Office of Cybersecurity, Energy Security, and Emergency Response
Bipartisan Infrastructure Law Section 40124

Improving Cybersecurity Posture of Rural and Municipal Utilities
REQUEST FOR INFORMATION
DE-FOA-0002877, Amendment 000001

Amendment	Purpose
000001	Correct the submission hyperlink on page 16

ISSUE DATE: October 24, 2022
RESPONSES DUE: December 19, 2022 at 5:00 PM ET
SUBJECT: Request for Information (RFI)

SUBMIT TO: DE-FOA-0002877@NETL.DOE.GOV

Description

This is a Request for Information issued by the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response. The RFI is requesting public input to inform DOE's implementation of the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program, Section 40124 of the Infrastructure Investment and Jobs Act (IIJA), also commonly known as the Bipartisan Infrastructure Law (BIL).[1]

The goal of the RMUC Program is to enhance the security posture of rural, municipal, and small investor-owned electric utilities through investments in operational capabilities, services, technology deployments, and increased participation in threat intelligence information sharing programs. The intent of this RFI is to obtain public input to inform the scope and priorities of the RMUC Program, and to enable DOE to design opportunities that improve an eligible utility's cybersecurity posture.

Information collected from this RFI may be used by DOE for planning purposes, which could include developing future Funding Opportunity Announcements (FOA), Broad Agency

[1] Public Law 117-58 (November 15, 2021).

Announcements, or other solicitations related to implementation of the RMUC Program. The information collected in response to this RFI will not be published.

Background

Rural, municipal, and small investor-owned electric utilities play a critical role in providing safe, affordable, reliable energy to homes, businesses, and industries. In particular, cooperative and municipal electric utilities are not-for-profit entities dedicated to serving their local communities, elected and governed by their local communities, and instrumental in creating stronger local economies. The approximately 2,900 cooperative, municipal, and small investor-owned utilities are an important part of our nation's electric infrastructure, key partners in advancing the deployment and success of new energy resources on the distribution grid, and an essential component of our national defense as energy providers to many of our country's military installations.

More than 92% of the nation's persistent poverty counties are served by cooperative utilities,[2] and more than 80% of the approximately 2,000 municipal utilities serve less than 4,000 customers[3]. Access to cybersecurity talent and expertise is limited in the remote locations these utilities serve, the communications infrastructures they rely on can be inadequate to support the fast pace of digital technology innovations, and financial resources are constrained by the economies of their local communities.

On November 15, 2021, President Joseph R. Biden, Jr. signed the Bipartisan Infrastructure Law (BIL). The BIL is a once-in-a-generation investment in infrastructure, which provides the backbone for a more sustainable, resilient, and equitable economy through enhancing U.S. competitiveness in the world, diversifying regional economies to include supply chain and manufacturing industries, creating good union jobs, and ensuring stronger access to economic and other benefits for underserved and disadvantaged communities.

Section 40124 of the BIL addresses challenges faced by rural, municipal, and small investor-owned electric utilities and authorizes a program, the RMUC Program, under which DOE can provide grants and technical assistance and enter into cooperative agreements. The RMUC Program was created to enhance the security posture of electric utilities through improvements in their ability to protect against, detect, respond to, and recover from cybersecurity threats. The BIL appropriates $250 million over a 5-year period for the RMUC Program.

[2] National Rural Electric Cooperative Association, Electric Co-op Facts & Figures, April 2022
[3] American Public Power Association, 2022 Public Power Statistical Report

Eligible entities under the RMUC Program are:

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

In awarding grants and technical assistance under the RMUC Program, priority will be given to eligible entities that:

(A) have limited cybersecurity resources;
(B) own assets critical to the reliability of the bulk power system; or,
(C) own defense critical electric infrastructure (as defined in section 215A(a) of the Federal Power Act (16 U.S.C. 824o–1(a))).

Principles of equity and justice will guide implementation of the RMUC Program, consistent with the Biden Administration's commitments to ensure that overburdened, underserved, and underrepresented individuals and communities have access to federal resources pursuant to EO 13985, *Advancing Racial Equity and Support for Underserved Communities*; EO 14020, *Establishment of the White House Gender Policy Council*; and EO 14008, *Tackling the Climate Crisis at Home and Abroad*. Implementation efforts shall support the goal that 40% of the overall benefits of certain federal investments flow to disadvantaged communities (the Justice40 Initiative, or Justice40).[4] These investments should not exacerbate existing inequalities, including disproportionate exposure to environmental hazards and harms.

Purpose

The purpose of this RFI is to solicit feedback from a wide range of partners and professionals, including staff from the eligible entities (electric cooperatives, electric public utilities, small investor-owned utilities, and not-for-profits in partnership with electric cooperative and/or public utilities) and from representatives of the broader ecosystem of third parties and organizations that support and interact with these utilities.

[4] The Justice40 initiative, established by E.O. 14008, establishes the goal that 40% of the overall benefits of certain federal investments should flow to disadvantaged communities. DOE's definition of disadvantaged communities, which should be used to determine benefits calculations, is available at https://www.energy.gov/diversity/office-economic-impact-and-diversity.

This is a Request for Information (RFI) only. DOE will not pay for information provided under this RFI and no project will be supported as a result of this RFI. This RFI is not accepting applications for financial assistance or financial incentives. DOE may or may not issue a Funding Opportunity Announcement (FOA) based on consideration of the input received from this RFI.

DOE is specifically interested in comments providing insight into:

- The people, process, and technology challenges and barriers electric cooperatives, public utilities, and small investor-owned utilities (eligible utilities) face in improving their cybersecurity posture.
- How to enhance the ability of eligible utilities to protect against, detect, respond to, and recover from cybersecurity threats and incidents.
- How to increase the participation of eligible utilities in cybersecurity threat information sharing programs.
- How to design opportunities that provide both immediate benefits and the ability to continue to expand after BIL funding ends.
- Ideas for national scale initiatives where DOE can partner with private, not-for-profit, and public sector organizations to accelerate improvements in the ability of eligible utilities to protect against, detect, respond to, and recover from cybersecurity threats and incidents
- Opportunities for strengthening local and regional partnerships between eligible utilities and eligible not-for-profit entities with other private, not-for-profit, and public sector organizations, especially in the areas of cybersecurity incident preparedness and incident response, and cybersecurity technical assistance.

This is solely a request for information and not a funding opportunity. DOE is not accepting applications for funding.

For this RFI, DOE is requesting input on four categories. You are not required to answer questions in every category, and you may answer as few or as many of the questions within each category as you would like. Select those topic categories that are most relevant. The topic categories are:

Category 1. Key Challenges and Opportunities Facing Eligible Utilities

1. Prioritizing and Implementing Cybersecurity Best Practices
2. Increasing Participation in Threat Information Sharing Programs and Improving Cybersecurity Incident Preparedness and Incident Response
3. Managing Third Party Risks
4. Managing Cybersecurity Risks Associated with New Energy Technologies Being Deployed in Electric Distribution Systems
5. Cybersecurity Workforce Development, Training, and Culture

---

This is a Request for Information (RFI) only. DOE will not pay for information provided under this RFI and no project will be supported as a result of this RFI. This RFI is not accepting applications for financial assistance or financial incentives. DOE may or may not issue a Funding Opportunity Announcement (FOA) based on consideration of the input received from this RFI.

Category 2. Key Challenges and Opportunities for Utilities Serving Military Installations

Category 3. Partnerships with Manufacturers, Vendors, Service Providers, Public Agencies, Labor Unions, and Other Stakeholders

Category 4. Equity, Environmental and Energy Justice (EEEJ) in Identification of Potential Applicants, Application Process, Criteria for Selection, and Stakeholder Engagement

1. EEEJ in Identification of Potential Applicants
2. EEEJ in the Application Process
3. EEEJ in Criteria for Selection
4. EEEJ in Stakeholder Engagement

To the greatest extent possible please use the bolded Category numbers and sub-numbers for each question as headings in the body of your response (for example "Cat 1.1", "Cat 2.12a", etc.). This will help save time both for the responder and the reviewers to summarize the responses.

Category 1: Key Challenges and Opportunities Facing Eligible Utilities

Category 1.1: Prioritizing and Implementing Cybersecurity Best Practices

The RMUC Program will need to focus on investments that will provide the greatest security benefits to eligible utilities. Cybersecurity best practices could include practices focused on:

- People – for example, cybersecurity awareness training; recruitment, hiring and training a security workforce to implement and effectively utilize cybersecurity tools and technologies; addressing internal cultural silos; etc.;
- Processes – for example, cybersecurity assessments and penetration tests; policies and procedures to manage third-party risks during the selection and hiring of vendors or purchasing of equipment and devices; increasing senior leadership support or budgets; etc.; and,
- Technologies – updating existing technology; implementing technical mitigations for legacy technologies; purchasing new technology solutions like multifactor authentication or intrusion detection systems; analyzing and addressing system architecture vulnerabilities using solutions like network segmentation, creating demilitarized zones, or implementing zero trust practices; etc.

Cat 1.1a: What are the most important cybersecurity threats and risks eligible utilities face? What actions, products, resources, and/or services would help eligible utilities identify and understand these threats and risks?

Cat 1.1b: Given the current cybersecurity maturity levels of eligible utilities, of the three categories – people, processes, and technologies – investments in which category will provide the greatest impact on threat/risk reduction? Are there specific best practices that could provide the greatest impact on threat/risk reduction for these utilities?

Cat 1.1c: Describe the kinds of challenges and barriers eligible utilities currently face in understanding and/or implementing cybersecurity best practices to support people, processes, or technologies? Please be as specific as you can for each instance, realizing that each one might have different challenges and barriers.

Cat 1.1d: What are possible solutions for these challenges and barriers and what resources are needed to implement these solutions?

Cat 1.1e: The RMUC Program is interested in identifying solutions that can be maintained over the long term after federal funding ends. What program support factors focused on people, process, and technology best practices should be considered that will enable and facilitate sustainable solutions?

Category 1.2: Increasing Participation in Threat Information Sharing Programs and Improving Cybersecurity Incident Preparedness and Incident Response

The RMUC Program is exploring options to increase the participation of eligible utilities in cybersecurity threat information sharing programs and ways to help eligible utilities improve response capabilities before, during, and after an incident. Some of the common barriers that have been identified that limit organizations from participating in threat information sharing include but are not limited to:

- The cost structure for participation
- Staff knowledge, skills, and abilities to understand and identify what data should be collected for efficient analysis
- Staff knowledge, skills, and abilities to understand what data should be shared with which organizations and when
- A disconnect between the information shared and the utility's definition of actionable intelligence
- A disconnect between the information shared and the utility staff's knowledge, skills, and abilities to understand and effectively act on the information provided

---

This is a Request for Information (RFI) only. DOE will not pay for information provided under this RFI and no project will be supported as a result of this RFI. This RFI is not accepting applications for financial assistance or financial incentives. DOE may or may not issue a Funding Opportunity Announcement (FOA) based on consideration of the input received from this RFI.

- Clear and compelling information provided to utility decision makers that effectively motivates increased participation
- Mutually acceptable data sharing agreements, including challenges in finding options to maintain control of the data that is shared while ensuring the right data and context is preserved for threat detection
- Staff knowledge, skills, and abilities to understand and identify critical monitoring points within operational technology utility networks
- Access to secure, high-speed information sharing technical solutions (devices, systems, etc.)
- Inadequate interoperability between information sharing technology solutions and industry tools
- Utility workforce limitations

Cat 1.2a: Please identify which of the barriers listed above provide the biggest obstacles to the participation of eligible utilities in threat information sharing programs. What other barriers might be limiting participation by these utilities? Please explain how and why these barriers are limiting sharing by eligible utilities.

Cat 1.2b: How can the RMUC Program increase participation of eligible utilities in threat information sharing programs?

Cat 1.2c: What actions, products, resources, and/or services could cybersecurity threat information sharing programs provide that would increase the value eligible utilities would find in participating in these programs?

Cat 1.2d: What methods have been effective in helping eligible utilities understand their gaps and strengths in cybersecurity incident preparedness and incident response? How can the RMUC Program assist eligible utilities in improving their incident preparedness and response capabilities?

Cat 1.2e: What kinds of utility-level, local-level, state-level, regional-level, or federal-level cybersecurity exercises have you found useful as a participant or an observer?

Cat 1.2f: How can other not-for-profit, public, and private organizations help eligible utilities improve their incident preparedness and response capabilities?

Category 1.3: Managing Third-Party Risks

During the RMUC Program Listening Sessions, the following methods were discussed as options to manage third-party risks.

- Reliance on existing standards, regulations, and laws to ensure vendors and third parties understand and implement appropriate cybersecurity practices and controls.
- Using contracts, service level agreements, purchasing agreements, memorandums of understanding, and other legal vehicles to clarify cybersecurity responsibilities/liabilities and to manage third-party risks with vendors and partners.
- Using cybersecurity insurance and related insurance policies to mitigate third-party risks.
- Staff with advanced training that understand how to implement appropriate technical controls, and actively monitor third-party activities within networks to manage third-party cybersecurity risks.
- Implementing internal governance processes, such as policies limiting third party remote access to only certain times, to manage third-party cybersecurity risks.
- Help needed identifying, prioritizing, and/or implementing methods to manage third-party risks

Cat 1.3a: Are there other methods eligible utilities could use to manage third-party risks? What would you modify, add to, or delete from this list?

Cat 1.3b: What activities would most help eligible utilities improve their ability to identify and prioritize third-party risks? What activities would most help eligible utilities implement methods to manage third-party risks?

Cat 1.3c: In addition to the legal mechanisms listed above, are there other legal mechanisms available to utilities to manage third-party cybersecurity risks? How familiar are the legal professionals serving eligible utilities with the details on how to effectively use these legal methods to manage third-party risks? What resources would help legal professionals increase their expertise in using available legal methods to manage their client's third-party risks?

Category 1.4: Managing Cybersecurity Risks Associated with New Technologies Being Deployed in Electric Distribution Systems

Many eligible utilities for the RMUC Program are on the grid edge, where the deployment of new technologies is occurring behind the meter and on the distribution systems they own and operate. The digital attack surface is increasing rapidly as a result of many changes, including the exponential increase in behind the meter network connected technologies that affect generation and load, and increasing deployments of distribution scale technologies that include thousands of communication and control points. In addition, there are new energy supplier and service entities in the system that are not part of a utility but might impact the reliability and

operations of distribution systems. At the same time, cybersecurity attack tactics and threats to operational systems and assets are evolving.

Cat 1.4a: How can the RMUC Program help eligible utilities identify cybersecurity threats and risks resulting from changes happening on distribution systems?

Cat 1.4b: What are the challenges eligible utilities face in managing these new threats and risks? How do these challenges differ across the unique business models of the utilities (i.e., cooperative, public utility, or small investor-owned utility)?

Cat 1.4c: How can the RMUC Program help eligible utilities protect against, detect, respond to, and recover from cybersecurity incidents that might result from the rapid changes happening on their distribution systems?

Category 1.5: Cybersecurity Workforce Development, Training, and Culture

Input collected during the RMUC Listening Sessions indicated that workforce issues are one of the hardest challenges and top priorities for eligible utilities. Providing relevant training for existing employees and being able to recruit, hire, and retain new employees with the necessary knowledge, skills, and abilities were highlighted as challenges. Addressing cultural challenges in the workforce are also critical to the success of a utility's cybersecurity efforts. Two important position categories essential to building a cybersecurity culture within a utility are the operations and engineering staff. If the operators and engineers are not strong advocates for cybersecurity it will be difficult for a utility to implement operational technology (OT) cybersecurity best practices in the operational systems that are the most critical to protect.

Cat 1.5a: What existing cybersecurity workforce education and training efforts (e.g., apprenticeship programs, labor management training programs, community college or technical school programs, etc.) are most effective at preparing workers to address cybersecurity issues at eligible utilities? How can the RMUC Program support or augment these efforts?

Cat 1.5b: What are they key training gaps for cybersecurity? What types of training and what training topics would be the most useful to eligible utilities? What cybersecurity OT training options are currently available to eligible utilities?

Cat 1.5c: What actions would be most impactful to improve access to cybersecurity training for existing employees? What are the potential impacts additional training could have on eligible utilities?

Cat 1.5d: What are some of the barriers to increasing the interest of operators and engineers to promote OT cybersecurity within their utility? What methods have you seen that have been successful in developing a cybersecurity culture within the operations and engineering communities? Who are the organizations, vendors, consultants, labor unions, and stakeholders that have the most influence on whether operators or engineers in utilities support and implement OT cybersecurity best practices?

Cat 1.5e: What actions or resources would improve the ability of eligible utilities to hire and retain new employees with relevant cybersecurity knowledge, skills, and abilities? Who are possible partners in this effort?

The RMUC Program is interested in identifying potential national scale initiatives where DOE can partner with private, not-for-profit, and public sector organizations to accelerate the ability of staff in cooperative, municipal, and small investor-owned utilities to improve the cybersecurity posture in their utilities. These initiatives could address a wide range of objectives, from workforce development to hardening systems, and could include a variety of partners.

Cat 1.5f: What national-scale workforce initiatives could increase the pipeline of new employees with the relevant cybersecurity knowledge, skills, and abilities into eligible utilities? What national-scale initiatives could help eligible utilities recruit these employees? Who are possible partners in this effort?

Category 2: Key Challenges and Opportunities for Utilities Serving Military Installations

The RMUC Program recognizes the unique importance of eligible utilities serving military installations. DOE intends to develop specific programs to support the utilities that are essential energy providers for our national defense infrastructure.

Cat 2a: What unique cybersecurity challenges do eligible utilities serving military installations face? For example, are there any unique compliance or security requirements for eligible utilities serving military installations either at the customer's request or from another source? What activities or resources could help utilities serving military installations address those challenges?

Cat 2b: What, if any, proactive cybersecurity measures do eligible utilities currently undertake that are unique to their military customers? What types of support would enable eligible utilities serving military installations to implement additional proactive cybersecurity practices?

Cat 2c: What external non-project partners/stakeholders will be critical to the success of RMUC Program efforts with these utilities? What types of outreach and engagement strategies are needed to make sure these stakeholders are involved during each phase of the Program's implementation?

Cat 2d: What types of cross-cutting support (e.g., technical assistance) would be valuable from the DOE/national laboratories, from other federal agencies, and/or from regional, state, or local experts to provide in proposal development or project execution? What approaches would you recommend for providing services and technical assistance to eligible utilities serving military installations?

Category 3: Partnerships with Manufacturers, Vendors, Service Providers, Public Agencies, Labor Unions, and Other Stakeholders

Cat 3a: If you are an original equipment manufacturer (OEM) or a software development company, are there cybersecurity features and capabilities in your products that could be more effectively utilized by eligible utilities? What could the RMUC Program do to improve the ability and success of eligible utilities in maximizing the cybersecurity options in your products?

Cat 3b: If you are a product or software vendor, or distributor of assets, equipment, and devices used in electric utilities, have you observed any cybersecurity features and capabilities in the products you provide that could be more effectively utilized by eligible utilities? What could the RMUC Program do to improve the ability and success of eligible utilities to maximize the cybersecurity options in the products you provide?

Cat 3c: If you are a consulting, engineering, security, or other utility service provider, what are some of the cybersecurity challenges, risks, and opportunities you have observed when working with eligible utilities? What solutions would you recommend for these utilities to address those challenges? What could the RMUC Program do in partnership with your organization to help electric utility staff,

especially operations and engineering staff, become strong advocates for OT cybersecurity best practices?

Cat 3d: If you are part of a State, Local, Tribal, or Territorial (SLTT) entity, what could the RMUC Program do in partnership with your entity to help eligible utilities improve their cybersecurity posture?

Cat 3e: If you are aware of other public-private national partnership initiatives that have been successful in accelerating the cybersecurity progress of utilities or other critical infrastructure entities, would you describe these efforts and what made them successful, and identify who were the organizations leading these efforts?

Category 4: Equity, Environmental and Energy Justice (EEEJ) in Identification of Potential Applicants, Application Process, Criteria for Selection, and Stakeholder Engagement

Category 4.1: EEEJ in Identification of Potential Applicants

Equity is ensuring that traditionally underserved populations, such as utilities serving persons living in rural or remote areas, have access to programs and opportunities. As part of the Section 40124 language in the BIL authorizing the RMUC Program, DOE was instructed to "establish a process to ensure that all eligible entities are informed about and can become aware of opportunities to receive grants or technical assistance."

Cat 4.1a: How can the RMUC Program meet this goal? What are the most effective methods to reach the smaller utilities that have not historically participated in federal programs like the RMUC Program? What are the most effective methods to identify the not-for-profits in partnership with at least 6 cooperative and/or public utilities?

Category 4.2: EEEJ in the Application Process

Utility participants in the RMUC Program Listening Sessions provided input on what level of effort they thought their utility would be able to meet to compete for funding, services, or technical assistance from the RMUC Program. The most frequently identified options were:

- Can fill out a 3-page application or worksheet.
- Can conduct a self-evaluation on needs and priorities and develop a cybersecurity roadmap to support funding requests.
- Can receive federal reimbursements for incurred costs.

There was a 50% drop in the number of times the option "Can prepare a 5-10 page proposal" was selected compared with the number of times the option "Can fill out a 3-page application or worksheet" was selected. The option selected the least by the utility participants was "Can hire consultants to assist in developing a comprehensive assessment to identify priority focus areas to support funding requests."

The RMUC Program seeks input on the existing barriers eligible utilities face when accessing Federal resources and how the RMUC Program and address and/or mitigate these barriers.

Cat 4.2a: For those program opportunities that eligible utilities will apply for directly, how can the RMUC Program ensure that the administrative burden of the application process does not inhibit or prevent eligible utilities from applying to participate? What issues could negatively impact the ability of eligible utilities to participate? What documentation should the application process for these utilities require? How long should applicants have to apply?

Cat 4.2b: What issues could negatively impact the ability of not-for-profits in partnership with at least 6 cooperative and/or public utilities to apply? What can the RMUC Program do to mitigate these issues?

Cat 4.2c: What data should DOE collect from eligible utilities and other participants to evaluate the impact of the RMUC Program? How sensitive is this data and how should it be protected?

Category 4.3: EEEJ in Criteria for Selection

Utility participants in the RMUC Program Listening Sessions provided input on what criteria they thought should be used to prioritize applications in a competitive selection process. The most frequently identified criteria included:

- Critical infrastructure loads served by the system
- Cybersecurity maturity level of the utility
- Total number of staff and/or number of information technology/cybersecurity staff
- Service area, number of meters, or other measurement of the utility's size
- Risk of potential cyberattack
- Service area demographics
- Economic need of the utility

Cat 4.3a: In addition to the criteria listed above, what are key equity-aligned review criteria that the RMCU Program should use to evaluate and select program participants?

Cat 4.3b: Are there other regional and/or local factors that should be considered when selecting applications submitted by eligible utilities (e.g., economic considerations, policy considerations, labor-management partnerships, environmental and energy justice considerations, geography and geology, workforce availability and skills, industry partners, minority-serving institutions (MSIs), minority-owned businesses, regionally specific resources, security of supply, climate risk, etc.)?

Cat 4.3c: What key review criteria should be used by the RMUC Program when evaluating and selecting applications submitted by the not-for-profits in partnership with at least 6 cooperative and/or public utilities, as well as when evaluating the readiness of the not-for-profit applicants to move from one phase to the next (e.g., technical merit, workplan, market transformation plan, team and resources, financial, regional economic and community benefits, quality jobs, workforce training strategies, environmental justice, diversity, equity, inclusion, etc.)?

Cat 4.3d: Please provide input on how the Justice40 policy priorities can be achieved through the RMUC Program to support the goal that 40% of the overall benefits from certain federal investments flow to disadvantaged communities and maximize implementation co-benefits.

Category 4.4: EEEJ in Stakeholder Engagement

The potential impact of the RMUC Program will be influenced by the participation of the broader cybersecurity stakeholder community supporting eligible utilities. Category 3 above specifically identifies potential partners that will be needed for these utility staff to continue to make progress improving the cybersecurity posture of their utilities after the federal funding ends.

Cat 4.4a: What equity, energy and environmental justice concerns or priorities are most relevant to eligible utilities and the partners that support these utilities that could impact the success of the RMUC Program?

Cat 4.4b: What external non-funded partners/stakeholders will be critical to the future success of the RMUC Program's efforts? What types of outreach and engagement strategies are needed to make sure these stakeholders are involved during each phase of the RMUC Program?

Cat 4.4c: What types of support (e.g., technical assistance) would be valuable from the DOE/national laboratories, from other federal agencies, and/or from regional, state, or local experts to advance the RMUC Program's goals and initiatives?

Cat 4.4d: Who are other not-for-profit entities DOE could fund to provide technical assistance to eligible utilities?

Cat 4.4e: How can the RMUC Program ensure relevant community-based stakeholders and organizations are engaged and included in the planning, decision-making, and implementation processes?

Cat 4.4f: How could funding under other DOE BIL provisions (Bipartisan Infrastructure Law Programs at Department of Energy) be leveraged to maximum the impact of RMUC Program goals and objectives?

Disclaimer and Important Notes

This RFI is not a Funding Opportunity Announcement (FOA); therefore, DOE is not accepting funding applications at this time. DOE may issue a FOA in the future based on or related to the content and responses to this RFI; however, DOE may also elect not to issue a FOA. There is no guarantee that a FOA will be issued as a result of this RFI. Responding to this RFI does not provide any advantage or disadvantage to potential applicants if DOE chooses to issue a FOA regarding the subject matter. Final details, including the anticipated award size, quantity, and timing of DOE-funded awards, will be subject to Congressional appropriations and direction.

Any information obtained as a result of this RFI is intended to be used by the Government on a non-attribution basis for planning and strategy development; this RFI does not constitute a formal solicitation for proposals or abstracts. Your response to this notice will be treated as information only. DOE will review and consider all responses in its formulation of program strategies for the identified materials of interest that are the subject of this request. DOE will not provide reimbursement for costs incurred in responding to this RFI. Respondents are advised that DOE is under no obligation to acknowledge receipt of the information received or provide feedback to respondents with respect to any information submitted under this RFI. Responses to this RFI do not bind DOE to any further actions related to this topic.

This is a Request for Information (RFI) only. DOE will not pay for information provided under this RFI and no project will be supported as a result of this RFI. This RFI is not accepting applications for financial assistance or financial incentives. DOE may or may not issue a Funding Opportunity Announcement (FOA) based on consideration of the input received from this RFI.

Freedom of Information Act

Pursuant to 10 CFR 1004.11, any person submitting information that he or she believes to be confidential and exempt by law from public disclosure should submit via email two well-marked copies: one copy of the document marked "confidential" including all the information believed to be confidential, and one copy of the document marked "non-confidential" with the information believed to be confidential deleted. Submit these documents via email. DOE will make its own determination about the confidential status of the information and treat it according to its determination. Because information received in response to this RFI may be used to structure future programs and funding opportunity announcements and/or otherwise be made available to the public, **respondents are strongly advised to NOT include any information in their responses that might be considered business sensitive (e.g., commercial or financial information that is privileged or confidential), trade secrets, proprietary, or otherwise confidential**.

Request for Information Response Guidelines

Responses to this RFI must be submitted electronically to DE-FOA-0002877@NETL.DOE.GOV no later than 5:00pm (ET) on **December 19, 2022**. Responses must be provided as attachments to an email. It is recommended that attachments with file sizes exceeding 25MB be compressed (i.e., zipped) to ensure message delivery. Responses must be provided as a Microsoft Word (.docx) or PDF attachment to the email, and no more than 15 pages in length, 12-point font, 1-inch margins. Only electronic responses will be accepted.

For ease of replying and to aid categorization of your responses, **please copy and paste the RFI questions, including the question numbering, and use them as a template for your response.** Respondents may answer as many or as few questions as they wish and may delete unanswered questions.

DOE will not respond to individual submissions or publish publicly a compendium of responses. A response to this RFI will not be viewed as a binding commitment to develop or pursue the project or ideas discussed.

Respondents are requested to provide the following information at the start of their response to this RFI:

1. Contact person's first and last name
2. Contract person's title
3. Contact person's organization / institution name, street address, city, state, and zip code

---

This is a Request for Information (RFI) only. DOE will not pay for information provided under this RFI and no project will be supported as a result of this RFI. This RFI is not accepting applications for financial assistance or financial incentives. DOE may or may not issue a Funding Opportunity Announcement (FOA) based on consideration of the input received from this RFI.

4. Contact person's phone number and e-mail address
5. Which organization type best categorizes your organization? If your organization provides more than one service, please identify all that apply.
    a. Electric cooperative utility
    b. Electric municipal/public power utility
    c. Small investor-owned electric utility (<4,000,000 megawatt hours electricity sales per year)
    d. Other investor-owned electric utility
    e. Other energy provider (solar, wind, hydropower, etc.)
    f. Not-for-profit that is not an electric utility owner/operator
    g. State, Local, Territorial, or Tribal government or commission
    h. Security service provider
    i. Consultant, integrator, engineering services, or other non-security service provider
    j. Equipment manufacturer, software company, or vendor
    k. Research community (e.g., academia, national laboratory, non-profit R&D, etc.)
    l. Legal professional
    m. Cybersecurity training community
    n. Incident response/incident preparedness community
    o. Military installation or facility
    p. Other Stakeholder – please specify
6. If you are from an electric utility, does your utility share any of its digital or communications network and infrastructure with any of the following other types of utilities or services? Please identify all that apply.
    a. Drinking water
    b. Wastewater treatment
    c. Gas
    d. Broadband
    e. Telephone service other than broadband
    f. Solar
    g. Wind
    h. Storage
    i. Hydropower
    j. Electric vehicle charging stations
    k. None of the above
    l. Other – please specify

7. If you are interested in applying for funding or services from the RMUC Program, which of the following RMUC Program categories would best fit your organization? Include all that apply.
    a. Utility with limited cybersecurity resources
    b. Utility that owns assets critical to the reliability of the bulk power system
    c. Utility that serves a military installation
    d. Not-for-profit in partnership with at least six (6) electric cooperative and/or public power utilities
    e. None of the above