9/29/22 RMUC Listening Session Questions

Thank you for participating in the Department of Energy September 29th RMUC Listening Session.

Based on your feedback from the first Listening Session, we are providing this survey after the call to give you an opportunity to respond at your own pace. Please be sure to **complete the survey by Saturday, October 8, 2022 2:59 AM ET.**

The information gathered in this short survey will help us ensure we are developing and designing a program that meets investment needs throughout rural, municipal, and small investor-owned utilities that have limited cybersecurity resources, are critical to the reliability of the bulk-power system, and/or those that serve military installations including those who own defense critical electric infrastructure.

Thank you for your time and your valuable input to this process.

If you have questions - please contact CESER.RMUC@hq.doe.gov.

OMB Control Number: 1910-5160 Paperwork Reduction Act Burden Disclosure Statement

This data is being collected to get feedback from the public on the RMUC program. The data you supply will be used for understanding ways we can improve our customers experience (i.e. better communication, new processes, etc.). Public reporting burden for this collection of information is estimated to average 5-8 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of the Chief Information Officer, Enterprise Policy Development & Implementation Office, IM-22, Information Collection Management Program (1910-5160), U.S. Department of Energy, 1000 Independence Ave SW, Washington, DC 20585; and to the Office of Management and Budget (OMB), OIRA, Paperwork Reduction Project (1910-5160), Washington, DC 20503. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB control number. Submission of this data is voluntary.

* Required

Demographics

1. Please identify the type of organization where you are currently employeed *

- ◯ Electric utility owner/operator
- ◯ Not-for-profit that is not an electric utility owner/operator
- ◯ State, Local, Territorial, or Tribal government or commission
- ◯ Security service provider
- ◯ Consulting, integrator, engineering services, and other non-security service provider
- ◯ Equipment manufacturer, software company, vendor
- ◯ Research community (e.g., academia, national lab, non-profit R&D, etc.)
- ◯ Cybersecurity education/training community
- ◯ Legal professional
- ◯ Federal government
- ◯ Other

2. Which of the following best describes your organization? (select one) *

- ◯ Rural electric cooperative utility
- ◯ Municipally owned electric utility
- ◯ Investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year
- ◯ Other

3. How many employees do you have in your utility? *

- ◯ 10 or fewer employees
- ◯ 11-30 employees
- ◯ 31-60 employees
- ◯ More than 60 employees

4. Which of the following best describes your organization's role(s) in the grid? (select all that apply) *

- [ ] Distribution utility (asset owner/operator)
- [ ] Generation utility (asset owner/operator)
- [ ] Transmission utility (asset owner/operator)
- [ ] Generation utility (non-asset owner/operator)
- [ ] Transmission utility (non-asset owner/operator)
- [ ] Renewable energy asset owner/operator generation provider
- [ ] Internet service or other communications technology provider
- [ ] Other

5. Does your utility share any of its digital or communications network and infrastructure with any of the following other types of utilities or energy services? (select all that apply) *

- ◯ Drinking water
- ◯ Wastewater treatment
- ◯ Gas
- ◯ Broadband
- ◯ Telephone service other than broadband
- ◯ Solar
- ◯ Wind
- ◯ Storage
- ◯ Hydropower
- ◯ Electric vehicle charging stations
- ◯ None of the above
- ◯ Other

6. Which of the following potential RMUC Program eligibility categories would fit your organization? (select all that apply) *

- [ ] Utility with limited cybersecurity resources
- [ ] Utility that owns assets critical to the reliability of the bulk power system
- [ ] Utility that serves a military installation
- [ ] None of the above

7. Please identify your role within the organization where you are currently employed. *

- ◯ Information Technology, Information Services
- ◯ Cybersecurity
- ◯ Technology, Technical Systems, Technology Services
- ◯ Engineering, Operations, Industrial Control Systems
- ◯ General Manager, President, CEO, Executive Director, Board of Directors
- ◯ Commissioner or Commission Staff, Regulatory Affairs, Compliance, Auditing
- ◯ Finance, Economist, Economic Development
- ◯ Legal Professional
- ◯ Policy, Government Relations
- ◯ Other

Help Design the Program

8. *Criteria for Defining "Critical"*
   The following criteria were suggested for the RMUC Program to use in defining whether a potential eligible utility played a 'critical' role in the reliability of the bulk power system.

   Select the criteria from this list that you think the RMUC Program should prioritize. If there are any criteria you think should be considered that are missing from this list, please enter them under the other category. (select all that apply)
   *

- [ ] Impact to service territory if a breach occurred
- [ ] Whether service territory includes government entities, military installations, first responders, critical customers
- [ ] Footprint, number of meters/members/customers impacted
- [ ] Demographics of service territory (population size, density, underserved regions, high risk regions, etc.)
- [ ] Role of the utility in the bulk power system and potential impacts to grid
- [ ] Any asset under NERC CIP Low/Medium/High
- [ ] Does not apply. We do not own assets critical to the reliability of the bulk power system.
- [ ] Other

9. *Criteria for Prioritizing Funding*

The following criteria were suggested for the RMUC Program to use in prioritizing funding applications.

Select the criteria from this list that you think the RMUC Program should consider? If there are any criteria you think should be considered that are missing from this list, please enter them under the other category. (select all that apply)

- [ ] Cybersecurity maturity level of the utility
- [ ] Demographics of community served by the utility
- [ ] Economic need of the utility
- [ ] Number of staff and/or whether the utility has staff with information technology and/or cybersecurity skills
- [ ] Size of the utility based on meters, customers, or other metrics
- [ ] Utility plays a critical role in community and/or grid reliability
- [ ] What risk level does the utility face from cybersecurity threats
- [ ] Whether the utility is a distribution, generation, or transmission utility
- [ ] Other

10. *Who are your trusted partners for cybersecurity advice, training, and services?*

The RMUC Program is allowed to provide funding to not-for-profits in partnership with 6 or more cooperative and/or municipal utilities. Below is a partial list of potential partners.

What not-for-profit organizations would your utility consider working with as a potential partner? (select all that apply)
*

- [ ] American Public Power Association (APPA)
- [ ] Joint Action Agency
- [ ] Hometown Connections
- [ ] State and Regional Associations
- [ ] Large Public Power Council
- [ ] Utilities Technology Council (UTC) Foundation
- [ ] Western Energy Institute
- [ ] CoBank
- [ ] National Rural Utilities Cooperative Finance Corporation (CFC)
- [ ] National Information Solutions Cooperative (NISC)
- [ ] Meridian Cooperative (fka SEDC)
- [ ] NRTC
- [ ] Federated Rural Electric Insurance Exchange
- [ ] National Rural Electric Cooperative Association (NRECA)
- [ ] Electric Power Research Institute (EPRI)
- [ ] Other

Best Practices

The following cybersecurity best practices were identified as either the most urgent to implement or the hardest to implement.

11. Select five best practices from this list that you think eligible utilities need help implementing that might benefit from RMUC Program investments. If you think there is a best practice that should be on this list that is missing, please add it under "Other". (PLEASE LIMIT SELECTIONS TO **FIVE (5)**)

- [ ] Asset inventory
- [ ] Culture
- [ ] Cybersecurity training for staff
- [ ] Incident response capabilities
- [ ] Information sharing
- [ ] Intrusion Detection System (IDS)
- [ ] Legacy technology
- [ ] Monitoring
- [ ] Multifactor authentication (MFA)
- [ ] Network segmentation
- [ ] Physical security
- [ ] Policy, governance, planning, procedures -> process issues
- [ ] Secure backups
- [ ] Technology generally
- [ ] Threat hunting
- [ ] Up-to-date firewall
- [ ] Vulnerability management
- [ ] Workforce (recruiting, hiring and retaining)
- [ ] Zero Trust
- [ ] Other

Challenges

12. Are you facing any of the challenges below in your efforts to improve your utility's cybersecurity? (select all that apply)

- [ ] Knowing where to start
- [ ] Evaluating and selecting appropriate solutions
- [ ] Access to appropriate solutions and technology
- [ ] Access to funding
- [ ] Support from senior leadership
- [ ] Governance and/or regulatory hurdles or barriers
- [ ] Access to appropriate training for current employees
- [ ] Access to/retention of new employees with the necessary knowledge, skills, and abilities
- [ ] Access to consulting and other technical assistance services
- [ ] Other

Where would you prioritize funding?

13. From the list of actions below, what are your top five spending priorities to improve the cybersecurity posture of your utility? Assume a world where all options are possible. (PLEASE LIMIT SELECTIONS TO **FIVE (5)**)

- [ ] Hiring new staff with appropriate knowledge, skills, and abilities
- [ ] Taining to increase the knowledge, skills, and abilities of existing staff
- [ ] Contracts with trusted accessible technical assistance providers to supplement staff knowledge, skills, and abilities
- [ ] Effective methods to address cultural challenges (staff resistance, internal silos and tensions between departments, etc.)
- [ ] Implementing personnel and staff cybersecurity best practices
- [ ] Assessments (policy, technical, cybersecurity, etc.) to help identify gaps and develop roadmaps/strategies for improvements
- [ ] Actionable threat intelligence
- [ ] Effective methods to manage third party and supply chain risks
- [ ] Effective methods to increase senior leadership support
- [ ] Effective methods to secure more funding (internal budgeting, federal/state grants, etc.)
- [ ] Implementing governance cybersecurity best practices
- [ ] Upgrading existing technology, digital infrastructure, software, etc.
- [ ] Purchasing new technology, digital infrastructure, software, etc.
- [ ] Effective methods to assess, verify, and validate technology solutions and options
- [ ] Implementing technical cybersecurity best practices
- [ ] Other

Training

The RMUC Program will be exploring information technology (IT) and cybersecurity (CS) training options. There are many training programs and classes currently offered or that could be created to fill a gap.

14. What types of training would be most useful for you and/or your organization? PLEASE SELECT **FOUR (4)**).

- [ ] Technical IT and/or CS skills training in specific areas
- [ ] General cybersecurity skills training
- [ ] Cybersecurity awareness training
- [ ] Cybersecurity incident preparedness and response training
- [ ] Training for senior leadership or governing bodies
- [ ] Other utility role specific training for operations staff, engineers, human resources, finance, administrative support roles, purchasing, legal professionals, etc.
- [ ] We need help understanding what training topics would be most useful to our utility.
- [ ] Other

15. What are the challenges that limit staff from attending information technology and cybersecurity training opportunities? (select all that apply)

- [ ] Multiple job responsibilities that are hard to back-fill with remaining staff
- [ ] Insufficient funding available for training
- [ ] Insufficient time available to complete training
- [ ] Limited leadership support to prioritize this type of training
- [ ] Insufficient training opportunities offered in the local community or region
- [ ] Difficulty assessing and prioritizing which of the many training options would be most appropriate
- [ ] Limited awareness of relevant training opportunities
- [ ] Other

Third-Party Cybersecurity Risks

16. Who manages third-party cybersecurity risks in your organization? (select all that apply)

- [ ] Our attorney and/or our legal professionals
- [ ] Board of Directors, City Council, or other governing body
- [ ] CEO, General Manager, Director, City Manager, Mayor
- [ ] Individual staff members responsible for purchasing decisions
- [ ] Procurement office
- [ ] Individual staff members working with the third party
- [ ] Finance and billing staff
- [ ] Other

Incident Preparedness and Incident Response (IP/IR)

Cybersecurity incident preparedness (IP) and incident response (IR) are important capabilities that improve with practice. There are many potential ways the RMUC Program can support improvements in a utility's IP/IR capabilities.

17. Which of the following options would be useful to your utility? (select all that apply)

- [ ] Increased opportunities to participate in existing cybersecurity exercises occurring at a local, regional, and/or national level
- [ ] Supporting discussion-based exercises like tabletops and workshops
- [ ] Supporting operational-based exercises like drills and simulated, realistic, real-time exercises
- [ ] Skills training in IP and IR
- [ ] Supporting initiatives to strengthen relationships between cooperatives to provide cybersecurity advice and/or assistance
- [ ] Supporting initiatives to strengthen relationships between cooperatives and other IP/IR stakeholders in their communities (e.g. Information Sharing and Analysis Centers (ISACs), FBI, Department of Homeland Security, National Guard, State and local cybersecurity responders, etc.)
- [ ] We need help understanding how to best utilize these options to improve our IP/IR capabilities.
- [ ] Other

Communities of Practice

Communities of practice are an effective method to share knowledge, insights, and lessons learned.

18. How can the RMUC Program encourage and foster cybersecurity communities of practice within the municipal and small investor-owned utility communities? (select all that apply)

- [ ] Topic-based working groups to explore solutions relevant to the municipal or small investor-owned utility communities
- [ ] Peer-to-peer workshops, meetings, and conferences
- [ ] Resource hubs to share best practices, information, resources, and contacts
- [ ] Communications networks and infrastructure to accelerate peer-to-peer information sharing
- [ ] Other

Additional Comments

19. Are there any other suggestions or comments you would like to contribute?