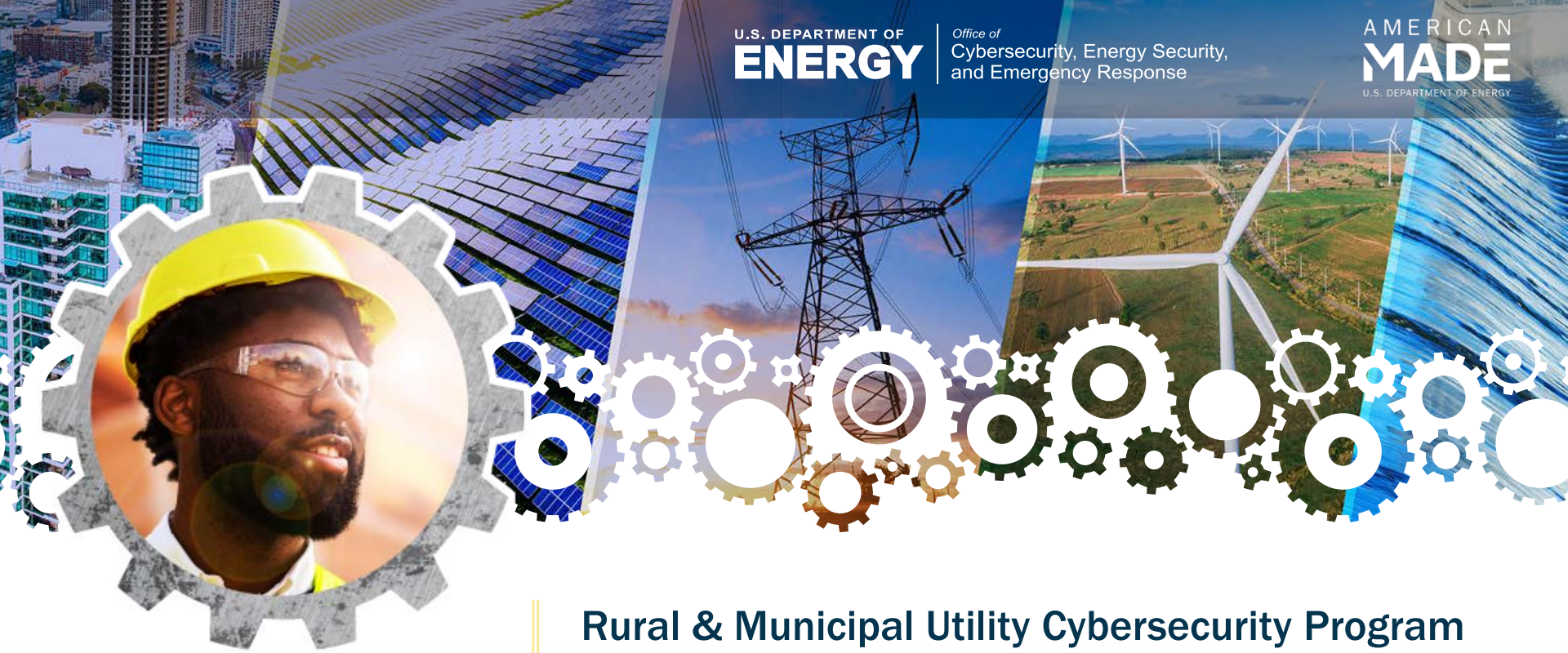U.S. DEPARTMENT OF **ENERGY** | *Office of* Cybersecurity, Energy Security, and Emergency Response

AMERICAN **MADE** U.S. DEPARTMENT OF ENERGY

AMERICAN **MADE** U.S. DEPARTMENT OF ENERGY

Rural & Municipal Utility Cybersecurity Program
Advanced Cybersecurity Technology Prize

ACT 1 Prize
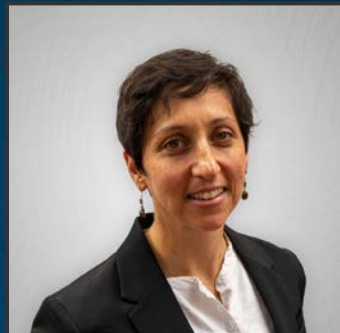Webinar 2: Future Phases Overview
October 11, 2023

THIS WEBINAR WILL BE RECORDED.

Gunnar Tande
Prize Lead
NREL

Cynthia Hsu
Cybersecurity Program Manager
RMUC Program
DOE CESER

Fania Barwick
Implementation Manager
RMUC Program
DOE CESER

AMERICAN
MADE
U.S. DEPARTMENT OF ENERGY

Agenda

1	Prize Timeline and Phases
2	Phase 1: Commitment Submission Highlights
3	RMUC Utility Service Territory Report
4	Key Goals of Future Phases
5	Technical Assistance Process Overview
6	Section 40126 Cybersecurity Plan Overview
7	Next Steps and FAQs

Housekeeping

This webinar is being recorded and will be posted on HeroX before end of Oct.

Questions?

- To submit a question, please type it into the Q&A box on the right-hand side of your screen next to the chat box.

- We will not respond to your questions during the webinar; we will post responses on HeroX next week.
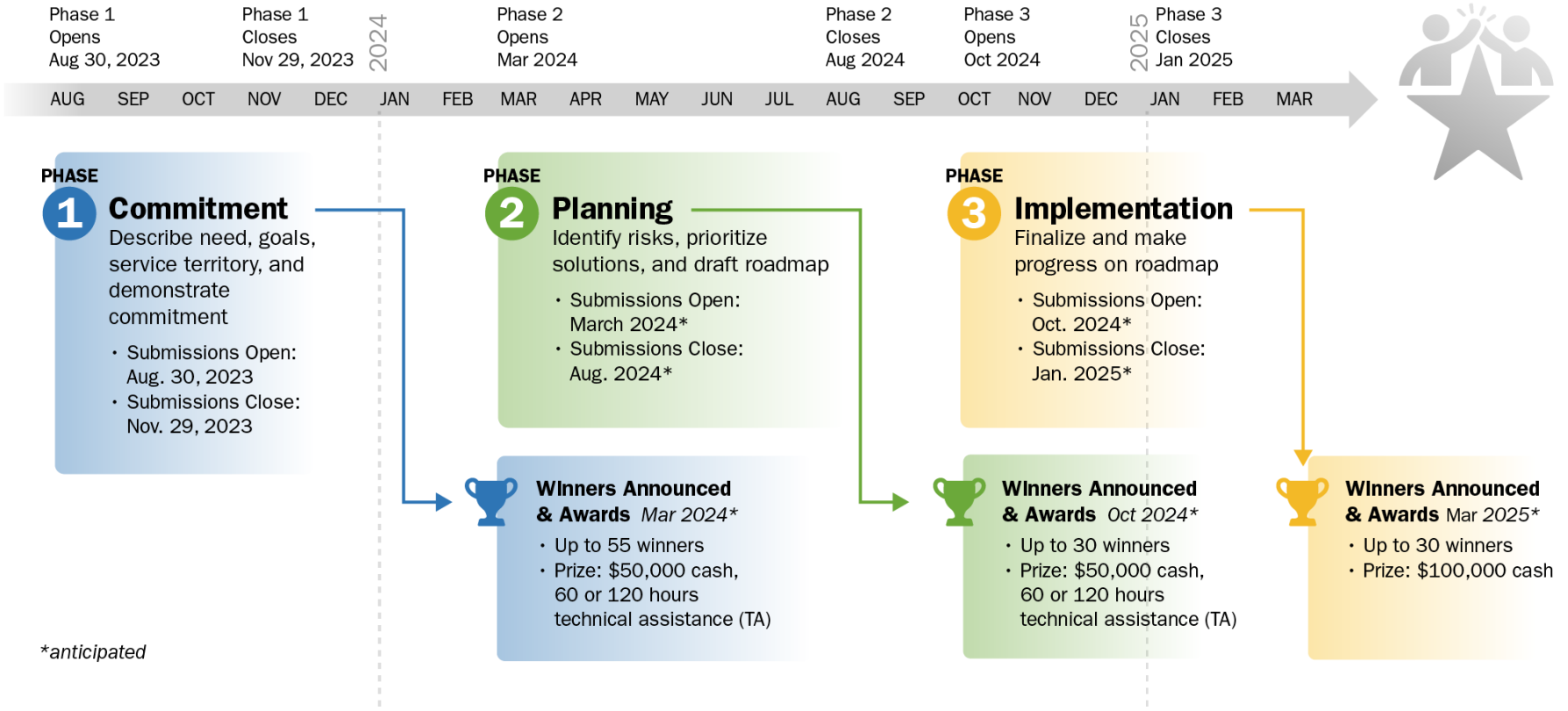
Technical items:

- In Zoom, the presentation appears in full screen by default. You can press the Escape key to exit the full screen and return to the Zoom window.

- If you experience technical issues, please check your audio settings under the Audio tab.

- If you continue experiencing issues, direct message the host.

RMUC Program:
Advanced Cybersecurity Technology (ACT) 1 Prize

Empowering utilities with limited cybersecurity resources to make critical investments in staff training, governance processes, and technologies to harden their systems against threats.

https://www.herox.com/ACT1Prize

Phase 1 Opens Aug 30, 2023

Phase 1 Closes Nov 29, 2023

2024

Phase 2 Opens Mar 2024

Phase 2 Closes Aug 2024

Phase 3 Opens Oct 2024

2025

Phase 3 Closes Jan 2025

AUG | SEP | OCT | NOV | DEC | JAN | FEB | MAR | APR | MAY | JUN | JUL | AUG | SEP | OCT | NOV | DEC | JAN | FEB | MAR

PHASE 1 — Commitment

Describe need, goals, service territory, and demonstrate commitment

- Submissions Open: Aug. 30, 2023
- Submissions Close: Nov. 29, 2023

PHASE 2 — Planning

Identify risks, prioritize solutions, and draft roadmap

- Submissions Open: March 2024*
- Submissions Close: Aug. 2024*

PHASE 3 — Implementation

Finalize and make progress on roadmap

- Submissions Open: Oct. 2024*
- Submissions Close: Jan. 2025*

Winners Announced & Awards *Mar 2024*

- Up to 55 winners
- Prize: $50,000 cash, 60 or 120 hours technical assistance (TA)

Winners Announced & Awards *Oct 2024*

- Up to 30 winners
- Prize: $50,000 cash, 60 or 120 hours technical assistance (TA)

Winners Announced & Awards *Mar 2025*

- Up to 30 winners
- Prize: $100,000 cash

anticipated

Phase 1: Commitment

Submission Highlights

AMERICAN MADE
U.S. DEPARTMENT OF ENERGY

To Apply for a Commitment Prize, the Utility Must:

☑ **Have staff from the utility attend or watch two required ACT 1 Prize webinars.**

☑ **Upload a submission package that includes all of the following items:**

1. Cover page and narrative (maximum 3,000 words)
2. Utility Profile Form (*Use form provided.*)
3. RMUC Utility Service Territory Report (USTR) (*Use report provided, or alternative source if USTR is not available.*)
4. Technical Assistance (TA) Request Form (*Use form provided.*)
5. Letter of support from your organization's authorizing official
6. Mandatory ACT 1 Prize virtual webinars attendance confirmation.

⚠ The utility's submission package must include **all of these items** to be considered complete. *Incomplete submission packages will be ineligible to compete and will not be forwarded to the reviewer panel for scoring.*

Scoring the Submission

Prize judges will review this information to score your submission:

- Narrative: This is required and scored, <u>up to 90 points total</u>.

- <u>*The following are required*</u> and reviewed but not scored:

    - **Letter of support** from your utility's authorizing official

    - **Utility Profile Form**

    - **RMUC USTR** (or alternative source if USTR is not available).

1.3.1 Cover Page & Narrative
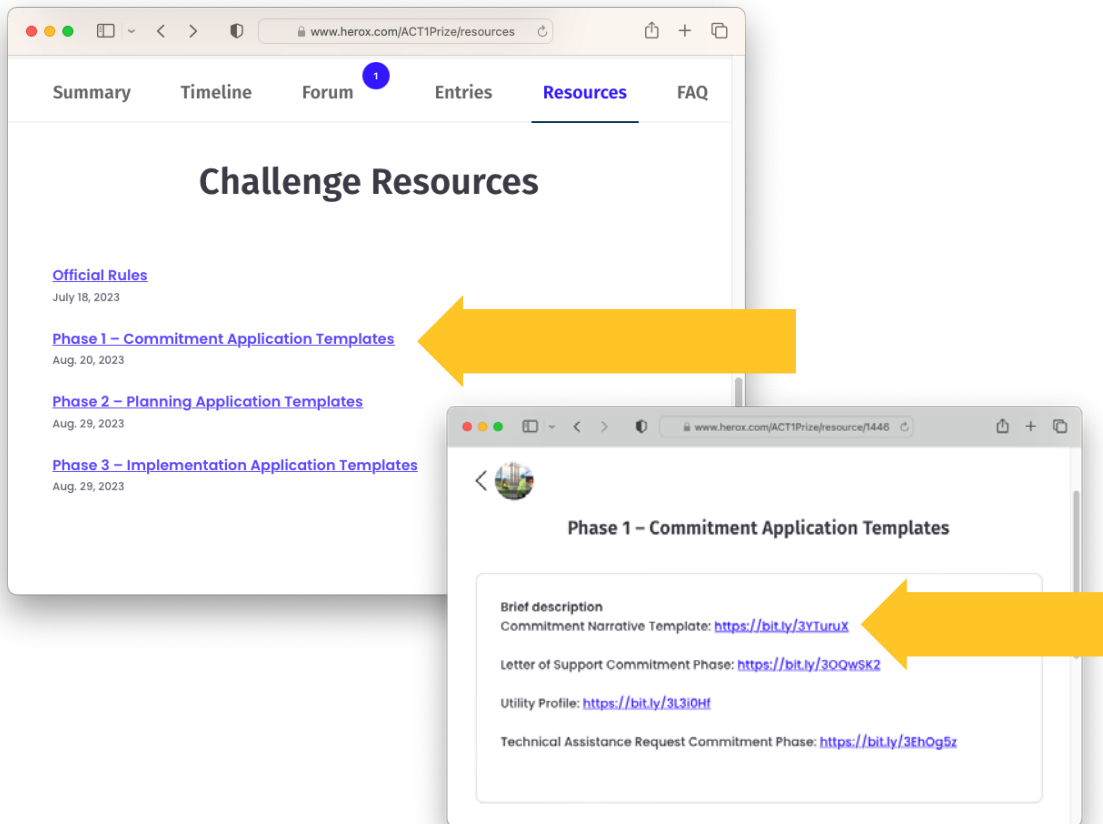
There is a **Narrative Template** that includes a cover page you can use.

The template provides additional guidance and is located on the ACT 1 HeroX Prize Platform under the "Challenge Resources" → "Phase 1 – Commitment Application Templates."

1.3.1 Cover Page & Narrative *TEMPLATE*

Advanced Cybersecurity Technology (ACT) 1 Prize
[Official Team Name Here]

Phase One: Commitment
Month Year

AMERICAN MADE
U.S. DEPARTMENT OF ENERGY

Page 1 of 11

Phase 1: Commitment Cover Page
Please delete or replace all bracketed guidance text prior to submission.

[Commitment Prize Project Title]

[ACT 1 Prize Track]

[Utility Name and City, State, and Nine-Digit Zip Code]

[Primary Point of Contact for ACT 1 Commitment Prize Submission Package (name, title, email, phone number)]

[List all of your utility's Commitment Prize Team members (names and job titles)]

Phase 1: Commitment Narrative
Please delete or replace all bracketed guidance text prior to submission.

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

Topic 1 – Utility Need and Cybersecurity Maturity Level

1. Describe your utility's current barriers and challenges to improving its cybersecurity posture.

   [For example, does your utility have access to service providers that can come on site to provide the level of technical assistance needed, do you have locally available cybersecurity training opportunities, can commercially available technical solutions be implemented and managed by your existing staff, are available solutions affordable, do you need help with policies and procedures, does your legal/purchasing/procurement staff understand how to negotiate purchases and contracts that minimize third-party cybersecurity risks, etc.]

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, please explain why.

   [If you are a utility serving military installations, briefly describe the military installations in your service territory. If you are competing in the LIMITED CYBERSECURITY RESOURCES track, describe the criteria you used to define your utility as a limited cybersecurity resources utility. For example: funding, number of staff, staff skills and abilities, time, leadership support, etc.]

3. What actions will your utility take to ensure the cybersecurity (confidentiality and integrity) of the information in your submission package?

   [As part of your application, your utility will assemble information that is sensitive and needs to be protected. What actions will your utility take to ensure the cybersecurity (confidentiality and integrity) of the information in your submission package? The steps you take now to ensure the cybersecurity of your submission package will be useful to your utility in the second phase, the Planning Phase, when you will create a Section 40126 Cybersecurity Plan.[1]]

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.

   [Please provide a description of your utility's cybersecurity maturity. On a scale ranging from very low maturity to very high maturity how would you rate your utility? Please give a brief description of why you scored your utility the way you did. If your answer is based on the results of one or more completed cybersecurity assessments (see examples below), please provide the names of the assessments and the organization that created the assessments. Do not provide specific results of the assessment(s).]

[1] Section 40216 of the Infrastructure Investment and Jobs Act (IIJA) provides a framework for ensuring that the U.S. Department of Energy's (DOE) 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. More information is available here: Bipartisan Infrastructure Law Implementation | Department of Energy.

Page 5 of 11

1.3.1 Cover Page & Narrative *TEMPLATE*

[Topic 1 Judging Criteria:

- 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)
  - o Limited geographic access to service providers
  - o Limited geographic access to cybersecurity training
  - o Limited staff knowledge, skills, and abilities to use and maintain existing off-the-shelf cybersecurity solutions
  - o Limited number of staff relative to its service territory and number of customers/members served
  - o Limited ability to afford existing off-the-shelf cybersecurity solutions
  - o 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.]

At the end of each topic area, the judging criteria from the prize rules are repeated.

You can use the judging criteria to understand what the judges will be looking for in your narrative responses. This can help you decide what to include in your narrative responses.

Narrative

> ⚠️ **NOTE:**
>
> Your narrative will be scored by the reviewers, and it is worth 90 points.
>
> This is one of the most important parts of your submission package.

Phase 1: Commitment Narrative
Please delete or replace all bracketed guidance text prior to submission.

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

Topic 1 – Utility Need and Cybersecurity Maturity Level

1. Describe your utility's current barriers and challenges to improving its cybersecurity posture.

   [For example, does your utility have access to service providers that can come on site to provide the level of technical assistance needed, do you have locally available cybersecurity training opportunities, can commercially available technical solutions be implemented and managed by your existing staff, are available solutions affordable, do you need help with policies and procedures, does your legal/purchasing/procurement staff understand how to negotiate purchases and contracts that minimize third-party cybersecurity risks, etc.]

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, please explain why.

   [If you are a utility serving military installations, briefly describe the military installations in your service territory. If you are competing in the LIMITED CYBERSECURITY RESOURCES track, describe the criteria you used to define your utility as a limited cybersecurity resources utility. For example: funding, number of staff, staff skills and abilities, time, leadership support, etc.]

3. What actions will your utility take to ensure the cybersecurity (confidentiality and integrity) of the information in your submission package?

   [As part of your application, your utility will assemble information that is sensitive and needs to be protected. What actions will your utility take to ensure the cybersecurity (confidentiality and integrity) of the information in your submission package? The steps you take now to ensure the cybersecurity of your submission package will be useful to your utility in the second phase, the Planning Phase, when you will create a Section 40126 Cybersecurity Plan.[1]]

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.

   [Please provide a description of your utility's cybersecurity maturity. On a scale ranging from very low maturity to very high maturity how would you rate your utility? Please give a brief description of why you scored your utility the way you did. If your answer is based on the results of one or more completed cybersecurity assessments (see examples below), please provide the names of the assessments and the organization that created the assessments. Do not provide specific results of the assessment(s).]

   _____
   [1] Section 40216 of the Infrastructure Investment and Jobs Act (IIJA) provides a framework for ensuring that the U.S. Department of Energy's (DOE) 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. More information is available here: Bipartisan Infrastructure Law Implementation | Department of Energy.

   Page 5 of 11

Phase 1: Commitment

RMUC Utility Service Territory Report (USTR)

AMERICAN
MADE
U.S. DEPARTMENT OF ENERGY

Reminder: How To Request Your USTR

Use this link to request your RMUC USTR:
https://forms.office.com/g/AjQPHvPbTh.

Find your utility name and utility number in the EIA-861 report on the HeroX Resources tab and enter them into this form. If you cannot find your EIA-861 number, please contact the prize administrator.

The ACT 1 Prize team will send the USTR to the requester.

This RMUC USTR is required in your submission package.

The prize deadline is Nov 29. Requests for USTRs must be received by Nov 15. USTRs will not be sent to any requests received after Nov 15.

Request Form for RMUC Utility Service Territory Report

Data collected from this form will be used by the Advanced Cybersecurity Technology (ACT) 1 Prize Team to generate your utility's RMUC Utility Service Territory Report.

The report will be emailed directly to you and will be necessary for the completion of your Planning Phase 1 application. A review of how to use the RMUC Utility Service Territory Report will be provided during the second ACT 1 Prize mandatory webinar.

You can register for this second webinar via this link: https://nrel.zoomgov.com/webinar/register/WN_a0DH-0gIT-irw55uGsqMzQQ

* Required

1. What is your first name? *

[Enter your answer]

2. What is your last name? *

[Enter your answer]

3. What is your work email address? *

[Enter your answer]

4. Enter your Utility Name as captured in column "D" of the EIA-861 Annual Electric Power Industry Report (see Herox Resources Tab for this report). *

[Enter your answer]

5. Enter your Utility Number as captured in column "C" of the EIA-861 Annual Electric Power Industry Report (see Herox Resources Tab for this report). *

[Enter your answer]

6. Enter the state that your utility is located in here *

[Enter your answer]

USTR Page 1

Includes:

- Sources for content

- How to use report content

- List of public tools you can use in addition to the USTR

- *The accuracy of this content is not guaranteed.*

RMUC Utility Service Territory Report

The information contained in this report was generated based on publicly available map layers which may not have been recently updated. Utility Service Territory boundaries may be outdated so please use your utility's internal service territory records to confirm whether the census tracts identified on this map are up to date with any changes in your service territory. Please utilize this information at your discretion as DOE does not guarantee its accuracy.

ACT 1 Prize Program competitors may use the enclosed report as background information when responding to questions that are part of the ACT 1 Prize Program submission package. The information in this report may be useful when completing the ACT 1 Prize Program Narrative, Applicant Profile Document, and other required submission package documents as appropriate. We encourage competitors to use the enclosed RMUC Utility Service Territory Report as well as the publicly available Energy Justice Mapping Tool, Climate and Economic Justice Screening Tool, OCED Rural or Remote Area Geospatial Dashboard, and any additional verifiable resources to complete their ACT 1 Prize submission packages.

This data is provided to you with no warranty, expressed or implied, regarding the accuracy or utility of the data on any other system, in derived products or data alterations, nor shall the act of distribution constitute any such warranty.

The information in this report is for general informational purposes only. For details on the definition of disadvantaged communities, please visit https://energyjustice.egs.anl.gov/. For details on Electric Power Retail Service Territories and military installation areas, please visit the Homeland Infrastructure Foundation-Level Data (HIFID) website (https://hifld-geoplatform.opendata.arcgis.com/).

USTR Page 2

Includes:

- Service territory map

- No. of census tracks

- Total population

- Average census track size.

Figure 1 Disadvantaged Communities (DACs) Within the Electric Retail Service Territory
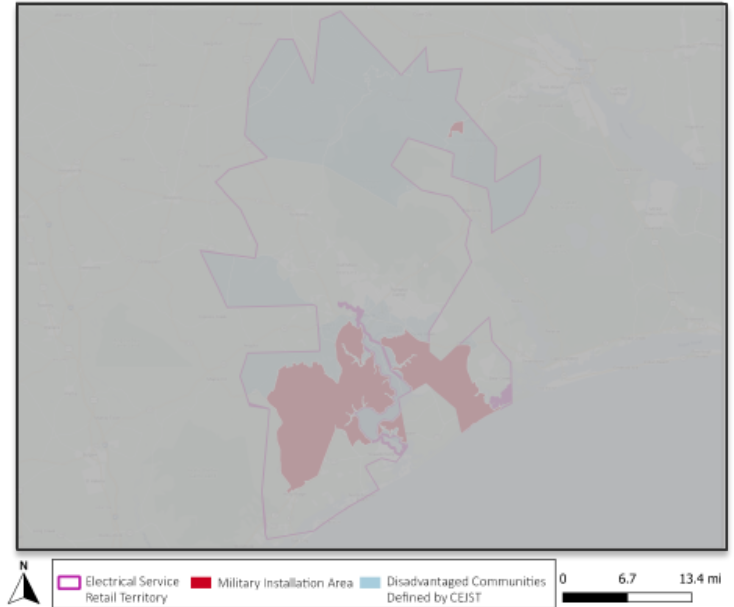

| Electrical Service Retail Territory | Military Installation Area | Disadvantaged Communities Defined by CEJST |

0   6.7   13.4 mi

Table 1. Utility Service Territory Overview

	Total Service Territory	Disadvantaged Communities*
Number of Census Tracts	43	22
Est. Total Population	178,757	72,523
Average Census Tract size	22.6 sq mi	24.9 sq mi

USTR Page 3

Includes:

Number of DACs within the utility service territory that exceed the CEJST threshold for each of eight CEJST burden categories.

Table 2. Number of Disadvantaged Community Census Tracts (DACs) within the Electrical Service Retail Territory that Exceed the Threshold for Each of the Eight CEJST* Burden Categories

Burden Category	Number of DACs
Climate	16
Energy	0
Traffic	5
Housing	1
Pollution	5
Water	2
Health	5
Workforce	9
Tribal land	0
Surrounded by disadvantaged communities	4

*The Council on Environmental Quality's Climate and Economic Justice Screening Tool (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 burden*, OR
2. Is on land within the boundaries of a Federally Recognized Tribe, OR
3. Is completely surrounded by disadvantaged communities and is at or above the 50% percentile for low income.

The eight burden categories and the thresholds used in the CEJST for each category are described at: https://screeningtool.geoplatform.gov/en/methodology#3/33.47/-97.5.

USTR Page 4

Includes (if relevant):

- Number of military installations within the service territory

- Site name and status

- Area (in acres).

Table 3. Military Installations Located within the Service Territory

Site Name	Component	Status	State Territory	Area (Acres)
Site	MC Active	Active	North Carolina	68,055
Grove	MC Active	Active	North Carolina	950
MCB Camp Lejeune	MC Active	Active	North Carolina	54,816

Completing and submitting the Utility Profile Form is required for the Commitment Phase.

Commitment Prize: Utility Profile Form	
Project Title	
Utility Name	
Nine Digit Zip	
Utility Type (Generation, Transmission, Distribution)	
Employees	
Total number of employees	
Total number of full time equivalent IT employees	
Total number of full time equivalent cybersecurity employees	
What is the employee to customer/member ratio of your utility?	
Budget and Funding	
Total Annual Organizational Revenue	
Total Annual Organizational Expense	
Have you received prior DOE funding?	
If yes, what years and which projects?	
What were your average estimated cybersecurity and IT expenses per year for last two years. (Please include license costs, service contracts, personnel, hardware, software non-license costs, Managed Service Providers (MSP), Information Technology Providers (ITP), consultants, digital infrastructure costs associated with other major projects)	
Service Territory Profile	
How many meters are in your service territory?	
What are the meters/mile?	
How many substations does your utility have?	
What is the size of your service territory?	
What kinds of critical infrastructure (non-defense) are in your utility's service area? For example: hospitals, water systems, regional communication providers, etc.?	
Describe the types of industrial and commercial customers/members you have in your service territory that rely on your utility to provide critical services to your community?	
Do you have any military installations in your service territory? How many and what kind?	
Are there Historically Black Colleges and Universities (HBCUs) and Minority Serving Institutions (MSIs) in your service area?	
What is the average size of the census tracts in your service territory?	
What is the approximate population of your service territory?	
Do you have any disadvantaged communities (DACs) in your service area?	
If so, what percent the population in your service territory falls into the Disadvantaged Communities census tract?	
Describe the programs and resources that your utility provides to your community to address DAC needs and foster diversity, equity, inclusion, and accessibility (DEIA).	
What services are you providing to your community? For example: Energy rebates, weatherization services, vehicle charging	

Use the
RMUC USTR
to complete questions on the
Utility Profile Form.

Service Territory Profile		
How many meters are in your service territory?		
What are the meters/mile?		
How many substations does your utility have?		
What is the size of your service territory?		
What kinds of critical infrastructure (non-defense) are in your utility's service area? For example: hospitals, water systems, regional communication providers, etc.?		
Describe the types of industrial and commercial customers/members you have in your service territory that rely on your utility to provide critical services to your community?		
Do you have any military installations in your service territory? How many and what kind?		
Are there Historically Black Colleges and Universities (HBCUs) and Minority Serving Institutions (MSIs) in your service area?		
What is the average size of the census tracts in your service territory?		
What is the approximate population of your service territory?		
Do you have any disadvantaged communities (DACs) in your service area?		
If so, what percent the population in your service territory falls into the Disadvantaged Communities census tract?		
Describe the programs and resources that your utility provides to your community to address DAC needs and foster diversity, equity, inclusion, and accessibility (DEIA).		
What services are you providing to your community? For example: Energy rebates, weatherization services, vehicle charging		

Use the **RMUC UTSR** to complete questions in the **Commitment Narrative Template** (*also required*).

Phase 1: Commitment Narrative

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

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

Topic 1 – Utility Need and Cybersecurity Maturity Level

1. Describe your utility's current barriers and challenges to improving its cybersecurity posture.

   [For example, does your utility have access to service providers that can come on site to provide the level of technical assistance needed, do you have locally available cybersecurity training opportunities, can commercially available technical solutions be implemented and managed by your existing staff, are available solutions affordable, do you need help with policies and procedures, does your legal/purchasing/procurement staff understand how to negotiate purchases and contracts that minimize third-party cybersecurity risks, etc.]

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, please explain why.

   [If you are a utility serving military installations, briefly describe the military installations in your service territory. If you are competing in the LIMITED CYBERSECURITY RESOURCES track, describe the criteria you used to define your utility as a limited cybersecurity resources utility. For example: funding, number of staff, staff skills and abilities, time, leadership support, etc.]

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 Rural and Municipal Utility Cybersecurity (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.

   [For example, are there major regional hospitals or other medical facilities, regional communication providers or data hubs, economically important industrial and/or commercial entities, minority serving institutions or other regionally important educational institutions, etc.? Do not list every example. Provide a summary of the kinds of services and facilities your utility serves and describe why they are important in your community or region.]

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 (DAC[2]).

   [How would you describe the economic conditions of the communities you serve? Use the RMUC Utility Service Territory Report or other links provided to calculate the proportion of the population in your utility's service territory that is located in a disadvantaged community (DAC).]

Phase 2: Planning

Key Goals

Key Goals

- Each utility will **assess** their network, their system architecture, and their technology tools.

- This information will be used by the utility to:

  - Identify cybersecurity risks and vulnerabilities.

  - Help prioritize potential solutions.

  - Develop a roadmap and budget to support improvements to the utility's cybersecurity posture.

- Each utility will begin work on their Section 40126 cybersecurity plan.

Evaluation Criteria

1. Identifies gaps and prioritizes risks

2. Drafts a roadmap

3. Captures project risks

4. Institutionalizes a culture of continuous improvement

5. Estimates roadmap budget

6. Includes draft section 40126 cybersecurity plan.

Successful Submission Demonstrates Utility Has:

1. Completed a network and system architecture review
2. Completed a cybersecurity technology stack assessment
3. Analyzed the results of the architecture review and stack assessment and created a cybersecurity gap/risk analysis
4. Used the cybersecurity gap/risk analysis to identify priority risks
5. Developed a draft cybersecurity roadmap for improvements that include solutions for staff training, changes in policies and procedures, and changes to technologies
6. Established program management processes to address common project risks
7. Identified technical risks and developed mitigation options
8. Created repeatable processes to assess and prioritize cybersecurity risks
9. Completed a draft budget for the implementation roadmap
10. Drafted an initial Section 40126 cybersecurity plan.

More Points Are Possible for Utilities That:

- Engage **all relevant staff** in the discussion and prioritization of cybersecurity risks and solutions.

- Select solutions that address prioritized risks.

- Establish clear roles, responsibilities, and program management strategies that can maximize the likelihood of success.

- Create long-term processes for continuous improvements in the ability to identify and prioritize cybersecurity risks.

Phase 3: Implementation

Key Goals

Key Goals

- Utilities will collaborate with TA providers and industry experts to implement the solutions outlined in the planning phase.

- The TA providers 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

  - Support the development of processes to confirm the cybersecurity of solutions after they are implemented.

Evaluation Criteria

1. Documents progress

2. Shows likelihood of continued progress

3. Demonstrates commitment

4. Includes completed Section 40126 cybersecurity plan.

Successful Submission Demonstrates Utility Has:

1. Completed its roadmap budget

2. Made significant progress on implementing its roadmap

3. Developed a process to test the cybersecurity of its systems after full integration of solutions

4. Committed to continuing to implement its roadmap

5. Completed its Section 40126 cybersecurity plan.

# More Points Are Possible for Utilities That:

1. Demonstrate a strong commitment to completing their roadmaps

2. Include solutions that specifically improve the cybersecurity posture of operational systems in the utility

3. Can be maintained by the existing utility staff with minimal additional TA

4. Have strong leadership support, as evidenced by supporting documents, such as long-term budget commitments.

Technical Assistance

Process Overview (Phases 2 and 3)

AMERICAN
MADE
U.S. DEPARTMENT OF ENERGY

Starts With Completed TA Request Form
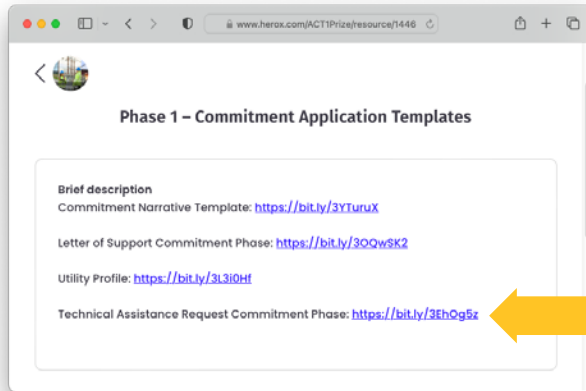
The **TA Request Form** is located on the ACT 1 HeroX Prize Platform under the "Challenge Resources" → "Phase 1 – Commitment Application Templates."

[Project Title]
[Organization Name]

Phase 1: Commitment Prize
Technical Assistance (TA) Request

If your utility would like to use the TA provided by the ACT 1 Prize Program, please select the specific TA categories your organization would like from the checklist on this page below (Select all that apply).

If your utility would like to request TA for something not listed below, please select "Other" and provide a detailed description of the kind of TA you would like. Please note that the ACT 1 Prize Program will attempt to provide TA requested under "Other" but may not be able to, and the ACT 1 Prize Program makes no commitment to meet TA requests under "Other".

If a utility has already conducted a stack assessment and architectural review and wishes to request TA not listed below, the utility may select from the available TA options on the following page. Please note that to win in the next phase, utilities will need to submit the 2.3.4 TA Provider Review Form, which confirms that the architectural review and cybersecurity technology stack assessment have been completed.

Winners of ACT 1 Prizes are not required to use the ACT 1 Prize Program TA provider(s) to help complete the work required to compete for a prize. However, all competitors for the Planning and Implementation Prizes are required to use an ACT 1 Prize TA provider to complete the TA Provider Review Forms required in the Planning and Implementation submission packages. If your utility only wants to utilize the ACT 1 Prize TA provider to complete the mandatory Forms, please select the "We only need a TA provider to complete the TA Provider Review Form" box.

☐ Architectural review of IT/OT environment:

☐ Cybersecurity technology stack assessment (assessing the IT/OT stack):

☐ Assistance with assessing maturity level:

☐ Assistance with developing and implementing a Section 40126 Cybersecurity Plan; or,

☐ We only need a TA provider to complete the TA Provider Review Form [ONLY select this box if you do not want any TA for the topics listed above.]

☐ Other. Please describe the type(s) of TA your utility is requesting.
_____

TA Process—Phase 2: Planning

- Winners will be matched with TA providers, and utilities will be given a choice in the selection of their TA provider.

- NREL will help kick off work with TA providers and winning utilities.

- TA providers will help utilities complete their stack assessments and architectural reviews.

- If "other" is selected on the TA Request Form, we will try to accommodate this request, but the ACT 1 Prize Team cannot commit to it.

TA Process—Phase 2: Planning

- Awarded TA hours will be leveraged to complete the TA work; utilities are not required to use all their TA hours.

- Phase 2 winners can use awarded TA hours until the Phase 3 winners are announced (*estimated 12 months: March 2024–March 2025*).

Phases 2 and 3

Section 40126 Cybersecurity Plan

AMERICAN MADE
U.S. DEPARTMENT OF ENERGY

40126 Cybersecurity Plan

Phase 2: Planning

- 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.

- Webinars will be offered to Phase 1 winners to train utilities on how to complete their draft 40126 cybersecurity plan using the templates CESER created for this purpose.

- These webinars are in addition to the TA that will be awarded to Commitment Phase winners.

40126 Cybersecurity Plan

Phase 3: Implementation

- Utilities competing for an Implementation Prize must **complete** a 40126 cybersecurity plan and **submit it** to the national support lab.

- Webinars will be offered to Phase 2 winners to train utilities on how to complete their 40126 cybersecurity plan using the templates CESER created for this purpose.

- These webinars are in addition to the TA that will be awarded to Planning Phase winners.
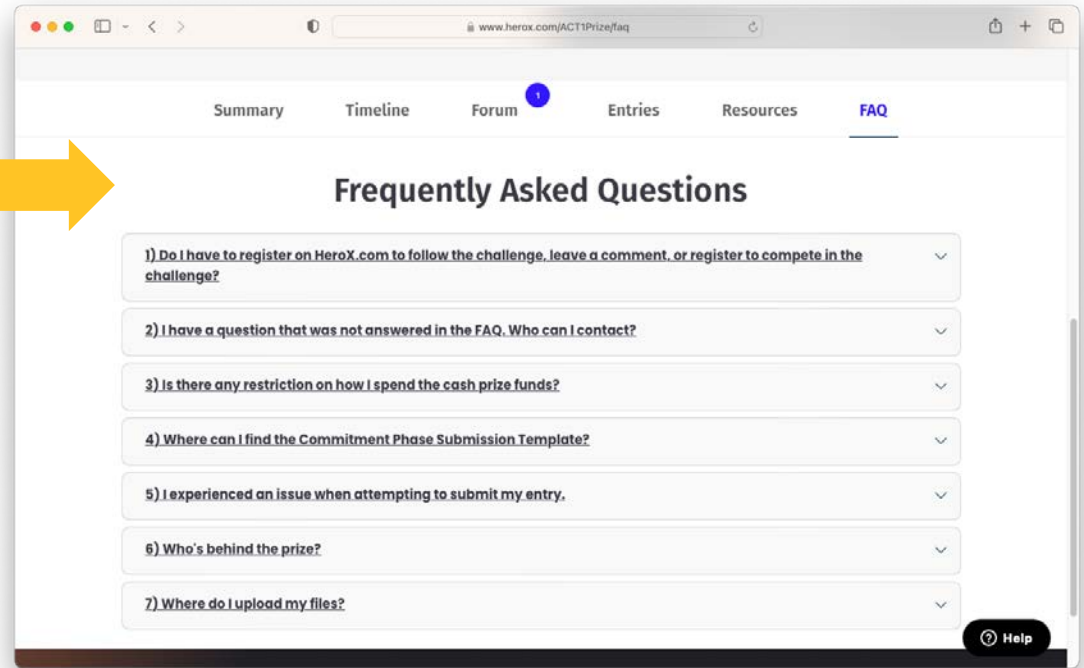
Next Steps

What's Next?

1. Follow the challenge on the HeroX Prize Platform: https://www.herox.com/ACT1Prize.

2. Read the rules: HeroX → Resources Tab.

3. Start your submission package!

4. Submit your completed package by **5 p.m. ET** on Nov. 29, 2023.
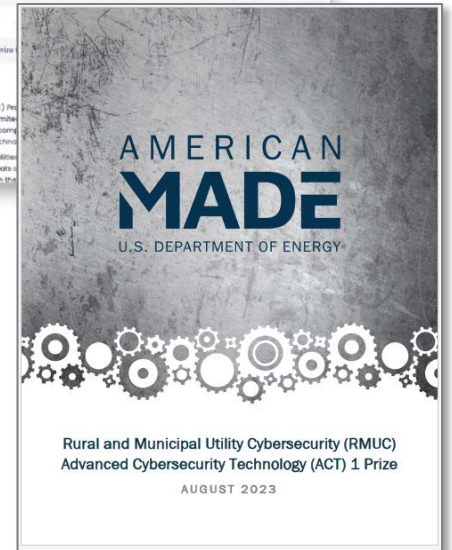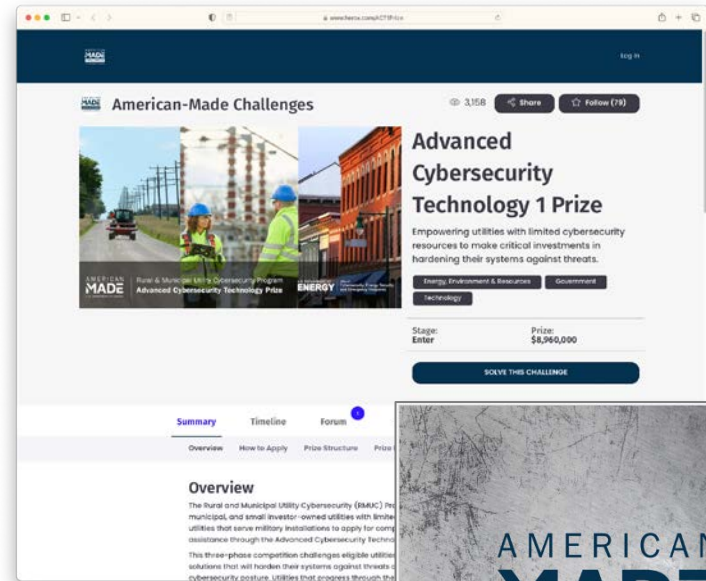
Questions?

Submit your questions to: ACT.Prizes@nrel.gov.

FAQs are posted on the ACT 1 Prize HeroX Prize Platform.

Frequently Asked Questions

1) Do I have to register on HeroX.com to follow the challenge, leave a comment, or register to compete in the challenge?

2) I have a question that was not answered in the FAQ. Who can I contact?

3) Is there any restriction on how I spend the cash prize funds?

4) Where can I find the Commitment Phase Submission Template?

5) I experienced an issue when attempting to submit my entry.

6) Who's behind the prize?

7) Where do I upload my files?

FAQs

13) Must the webinars be viewed in real-time only, or can we view the recordings and still meet the attendance requirement for this Prize? ∧

You can view the recordings and still meet the attendance requirements for this prize.
Participation in both webinars is required for this Prize. Confirmation of attendance requirements are on page 17 of the Prize rules.

18) I submitted my request for the RMUC USTR Report, when should I expect to receive this report via email? ∧

The Prize team is striving to send the report to the requestor within 7-10 business days from receiving the request.

All requests for a RMUC USTR Report must be received by 5:00 PM ET on Wednesday November 15th, which is two weeks before the Commitment Phase submission deadline of November 29th. RMUC USTR reports will not be sent to any requests that are received after November 15th.

FAQs (Cont.)

17) A few of the Phase 1 forms ask for a Project Title. Can you provide more information on what is expected in that field?

The Commitment Prize project title is something that the submitter creates, and it can be entered into the "title" field of the submission form and the "Commitment Narrative Template" available on the resources tab of the HeroX Prize Platform. https://www.herox.com/ACT1Prize/resources

Thank you

AMERICAN MADE
U.S. DEPARTMENT OF ENERGY