Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) 1 Prize

APRIL 2024

Preface

The U.S. Department of Energy's (DOE) Advanced Cybersecurity Technology (ACT) 1 Prize will be governed by 15 U.S.C. §3719 and this Official Rules document. This is not a procurement under the Federal Acquisitions Regulations and will not result in a grant or cooperative agreement under 2 CFR 200. The Prize Administrator reserves the right to modify this Official Rules document if necessary and will publicly post any such notifications as well as notify registered prize participants.

Date	Modification
10/23/2023	The Program Summary Introduction has been modified on page 5 to include a reference to the objectives of the RMUC Program in the Infrastructure Investment and Jobs Act (IIJA) §40124 (Public Law 117-58). The Commitment Criterion 2: Initial Goals, Expected Outcomes, and Impacts on Utility section has been updated on page 19 to include a reference to the objectives of the RMUC Program.
03/22/2024	The cash awards for Phase 2: Planning and Phase 3: Implementation have been changed. All winners in the Planning Phase will receive $100,000 in cash, and all winners in the Implementation Phase will receive $50,000 in cash. Table 1 on page 6 has been updated, and these changes have been made throughout the document. The hours of technical assistance (TA) for winners in the Limited Cybersecurity Resources Track have been changed. All Limited Cybersecurity Resources winners in Phase 1: Commitment will receive up to 80 hours of TA, and all Limited Cybersecurity Resources Track winners in Phase 2: Planning will receive up to 40 hours of TA. Table 1 on page 6 has been updated, and these changes have been made throughout the document. The date for "Winners Announced and Awards" for Phase 1: Commitment in the Key Dates table on page 7 has been updated to March 28, 2024, and the "(anticipated)" annotation has been deleted. The date for "Submission Opens" for Phase 2: Planning in the Key Dates table on page 7 has been updated to April 2024. The Timeline graphic on page 7 has been updated to reflect this change.
04/18/24	Edits have been made to Phase 2: Planning and Phase 3: Implementation.
04/22/24	Edits have been made to: • Narrative Topic 6: Section 40126 Cybersecurity Plan on page 27 • Section 2.3.6 Project Team Information Forms on page 30, and • Planning Criteria 4: Institutionalizing a Culture of Continuous Improvement on page 33.

Contents

Program Summary

Introduction

The goal of the Advanced Cybersecurity Technology[1] (ACT) 1 Prize Program is to improve the ability of eligible utilities to protect against, detect, respond to, and recover from cybersecurity threats. The ACT 1 Prize Program is supported by the Rural and Municipal Utility Cybersecurity (RMUC) Program led by the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response.

The ACT 1 Prize Program will award up to $7.25 million in cash prizes and up to $1.71 million in technical assistance (TA) for a total of up to $8.96 million in prizes.

ACT 1 cash prizes will be available to eligible utilities to incentivize meaningful, impactful investments in cybersecurity technologies "to deploy advanced cybersecurity technologies for electric utility systems"[2] and to support training to increase the knowledge, skills, and abilities of utility staff. Successful competitors to this prize competition will propose and complete work implementing solutions that address cybersecurity risks. In partnership with qualified cybersecurity TA professionals, ACT 1 Prize winners will:

What is a prize competition? A prize competition incentivizes competitors, typically via cash awards, to achieve objectives set by the sponsoring agency. Funding is provided to winners for work that has already been performed. Once a prize is awarded, winners determine how best to use the funds, with no further commitments.

- Develop network architectures of their digital systems to identify and prioritize where interventions might be most effective
- Assess current cybersecurity technical stacks for gaps, duplication of functions, and opportunities to fully use existing capabilities
- Create cybersecurity plans and roadmaps to improve their cybersecurity posture
- Identify solutions that can be operated and maintained by existing staff and budgets
- Develop budgets, cost projections, and purchasing plans to minimize third-party risks when selecting solutions
- Implement solutions
- Develop and implement processes to ensure solutions are installed securely and perform as intended.

The ACT 1 Prize Program will prioritize utilities eligible to participate in the RMUC Program that have limited cybersecurity resources or serve military installations. Utilities are strongly encouraged to apply if they: (1) have limited economic and staff resources; (2) have limited access to cybersecurity training, TA, and support services; and (3) have a low cybersecurity maturity level. Utilities that serve military

[1] The Infrastructure Investment and Jobs Act (IIJA) §40124 (Public Law 117-58) defines the term "advanced cybersecurity technology" as any technology, operational capability, or service, including computer hardware, software, or a related asset, that enhances the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat (as defined in Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)).

[2] The Infrastructure Investment and Jobs Act (IIJA) §40124 (Public Law 117-58) outlines the objectives of the program: "(1) to deploy advanced cybersecurity technologies for electric utility systems; and (2) to increase the participation of eligible entities in cybersecurity threat information sharing programs."

installations are also strongly encouraged to apply. The Office of Cybersecurity, Energy Security, and Emergency Response intends to offer a series of ACT Prize competitions to further support additional utilities with limited cybersecurity resources and utilities serving military installations.

Utilities with mature cybersecurity programs are unlikely to win prizes under this competition unless they own or operate electric infrastructure that serves military installations. The Office of Cybersecurity, Energy Security, and Emergency Response intends to issue a competitive funding opportunity announcement that will support eligible RMUC Program utilities with more mature cybersecurity programs and not-for-profit entities in partnership with eligible utilities.

The ACT 1 Prize Program has three consecutive phases:

Phase 1. Commitment: Utilities describe their resources, need for improving their cybersecurity posture, and commitment to participating in the ACT 1 Prize Program.
Phase 2. Planning: Utilities work with TA professionals to complete technical assessments of their systems; identify areas where training would improve staff skills and abilities; gain a better understanding of potential risks and solutions; identify solutions to address prioritized risks; and draft a roadmap for implementation.
Phase 3. Implementation: Utilities make substantial progress toward completing their roadmap.

Winners in the first phase, the Commitment Phase, will receive a cash prize of $50,000 and up to either 80 or 120 hours of TA. **Table 1** shows all three phases, the maximum number of prize winners, and the maximum cash and TA prizes for each phase. The ACT 1 Prize Program has two tracks, LIMITED CYBERSECURITY RESOURCES and MILITARY. The goals and cash prizes for the two tracks are the same. The difference between the two tracks is utilities serving military installations in the MILTARY track are eligible to receive additional specialized TA.

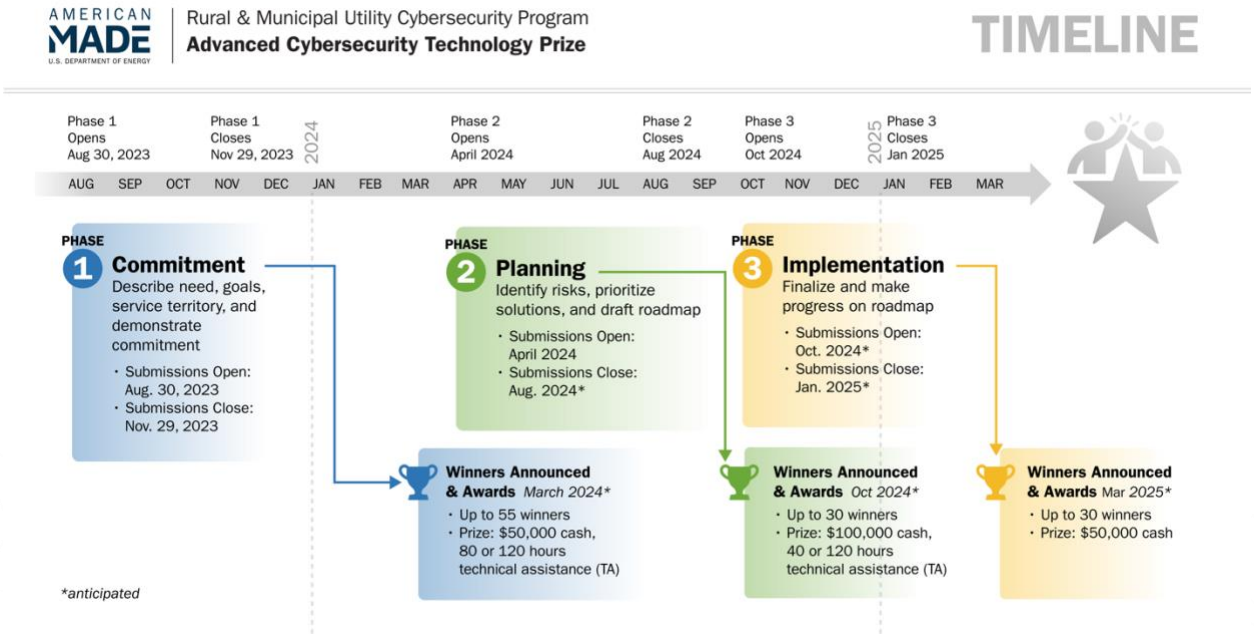
Each phase has a separate application process and different deadlines. All instructions for the first phase, Commitment, are contained within the first 20 pages of this document and the Appendix. If you decide to compete for a Planning Prize (Phase 2) and an Implementation Prize (Phase 3), see Sections 2 (Planning Phase) and 3 (Implementation Phase) for application instructions and deadlines.

Table 1. RMUC Program ACT 1 Prize Cash and TA

Phase	LIMITED CYBERSECURITY RESOURCES Track	MILITARY Track
Commitment	• $50,000 • Up to 80 hours of TA • Up to 50 winners.	• $50,000 • Up to 120 hours of TA • Up to 5 winners.
Planning	• $100,000 • Up to 40 hours of TA • Up to 25 winners.	• $100,000 • Up to 120 hours of TA • Up to 5 winners.
Implementation	• $50,000 • Up to 25 winners.	• $50,000 • Up to 5 winners.

Key Dates

Phase	Dates and Milestones
Phase 1: **Commitment**	• Submission opens: August 30, 2023 • Submission closes: November 29, 2023 (5 p.m. ET) • Winners announced and awards: March 28, 2024.
Phase 2: **Planning**	• Submission opens: April 19, 2024 (anticipated) • Submission closes: August 2024 (anticipated) • Winners announced and awards: October 2024 (anticipated).
Phase 3: **Implementation**	• Submission opens: October 2024 (anticipated) • Submission closes: January 2025 (anticipated) • Winners announced and awards: March 2025 (anticipated).



ACT 1 Prize Program Goals

The ACT 1 Prize Program offers a total prize pool of up to $7.25 million in cash and up to $1.71 million in TA across three phases—Commitment, Planning, and Implementation—where each phase concludes with a prize award.

Successful utilities in the ACT 1 Prize Program competition will identify cybersecurity risks, identify solutions that reduce or eliminate those risks, and implement selected solutions. Work completed by these utilities should accomplish one or more of the following goals:

- Increase a utility's ability to identify cybersecurity threats within their information technology (IT) and operational technology (OT) systems

- Improve a utility's ability to protect against cybersecurity threats
- Improve a utility's ability to detect cybersecurity events and incidents soon after they occur
- Prepare a utility to respond to and mitigate damage from a cybersecurity incident rapidly and effectively
- Recover from a cybersecurity incident and identify and implement process improvements.

Phase 1: Commitment. Competitors will describe their utility's need for assistance, the communities they serve, and their commitment to improving their utility's cybersecurity posture. Up to 50 limited cybersecurity resource utilities and 5 utilities serving military installations that most successfully describe and demonstrate their cybersecurity needs, capacity to work with TA professionals, and leadership commitment to the Program will be selected to win a Commitment Prize. Only utilities that have won a Commitment Prize are eligible to enter the Planning Phase and compete for a Planning Prize.

Phase 2: Planning. Up to 25 utilities in the limited cybersecurity resources track and up to 5 utilities serving military installations will win Planning Prizes. During this phase, utilities will demonstrate that they have a better understanding of their systems and cybersecurity risks, prioritize where system hardening improvements could be made, identify potential solutions, identify relevant cybersecurity training options, and draft a roadmap for implementing technical and training solutions. Competitors will be expected to complete assessments, provide justifications for proposed solutions, and develop estimated budgets for implementation of their roadmaps. In addition, competitors will draft a Section 40126 Cybersecurity Plan.[3] Only winners of a Planning Prize will be eligible to compete in the Implementation Phase.

Phase 3: Implementation. Up to 25 utilities from the limited cybersecurity resources track and up to 5 from the military track will win Implementation Prizes. The goal of the Implementation Phase is for utilities to begin implementing the solutions proposed in the Planning Phase. Activities in the Implementation Phase might include but are not limited to receiving training necessary to install, operate, and maintain the proposed cybersecurity solutions; developing and negotiating contracts; purchasing and installing hardware, software, firmware, and IT and/or OT equipment or components to support cybersecurity goals; purchasing and implementing licenses or subscriptions for a security solution; and developing processes to confirm the security of deployed solutions after implementation. Success in the Implementation Phase will be based on the progress each utility made in implementing their solutions.

Many utilities serving rural America are in areas of the country with limited economic opportunities and financial resources. The RMUC Program, as one of the Justice40[4] programs, is committed to ensuring that overburdened, underserved, and underrepresented communities have equitable access to federal

---

[3] Section 40126 of the IIJA provides a framework for ensuring that DOE's investments in energy sector research and infrastructure are secure and resilient from cybersecurity threats and requires all relevant IIJA provisions to have cybersecurity plans. DOE developed three cybersecurity plan templates—one for high-risk projects, one for medium-risk projects, and one for low-risk projects—to streamline the development and review of Section 40126 Cybersecurity Plans.

[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. Pursuant to E.O. 14008 and the Office of Management and Budget's Interim Justice40 Implementation Guidance M-21-28 and M-23-09 (whitehouse.gov), 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.

resources and receive benefits from federal investments. Utilities that compete for an ACT 1 Prize must demonstrate a commitment to serving the disadvantaged communities[5] in their service territory.

Overview of Prize Submission, Assessment, and Announcement Process

All utilities interested in competing in the ACT 1 Prize Program will need to create an account using the HeroX website and then submit required materials to that account. Each utility will be responsible for uploading all required materials into HeroX before the deadline associated with each of the ACT 1 Prize phases.

HeroX is a web-based platform that is used to manage the American-Made Challenge Prizes sponsored by DOE. Questions about HeroX can be posted to the Forum tab on the HeroX platform, and the Prize Administrator will respond.

1. **Submission**: Utilities assemble all required documents for each phase of the ACT 1 Prize into a submission package and upload their submission package to HeroX by the phase deadline.

2. **Assessment:** The Prize Administrator screens submissions for eligibility, confirms that all required documents are included in the submission package, and assigns subject matter expert reviewers to independently score the content of each submission. See Section 4 How We Determine Winners for additional information.

3. **Announcement:** After the winners are selected, the Prize Administrator notifies each prize winner and requests the information necessary to distribute the cash prizes and TA.

Phase 1: Commitment will use the public ACT 1 Prize platform. Phase 2: Planning and Phase 3: Implementation will use the nonpublic HeroX Prize platform.

Eligibility

General Eligibility Requirements

The ACT 1 Prize Program competition is open only to eligible utilities as defined in the RMUC Program's authorizing legislation.[6] The following entities are eligible to compete in the ACT 1 Prize Program:

- Rural electric cooperatives
- Utilities owned by a political subdivision of a state, such as a municipally owned electric utility
- Utilities owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a state

[5] CEJST identifies disadvantaged census tracts across the United States. Under the definition of CEJST, a census tract is considered disadvantaged if it meets one of the following three categories: (1) meets or exceeds the threshold of at least one of the eight categories of burdens; (2) is on land within a federally recognized tribe; or (3) is completely surrounded by disadvantaged communities and is at or above the 50th percentile for low income. CEJST's eight categories of burdens can be found at: https://screeningtool.geoplatform.gov/en/methodology#3/33.47/-97.5.

[6] IIJA Section 40124 (Public Law 117-58).

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

If an eligible entity under IIJA Section 40124(a)(3)(E) is owned by a holding company, the eligible entity, and not the holding company, must submit the prize submission package. 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 submission package 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 noneligible subsidiaries of the holding company.

To be successful in competing in the LIMITED CYBERSECURITY RESOURCES track, a utility must demonstrate that they have limited cybersecurity resources in their submission package.

To be successful in competing in the MILITARY track, a utility must provide service to at least one military installation in its service territory.

If a competitor wishes to be considered for both the LIMITED CYBERSECURITY RESOURCES and MILITARY tracks, the competitor must indicate on their submission package cover page that they want to be considered for both tracks. Competitors may apply to and be selected for either track at the discretion of the Prize Judge based on program policy factors, but a utility can only win in one of the two tracks; competitors may not receive prizes from both tracks.

As part of your submission to this Prize Program, all competitors will be required to sign the following statement:

> I am providing this submission package as part of my participation in this prize. I understand that the information contained in this submission will be relied on by the federal government to determine whether to issue a prize to the named competitor. I certify under penalty of perjury that the named competitor meets the eligibility requirements for this prize competition and complies with all other rules contained in the Official Rules document. I further represent that the information contained in the submission is true and contains no misrepresentations. I understand false statements or misrepresentations to the federal government may result in civil and/or criminal penalties under 18 U.S.C. § 1001 and § 287, and 31 U.S.C. §§ 3729-3733 and 3801-3812.

Specific Eligibility Requirements for Each Phase

Phase 1: Commitment: Eligibility

- A single utility may submit only one submission package on behalf of their eligible utility.
- The utility's submission package must be complete.
- Each competitor must attend two mandatory virtual ACT 1 Virtual Commitment Phase Workshops (See Section 1.3.6 for additional information.).

Phase 2: Planning: Eligibility

- Only winners of a Commitment Prize are eligible to compete in the Planning Phase for a Planning Prize.
- A single utility may submit only one submission package on behalf of their eligible utility.
- The utility's submission package must be complete.
- A utility must partner with at least one of the ACT 1 Prize Program TA Navigators.

- Each competitor must attend one mandatory ACT 1 Virtual Planning Phase Workshop. (See Section 2.3.7 for additional information.)

Phase 3: Implementation: Eligibility

- Only winners of a Planning Prize are eligible to compete in the Implementation Phase for an Implementation Prize.
- A single utility may submit only one submission package on behalf of their eligible utility.
- The utility's submission package must be complete.
- A utility must partner with at least one of the ACT 1 Prize Program TA Navigators.

Changes in Eligibility Determined by DOE

The following persons and entities are not eligible to compete in the ACT 1 Prize Program.

- DOE employees, employees of sponsoring organizations, members of their immediate families (e.g., spouses, children, siblings, or parents), and persons living in the same household as such persons, whether or not related, are not eligible to participate in this prize contest.
- Individuals who worked at DOE (federal employees or support service contractors) within 6 months prior to the submission deadline of any contest are not eligible to participate in any prize contests in this program.
- Federal entities and federal employees are not eligible to participate in any portion of the prize.
- DOE national laboratory employees cannot compete in the prize.
- Entities and individuals publicly banned from doing business with the U.S. government such as entities and individuals debarred, suspended, or otherwise excluded from or ineligible for participating in federal programs are not eligible to compete.
- Entities and individuals identified as a restricted party on one or more screening lists of the U.S. Departments of Commerce, State, and the Treasury are not eligible to compete. See Consolidated Screening List.
- Individuals participating in a foreign government talent recruitment program[1] sponsored by a country of risk[2] and teams that include such individuals are not eligible to compete.
- Entities owned by, controlled by, or subject to the jurisdiction or direction of a government of a country of risk are not eligible to compete.

[1] A foreign government talent recruitment program is defined as an effort directly or indirectly organized, managed, or funded by a foreign government to recruit science and technology professionals or students (regardless of citizenship or national origin, and whether having a full-time or part-time position). Some foreign government-sponsored talent recruitment programs operate with the intent to import or otherwise acquire from abroad, sometimes through illicit means, proprietary technology or software, unpublished data and methods, and intellectual property to further the military modernization goals and/or economic goals of a foreign government. Many, but not all, programs aim to incentivize the targeted individual to physically relocate to the foreign state for the above purpose. Some programs allow for or encourage continued employment at U.S. research facilities or receipt of federal research funds while concurrently working at and/or receiving compensation from a foreign institution, and some direct participants not to disclose their participation to U.S. entities. Compensation could take many forms, including cash, research funding, complimentary foreign travel, honorific titles, career advancement opportunities, promised future compensation, or other types of remuneration or consideration, including in-kind compensation.

[2] Currently, the list of countries of risk includes Russia, Iran, North Korea, and China.

1 Commitment Phase

1.1 Goal

The goal of the Commitment Phase is to begin identifying the cybersecurity improvements your utility would like to accomplish and gaining your leadership's commitment to making improvements. In the Commitment Phase, you will describe why your utility should qualify as a limited cybersecurity resources utility if you are competing in the LIMITED CYBERSECURITY RESOURCES track. Utilities in both tracks must describe the utility's current cybersecurity maturity level and demonstrate in your submission package that your utility and its staff have the capacity to work with TA professionals. Utilities will need to provide a letter of support from their authorizing official (CEO, general manager, or governing board) supporting staff resources and time to this effort and affirming the utility's commitment to fully participate. The RMUC Program recognizes the economic challenges many rural communities face, and competitors will also be asked to describe their utility service territory, the communities they serve, and the work they do to support disadvantaged communities in their service territory.

Submission packages for the Commitment Prize will be evaluated based on the following criteria (See Section 1.4 for more information):

- **Criterion 1:** Utility Need and Cybersecurity Maturity Level
- **Criterion 2:** Initial Goals, Expected Outcomes, and Impacts on Utility
- **Criterion 3:** Commitment to Implement Cybersecurity Improvements and Capacity to Utilize TA
- **Criterion 4:** Description of Service Territory and Community Benefits.

Priority will be given to utilities that have limited cybersecurity resources and cybersecurity capabilities, have a commitment and capacity to work with TA professionals, have strong leadership support, and/or serve a high proportion of low-income and disadvantaged communities.

1.2 Prize Amounts and Important Dates

Up to 50 winners in the LIMITED CYBERSECURITY RESOURCES track will each receive a cash prize of $50,000 and will be provided with up to 80 hours of TA. Up to 5 winners in the MILITARY track will each receive a cash prize of $50,000 and will be provided with up to 120 hours of TA.

- Commitment Phase Opens: Wednesday, August 30, 2023
- Commitment Phase Submission Package Deadline: November 29, 2023 (5 p.m. ET).

1.3 What to Submit for the Commitment Prize

To apply for a Commitment Prize, the utility must:

- Have a staff member attend two required ACT 1 Prize Program workshops
- Upload a submission package that includes all the items listed below:
    1. **Cover page and narrative**
    2. **Letter of support from your organization's authorizing official (e.g., CEO, general manager, board of directors)**
    3. **Utility Profile Form (use form provided)**

4. **RMUC Utility Service Territory Report (use Report provided)**
5. **TA Request Form (use form provided)**
6. **Mandatory ACT 1 Commitment Phase virtual workshops attendance confirmation.**

Each of these six items must be uploaded as a PDF and submitted to your utility's account through the HeroX platform. Each item is described in more detail in the following sections. Your submission will not be considered if it does not include all six items listed above. Recommended templates are available to use for the cover page and narrative, letter of support from your organization's authorizing official, and mandatory workshops attendance confirmation.

Do not include specific cybersecurity vulnerabilities, risks, or other sensitive information in any of your application materials.

A prize does not require a cost share. However, to effectively use the prize funding and TA provided, winning utilities will need leadership support and a commitment of staff time and attention. If your utility decides to compete in the second phase of this prize, the Planning Phase, you will use the TA you won in the Commitment Phase to partner with at least one ACT 1 Prize Program TA Navigator to review the assessments, conclusions, and proposed solutions completed during the Planning Phase.

1.3.1 Cover Page and Narrative

Cover Page

Your submission package cover page must include the following information:

- Commitment Prize project title
- ACT 1 Prize Track
- Utility name
- City, state, and nine-digit zip code
- Primary point of contact for ACT 1 Commitment Prize submission package (name, title, email, phone number)
- List of names and job titles for all members of your utility's Commitment Prize Team.

In your narrative, you should respond to all of the questions under each of the following four topic sections. There is not a specific word limit for each topic section, but the aggregate response to all four sections must not exceed 3,000 words. **A word count must be included at the end of your submission**. The word count does not include captions, figures/graphs, or references. You may include up to five supporting images, figures, or graphs. Information contained in hyperlinks to external sources, and any text or graphics beyond the designated limits, will not be reviewed or considered by reviewers or the judge.

The prize reviewers will score your responses to the questions below based on criteria defined in Section 1.4 How Your Submission Will be Judged. It is strongly recommended that you use the narrative template provided, which includes the scoring criteria listed in Section 1.4, and that you understand how the reviewers will judge your responses to the narrative questions to help guide what you write in your narrative.

Commitment Prize Narrative (template available)

Commitment Prize Topic 1: Utility Need and Cybersecurity Maturity Level

1. Describe your utility's current barriers and challenges to improving its cybersecurity posture.
2. If your utility should be considered in the MILITARY track, briefly describe the military installations in your service territory. If your utility should be considered a LIMITED CYBERSECURITY RESOURCES utility, explain why.
3. What actions will your utility take to ensure the cybersecurity (confidentiality and integrity) of the information in your submission package?
4. Describe your utility's cybersecurity maturity and explain why you think this is an accurate assessment. **Do not include specific cybersecurity vulnerabilities, risks, or other sensitive information in your response.**

   If your answer is based on the results of one or more completed cybersecurity assessments (see examples below), provide the names of the assessments and the organization that created the assessments. Do not provide specific results of the assessment(s).

   Examples of cybersecurity assessments (assessment name, organization that created the assessment):
   - Co-op Cyber Goals, National Rural Electric Cooperative Association
   - Critical Security Controls, Center for Internet Security
   - Cross-Sector Cybersecurity Performance Goals, Cybersecurity Infrastructure and Security Agency
   - Cybersecurity Capability Maturity Model, DOE
   - Cybersecurity Framework, National Institute of Standards and Technology
   - Cybersecurity Maturity Model Certification, U.S. Department of Defense
   - Cybersecurity Scorecard, American Public Power Association
   - Rural Cooperative Cybersecurity Capabilities Program Self-Assessment tool, National Rural Electric Cooperative Association.

Commitment Prize Topic 2: Initial Goals, Expected Outcomes, and Impacts on Utility

The purpose of this Prize is to provide financial prizes and TA to enable your utility to invest in technologies, services, and training to improve your utility's cybersecurity. **Do not include specific cybersecurity vulnerabilities, risks, or other sensitive information in your response.**

1. Describe the problem(s) or challenge(s) that your utility would address if you received a Commitment Prize.
2. How would you use the prize funding and TA to resolve the problem(s) or challenge(s) you identified?
3. Describe how these actions and changes would improve your utility's cybersecurity.

Commitment Prize Topic 3: Commitment to Implement Cybersecurity Improvements and Capacity to Utilize TA

The work required to compete for a prize in the next phase, the Planning Phase, will require the involvement of technical and nontechnical utility staff. If your utility intends to compete for a Planning

Prize, utility staff may spend 5–20 hours in a single week during the Planning Phase either working directly with a TA professional or between meetings with the TA professional. Ideally, your utility will identify an internal Prize Team that consists of more than one employee to work with the TA professional.

1. Who will be the primary point of contact in your utility responsible for working with the TA professional, what is that person's job title and experience, and what are the expected responsibilities and activities of this person in their role as the point of contact?
2. Describe the responsibilities and activities of other staff members who will be part of your Prize Team, their job titles and experience, and how they will work with the TA professional.
3. Describe any challenges your Prize Team might face in planning and implementing the cybersecurity solution(s) you select and how you will address those challenges.
4. In addition to the letter of support, describe any other actions your utility's senior leadership has taken to support your Commitment Prize submission package and to ensure appropriate support for continued participation in the ACT 1 Prize Program.

Commitment Prize Topic 4: Description of Service Territory and Community Benefits

Many utilities serving rural America are in areas of the country with limited economic opportunities and financial resources. The RMUC Program is committed to ensuring that overburdened, underserved, and underrepresented communities have equitable access to federal resources and receive benefits from federal investments. Every utility will be expected to provide descriptive data about its utility and service territory. Use the links and resources provided on the Utility Profile Template and in your utility's RMUC Utility Service Territory Report (See Section 1.3.4) to help you answer questions in Topic 4.

1. Describe your utility's service territory and provide a summary of any critical services or regionally important customers/members in your service territory. Critical community services include but are not limited to health care facilities, communications facilities, water facilities, and critical care facilities.
2. Describe the economic conditions of the communities you serve and the proportion of the population in your service territory that is located in a disadvantaged community.
3. What program(s) does your utility provide to assist minority, low-income, or other disadvantaged communities in your service territory?
4. How many hours of paid on-the-job IT or cybersecurity training do you anticipate staff will receive over the course of this prize?

1.3.2 Letter of Support

You are required to attach a one-page letter of support, intent, and commitment signed by your utility's authorizing official. This letter must state that the official supports your utility's submission package for the Commitment Prize. The letter should also recognize that successfully competing in the ACT 1 Prize Program will require an ongoing commitment of staff time and resources, and the official is supportive of the use of staff time and resources for this purpose. Your utility's letter of support will be considered by the prize reviewers and will count in the evaluation of your submission package. Do not submit multipage letters.

Only one letter of support is required for the Commitment Prize submission package. Additional letters and general letters of support will not improve your score.

1.3.3 Utility Profile Form

Use the Utility Profile Form to provide information about your utility and its service territory and information about your utility's access to cybersecurity training, resources, and consulting services. The Utility Profile Form collects data on the number and types of employees at your utility relative to the number of members your utility serves; your organizational budget, cybersecurity, and IT expenses; the population density of your service territory; critical services and infrastructure in your territory; and disadvantaged communities in your territory. This form also collects data about the services you are providing to your community.

You can use this information to support your responses in the narrative, and it will be used by the prize reviewers in the evaluation of your Commitment Prize submission package. If you win a Commitment Prize and you decide to compete in the second phase, your TA Navigator will be required to verify the information provided in your Utility Profile Form as part of your Planning Prize submission package.

We encourage you to use the RMUC Utility Service Territory Report and publicly available tools such as CEJST, Energy Justice Mapping Tool, the Office of Clean Energy Demonstrations Rural or Remote Area Geospatial Dashboard, and any additional resources to complete your Utility Profile. The RMUC Utility Service Territory Report provides basic information about the communities in your utility's service territory.

1.3.4 RMUC Utility Service Territory Report

A RMUC Utility Service Territory Report will be available to your utility after you participate in one of the required ACT 1 Prize workshops (see Section 1.3.6). Instructions will be provided during the workshop on how to access your RMUC Utility Service Territory Report. This report will include an estimated map of your utility's service territory, the number of census tracts that have been defined as disadvantage community census tracts using metrics defined by the Council on Environmental Quality's CEJST,[7] and other information that will be useful to your utility when completing your Utility Profile Form and your narrative responses.

If you are provided with an RMUC Utility Service Territory Report, you must include it as part of your submission package. If a report was not available for your utility, upload a document that lists the sources of information your utility used to complete your Utility Profile Form and narrative—for example, list any websites, internal records, census data, or other sources of data you used to complete your Utility Profile Form.

1.3.5 TA Request Form

All utilities must complete the TA Request Form provided to be eligible to compete for a Commitment Prize. Using the TA Request Form, select the TA topics that would benefit your utility in the next phase of the Prize Program.

[7] https://screeningtool.geoplatform.gov/en/about#3/33.47/-97.5.

Your TA Request Form will not be used by the prize reviewers in the evaluation of your submission package. The information on your TA Request Form will not affect your score. However, submission of your TA Request Form is required for your Commitment Prize submission package to be considered complete. Incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.

The TA Request Forms will be shared with the ACT 1 Prize Administrator. If your utility wins a Commitment Prize, the Prize Administrator will use this form to assess your utility's needs and identify appropriate well-qualified TA professionals to work with you during the next phase Planning. TA professionals will execute nondisclosure agreements with your utility and will not share specific information that would identify an individual utility's systems or cybersecurity risks with DOE.

Every winner of a Commitment Prize will have access to up to 80 or 120 hours of TA (depending on the Prize Track) from a qualified cybersecurity provider at no cost to the utility starting on the date of selection for the Commitment Prize winners. Winners will receive vouchers that they can redeem to receive the TA. Commitment Prize winners are not required to use all of their TA hours. All Commitment Prize winners will have until the Planning Prize winners are announced to use their vouchers. Planning Prize winners may carry over any unused TA hours into the third phase, Implementation.

1.3.6 ACT 1 Virtual Commitment Phase Workshop Confirmation

The ACT 1 Prize Program will hold two virtual prize workshops. The first workshop will address the prize administrative processes, requirements, overview, and Phase 1 application information. The second workshop will go into more detail on how to use the RMUC Utility Service Territory Report, how TA will be provided, and the technical requirements to complete a prize application.

Completion of these workshops is mandatory to be eligible for a Commitment Prize. The workshops will be offered live and recorded. If your utility cannot make the live sessions, you will be able to access the recorded versions up until November 22, 2023, which is one week before the Commitment Prize submission deadline. One person from your utility must complete each workshop, but it does not have to be the same person. Your utility's primary point of contact for the ACT 1 Commitment Prize must confirm the registration and attendance of your utility's workshop participants for each of the two mandatory prize workshops as part of your Commitment Prize submission package. Your utility's point of contact must submit a written letter addressed to the ACT 1 Prize Administrator stating the name, title, email address, and utility name and address for each person that completed the workshop, and providing the date each person completed the workshop. This letter must be signed by the point of contact.

Your mandatory attendance confirmation letter will not be used by the prize reviewers in the evaluation of your submission package. The information in this letter will not affect your score. However, submission of your mandatory attendance confirmation letter is required for your Commitment Prize submission package to be considered complete. Incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.

Workshop announcements with the dates and times will be posted on HeroX, announced on DOE's RMUC Program website, and announced to everyone on the RMUC Program email list.

1.4 How Your Submission Will be Judged

The following information will be used by the reviewers to judge your Commitment Prize submission package:

- Narrative
- Authorizing official letter of support
- Utility Profile Form
- RMUC Utility Service Territory Report.

After reviewing these four items in your submission package, expert reviewers will use the point scale in the table below to assign a score between 1 and 6 for each bulleted statement listed.

Your cover page, TA Request Form, and Mandatory Virtual Commitment Phase Workshop Confirmation Letter will not be included in the scoring of your submission package but will be required for your submission package to be considered complete.

Point Scale Used by Reviewers

1	2	3	4	5	6
Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree

Expert reviewers give a score of 1 to 6 for each statement below (maximum score 90 points):

Commitment Criterion 1: Utility Need and Cybersecurity Maturity Level (maximum 24 points)

- The utility identified relevant conditions that create significant barriers to improving its cybersecurity posture.
- If the utility is defining itself as a MILITARY track utility, the utility identified at least one military installation that is in its service territory. If the utility is defining itself as a LIMITED CYBERSECURITY RESOURCES utility, it included the factors listed below, or other relevant factors, in its description to justify why it should be considered a LIMITED CYBERSECURITY RESOURCES utility (Reviewers will consider both the response to Narrative Topic 1 and the Utility Profile Form.).
    - Limited geographic access to service providers
    - Limited geographic access to cybersecurity training
    - Limited staff knowledge, skills, and abilities to use and maintain existing off-the-shelf cybersecurity solutions
    - Limited number of staff relative to its service territory and number of customers/members served
    - Limited ability to afford existing off-the-shelf cybersecurity solutions
    - Limited annual income based on energy sales.
- The utility described specific and appropriate measures it will take to protect the confidentiality and integrity of information in its submission package.
- The examples, descriptions, and/or summaries of results from cybersecurity assessments the utility

described support the cybersecurity maturity level it selected.

Commitment Criterion 2: Initial Goals, Expected Outcomes, and Impacts on Utility (maximum 18 points)

- The utility described cybersecurity problem(s) or challenge(s) that are relevant and important cybersecurity issues to address.
- The utility's plan for how it would use the prize funding and TA is achievable within the estimated timeframe and is highly likely to be successful in resolving the problem(s) or challenge(s) it identified.
- The utility identified goals that are likely to have a substantial impact on improving their cybersecurity posture and accomplishing the objectives of the RMUC Program to deploy advanced cybersecurity technologies that enhance the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat.

Commitment Criterion 3: Commitment to Implement Cybersecurity Improvements and Capacity to Utilize TA (maximum 24 points)

- The utility committed relevant job roles and sufficient staff time to work with and fully use TA professionals (Reviewers will consider the letter of support to assess staff resources allocated, the utility profile data to evaluate the allocation of staff resources relative to the size of the utility, and the response to Narrative Topic 3.).
- The utility demonstrated a commitment to success by including all relevant staff positions (e.g., operations, IT, engineering, leadership, management, finance, legal, communications) in its Prize Team, defining appropriate roles and responsibilities, and setting expectations that this effort will require technical and nontechnical staff participation.
- The utility has comprehensively identified likely challenges and proposed realistic and actionable solutions to successfully resolve those challenges.
- The utility's senior leadership has taken actions that demonstrate strong support for participation in the Commitment Phase and the subsequent phases of the ACT 1 Prize Program (Reviewers will consider the letter of support and the response to Narrative Topic 3.).

Commitment Criterion 4: Service Territory and Community Benefits (maximum 24 points)

- The utility's service territory includes a substantial number of entities that provide critical services to the community or region, including but not limited to health care facilities, communications facilities, water facilities, and critical care facilities (Reviewers will consider the utility profile, RMUC Utility Service Territory Report, and response to Narrative Topic 4.).
- The utility serves a very high proportion of members/customers who live in disadvantaged communities within its service territory (Reviewers will consider the utility profile and response to Narrative Topic 4.).

- The utility has many programs that provide relevant and substantial assistance to help minority, low-income, and disadvantaged communities within their service territory (Reviewers will consider the utility profile and response to Narrative Topic 4.).
- The utility demonstrates a strong commitment to providing paid on-the-job training that will enable employees to improve their cybersecurity knowledge, skills, and abilities.

2 Planning Phase

2.1 Goal

In the Planning Phase, utilities will conduct assessments of their network and system architecture and their technology tools. This information will be used by the utility to identify cybersecurity risks and vulnerabilities, prioritize potential solutions, and develop roadmaps and budgets to support improvements to the utility's cybersecurity posture. In addition, utilities will begin work on their Section 40126 Cybersecurity Plan.

Submission packages for the Planning Prize will be evaluated based on the following criteria (See Section 2.4):

- **Criteria 1:** Identifying Gaps and Prioritizing Risks
- **Criteria 2:** Drafting Your Utility's Cybersecurity Roadmap
- **Criteria 3:** Project Management
- **Criteria 4:** Institutionalizing a Culture of Continuous Improvement
- **Criteria 5:** Utility Cybersecurity Roadmap Budget
- **Criteria 6:** Section 40126 Cybersecurity Plan.

A successful Planning Prize submission package will demonstrate that the utility has:

1. Completed a network and system architecture review within the past year[8]
2. Completed a cybersecurity technology stack assessment within the past year[9]
3. Analyzed the results of the architecture review and stack assessment and created a cybersecurity gap/risk analysis within the past year
4. Utilized the cybersecurity gap/risk analysis to identify priority risks
5. Developed a draft Cybersecurity Roadmap for the utility that describes prioritized risks, planned improvements over a specified period of time, and proposed solutions for staff training, changes in policies and procedures, and changes to technologies
6. Created repeatable processes to assess and prioritize cybersecurity risks
7. Completed a draft budget for the Cybersecurity Roadmap implementation
8. Completed an initial Section 40126 Cybersecurity Plan.

Priority will be given to utilities that engage all relevant staff in the discussion and prioritization of cybersecurity risks and solutions; select solutions that address prioritized risks; use program management strategies that can maximize the likelihood of success; and create long-term processes for continuous improvements in the ability to identify and prioritize cybersecurity risks.

---

[8] A network and system architecture review results in a network map/topology showing the logical structure and digital connections between the utility's assets and systems. It is used to help identify cybersecurity weaknesses.

[9] The cybersecurity technology stack assessment examines existing technology tools that affect the utility's cybersecurity posture. Tools may be primarily cybersecurity technologies, but other tools (IT and OT) may also be included in the assessment if they can impact the utility's enterprise or operational cybersecurity. Results from a stack assessment might include identifying opportunities for simplifying or improving the effectiveness of the stack without degrading cybersecurity, and gaps in coverage where additional tools or nontechnical solutions could reduce cybersecurity risks.

2.2 Prize Amounts and Important Dates

Up to 25 LIMITED CYBERSECURITY RESOURCES winners will each receive a cash prize of $100,000 in the Planning Prize and will be provided with vouchers for up to 40 hours of TA. Up to five MILITARY track winners will each receive a cash prize of $100,000 in the Planning Prize and will be provided with vouchers for up to 120 hours of TA.

- Planning Phase Opens: April 22, 2024
- Planning Phase Submission Package Deadline: August 2024.

2.3 What to Submit for Planning Prize

To apply for a Planning Prize, the Planning Phase submission package must include all the items listed below:

1. **Cover page and narrative** (template provided)
2. **A letter of support from your utility's authorizing official supporting your submission to compete in Phase 2 (CEO, general manager, or board of directors)** (template provided)
3. **A letter of support from your utility's finance department** (template provided)
4. **Estimated monthly budget to implement your utility's Cybersecurity Roadmap**
5. **Section 40126 Cybersecurity Plan Confirmation** (template provided)
6. **Phase 2 TA Navigator Review Form** (use form provided)
7. **TA Request Form for Implementation Phase Work** (use form provided)
8. **Project Team Information Forms** (use forms provided)
9. **Mandatory Virtual Planning Phase Workshop Confirmation** (template provided).

All documents for Phase 2 will be uploaded to the nonpublic ACT 1 HeroX site. Team captains for the winning utilities in Phase 1 will receive instructions to access and use the nonpublic ACT 1 HeroX site.

Each of the nine items listed above must be uploaded as separate PDF files and submitted through the nonpublic HeroX platform. Each item is described in more detail in the following sections. Your submission will not be considered if it does not include all nine items listed above.

Do not include specific cybersecurity vulnerabilities, risks, or other sensitive information in any of your application materials.

Recommended templates are available for the cover page and narrative; letter of support from your utility's authorizing official; letter of support from your finance department; Section 40126 Cybersecurity Plan confirmation; and mandatory workshop attendance confirmation. If you decide not to use the templates, you are responsible for ensuring that your submission package includes the information described in the following sections related to each item.

The Phase 2 TA Navigator Review Form, TA Request Form, and Project Team Information Forms must be submitted using the forms provided.

There are no templates or forms for the estimated budget. Your estimated budget must include monthly cost estimates for the items listed in the Phase 2 Narrative questions below.

If your utility decides to compete in the third phase of this prize, the Implementation Phase, you will use the TA you won in Phase 2: Planning to partner with at least one ACT 1 Prize Program TA Navigator to review the work completed during Phase 3: Implementation.

2.3.1 Cover Page and Narrative

Cover Page

Your submission package cover page should include the following information:

- Planning Prize project title
- Organization name
- Organization city, state, and nine-digit zip code
- Primary point of contact for ACT 1 Planning Prize submission package (name, title, email, phone number)
- Secondary point of contact for ACT 1 Planning Prize submission package (name, title, email, phone number)

In your narrative, you should respond to all of the questions under each of the following six topic sections. There is not a specific word limit for each topic section, but the aggregate response to all four sections must not exceed 3,500 words. **A word count must be included at the end of your submission**. The word count does not include captions, figures/graphs, or references. You may include up to five supporting images, figures, or graphs. Information contained in hyperlinks to external sources, and any text or graphics beyond the designated limits will not be reviewed or considered by reviewers or the judge.

The reviewers will score your responses to the questions below based on criteria defined in Section 2.4 How Your Submission Will be Judged. It is recommended that you read the scoring criteria and understand how the reviewers will judge your responses to the narrative questions to help guide what you write in your narrative. The information provided in your narrative should not contradict information provided in the other documents that are part of your submission package.

Planning Prize Narrative

Planning Prize Topic 1: Identifying Gaps and Prioritizing Risks

Clearly identify the gaps and risks. Identifying the vulnerabilities and risks in your utility's network architecture, assets (hardware, software, firmware), devices (including internet of things), and systems can help you prioritize funding decisions. Similarly, understanding how to effectively use the cybersecurity tools you already own can help eliminate duplication and unnecessary purchases. Creating a repeatable process to prioritize risks can help you focus your utility's limited resources on the highest priority risks in the future.

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

1. Provide the dates for when your utility completed:
    - A network and systems architecture review

- A cybersecurity technology stack assessment
- A cybersecurity gap/risk analysis.

2. Using either a table that lists the departments/business units in your utility (see example below) or an organizational chart (do not include employee names), indicate which departments/units in your utility were or were not included in the scope of your architecture review and which departments/units were and were not included in the scope of your technology stack assessment. For each department/unit that was not included, explain why it was not included in the scope.

List Utility Departments/ Business Units	Included in Architecture Review (Yes/No)	Included in Technology Stack Assessment (Yes/No)	If not included, explain why.
1.			
2.			
Etc.			

3. List the 10 Cybersecurity Capability Maturity Model (C2M2) domains, and indicate whether there were any major or minor findings for each domain based on the results of your gap/risk analysis. If there were C2M2 domains that had no findings, indicate "no findings." If there were domains that were not addressed in your gap/risk analysis, indicate "not addressed," and explain why those domains were not in the scope of your gap/risk analysis. (Do not provide specific details.)
4. How did your utility determine which cybersecurity risks would be addressed first from your cybersecurity gap/risk analysis? (In your answer, address all bullet points below.)
    - How did you choose the most relevant criteria to compare and prioritize risks?
    - List the criteria that you considered, and identify the top three to five criteria that were most important when you determined which risks you would address first in your Cybersecurity Roadmap.
    - Did your criteria include business risks (e.g., potential loss of power delivery or reliability, utility reputation, potential financial impact on members/customers, impact of quick wins to support continued cybersecurity investments, regulatory penalties)?
5. How did you prioritize the gap/risk analysis results, and how did you decide what to include in your Cybersecurity Roadmap? (In your answer, address all bullet points below.)
    - Did you apply the criteria to each risk identified in your gap/risk analysis and assign point scores? Was the decision ad hoc based on discussions? If the decision was delegated to a third party to prioritize the risks, what criteria did the third party use? If you used a different method, describe the method you used.
    - List the departments/business units that were involved in discussions to determine which risks to address first. Were any of your OT staff or senior leadership involved? If not, describe why.
    - If any external partners or third parties helped you prioritize the risks, describe the relationship of those partners to your utility. For example, did you work with your joint action

agency, generation/transmission cooperative, statewide association, trade association, external consultant or service provider, or ACT 1 TA professional?

Planning Prize Topic 2: Your Utility's Cybersecurity Roadmap

Develop a Cybersecurity Roadmap. Your utility's Cybersecurity Roadmap will describe which of the highest priority risks identified in your gap/risk analysis you want to address within a specified timeframe and the steps you will take to implement solutions. Deciding what to include in the scope of your Roadmap, and evaluating and selecting solutions will take time. Your Cybersecurity Roadmap budget should include consideration of immediate costs and long-term operation and maintenance costs.

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

1. Describe the current status of your Cybersecurity Roadmap. **DO NOT** upload roadmaps to HeroX! (In your answer, address all bullet points below.)
    - Does your Cybersecurity Roadmap address the highest priority risks you identified in your gap/risk analysis? If you decided to focus on risks that were not considered "highest priority," explain why you included lower priority risks.
    - What additional information will your utility need, and what issues need to be addressed before you can finalize your Cybersecurity Roadmap?
2. How did your utility determine which solutions to select to address the risks you included in your Cybersecurity Roadmap? (In your answer, address all bullet points below.)
    - List the departments that were involved in helping to select solutions. How did you communicate the impacts that different solutions might have on the staff and work processes of each department?
    - List the criteria that you used to evaluate and select your solutions, and identify the three to five that were most important in your decision process (e.g., regulatory requirements, budget limitations, availability of staff resources, staff skills and abilities, financial impact on customers/members, geographic access to solution providers, supply chain security issues, supply chain access issues).
3. Based on your estimated Cybersecurity Roadmap budget, provide the estimated percentage of costs for the following categories. The five categories should add up to 100%.
    a. New assets or technology that can be operated and maintained by existing staff without any new training
    b. New assets or technology that can be operated and maintained by existing staff but will require additional training—include product and training costs
    c. New assets or technology that will be operated and maintained by a third party on your behalf—include product costs and costs associated with hiring and retaining third parties in this estimate
    d. Do not require purchasing any new assets or technology—include utility personnel time (e.g., staff time to change policies/procedures, training not specific to a new technology purchases, exercises, consultants, security service contracts)

e. Other (please describe).

Planning Prize Topic 3: Project Management

Describe how you will successfully manage your project and eliminate risks. Common risks affecting the success of a project are ineffective or inadequate internal communications and unclear expectations between technical and nontechnical staff. Another risk is the inability of staff to continue to operate and maintain solutions that require technical expertise. Technical risks that could affect the success of a project include supply chain availability and interoperability and integration challenges associated with combining new technologies with legacy technologies. Consider how these and other risks could impact your success and how you will address these risks.

1. Describe the program management approach you used to ensure that all staff received relevant and timely information to support your Phase 2 efforts. What methods did you use to share information? (Include how often you shared information with staff directly involved in your Prize Team, other utility leadership, technical staff not directly involved in your Cybersecurity Roadmap planning efforts, and nontechnical staff.)
2. If your gap/risk analysis was comprehensive across your utility, it likely identified vulnerabilities and risks in many departments. (In your answer, address all bullet points below.)
    - How did you educate staff from departments where high priority vulnerabilities and risks were identified about the potential security and business impacts of the findings?
    - What actions did you take to enable staff from those departments to provide input into the risk prioritization and solution selection processes?
3. The behavior of staff can impact the success of an effort to improve cybersecurity. How have you addressed challenges involving staff behavior in the past, and how will you address those challenges during your Cybersecurity Roadmap implementation?
4. Provide an estimated monthly timeline showing major tasks and milestones for the work you intend to accomplish in your Cybersecurity Roadmap. (Do not provide details on vendors or vendor solutions.)
5. Describe how your utility used the ACT 1 TA professionals or other third-party partners to help you complete Phase 2. When were the ACT 1 TA professionals or your other partners useful in helping you complete the work required in the Planning Phase? What could the RMUC Program do to improve your ability to access and use TA professionals?

Planning Prize Topic 4: Institutionalizing a Culture of Continuous Improvement

Describe your efforts toward developing a culture of continuous improvement. Documenting your selection criteria and processes used to complete the Planning Phase work can inform the development of policies and repeatable procedures that can be institutionalized. Lessons learned during the Planning Phase can help your utility improve its cybersecurity maturity and capacity to repeat these processes in the future.

1. Are the processes you used to identify high priority cybersecurity risks and solutions easily repeatable? (In your answer, address all bullet points below.)
    - What challenges did you experience in completing the risk identification, risk analysis, risk prioritization, and solution selection?

- What changes would you make to improve the processes you used? Would you use the same criteria to prioritize risks and solutions?

2. Does your utility have a policy requiring periodic assessments of its cybersecurity risks? When will you do your next risk assessment and update your gap/risk analysis results?
3. What is your utility's plan to maintain and update training, policy, and technical solutions after they are implemented? (In your answer, address all bullet points below.)
    - For new technologies included in your Cybersecurity Roadmap, how many hours per week will your staff need to dedicate to (1) install the technologies—provide a start and end date for this estimate; (2) operate the technical solutions each year; and (3) maintain/update the technologies each year?
    - What knowledge, skills, and abilities will your staff need to master to operate and update the technical solutions you selected? Will additional training be needed for your current staff to be successful in effectively using any of the technical solutions selected?
    - What source(s) of funding does your utility plan to use to support any ongoing costs associated with your solutions? (These costs might include service contracts, additional training, hiring new staff, license fees, etc.) If your leadership has committed funding for future years, the commitment should be described in your utility's leadership and finance letters of support.

Planning Prize Topic 5: Estimated Cybersecurity Roadmap Budget

As part of your Planning Phase submission package, you must provide a monthly budget that includes all costs to fully implement your Cybersecurity Roadmap. This budget should align with the estimated monthly timeline you presented in response to Narrative Topic 3: Project Management question #4.

1. In your Cybersecurity Roadmap budget, list all of the relevant cost categories and estimated monthly expenses.
2. Ensure that all of the cost estimates in your budget are reasonable.
3. Ensure that your finance department has reviewed and approved your budget and submits a signed letter of support.

Planning Prize Topic 6: Section 40126 Cybersecurity Plan

Your draft Section 40126 Cybersecurity Plan is different from your utility's Cybersecurity Roadmap, but there will be some overlap between the two documents. The purpose of your Section 40126 Cybersecurity Plan is to ensure that your team has a specific plan for managing the cybersecurity of your Prize efforts. It is narrower in scope than your Cybersecurity Roadmap.

1. In your Section 40126 Cybersecurity Plan Confirmation letter (Section 2.3.3 below), describe the steps your utility has taken to develop a draft or to complete its Section 40126 Cybersecurity Plan.

2.3.2 Letters of Support and Cybersecurity Roadmap Budget

To compete for a Planning Prize, you need to submit a letter of support from your utility's authorizing official for your Phase 2 submission package; a letter of support from your finance department; and an estimated monthly Cybersecurity Roadmap budget. The following descriptions provide more details on the required documents.

You are required to submit the following two letters of support. Each letter should be one page long and signed by the appropriate staff member.

1. A signed letter of support from your utility's authorizing official supporting your Phase 2 submission package. This letter must:
    a. State that your utility supports your submission package for the ACT 1 Phase 2 Planning Prize
    b. Include a statement that the official signing the letter is authorized to make these commitments
    c. Recognize that successfully competing in the ACT 1 Prize Program will require an ongoing commitment of staff time and resources and that the utility is supportive of the use of staff time and resources for this purpose.
    d. Describe your leadership's commitment to any required funding to continue work to complete your Cybersecurity Roadmap or to cover ongoing costs of your Cybersecurity Roadmap solutions in future years.

2. A signed letter of support on your organization's letterhead from your organization's finance department that indicates that the appropriate finance person has:
    a. Reviewed and approved the proposed estimated monthly Cybersecurity Roadmap budget
    b. Ensured that the estimated costs are reasonable.

General letters of support from parties that are not critical to the execution of your solution will not factor into your score. Do not submit multipage letters.

You are required to submit the following estimated budget:

1. An estimated monthly Cybersecurity Roadmap budget to support the implementation of your Cybersecurity Roadmap. This monthly budget should include all costs through the time required to fully implement your Cybersecurity Roadmap, including, but not limited to, staff and personnel; training; conferences; travel/transportation; supplies; IT equipment, licenses, and related products; cybersecurity equipment, licenses, and related products; consulting services; IT and managed security service provider contracts; other subcontracts; other direct costs; indirect costs; other anticipated expenses (please describe).

2.3.3 Section 40126 Cybersecurity Plan Confirmation

All utilities competing for a Planning Prize must document that they have completed a draft of their utility's Section 40126 Cybersecurity Plan as part of their submission package. Your utility must create a single-page written letter that describes the steps your utility has taken to complete your Section 40126 Cybersecurity Plan. This confirmation letter must be signed by the appropriate staff member and uploaded as part of your Planning Prize submission package.

Your Section 40126 Cybersecurity Plan confirmation will not be used by the prize reviewers in the evaluation of your submission package and will not affect your score; however, submission of your Section 40126 Cybersecurity Plan confirmation is required for your Planning Prize submission package to be considered complete. Incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.

After you have completed a draft Section 40126 Cybersecurity Plan, you will be able to work with the Section 40126 team led by the Pacific Northwest National Laboratory (PNNL) to help you complete your Section 40126 Cybersecurity Plan at no cost. The PNNL team is dedicated to providing TA specifically focused on helping organizations complete these plans. The TA provided by the PNNL team is in addition to the 80 or 120 hours of TA that a Commitment Prize winner will receive. The Section 40126 Cybersecurity Plans are separated into high-, medium-, and low-risk project categories, and each category has a unique cybersecurity plan template. Utilities competing for a Planning Prize will work with the PNNL team to determine which template is most appropriate.

For additional information and to view and download the templates, see: https://www.energy.gov/ceser/bipartisan-infrastructure-law-implementation. This website also provides a link to the instructions on how to submit your utility's Section 40126 Cybersecurity Plan to the PNNL team. **Do not upload your Section 40126 Cybersecurity Plan to HeroX!**

2.3.4 Phase 2 TA Navigator Review Form

DOE does not want your utility to submit sensitive information about your utility's systems in your prize submission package. Therefore, to verify that the actions required in the Planning Phase were completed and met the expectations outlined in the Prize Rules, an ACT 1 TA Navigator will review the products of your Planning Phase and provide the results of that review using the Phase 2 TA Navigator Review Form. There will be two kinds of TA professionals available to you: a TA Navigator and a TA Provider. The different roles and responsibilities of the two kinds of TA professionals will be explained during the mandatory Phase 2 virtual workshop.

You must submit this form to demonstrate that an ACT 1 TA Navigator has reviewed your Planning Phase work. This form must be signed by an ACT 1 TA Navigator. The TA Navigator will:

1) Review and verify the information in your Utility Profile Form submitted in Phase 1
2) Confirm that a network and systems architecture review and a cybersecurity technology stack assessment were completed and comment on the comprehensiveness and quality of the review and assessment
3) Confirm that a cybersecurity gap/risk analysis was completed and comment on the comprehensiveness and quality of the assessment
4) Confirm that a draft Cybersecurity Roadmap was completed and comment on the comprehensiveness of the Cybersecurity Roadmap, whether the risks were appropriately prioritized based on the gap/risk analysis results, and whether the proposed solutions were reasonable and highly likely to be maintained based on the utility's current staff and budget
5) Review and comment on the estimated Cybersecurity Roadmap budget, whether the costs were reasonable, and whether the timing of the incurred costs reflected a realistic pace for the Cybersecurity Roadmap work to be completed.

You are responsible for ensuring that an ACT 1 TA Navigator completes this form, and you must include the TA Navigator Review Form in your Planning Prize submission package.

Do not upload or submit any reviews, assessments, analyses, or your utility's Cybersecurity Roadmap! Only the TA Navigator Review Form should be included in your submission package.

2.3.5 TA Request Form for Implementation Phase Work

You will use the TA Request Form for Implementation Phase Work to identify areas where your utility would benefit from assistance in the next phase of the Prize Program. Your TA Request Form will not be used by the prize reviewers in the evaluation of your submission package and will not affect your score. However, submission of your TA Request Form is required for your Planning Prize submission package to be considered complete. Incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.

The TA Request Forms will be shared with the Prize Administrator. If your utility wins a Planning Prize, the Prize Administrator will use this form to identify TA professionals to work with you during the next phase, Implementation. TA professionals will execute nondisclosure agreements and will not be sharing cybersecurity details with DOE.

Every winner of a Planning Prize will have access to up to either 40 or 120 hours of additional TA (depending on the Prize Track) from a cybersecurity professional at no cost. Winners will receive vouchers that they can redeem to receive the TA. Planning Prize winners are not required to use all of their TA hours. Utilities will have until the Implementation Prize winners are announced to use their vouchers.

2.3.6 Project Team Information Forms

Project Team Information Forms are required for your Planning Prize submission package to be considered complete. DOE will use your Project Team Information Forms to ensure eligibility of your team to win a prize. Eligibility requirements are included in the Eligibility section of the Prize Rules. Teams found to include members who are not eligible to compete, as per "Changes in Eligibility Determined by DOE," may be disqualified or required to take corrective action to receive a prize. Your mandatory Project Team Information Forms will not be used by the prize reviewers in the evaluation of your submission package. The information in these forms will not affect your score; however, incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.

The packet of Project Team Information Forms will include a Planning Team Cover Page and a collection of Individual Team Member Forms. Your Project Team Cover Page must include the name, title, and a brief description of the role and responsibilities of each person, technical and nontechnical, who contributed to your Planning Phase work. Include all individuals who participated, including administrative and non-technical staff that supported your Planning Phase work, and individuals from subcontracting firms or other third-party organizations. Identify your Team Lead and the people who were Key Project Team members. Key Project Team members are individuals who contributed in a substantive, meaningful way to design, manage, and implement your Planning Phase project, including utility staff and individuals from subcontracting firms or other third-parties.

Individual Team Member Forms must be completed by your Team Lead and all Key Project Team members. Team Member Forms must provide the information requested on the Form. A resume can be used instead of the Team Member Form if it includes all of the information required and is limited to two pages. You do not need to submit an Individual Team Member Form or resume for any of the ACT 1 TA professionals listed on your Planning Team Cover Page.

Combine the Planning Team Cover Page and all of the Individual Team Member Forms and resumes into one document or PDF file and upload one single file to the non-public HeroX site as part of your Planning Phase submission package.

2.3.7 Mandatory Virtual Planning Phase Workshop Confirmation

The ACT 1 Prize Program will hold one mandatory virtual prize workshop during the Planning Phase. The workshop will address the Phase 2 process, how to access and use the TA professionals, the difference between a TA Navigator and a TA Provider, and the technical requirements to complete a Phase 2 Prize submission package.

Completion of this workshop is mandatory to be eligible for a Planning Prize. The workshop will be offered live and recorded. If your utility cannot attend the live session, you will be able to access the recorded version up until two weeks prior to the Planning Prize submission deadline. One person from your utility must complete the Planning Phase Workshop. Your utility's primary point of contact for the ACT 1 Planning Prize must confirm the registration and attendance of your utility's workshop participant for the mandatory prize workshop as part of your Planning Prize submission package. Your utility's point of contact must submit a written letter addressed to the ACT 1 Prize Administrator stating the name, title, email address, and utility name and address for the person that completed the workshop and the date the person completed the workshop. This letter must be signed by the point of contact.

Your mandatory attendance confirmation letter will not be used by the prize reviewers in the evaluation of your submission package. The information in this letter will not affect your score; however, submission of your mandatory attendance confirmation letter is required for your Planning Prize submission package to be considered complete. Incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.

A workshop announcement with the date and time will be posted on the nonpublic HeroX site.

2.4 How Your Submission Will be Judged

The following information will be used by the reviewers to judge your Planning Prize submission package:

1. Narrative responses
2. Authorizing official letter of support
3. Letter of support from your finance department
4. Estimated monthly budget for work proposed to implement your utility's Cybersecurity Roadmap
5. Section 40126 Cybersecurity Plan Confirmation
6. Phase 2 TA Navigator Review Form.

After reviewing these items in your submission package, expert reviewers will evaluate your narrative responses and relevant submission package documents and assign a score for each bulleted statement listed below. The maximum score for each bulleted statement is provided in parentheses after the statement. Reviewers will give a score of "1" to the bulleted statement if they "strongly disagree," and the highest point score will be given if the reviewer "strongly agrees" with the bulleted statement.

Example: Point Scale Used by Reviewers for a Bulleted Statement Worth 6 Points

1	2	3	4	5	6
Strongly disagree	Disagree	Slightly Disagree	Slightly agree	Agree	Strongly agree

Your cover page, TA Request Form for Implementation Phase Work, Mandatory Virtual Planning Phase Workshop Confirmation, and Project Team Information Forms will not be included in the scoring of your submission package but will be required for your submission package to be considered complete.

Expert reviewers give a score of 1 to 6 for each statement below (unless otherwise indicated) (maximum score 114 points):

Planning Criterion 1: Identifying Gaps and Prioritizing Risks (maximum 24 points)

- The architectural review and technology stack assessment were completed within the past year and were comprehensive and of high quality. (Reviewers will consider both the TA Navigator Review Form and Narrative Topic 1.) (3 points)
- The scope of the utility's architecture review and stack assessment enabled the utility to identify vulnerabilities and risks across its business systems (e.g., finance, billing, communications, human resources, administration) and its OT systems. (Reviewers will consider both the TA Navigator Review Form and Narrative Topic 1.) (6 points)
- The utility's gap/risk analysis was comprehensive and based on results from appropriate reviews and assessments, covered all relevant C2M2 domains, and was of high quality. (Reviewers will consider both the TA Navigator Review Form and Narrative Topic 1.) (6 points)
- The utility identified appropriate and specific criteria to prioritize risks that included both cybersecurity risks and business/enterprise risks. (3 points)
- The utility described a reasonable decision process to use specific criteria to prioritize which risks to address in their Cybersecurity Roadmap, and the utility included relevant technical and nontechnical staff, partners, and representatives from departments where cybersecurity risks were identified in the decision process to prioritize risks. (Reviewers will consider both the TA Navigator Review Form and Narrative Topic 1.) (6 points)

Planning Criterion 2: Drafting your Utility's Cybersecurity Roadmap (maximum 18 points)

- The utility completed a draft Cybersecurity Roadmap that addresses relevant risks identified in their gap/risk analysis and identified key tasks to finalize the Cybersecurity Roadmap. (Reviewers will consider both the TA Navigator Review Form and Narrative Topics 1 and 2.) (6 points)
- The utility described a reasonable decision process to use specific criteria to prioritize which solutions would be selected to address prioritized risks, and the utility included relevant technical and nontechnical staff, partners, and department representatives in the decision process to ensure they understood how the solutions might impact their staff. (Reviewers will consider both the TA Navigator Review Form and Narrative Topics 1 and 2.) (6 points)
- The utility will use a reasonable combination of investments in people, process, and technology solutions to address priority risks included in the Cybersecurity Roadmap. These investments may include, for example, investments in staff training and changes to policies and procedures. (Reviewers will consider the TA Navigator Review Form, Narrative Topic 2, and the estimated Cybersecurity Roadmap budget.) (6 points)

Planning Criterion 3: Project Management (maximum 30 points)

- The utility established an appropriate and effective program management strategy for communications. The frequency of communications and the format used was highly likely to result in all relevant parties and departments being informed of activities that could impact each department or its staff in a timely manner. (6 points)
- The utility used methods that were likely to be highly effective in educating staff from departments where high priority vulnerabilities and risks were found about the security and business risk implications of the findings, and the utility included relevant department staff in discussions to select solutions. (6 points)
- The utility described appropriate and effective methods to manage implementation challenges associated with solutions that require participation from other utility staff to be successful and has described approaches that are highly likely to achieve "buy-in" by the relevant staff. (6 points)
- The utility's monthly timeline reflects a realistic pace for the work to be completed. (Reviewers will consider both the TA Navigator Review Form and estimated Cybersecurity Roadmap budget.) (9 points)
- The utility's approach to leverage the ACT 1 TA professionals and other third-party partners was successful in helping the utility make progress on its Phase 2 work. (3 points)

Planning Criterion 4: Institutionalizing a Culture of Continuous Improvement (maximum 18 points)

- The utility described relevant lessons learned on how to identify and prioritize cybersecurity risks and evaluate and prioritize possible solutions, and the utility identified potential changes based on lessons learned that could improve their risk management outcomes. (Reviewers will consider Narrative Topics 1–4.) (3 points)
- The utility has established a policy requiring periodic assessments of its cybersecurity risks and will complete another risk assessment and gap/analysis within a reasonable time. (6 points)
- The utility provided realistic estimates of staff time and training needed to ensure the effective use of solutions. (Reviewers will consider Narrative Topic 4, the finance department letter of support, and the estimated monthly Cybersecurity Roadmap budget.) (6 points)
- The utility has identified funding and/or leadership commitments to cover costs associated with the continued operations and maintenance of solutions after the Prize Program ends. (Reviewers will consider Narrative Topic 4, the utility's leadership and finance department letters of support, and the estimated Cybersecurity Roadmap budget.) (3 points)

Planning Criterion 5: Estimated Budgets (maximum 18 points)

- The utility's estimated Cybersecurity Roadmap budget includes all relevant costs associated with the complete implementation of its Roadmap. (Reviewers will consider both the TA Navigator Review Form and estimated Cybersecurity Roadmap budget.) (6 points)
- The utility's estimated costs are reasonable. (Reviewers will consider the TA Navigator Review Form and the estimated Cybersecurity Roadmap budget.) (6 points)
- The utility's finance department has reviewed and approved the estimated Cybersecurity Roadmap

budget. (Reviewers will consider the letter of support from the utility's finance department.) (6 points)

Planning Criterion 6: Section 40126 Cybersecurity Plan (maximum 6 points)

- The utility has taken steps to draft or complete a Section 40126 Cybersecurity Plan. (Reviewers will consider the utility's Section 40126 Cybersecurity Plan confirmation letter.) (6 points)

3 Implementation Phase

3.1 Goal

In the Implementation Phase, utilities will collaborate with TA professionals and industry experts to implement the solutions outlined in the Planning Phase. The TA professionals will help utilities identify potential solutions, develop criteria for selecting appropriate solutions, coach utilities on negotiating favorable service-level agreements and contracts, facilitate continued use planning for new technologies, assist with the implementation of technology solutions, and support the development of processes to confirm the cybersecurity of solutions after they are implemented.

Submission packages for the Implementation Prize will be evaluated based on the following criteria (See Section 3.4):

- **Criteria 1:** Documented Progress
- **Criteria 2:** Likelihood of Continued Progress
- **Criteria 3:** Commitment
- **Criteria 4:** Section 40126 Cybersecurity Plan.

A successful Implementation Prize submission package will demonstrate that the utility has:

1. Completed its Cybersecurity Roadmap budget
2. Made significant progress implementing its Cybersecurity Roadmap
3. Developed a process to test the cybersecurity of its systems after full integration of solutions
4. Committed to continue to implement its Cybersecurity Roadmap
5. Completed its Section 40126 Cybersecurity Plan.

Priority will be given to utilities that demonstrate a strong commitment to completing their roadmaps, that include solutions that specifically improve the cybersecurity posture of operational systems in the utility, can be maintained by the existing utility staff with minimal additional TA, and have strong leadership support, as evidenced by supporting documents such as long-term budget commitments.

3.2 Prize Amounts and Important Dates

Up to 25 LIMITED CYBERSECURITY RESOURCE TRACK and 5 MILITARY TRACK winners will each receive a cash prize of $50,000.

- Implementation Phase Opens: October 2024
- Implementation Phase Submission Package Deadline: January 2025.

3.3 What to Submit for the Implementation Prize

To apply for an Implementation Prize, the Implementation Phase submission package must include all the items listed below:

1. **Cover page and narrative** (template provided)
2. **A letter from your utility's authorizing official supporting your submission to compete in Phase 3 (CEO, general manager, or board of directors)** (template provided)

3. **A letter from your utility's finance department** (template provided)
4. **Final monthly Cybersecurity Roadmap budget**
5. **Final annual post-implementation budget**
6. **Section 40126 Cybersecurity Plan Progress Confirmation** (template provided)
7. **Phase 3 TA Navigator Review Form** (use form provided).

You are strongly encouraged to submit any additional supporting documents as part of your submission package (see Section 3.3.2).

Do not include specific cybersecurity vulnerabilities, risks, or other sensitive information in any of your application materials.

Each of these seven items must be uploaded as a PDF and submitted through the nonpublic HeroX platform. Each item is described in more detail in the following sections. Your submission will not be considered complete if it does not include all seven of the required items listed above. Recommended templates are available to use for the cover page and narrative; letter of support from your utility's authorizing office; letter of support from your utility's finance department; and Section 40126 Cybersecurity Plan Progress Confirmation.

The Phase 3 TA Navigator Review Form must be submitted using the form provided.

There are no templates or forms for the budgets. Your final budgets must include cost estimates for the items listed in the Phase 3 narrative questions below.

3.3.1 Cover Page and Narrative

Cover Page

Your submission package cover page should include the following information:

- Implementation Prize project title
- Organization name
- Organization city, state, and nine-digit zip code
- Primary point of contact for ACT 1 Implementation Prize submission package (name, title, email, phone number)
- Secondary point of contact for ACT 1 Implementation Prize submission package (name, title, email, phone number)

In your narrative, you should respond to all the questions under each of the following two topic sections. There is not a specific word limit for each topic section, but the aggregate response to both sections must not exceed 3,000 words. **A word count must be included at the end of your submission**. The word count does not include captions, figures/graphs, or references. You may include up to five supporting images, figures, or graphs. Information contained in hyperlinks to external sources, and any text or graphics beyond the designated limits, will not be reviewed or considered by reviewers or the judge.

The reviewers will score your responses to the questions below based on criteria defined in Section 3.4 How Your Submission Will be Judged. It is recommended that you read the scoring criteria and understand how the reviewers will judge your responses to the narrative questions to help guide what you write in your narrative. The information provided in your narrative should not contradict information provided in the other documents that are part of your submission package.

Implementation Prize Narrative

Implementation Prize Topic 1: Documented Progress

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

1. Describe your utility's progress implementing your Cybersecurity Roadmap. What work has been completed?
2. How has the progress you have made implementing your Cybersecurity Roadmap improved the cybersecurity posture of your utility's **IT** systems?
3. How have the changes you have made improved the cybersecurity of your utility's **operational systems**?
4. Describe the process you used to engage nontechnical staff in changing their behavior to ensure solutions were effective and how you measured the success of this process.
5. What actions did your utility take to minimize third-party cybersecurity risks associated with solution identification, solution selection, and contract/purchase negotiations with solution providers?
6. At the time of submission, how many hours of paid on-the-job IT or cybersecurity training did staff receive over the course of this prize?

Implementation Prize Topic 2: Likelihood of Continued Progress

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

1. What work remains in your Cybersecurity Roadmap, what delays have you experienced and how did you resolve them, and what is your current timeline to complete the remaining work?
2. How will you operate, maintain, and update the solutions in your Cybersecurity Roadmap?
3. What processes, policies, and procedures have you established to periodically reassess cybersecurity risks in your utility?
4. What processes, policies, and procedures have you established to adequately test the cybersecurity of the remaining solutions in your roadmap after they are fully implemented and to test future technology deployments after full implementation?
5. What processes have you created to enable ongoing communications with senior leadership about the business value that results from the cybersecurity investments your utility has made during the ACT 1 Prize Program?

6. How has your utility benefited from participating in the ACT 1 Prize Program so far, and what would you do differently?

3.3.2 Letters of Support and Cybersecurity Roadmap and Post-Implementation Budgets

To compete for an Implementation Prize, you need to submit two letters and two budgets.

You are required to submit two letters of support. Each letter should be one page long and signed by the appropriate staff member.

1. A signed letter of support from your utility's authorizing official supporting your Phase 3 submission package. This letter must:
   - State that your utility supports your submission package for the ACT 1 Phase 3 Implementation Prize
   - Include a statement that the official signing the letter is authorized to make these commitments
   - Describe your leadership's commitment to any required funding to continue work to complete your Cybersecurity Roadmap or to cover ongoing costs of your Cybersecurity Roadmap solutions in future years, if applicable.
2. A signed letter of support on your organization's letterhead from your organization's finance department that indicates that the appropriate finance person has:
   - Reviewed and approved the final monthly Cybersecurity Roadmap budget
   - Reviewed and approve the final 3-year annual post-implementation budget
   - Ensured that the estimated costs are reasonable.

You are required to submit the following two final budgets.

1. A copy of your final monthly budget and associated timeline for the implementation of your Cybersecurity Roadmap. Your final Cybersecurity Roadmap budget should cover the costs by month required to fully implement your plan and include a breakdown of estimated costs associated with personnel, software licenses and fees, hardware/firmware, materials/components/equipment, service contracts (for both IT services and OT cybersecurity services), consultants, training, etc.
2. A copy of your final 3-year budget for annual costs associated with the continued operations and maintenance of the solutions you selected. Your post-implementation budget should include the annual costs for personnel, software licenses and fees, service contracts (for both IT services and OT cybersecurity services), consultants, training, etc.

In addition to these required documents, you are encouraged to provide additional letters or evidence of your utility's commitment to complete its roadmap. Provide as much evidence as you can of your utility's long-term commitment to complete your roadmap. For example:

a) A signed letter from your utility supporting the necessary budget to cover the annual post-implementation costs and that states the number of years that this funding will be included in your utility's annual budget request. The letter must include a statement that the official signing the letter is authorized to make these commitments.
b) A utility board or local government resolution describing the governing body's commitment to fully

support the utility's staff time and funding resources to complete its roadmap.

c) A letter of intent from the city manager, mayor, or county commissioner to support the utility's staff time, efforts, and funding allocations to implement the plan (if applicable).
d) Copies of press releases and any press coverage, social media postings, published articles, external communications with stakeholders, and other utility communications celebrating your utility's success in winning Commitment and Planning Prizes.
e) A letter from your utility's communications team describing their communications plan for press releases, social media postings, and other public efforts to celebrate your utility's success if you win an Implementation Prize.
f) Other documents demonstrating a long-term commitment.

General letters of support from parties that are not critical to the execution of your solution will not factor into your score.

3.3.3 Section 40126 Cybersecurity Plan

Competitors for an Implementation Prize must provide documentation of their work to complete the utility's Section 40126 Cybersecurity Plan. Below are the options:

- Your utility's point of contact must submit a signed confirmation letter indicating that a Section 40126 Cybersecurity Plan has been completed and that the plan has been securely transmitted to the PNNL team. This confirmation letter must be uploaded as part of your Implementation Prize submission package.
- If you have not completed your Section 40126 Cybersecurity Plan, your utility must:
    - Submit written documentation from the PNNL team that confirms the status of your Section 40126 Cybersecurity Plan.
    - Submit a signed letter from the appropriate staff member at your utility describing why the plan is not complete and your utility's timeline for completing the plan.

Additional information on the Section 40126 Cybersecurity Plans and access to the templates is available at: https://www.energy.gov/ceser/bipartisan-infrastructure-law-implementation.

Do not upload your Cybersecurity Plan to HeroX. All completed Section 40126 Cybersecurity Plans must be submitted directly to the PNNL team using the secure transmittal instructions found at the website listed above.

3.3.4 Phase 3 TA Navigator Review Form

DOE does not want your utility to submit sensitive information about your utility's systems in your prize submission package. Therefore, to verify that the actions required in the Implementation Phase were completed and met the expectations outline in the Prize Rules, an ACT 1 TA Navigator will review the products of your Implementation Phase and provide the results of that review using the Phase 3 TA Navigator Review Form.

You must submit this form to demonstrate that an ACT 1 TA Navigator has reviewed your Implementation Phase work. This form must be signed by an ACT 1 TA Navigator. The TA Navigator will:

1) Confirm that an appropriate process has been established to test that systems are secure after new technologies are installed

2) Review and comment on the success of processes used by the utility to engage nontechnical staff for any solutions that required staff behavioral changes for the solution to be successful in reducing cybersecurity risks
3) Review and comment on how the utility will ensure that all solutions can be effectively operated and maintained by the existing staff or that sufficient funding has been budgeted for appropriate staff training and/or ongoing costs for necessary service providers
4) Review and comment on the final budget and whether it includes all relevant costs associated with the roadmap; costs are reasonable; and the utility's timeline of when costs will be incurred reflects a realistic pace for the remaining work to be completed.

3.4 How Your Submission Will be Judged

The following information will be used by the reviewers to judge your Implementation Prize submission package:

1) Narrative responses
2) Authorizing official letter of support
3) Finance staff letter of support
4) Final monthly Cybersecurity Roadmap budget
5) Final 3-year annual post-implementation budget
6) Additional supporting documents demonstrating long-term commitment
7) Section 40126 Cybersecurity Plan Confirmation
8) Phase 3 TA Navigator Review Form.

After reviewing these items in your submission package, expert reviewers will evaluate your narrative responses and relevant submission package documents and assign a score for each bulleted statement listed below. The scores will range between 1 and 6.

Your cover page will not be included in the scoring of your submission package but will be required for your submission package to be considered complete.

Point Scale Used by Reviewers

1	2	3	4	5	6
Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree

Expert reviewers give a score of 1 to 6 for each statement below (maximum score 96 points):

Implementation Criterion 1: Documented Progress (maximum 36 points)

- Given the time allotted, the utility made substantial progress toward completing its roadmap.
- The utility provided compelling evidence that the changes they implemented resulted in an improvement in the cybersecurity posture of their IT systems.
- The utility provided compelling evidence that they have made improvements in the cybersecurity of their OT systems.

- The utility implemented a highly successful process that resulted in staff behavioral changes that were necessary to the success of the solution (Reviewers should consider both the TA Navigator Review Form and the response to Narrative Topic 1.).
- The utility used effective methods to identify and minimize third-party cybersecurity risks during the selection of solutions and in the contracting and purchasing stages.
- The utility's commitment to providing paid on-the-job training that enabled employees to improve their cybersecurity knowledge, skills, and abilities was supported by their response.

Implementation Criterion 2: Likelihood of Continued Progress (maximum 36 points)

- The utility effectively addressed challenges and, considering the work that has been completed, the quantity of remaining work scheduled, and the proposed budget and timeline, it is highly likely the utility will complete its roadmap (Reviewers should consider the final budget submitted, TA Navigator Review Form, and Narrative Topic 2.).
- The utility presented a realistic strategy that includes staff training and sufficient future budget allocations to effectively operate and maintain the cybersecurity solutions that are being implemented (Reviewers should consider both the final budget submitted and Narrative Topic 2.).
- The utility described documented processes it has institutionalized that appropriately engage relevant staff members to identify new and emerging cybersecurity risks.
- The utility developed and institutionalized appropriate processes to test the final configurations and settings of their technical solutions after implementation and to identify and address any cybersecurity risks that were discovered (Reviewers should consider both the TA Navigator Review Form and response to Narrative Topic 2.).
- The utility has identified the most important economic benefits and cybersecurity risk reductions associated with the solutions being implemented and has established a process that is highly likely to be successful at effectively communicating these values to senior leadership.
- The utility has demonstrated thoughtful reflection on how the work completed during the Commitment and Planning Phases has improved the cybersecurity capacity of its people and processes and institutionalized the lessons learned to facilitate continuous improvements in its cybersecurity posture.

Implementation Criterion 3: Commitment (maximum 18 points)

- The utility leadership fully supports implementing plans developed under this prize (Reviewers should consider the submitted budgets, letters of support or commitment, and Narrative Topic 2.).
- The utility developed a realistic budget and timeline to implement the cybersecurity solutions in its roadmap and has identified and committed the support and resources necessary for the ongoing operations and maintenance costs of solutions after the roadmap is fully implemented (Reviewers should consider the submitted budgets, letters of support or commitment, and Narrative Topic 2.).
- The additional evidence provided by the utility is compelling and supports the conclusion that it is committed to completing its roadmap and continuing to improve its cybersecurity (Reviewers should consider the submitted budgets, letters of support or commitment, and Narrative Topic 2.).

Implementation Criterion 4: Section 40126 Cybersecurity Plan (maximum 6 points)

- The utility has either completed or made substantial progress completing its Section 40126 Cybersecurity Plan and is working to address challenges in completing the plan (Reviewers will

consider the signed confirmation or other written document submitted by the utility.).

4 How We Determine Winners

A Prize Administrator will screen all submission packages for eligibility and confirm that all required documents are included in the submission package. The Prize Administrator, in consultation with DOE, will assemble a reviewer panel composed of subject matter experts and assign reviewers to independently score the content of each submission package. The expert reviewers may be composed of federal and nonfederal subject matter experts with expertise in relevant areas. Expert reviewers will review each submission package and provide a score for every criterion statement and a total score for each submission package. A final score for each submission package will be calculated and provided to the ACT 1 Prize Judge. The Prize Judge will consider the final scores and other factors to make a final determination of winners.

The expert reviewers and Prize Judge may not (a) have personal or financial interests in, or be an employee, officer, director, or agent of any entity that is a registered participant in the prize; or (b) have a familial or financial relationship with an individual who is a registered participant.

4.1 How the Final Score for a Submission Package is Calculated

The scoring of submission packages will proceed as follows:

- Experts will review each submission package individually.
- At least three expert reviewers will score each submission package.
- Reviewers will assign a score between 1 and 9 to each statement listed for each phase criterion. A score of 1 indicates that the reviewer strongly disagrees that the information provided in the competitor's submission package supports the statement, and the highest possible score indicates that the reviewer strongly agrees that the statement is supported by the information provided in the submission package.
- The reviewer's score for each criterion will be calculated by adding together the scores for each statement associated with that criterion.
- The reviewer's total score for the submission package will be calculated by adding together the reviewer's scores for each of the criterion.
- The final score for the submission package will be calculated by averaging the total scores from each reviewer that read the same submission package. For example, if there are three reviewers for the same submission package, the final score will be the average of the three reviewers' total scores.
- The final score will be used to inform the Prize Judge's decision on winners.

Example: Point Scale Used by Reviewers for a Bulleted Statement Worth 6 Points

1	2	3	4	5	6
Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree

4.2 Program Policy Factors

While the scores of the expert reviewers will be carefully considered, it is the role of the Prize Judge to maximize the impact of prize funds. Some factors outside of the control of competitors and beyond the independent expert reviewers' scope of review may need to be considered to accomplish this goal. The

following is a list of such factors. In addition to the reviewers' scores, the program policy factors listed below may be considered by the Prize Judge in determining winners:

- Geographic diversity and potential economic impact of projects.
- Whether the use of additional DOE funds and provided resources is nonduplicative and compatible with the stated goals of the RMUC Program and the DOE mission generally.
- The degree to which the submission is likely to lead to increased employment and manufacturing in the United States or provide other economic benefits to U.S. taxpayers.
- The degree to which the submission supports complementary DOE-funded efforts or projects, which, when taken together, will best achieve the goals and objectives of DOE.
- The degree to which the submission expands DOE's funding to new competitors and recipients who have not been supported by DOE in the past.
- The degree to which the submission enables new and expanding market segments.
- Whether the project promotes increased coordination with nongovernmental entities toward enabling a just and equitable clean energy economy in their region and/or community.
- The degree to which the submission enhances reliable access to electricity to disadvantaged or underserved communities.
- The degree to which the submission reduces the energy burden for customers/members in disadvantaged communities that are served by the utility.
- The degree to which the utility operates Defense Critical Electric Infrastructure, defined as any electric infrastructure located in any of the 48 contiguous states or the District of Columbia that serves a facility designated by the Secretary of Energy, pursuant to section 215A(c) of the Federal Power Act (16 U.S.C. § 824o-1(c)), but is not owned or operated by the owner or operator of such facility. See paragraph (4) of Section 215A(a) of the Federal Power Act (16 U.S.C. § 824o-1(a)(4)).
- The presence of important community services, including healthcare facilities, communications facilities, water facilities, and critical care facilities.
- Presence of regionally important economic drivers.

4.3 Final Determination

DOE will designate a federal employee as the ACT 1 Prize Judge before the final determination of the winners. Final determination of the winners by the Prize Judge will consider the reviewers' feedback and scores, your utility's submission package, and program policy factors.

4.4 Announcement of Winners

Approximately 60 days after the phase closes, the Prize Administrator will notify the winners and request the necessary information to distribute the prizes. The Prize Administrator will then publicly announce the winners.

Additional Requirements

Competitors are responsible for reading and complying with additional requirements described in Appendix 1.

COMPETITORS WHO DO NOT COMPLY WITH ALL APPENDIX 1 REQUIREMENTS MAY BE DISQUALIFIED.

5 RMUC Program Background

The IIJA, commonly referred to as the Bipartisan Infrastructure Law, directs DOE to invest $250 million in an RMUC Grant and Technical Assistance Program (RMUC Program) to improve the cybersecurity posture of eligible electric utilities. DOE will provide financial investments, TA, training, and other resources to enhance the cybersecurity posture of entities eligible to participate in the RMUC Program to help them protect against, detect, respond to, and recover from cybersecurity threats, and to increase their participation in cybersecurity threat information-sharing programs. Entities eligible to participate in the RMUC Program are:

- A rural electric cooperative
- A utility owned by a political subdivision of a state, such as a municipally owned electric utility
- A utility owned by any agency, authority, corporation, or instrumentality of one or more political subdivisions of a state
- A not-for-profit entity that is in a partnership with no fewer than six entities described above
- An investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year.

The RMUC Program is authorized to prioritize three segments of the eligible population: utilities with limited cybersecurity resources; utilities with assets critical to the reliability of the bulk power system; and utilities that own Defense Critical Electric Infrastructure. More information about the RMUC Program can be found at the RMUC Program website.

The ACT 1 Prize Program is one of the cornerstones of the RMUC Program intended to provide funding to reward eligible utilities for making informed decisions on purchasing and implementing solutions to address areas of highest risk. ACT 1 will focus on providing financial prizes and TA to eligible entities that have limited cybersecurity resources and/or serve military installations.

Appendix 1: Additional Terms and Conditions

A.1 Requirements

Your submission for the ACT 1 Prize Program is subject to the following terms and conditions:

- You must post the final content of your submission or upload the submission form before the submission period closes. Late submissions or any other form of submission may be rejected.
- All submissions that you wish to protect from public disclosure must be marked according to the instructions in Section 10 of Appendix 1 (Section A.10). Unmarked or improperly marked submissions will be deemed to have been provided with unlimited rights and may be used in any manner and for any purpose whatsoever.
- You must include all the required elements in your submission. The Prize Administrator may disqualify your submission after an initial screening if you fail to provide all required submission elements. Competitors may be given an opportunity to rectify submission errors due to technical challenges.
- Your submission must be in English and in a format readable by Microsoft Word or Adobe PDF. Scanned handwritten submissions will be disqualified.
- Submissions will be disqualified if they contain any matter that, in the sole discretion of DOE or NREL, is indecent, obscene, defamatory, libelous, and/or lacking in professionalism, or demonstrates a lack of respect for people or life on this planet.
- If you click "Accept" on the HeroX platform and proceed to register for any of the prizes described in this document, these rules will form a valid and binding agreement between you and DOE and are in addition to the existing HeroX Terms of Use for all purposes relating to these contests. You should print and keep a copy of these rules. These provisions only apply to the prize described here and no other prize on the HeroX platform or anywhere else.
- The Prize Administrator, when feasible, may give competitors an opportunity to fix nonsubstantive mistakes or errors in their submission packages.
- As part of your submission to this prize, you will be required to sign the following statement:

> I am providing this submission package as part of my participation in this prize. I understand that the information contained in this submission will be relied on by the federal government to determine whether to issue a prize to the named competitor. I certify under penalty of perjury that the named competitor meets the eligibility requirements for this prize competition and complies with all other rules contained in the Official Rules document. I further represent that the information contained in the submission is true and contains no misrepresentations. I understand false statements or misrepresentations to the federal government may result in civil and/or criminal penalties under 18 U.S.C. § 1001 and § 287, and 31 U.S.C. §§ 3729-3733 and 3801-3812.

A.2 Verification for Payments

The Prize Administrator will verify the identity and role of all competitors before distributing any prizes. Receiving a prize payment is contingent upon fulfilling all requirements contained herein. The Prize Administrator will notify winning competitors using provided email contact information for the individual or entity that was responsible for the submission. Each competitor will be required to sign and return to the

Prize Administrator, within 30 days of the date on the notice, a completed NREL Request for ACH Banking Information form and a completed W9 form (https://www.irs.gov/pub/irs-pdf/fw9.pdf). In the sole discretion of the Prize Administrator, a winning competitor will be disqualified from the competition and receive no prize funds if: (1) the person/entity does not respond to notifications; (2) the person/entity fails to sign and return the required documentation within the required time period; (3) the notification is returned as undeliverable; or (4) the submission or person/entity is disqualified for any other reason.

In the event of a dispute as to any registration, the authorized account holder of the email address used to register will be deemed to be the competitor. The "authorized account holder" is the natural person or legal entity assigned an email address by an internet access provider, online service provider, or other organization responsible for assigning email addresses for the domain associated with the submitted address. All competitors may be required to show proof of being the authorized account holder.

A.3 Teams and Single-Entity Awards

The Prize Administrator will award a single dollar amount to the designated primary submitter, whether consisting of a single or multiple entities. The primary submitter is solely responsible for allocating any prize funds among its member competitors or teammates as they deem appropriate. The Prize Administrator will not arbitrate, intervene, advise on, or resolve any matters or disputes between team members or competitors.

A.4 Submission Rights

By making a submission and consenting to the rules of the contest, a competitor is granting to DOE, the Prize Administrator, and any other third parties supporting DOE in the contest, a license to display publicly and use the parts of the submission that are designated as “public” for government purposes. This license includes posting or linking to the public portions of the submission on the Prize Administrator or HeroX applications, including the contest website, DOE websites, and partner websites, and the inclusion of the submission in any other media worldwide. The submission may be viewed by DOE, Prize Administrator, and judges and reviewers for purposes of the contests, including but not limited to screening and evaluation purposes. The Prize Administrator and any third parties acting on their behalf will also have the right to publicize competitors’ names and, as applicable, the names of competitors’ team members and organization that participated in the submission on the contest website indefinitely.

By entering, the competitor represents and warrants that:

1. The competitor’s entire submission is an original work by the competitor, and the competitor has not included third-party content (such as writing, text, graphics, artwork, logos, photographs, likeness of any third party, musical recordings, clips of videos, television programs or motion pictures) in or in connection with the submission, unless: (1) otherwise requested by the Prize Administrator and/or disclosed by the competitor in the submission, and (2) competitor has either obtained the rights to use such third-party content, or the content of the submission is considered in the public domain without any limitations on use.
2. Unless otherwise disclosed in the submission, the use thereof by Prize Administrator, or the exercise by Prize Administrator of any of the rights granted by competitor under these rules, does not and will not infringe or violate any rights of any third party or entity, including, without limitation, patent, copyright, trademark, trade secret, defamation, privacy, publicity, false light, misappropriation, intentional or negligent infliction of emotional distress, confidentiality, or any contractual or other rights.

3. All persons who were engaged by the competitor to work on the submission or who appear in the submission in any manner have:
    a. Given the competitor their express written consent to submit the submission for exhibition and other exploitation in any manner and in any and all media, whether now existing or hereafter discovered, throughout the world
    b. Provided written permission to include their name, image, or pictures in or with the submission (or, if a minor who is not competitor's child, competitor must have the permission of the minor's parent or legal guardian), and the competitor may be asked by the Prize Administrator to provide permission in writing
    c. Not been and are not currently under any union or guild agreement that results in any ongoing obligations resulting from the use, exhibition, or other exploitation of the submission.

A.5 Copyright

Each competitor represents and warrants that the competitor is the sole author and copyright owner of the submission; that the submission is an original work of the competitor or that the competitor has acquired sufficient rights to use and to authorize others, including DOE, to use the submission, as specified throughout the rules; that the submission does not infringe upon any copyright or any other third-party rights of which the competitor is aware; and that the submission is free of malware.

A.6 Contest Subject to Applicable Law

All contests are subject to all applicable federal laws and regulations. Participation constitutes each participant's full and unconditional agreement to these Official Rules and administrative decisions, which are final and binding in all matters related to the contest. This notice is not an obligation of funds; the final award is contingent upon the availability of appropriations.

A.7 Resolution of Disputes

DOE is solely responsible for administrative decisions, which are final and binding in all matters related to the contest.

Neither DOE nor the Prize Administrator will arbitrate, intervene, advise on, or resolve any matters between team members or among competitors.

A.8 Publicity

The winners of these prizes (collectively, "winners") will be featured on DOE and NREL websites.

Except where prohibited, participation in the contest constitutes each winner's consent to DOE's and its agents' use of each winner's name, likeness, photograph, voice, opinions, and/or hometown and state information for promotional purposes through any form of media worldwide, without further permission, payment, or consideration.

A.9 Liability

Upon registration, all participants agree to assume any and all risks of injury or loss in connection with or in any way arising from participation in this contest. Upon registration, except in the case of willful misconduct, all participants agree to and thereby do waive and release any and all claims or causes of action against the federal government and its officers, employees, and agents for any and all injury and damage of any nature whatsoever (whether existing or thereafter arising, whether direct, indirect, or consequential, and whether foreseeable or not), arising from their participation in the contest, whether the claim or cause of action arises under contract or tort.

In accordance with the delegation of authority to run this contest delegated to the judge responsible for this prize, the judge has determined that no liability insurance naming DOE as an insured will be required of competitors to compete in this competition per 15 U.S.C. § 3719(i)(2). Competitors should assess the risks associated with their proposed activities and adequately insure themselves against possible losses.

A.10 Records Retention and Freedom of Information Act

All materials submitted to DOE as part of a submission become DOE records and are subject to the Freedom of Information Act. The following applies only to portions of the submission not designated as public information in the instructions for submission. If a submission includes trade secrets or information that is commercial or financial, or information that is confidential or privileged, it is furnished to the government in confidence with the understanding that the information shall be used or disclosed only for evaluation of the application. Such information will be withheld from public disclosure to the extent permitted by law, including the Freedom of Information Act. Without assuming any liability for inadvertent disclosure, DOE will seek to limit disclosure of such information to its employees and to outside reviewers when necessary for review of the application or as otherwise authorized by law. This restriction does not limit the government's right to use the information if it is obtained from another source.

Submissions containing confidential, proprietary, or privileged information must be marked as described below. Failure to comply with these marking requirements may result in the disclosure of the unmarked information under the Freedom of Information Act or otherwise. The U.S. government is not liable for the disclosure or use of unmarked information and may use or disclose such information for any purpose.

The submission must be marked as follows and identify the specific pages containing trade secrets, confidential, proprietary, or privileged information: "Notice of Restriction on Disclosure and Use of Data: Pages [list applicable pages] of this document may contain trade secrets, confidential, proprietary, or privileged information that is exempt from public disclosure. Such information shall be used or disclosed only for evaluation purposes. [End of Notice]"

The header and footer of every page that contains confidential, proprietary, or privileged information must be marked as follows: "Contains Trade Secrets, Confidential, Proprietary, or Privileged Information Exempt from Public Disclosure." In addition, each line or paragraph containing proprietary, privileged, or trade secret information must be clearly marked with double brackets.

Competitors will be notified of any Freedom of Information Act requests for their submissions in accordance with 10 C.F.R. Part 1004. Competitors may then have the opportunity to review materials and

work with a Freedom of Information Act representative prior to the release of materials. DOE does intend to keep all submission materials private except for those materials designated as "will be made public."

IIJA §40124 (e) Protection of Information, states that information provided to, or collected by, the federal government pursuant to this section the disclosure of which the Secretary reasonably foresees could be detrimental to the physical security or cybersecurity of any electric utility or the bulk power system:

(1) Shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code
(2) Shall not be made available by any Federal agency, State, political subdivision of a State, or Tribal authority pursuant to any Federal, State, political subdivision of a State, or Tribal law, respectively, requiring public disclosure of information or records.

A.11 Privacy

If you choose to provide HeroX with personal information by registering or completing the submission package through the contest website, you understand that such information will be transmitted to DOE and may be kept in a system of records. Such information will be used only to respond to you in matters regarding your submission and/or the contest unless you choose to receive updates or notifications about other contests or programs from DOE on an opt-in basis. DOE and NREL are not collecting any information for commercial marketing.

A.12 General Conditions

DOE reserves the right to cancel, suspend, and/or modify the prize, or any part of it, at any time. If any fraud, technical failures, or any other factor beyond DOE's reasonable control impairs the integrity or proper functioning of the prize, as determined by DOE in its sole discretion, DOE may cancel the prize. Any performance toward prize goals is conducted entirely at the risk of the competitor, and DOE shall not compensate any competitors for any activities performed in furtherance of this prize.

Although DOE may indicate that it will select up to several winners for each prize, DOE reserves the right to only select competitors that are likely to achieve the goals of the program. If, in DOE's determination, no competitors are likely to achieve the goals of the program, DOE will select no competitors to be winners and will award no prize money.

DOE may conduct a risk review, using government resources, of the competitor and project personnel for potential risks of foreign interference. The outcomes of the risk review may result in the submission being eliminated from the prize competition. This risk review, and potential elimination, can occur at any time during the prize competition. An elimination based on a risk review is not appealable.

A.13 National Environmental Policy Act Compliance

This prize is subject to the National Environmental Policy Act (NEPA) (42 U.S.C. § 4321, et seq.). NEPA requires federal agencies to integrate environmental values into their decision-making processes by considering the potential environmental impacts of their proposed actions. For additional background on NEPA, see DOE's NEPA website at http://nepa.energy.gov/.

While NEPA compliance is a federal agency responsibility and the ultimate decisions remain with the federal agency, all participants in the ACT 1 Prize will be required to assist in the timely and effective

completion of the NEPA process in the manner most pertinent to their participation in the prize competition. Participants may be asked to provide DOE with information on fabrication and testing of their device such that DOE can conduct a meaningful evaluation of the potential environmental impacts.

A.14 Return of Funds

As a condition of receiving a prize, competitors agree that if the prize was made based on fraudulent or inaccurate information provided by the competitor to DOE, DOE has the right to demand that any prize funds or the value of other noncash prizes be returned to the government.

ALL DECISIONS BY DOE ARE FINAL AND BINDING IN ALL MATTERS RELATED TO THE PRIZE.