, including the timeline required to accomplish each phase of work. What are the tasks your organization will need to complete to advance each phase of work and the measurable milestones you will use to document your progress? Consider milestones that are specific, measurable, achievable, relevant, and timely (SMART), and that are appropriate, verifiable, and show a critical path toward achievement of project goals.
3. Describe the program evaluation process you will use to assess the success and impacts of your project. What criteria will you use to measure success? What are the most likely benefits you will provide to your Participating Utilities and how will you document those benefits? How does your program design ensure that you will be able to collect the relevant data to measure your success and what milestone points will you use to trigger program evaluation efforts?
4. Describe the steps your organization took to generate the Budget Justification provided with your application and describe the rationale for your estimates. What proportion of the budget will be spent on solutions that are focused on your Participating Utilities' people, their process, and on technology and tools?
5. Describe the non-technical and organizational challenges you anticipate within your organization, with members of your project team, with your utility participants, or with other entities interested in providing technical assistance that may impact your ability to successfully complete the proposed work. How will your organization address these challenges? What process will your organization use to continually assess and identify similar project risks?
6. Provide a list of the Participating Utilities in your project, indicate the type of utility (distribution, generation, transmission, or specify what type of electric utility if not one of these three types), and provide a name and title for the point of contact at each utility.
7. Within the first two pages of the Project Plan, include a short statement on whether the project will involve the construction, alteration, and/or repair of infrastructure in the United States. See ACT FOA Administrative Requirements Section III.B.vii and Appendix D for applicable definitions and other information to inform this statement.

ii. Assessment and Analysis Approach

1. How many of your Participating Utilities have already completed cybersecurity risks assessments and what assessments did they use? How many of your Participating Utilities will need to complete risk assessments to advance your project? What assessments will your organization recommend

for them to complete and how will your organization work with these utilities to help them complete the assessments?

2. Describe the sources of information you will use, including assessments, to help your Participating Utilities identify gaps in their cybersecurity posture and the process you will use to help them analyze the results.
3. Describe the process you will use with your Participating Utilities to help them prioritize identified cybersecurity risks. What criteria will you recommend, which job roles will be involved in the conversations to prioritize risks, and why do you think these perspectives are critical to the prioritization process?
4. If your project includes work to build a stronger ecosystem of cybersecurity technical assistance providers, describe the process you will use to identify needs in the community and the criteria you will use to decide where to focus your efforts.

iii. Implementation and Operations Plan

1. Describe the process you will use to engage with your Participating Utilities to help them evaluate and select solutions that mitigate the prioritized cybersecurity risks identified. How will you help your utilities evaluate whether their existing products and services can accomplish their security goals? What strategy will you use to ensure your utilities include solutions focused on people, process, and technology?
2. What steps will your organization take with your Participating Utilities prior to implementing any new cybersecurity solutions and how will you help your utilities mitigate business and/or operational risks before the solutions are implemented?
3. Describe the approach your organization will take for purchasing training, services, and product solutions on behalf of your Participating Utilities. What role will each organization play? Who will make the purchases? Who will be responsible for the successful implementation of the solutions? For purchases of products or services, how will ownership of the solutions be determined?
4. Describe the process you will use to help your Participating Utilities achieve buy-in and active participation from technical and non-technical staff to ensure solutions that require staff participation are successful after implementation. What solutions are proposed in your project that will require a rollout strategy to engage the utility's staff?
5. What challenges will your organization face helping your utilities integrate technology solutions into their existing technology stacks and how will you address those challenges?
6. Describe how you will work with your Participating Utilities to conduct testing after technical solutions are implemented to help your utilities identify residual security risks and to confirm security controls work as expected after implementation.

7. How will you help your Participating Utilities minimize third-party risks associated with purchasing and implementing the selected solutions? How will your organization minimize and mitigate third-party risks associated with the IT and cybersecurity services you are providing to your Participating Utilities?

iv. Commitment, Team, and Resources

1. Describe the responsibilities and activities of all staff members who will be part of your project team, their job titles and experience, and why they are appropriately equipped to handle the requirements of this project and of a federal award. Identify who on your project team will be the primary point of contact (POC) responsible for ensuring project coordination and describe the expected responsibilities for your POC. For staff that will be responsible for providing technical assistance and services to your utilities, indicate whether they are currently providing these services or if this will be a new responsibility for them. What training will you provide for your technical and non-technical staff to support this effort? Include a list of external partners you anticipate using to complete your project with the company name, address, and POC for each partner.
2. Describe the responsibilities and activities expected from the staff at your Participating Utilities and the anticipated time commitment of the staff in your Participating Utilities who will be responsible for ensuring the project is carried out at their utility. What challenges do you anticipate in retaining high levels of engagement with your Participating Utilities? How will you address these challenges?
3. Describe the additional or ongoing training the staff at your Participating Utilities will need to continue to maintain and update the solutions implemented during your project after the funding ends? How will your organization continue to support this training?
4. Describe the changes that will be made to written documentation, policies, processes, and procedures in your Participating Utilities to institutionalize and support the continued effectiveness of the solutions and to ensure periodic reassessments of their cybersecurity posture and risks.
5. Describe the additional or ongoing training the staff at your Participating Utilities will need to continue to maintain and update the solutions implemented during your project after the funding ends? How will your organization continue to support this training?
6. How will your organization continue to maintain and support the products and services implemented during your project after the funding ends?

E. Topic Area 2 Full Application Review Criteria

Review Criteria will be evaluated against the entirety of your full application package including narrative project plan. An applicant can receive a maximum of 162 total points.

i. Criterion 1: Project Design and Management (Maximum Points: 39)

Criterion Number		Maximum Points
FA-1.1	The overall objectives and desired impacts of the proposed work will result in improvements in the cybersecurity posture of the operational systems in the Participating Utilities and will increase the participation and engagement of the Participating Utilities in cybersecurity threat information sharing programs.	6
FA-1.2	The objectives for each phase of work (if applicable) are clearly described and responsive to the objectives of Topic Area 2.	3
FA-1.3	Applicant describes a realistic project schedule taking into consideration the internal capacity of the organization and the Participating Utilities, availability of materials and hardware, and technical assistance needs of the Participating Utilities.	3
FA-1.4	Applicant includes relevant tasks in a logical sequence that increases the likelihood of achieving the objectives of the proposed project.	6
FA-1.5	Applicant identifies meaningful milestones that are specific, measurable, achievable, relevant, and timely (SMART), and that are appropriate, verifiable and show a critical path toward achievement of project goals.	6
FA-1.6	Applicant identifies relevant metrics for measuring success, presents a concrete plan for ongoing program evaluation, and describes a process built into the project design for ensuring that relevant data are collected during program implementation at appropriate milestones to measure and document success.	3
FA-1.7	Applicant's budget reflects realistic costs to accomplish the proposed scope of work and an appropriate balance of investments in people, processes, and technologies. (Reviewers will consider both Applicant's Project Plan and the Budget Justification.)	6
FA-1.8	Applicant provides a thorough assessment of potential non-technical and organizational challenges that may impact project success and describes a reasonable approach to manage identified challenges, and to continue to assess and address risks throughout the project.	3
FA-1.9	The application includes 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. Reviewers will consider the	3

	Applicant's Program Plan and the Letters of Commitment from Participating Utilities.)	

ii. Criterion 2: Assessment and Analysis Approach (Maximum Points: 24)

Criterion Number		Maximum Points
FA-2.1	Applicant demonstrates a detailed understanding of their Participating Utilities and how many have completed assessments and still need assessments. Applicant proposes a reasonable approach to work with their utilities to complete assessments using a list of recommended assessments that demonstrates a meaningful understanding of how to use the different assessments to efficiently assess the cybersecurity risks in their utilities.	6
FA-2.2	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-technical job roles from those departments in conversations on the gap/risk analysis results.	6
FA-2.3	Applicant describes a robust process to help their Participating Utilities prioritize the cybersecurity risks identified in their assessments. The proposed process includes an appropriate level of project management communication to ensure a shared understanding across each utility's departments on the implications of the risks, and why certain risks will be prioritized in the proposed project.	6
FA-2.4	Applicant describes an effective process to identify what other potential providers of technical assistance need and proposes criteria that clearly align with the organization's strengths and successes delivering technical assistance to focus on efforts that have a high likelihood of success.	6

iii. Criterion 3: Implementation and Operations Plan (Maximum Points: 30)

Criterion Number		Maximum Points
FA-3.1	Applicant demonstrates an understanding of the key considerations in selecting cybersecurity solutions based on prioritized risks and describes a strategy for working with their Participating Utilities to evaluate existing and alternative solutions, and to ensure that their	6

	Participating Utilities invest in solutions focused on people, process, and technology.	
FA-3.2	Applicant demonstrates an understanding of potential business and/or operational risks associated with new cybersecurity solutions and describes an appropriate approach to work with their Participating Utilities to manage the unique risks at each utility before solutions are implemented.	3
FA-3.3	Applicant clearly describes the roles and responsibilities of the applicant and their Participating Utilities when the applicant purchases products or services on behalf of their utilities and proposes a reasonable strategy to manage liability, ownership, and accountability risks.	6
FA-3.4	Applicant accurately identifies solutions that might be used by their Participating Utilities that will require participation from other utility staff to be successful, and describes a thoughtful, appropriate, and comprehensive approach to work with their utilities to develop and implement rollout plans that are highly likely to achieve buy-in from the relevant utility staff necessary for the success of the solutions.	3
FA-3.5	Applicant demonstrates a thorough understanding of the potential challenges of integrating cybersecurity solutions into the legacy systems of their Participating Utilities and describes a realistic plan to overcome these challenges.	3
FA-3.6	Applicant describes an interactive process to work with their utilities to test solutions after implementation that addresses potential utility governance and vendor management challenges and describes how these challenges will be managed to enable adequate levels of testing.	6
FA-3.7	Applicant describes relevant services and technical assistance they will provide to their Participating Utilities to help minimize third-party cybersecurity risks and describes a strong internal cybersecurity program that appropriately mitigates the risks they create as third-party a service provider to their Participating Utilities.	3

iv. Criterion 4: Commitment, Team, and Resources (Maximum Points: 33)

Criterion Number		**Maximum Points**
FA-4.1	Applicant describes an adequate level of staff resources dedicated to the project team. (Reviewers will consider the Applicant's Program Plan, Budget Justification, resumes, and the Leadership Letter of Commitment to Long-Term Success.)	3
FA-4.2	The internal organization roles and responsibilities are clearly defined, the roles and responsibilities of staff coordinating with the	3

	Participating Utilities are clearly defined, and the qualifications, expertise, and experience of key personnel and team members are appropriate for the proposed project and for managing a federal award. The applicant's POC has the appropriate skills and experience to handle project coordination.	
FA-4.3	Applicant demonstrates a commitment to successful program management and communication by including all relevant technical and non-technical staff positions on the project team (e.g., operations, information technology (IT), engineering, leadership, management, finance, legal, communications, etc.) and providing appropriate training to support their project roles. (Reviewers will consider both Applicant's Program Plan, resumes, and the Budget Justification.)	3
FA-4.4	Applicant demonstrates a realistic understanding of the staff commitment needed from the Participating Utilities for the project to be successful, identifies other likely challenges to maintaining engagement with their Participating Utilities, and describes reasonable solutions to address these challenges.	6
FA-4.5	Applicant clearly describes how they will help their Participating Utilities make changes to written policies, processes, and procedures to institutionalize and support the continued effectiveness of the implemented solutions, including how the applicant will help their utilities periodically reassess cybersecurity posture and risks.	6
FA-4.6	Applicant demonstrates a realistic understanding of the additional and ongoing staff training necessary for their Participating Utilities to ensure policy and technical solutions maintain their effectiveness as the threat landscape changes and describes how the applicant and the Participating Utilities will continue to support this training.	6
FA-4.7	Applicant provides a compelling and realistic proposal for how they will continue to finance and allocate needed staff to continue to provide the products and services that were funded.	6

v. Criterion 5: Community Benefits Plan (Maximum Points: 36)

Criterion Number		**Maximum Points**
FA-5.1	<u>Community Engagement</u> • Extent to which the applicant demonstrates community and labor engagement to date that results in support for the proposed project; • Extent to which Applicant plans to communicate benefits of the project to service members/customers.	6

FA-5.2	• Extent to which the applicant thoughtfully demonstrates how they will benefit their local communities. This could include engaging with local communities to increase cybersecurity awareness or sharing knowledge and skills attained through this project with local communities.	3
FA-5.3	<u>Job Quality and Workforce Continuity</u> • Quality and manner in which the proposed project will create and/or retain high quality, good-paying jobs with employer-sponsored benefits for both Applicant and sub-contractors; • Extent to which the project provides employees with the ability to organize, bargain collectively, and participate, through labor organizations of their choosing, in decisions that affect them and that contribute to the effective conduct of business and facilitates amicable settlements of any potential disputes between employees and employers, providing assurances of project efficiency, continuity, and multiple public benefits; and • Extent to which applicant demonstrates that they are a responsible employer.	6
FA-5.4	• Extent to which the applicant demonstrates a strong commitment to providing paid on-the-job training that will enable employees to improve their cybersecurity knowledge, skills, and abilities.	3
FA-5.5	<u>Diversity, Equity, Inclusion, and Accessibility</u> • Extent to which the Community Benefits Plan includes specific and high-quality actions to meet DEIA goals, which may include DEIA recruitment procedures, supplier diversity plans, and other DEIA initiatives; and • Quality of any partnerships and agreements with apprenticeship readiness programs, or community-based workforce training and support organizations serving workers facing systematic barriers to employment to facilitate participation in the project's construction and operations.	9
FA-5.6	<u>Justice40 Initiative</u> • Extent to which the Community Benefits Plan identifies: specific, measurable benefits for disadvantaged communities and how the benefits will flow to disadvantaged communities; and • Extent to which the project would contribute to meeting the objective that 40% of the benefits of climate and clean energy investments will flow to disadvantaged communities.	9

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

ensures the applicant will continue to provide services, and the Participating Utilities will continue to maintain the effectiveness of cybersecurity improvements after the project funding ends; and create a documented replicable, scalable model for delivering cybersecurity services that can be used by other eligible entities.

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 <u>will not</u> support cybersecurity technology or tool purchases, technology deployment activities, or the purchase of other IT or cybersecurity related equipment or assets.**

Projects can include costs associated with hiring subject matter experts or consulting services to help the applicant accomplish the goals of this Topic Area.

B. Topic Area 3 Pre-Application Content Requirements

All applicants for Topic Area 3 must submit a Pre-Application that addresses the information requested in Table 7. It is recommended that applicants review *Section VIII.C. Pre-Application Review Criteria* to help guide responses to the Pre-Application questions. Pre-Applications must not exceed 12 pages. Do not describe specific cybersecurity vulnerabilities, risks, or other sensitive information in your responses.

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 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. 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 administrative challenges might 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?	

C. Topic Area 3 Pre-Application Review Criteria

This section describes the criteria reviewers will use to score the applicant's Pre-Application. It is recommended that applicants review these criteria and consider the weighting of each of the criterion as they complete their Pre-Applications. An applicant can receive a maximum of 105 total 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		**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-technical job roles from 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

D. Topic Area 3: Full Application Project Plan Content Requirements

The applicant should review and consider the weighting of each of the review criteria (see Section VIII.E) when preparing the Project Plan. The Full Application Project Plan must clearly relate to and expand upon the information provided in the applicant's Pre-Application.

i. Project Design and Management

1. Describe your project including the overall project objectives and the desired impacts and outcomes of the proposed work. Identify those project goals that you anticipate will have a substantial impact on improving the cybersecurity posture of your Participating Utilities or improving the ability of other organizations to provide technical assistance and services to eligible utilities.
2. Describe the objectives for high-level phases or stages of the proposed work, including the timeline required to accomplish each phase of work. What are the tasks your organization will need to complete to advance each phase of work and the measurable milestones you will use to document your progress? Consider milestones that are specific, measurable, achievable, relevant, and timely (SMART), and that are appropriate, verifiable, and show a critical path toward achievement of project goals.
3. Describe the program evaluation process you will use to assess the success and impacts of your project. What criteria will you use to measure success? What are the most likely benefits you will provide to your Participating Utilities or the community of service providers and how will you document those benefits? How does your program design ensure that you will be able to collect the relevant data to measure your success and what milestone points will you use to trigger program evaluation efforts?
4. Describe the steps your organization took to generate the Budget Justification provided with your application and describe the rationale for your estimates including personnel costs and your organization's estimated training costs for your staff.
5. Describe the non-technical and organizational challenges you anticipate within your organization, with members of your project team, with your

utility participants, or with other entities interested in providing technical assistance that may impact your ability to successfully complete the proposed work. How will your organization address these challenges? What process will your organization use to continually assess and identify similar project risks?

6. Provide a list of the Participating Utilities in your project, indicate the type of utility (distribution, generation, or transmission), provide a name and title for the point of contact at each utility, and indicate whether your organization considers the utility to be a limited cybersecurity resource utility and why?
7. Within the first two pages of the Project Plan, include a short statement on whether the project will involve the construction, alteration, and/or repair of infrastructure in the United States. See ACT FOA Administrative Requirements Section III.B.vii and Appendix D for applicable definitions and other information to inform this statement.

ii. Assessment and Analysis Approach

1. How many of your Participating Utilities have already completed cybersecurity risks assessments and what assessments did they use? How many of your Participating Utilities will need to complete risk assessments to advance your project? What assessments will your organization recommend for them to complete and how will your organization work with these utilities to help them complete the assessments?
2. Describe the sources of information you will use, including assessments, to help your Participating Utilities identify gaps in their cybersecurity posture and the process you will use to help them analyze the results.
3. Describe the process you will use with your Participating Utilities to help them prioritize identified cybersecurity risks. What criteria will you recommend, which job roles will be involved in the conversations to prioritize risks, and why do you think these perspectives are critical to the prioritization process?
4. Describe the process you will use to identify and prioritize the technical assistance, training, and services you will provide based on the highest priority cybersecurity risks identified in your Participating Utilities?
5. If your project includes work to build a stronger ecosystem of cybersecurity technical assistance providers, how will you engage with other entities to understand their challenges and needs, what criteria will you use to decide where to focus your efforts, and what methods will you use to provide support to help create or improve their service delivery models?
6. How will you assess the financial value of the technical assistance and services you provide to your Participating Utilities, such as cost savings that come from economies of scale, or the ability to minimize costs as a not-for-profit service provider?

iii. Implementation and Operations Plan

1. What types of technical assistance and services will your organization be providing to each of the Participating Utilities in your project and how do these services fit within the C2M2 domains? Describe who will be providing the different types of assistance/services: your organization's staff, consultants, MSPs/MSSPs, training providers, etc.
2. How will you manage requests for assistance from your Participating Utilities? What criteria will you use to prioritization resource allocations and service delivery times?
3. How will your project improve the number of utilities participating in cybersecurity threat information sharing programs, the level of engagement your utilities will have with information sharing organizations, and 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?
4. How will your organization assist utility participants in the process of evaluating and selecting potential people, process, and technology solutions? Describe the process you will use to help them identify the appropriate proportion of resources to dedicate to training, modifying policies and procedures, and deploying technologies to ensure that the solutions will be successfully implemented, maintained, and updated after the project funding ends.
5. How will you assist your Participating Utilities in evaluating whether their existing products and services can accomplish their goals or whether they need new tools and technologies? What factors will you take into consideration?
6. Describe the process you will use to help your Participating Utilities achieve buy-in and active participation from technical and non-technical staff to ensure solutions that require staff participation are successful after implementation. What solutions are proposed in your project that will require a rollout strategy to engage the utility's staff?
7. How will you help your Participating Utilities minimize third-party risks associated with purchasing and implementing the selected solutions? How will your organization minimize and mitigate third-party risks associated with the IT and cybersecurity services you are providing to your Participating Utilities?

iv. Commitment, Team, and Resources

1. Describe the responsibilities and activities of all staff members who will be part of your project team, their job titles and experience, and why they are appropriately equipped to handle the requirements of this project and of a federal award. Identify who on your project team will be the primary point of

contact (POC) responsible for ensuring project coordination and describe the expected responsibilities for your POC. For staff that will be responsible for providing technical assistance and services to your utilities, indicate whether they are currently providing these services or if this will be a new responsibility for them. What training will you provide for your technical and non-technical staff to support this effort? Include a list of external partners you anticipate using to complete your project with the company name, address, and POC for each partner.

2. Describe the responsibilities and activities expected from the staff at your Participating Utilities and the anticipated time commitment of the staff in your Participating Utilities who will be responsible for ensuring the project is carried out at their utility. What challenges do you anticipate in retaining high levels of engagement with your Participating Utilities? How will you address these challenges.
3. Describe the additional or ongoing training the staff at your Participating Utilities will need to continue to maintain and update the solutions implemented during your project after the funding ends? How will your organization continue to support this training?
4. How will your organization continue to maintain and support the technical assistance and other services implemented during your project after the funding ends?

E. Topic Area 3 Full Application Review Criteria

Review Criteria will be evaluated against the entirety of your Full Application package including your project plan and Community Benefits Plan. An applicant can receive a maximum of 162 total points.

i. Criterion 1: Project Design and Management (Maximum Points: 48)

Criterion Number		Maximum Points
FA-1.1	The overall objectives and desired impacts of the proposed work will result in improvements in the cybersecurity posture of the Participating Utilities or in documented, replicable, scalable models that can be used by other entities to deliver IT and cybersecurity services to eligible utilities.	6
FA-1.2	The objectives for each phase of work (if applicable) are clearly described and responsive to the objectives of Topic Area 3.	3
FA-1.3	Applicant describes a realistic project schedule taking into consideration the internal capacity of the organization and the Participating Utilities, availability of materials and hardware, and technical assistance needs of the Participating Utilities.	3

FA-1.4	Applicant includes relevant tasks in a logical sequence that increases the likelihood of achieving the objectives of the proposed project.	6
FA-1.5	Applicant identifies meaningful milestones that are specific, measurable, achievable, relevant, and timely (SMART), and that are appropriate, verifiable and show a critical path toward achievement of project goals.	6
FA-1.6	Applicant identifies relevant metrics for measuring success, presents a concrete plan for ongoing program evaluation, and describes a process built into the project design for ensuring that relevant data are collected during program implementation at appropriate milestones to measure and document success.	3
FA-1.7	Applicant's budget reflects realistic costs to accomplish the proposed scope of work and an appropriate balance of investments in internal staff training and in providing technical assistance, training, and services to their Participating Utilities. (Reviewers will consider both Applicant's Project Plan and the Budget Justification.)	6
FA-1.8	Applicant provides a thorough assessment of potential non-technical and organizational challenges that may impact project success and describes a reasonable approach to manage identified challenges, and to continue to assess and address risks throughout the project.	3
FA-1.9	Applicant provides a compelling argument for how they will define whether a participating utility should be considered a limited cybersecurity resources utility.	6
FA-1.10	The application clearly prioritizes providing services to utilities with limited cybersecurity resources based on the number of limited cybersecurity resource utilities on the list of Participating Utilities (Reviewers should score applications proposing 5 or fewer utilities low, 6-8 utilities medium, and 8+ utilities high for this criterion. Reviewers will consider the Applicant's Program Plan and the Letters of Commitment from Participating Utilities.)	6

ii. Criterion 2: Assessment and Analysis Approach (Maximum Points: 27)

Criterion Number		**Maximum Points**
FA-2.1	Applicant demonstrates a detailed understanding of their Participating Utilities and how many have completed assessments and still need assessments. Applicant proposes a reasonable approach to work with their utilities to complete assessments using a list of recommended assessments that demonstrates a meaningful understanding of how to use the different assessments to efficiently assess the cybersecurity risks in their utilities.	3

FA-2.2	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-technical job roles from those departments in conversations on the gap/risk analysis results.	6
FA-2.3	Applicant describes a robust process to help their Participating Utilities prioritize the cybersecurity risks identified in their assessments. The proposed process includes an appropriate level of project management communication to ensure a shared understanding across each utility's departments on the implications of the risks, and why certain risks will be prioritized in the proposed project.	6
FA-2.4	Applicant demonstrates an understanding of the most relevant technical assistance, training, and other services they can provide to address the highest priority cybersecurity risks identified in their Participating Utilities.	6
FA-2.5	Applicant describes an effective process to identify what other potential providers of technical assistance need and proposes criteria that clearly align with the organization's strengths and successes delivering technical assistance to focus on efforts that have a high likelihood of success.	3
FA-2.6	Applicant provides a realistic approach to estimating the financial value of the technical assistance/services provided to their utilities and dedicates sufficient resources to successfully document the value of these services.	3

iii. Criterion 3: Implementation and Operations Plan (Maximum Points: 24)

Criterion Number		**Maximum Points**
FA-3.1	Applicant provides a realistic strategy for increasing the engagement of their Participating Utilities with cybersecurity threat information sharing programs that has high likelihood of success.	6
FA-3.2	Applicant demonstrates an understanding of the key considerations in selecting cybersecurity solutions based on prioritized risks, and describes a strategy for working with their Participating Utilities to evaluate existing and alternative solutions, and to ensure that their Participating Utilities invest in solutions focused on people, process, and technology.	6

FA-3.3	Applicant accurately identifies solutions that might be used by their Participating Utilities that will require participation from other utility staff to be successful, and describes a thoughtful, appropriate, and comprehensive approach to work with their utilities to develop and implement rollout plans that are highly likely to achieve buy-in from the relevant utility staff necessary for the success of the solutions.	3
FA-3.4	Applicant demonstrates an understanding of potential business and/or operational risks associated with new cybersecurity solutions and describes an appropriate approach to work with their Participating Utilities to manage the unique risks at each utility before solutions are implemented.	3
FA-3.5	Applicant describes relevant services and technical assistance they will provide to their Participating Utilities to help minimize third-party cybersecurity risks and describes a strong internal cybersecurity program that appropriately mitigates the risks they create as third-party a service provider to their Participating Utilities.	6

iv. Criterion 4: Commitment, Team, and Resources (Maximum Points: 27)

Criterion Number		**Maximum Points**
FA-4.1	Applicant describes an adequate level of staff resources dedicated to the project team. (Reviewers will consider the Applicant's Program Plan, Budget Justification, resumes, and the Leadership Letter of Commitment to Long-Term Success.)	3
FA-4.2	The internal organization roles and responsibilities are clearly defined, the roles and responsibilities of staff coordinating with the Participating Utilities are clearly defined, and the qualifications, expertise, and experience of key personnel and team members are appropriate for the proposed project and for managing a federal award. The applicant's POC has the appropriate skills and experience to handle project coordination.	3
FA-4.3	Applicant demonstrates a commitment to successful program management and communication by including all relevant technical and non-technical staff positions on the project team (e.g., operations, information technology (IT), engineering, leadership, management, finance, legal, communications, etc.) and providing appropriate training to support their project roles. (Reviewers will consider both Applicant's Program Plan, resumes, and the Budget Justification.)	3
FA-4.4	Applicant demonstrates a realistic understanding of the staff commitment needed from the Participating Utilities for the project to	6

	be successful, identifies other likely challenges to maintaining engagement with their Participating Utilities, and describes reasonable solutions to address these challenges.	
FA-4.5	Applicant demonstrates a realistic understanding of the additional and ongoing staff training necessary for their Participating Utilities to ensure policy and technical solutions maintain their effectiveness as the threat landscape changes, and describes how the applicant and the Participating Utilities will continue to support this training.	6
FA-4.6	Applicant provides a compelling and realistic plan describing how they will continue to finance and allocate needed staff to continue to provide technical assistance and services after the project funding ends.	6

v. Criterion 5: Community Benefits Plan (Maximum Points: 36)

Criterion Number		**Maximum Points**
FA-5.1	<u>Community and Labor Engagement</u> • Extent to which the applicant demonstrates community engagement to date that results in support for the proposed project; and • Extent to which the Applicant plans to communicate benefit of the project to service customers.	6
FA-5.2	• Extent to which the applicant thoughtfully demonstrates how they will benefit their local communities. This could include sharing the results of the project.	3
FA-5.3	<u>Job Quality and Workforce Continuity</u> • Quality and manner in which the proposed project will create and/or retain high quality, good-paying jobs with employer-sponsored benefits for both Applicant and sub-contractors; • Extent to which the project provides employees with the ability to organize, bargain collectively, and participate, through labor organizations of their choosing, in decisions that affect them and that contribute to the effective conduct of business and facilitates amicable settlements of any potential disputes between employees and employers, providing assurances of project efficiency, continuity, and multiple public benefits; and • Extent to which applicant demonstrates that they are a responsible employer.	6
FA-5.4	• Extent to which the applicant demonstrates a strong commitment to providing paid on-the-job training that will enable employees to improve their cybersecurity knowledge, skills, and abilities.	3

FA-5.5	<u>Diversity, Equity, Inclusion, and Accessibility</u> • Extent to which the Community Benefits Plan includes specific and high-quality actions to meet DEIA goals, which may include DEIA recruitment procedures, supplier diversity plans, and other DEIA initiatives; and • Quality of any partnerships and agreements with apprenticeship readiness programs, or community-based workforce training and support organizations serving workers facing systematic barriers to employment to facilitate participation in the project's construction and operations.	9
FA-5.6	<u>Justice40 Initiative</u> • Extent to which the Community Benefits Plan identifies: specific, measurable benefits for disadvantaged communities and how the benefits will flow to disadvantaged communities; and • Extent to which the project would contribute to meeting the objective that 40% of the benefits of climate and clean energy investments will flow to disadvantaged communities.	9

IX. Evaluation and Selection Process

A. Overview

The evaluation process consists of multiple phases; each includes an initial eligibility review and a thorough technical review. Rigorous technical reviews of eligible submissions are conducted by reviewers that are experts in the subject matter of the FOA. Ultimately, the Selection Official considers the recommendations of the reviewers, along with other considerations such as program policy factors, in determining which applications to select.

i. Standards for Application Evaluation

Applications that pass the compliance/responsiveness review will be subjected to a merit review in accordance with the Merit Review Criteria listed in the FOA and the guidance provided in the "Merit Review Guide for Financial Assistance and Unsolicited Proposals." This guide is available at https://www.energy.gov/management/downloads/merit-review-guide-financial-assistance-and-unsolicited-proposals-current.

ii. Selection

The Selection Official may consider the technical merit, the Federal Consensus Board's recommendations, program policy factors, and the amount of funds available in arriving at selections for this FOA.

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.

iv. Recipient Responsibility and Qualifications

DOE, prior to making a federal award with a total amount of federal share greater than the simplified acquisition threshold, is required to review and consider any responsibility and qualification information about the applicant that is in the entity information domain in SAM.gov (see 41 U.S.C. § 2313).

The applicant, at its option, may review information in the entity information domain in SAM.gov and comment on any information about itself that a federal awarding agency previously entered and is currently in the entity information domain in SAM.gov.

DOE will consider any written comments by the applicant, in addition to the other information in the entity information domain in SAM.gov, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 CFR 200.206.

B. Anticipated Notice of Selection and Award Negotiation Dates

DOE anticipates notifying applicants selected for negotiation of award and negotiating awards by the dates provided on the cover page of this FOA.