

Informational Office Hours

CWX-028-CESER

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

ConnectWerx (CWX) Resources



COMMUNICATIONS

Stay **engaged and connected** with our various outreach channels

- CWX web & opportunities page
 - Opportunities / Awards
 - Events
 - Resources
- CWX emails and outreach
- **Join the Network!**
- CWX social media



VIRTUAL EVENTS

Take part in **opportunities** through virtual events

- CWX & DOE Informational Webinar Sessions
 - Learn about PIA opportunities facilitated by CWX.
 - Overview of opportunity and additional details to participants.
 - Q & A
- CWX & DOE Office Hours
 - Ask direct question to DOE and CWX.
 - Note: review application prior.



CONFERENCES

Encourage & coordinate **involvement** at conferences



March 23-25, 2027
Boston, MA

The mission of ConnectWerx is to **Engage, Match,**
and **Collaborate** across the US Industrial and
Academic base to help the Department of Energy
(DOE) address **energy, environmental** and **nuclear**
challenges through transformative science and
technology solutions.



@connectwerx



info@connectwerx.org

Join the Network!



The background is a solid purple color with a subtle, isometric grid pattern that recedes into the distance. Scattered across the grid are numerous white-outlined circles of varying sizes, some of which are slightly blurred, giving a sense of depth and movement.

CESER Overview

About CESER

- Mission
 - Strengthen the security of the U.S. energy sector
- Vision
 - A secure, resilient, and adaptive energy sector capable of withstanding emerging threats and providing reliable energy for national defense and all Americans.

CESER Core Capabilities



Risk Analysis

Develop and distribute actionable risk information to energy stakeholders to mitigate the impact of threats and disruptions.



Energy Infrastructure Hardening

Mitigate risk to the Energy Sector and its supply chains through planning, deployment of tools, training, and exercises.



Cutting Edge Innovation

Build resilience within the energy sector through research and development and capacity building activities.



Response, Restoration, and Recovery

Enable the Energy Sector to quickly respond, restore, and recover from disruptions.



Rural and Municipal Utility Advanced Cybersecurity (RMUC) Technical Assistance (TA) Overview

Program Objectives

The overall objective of this program is to strengthen the operational and cybersecurity resilience of utilities. This will be achieved by working primarily through nonprofit entities that are partnering with 6 or more electric rural cooperatives, municipally owned utilities, or utilities owned by a State or political subdivision, by providing technical assistance and shared services. Key objectives include:

- Facilitating the adoption of best practices in utility resilience planning and execution.
- Providing tailored technical assistance to address sector-specific challenges.
- Facilitating the implementation of advanced cybersecurity technologies within eligible utility systems, directly improving their ability to protect against, detect, respond to, and recover from cyber threats.
- Establishing and maintaining a method for threat intelligence sharing among utilities partners.
- Promoting innovative solutions for energy infrastructure protection

Eligibility



Applicants must be not-for-profit entities that are in a formal partnership with no fewer than six (6) electric rural cooperatives, municipally owned utilities, or utilities owned by a State or political subdivision.



Proposed project aligns with "advanced cybersecurity technology" definition (enhances security posture, protection, detection, response, recovery).



Must meet the "domestic entity" definition for GSA (organized under US laws, majority domestic ownership/control, physical US place of business, and not owned/controlled by a Country of Risk).



Applicant has demonstrated need or members with a need for cybersecurity enhancement (e.g., limited cybersecurity resources as per prioritization criteria).



Ability to demonstrate sufficient financial resources or access to capital to commence and sustain initial project activities prior to initial payment milestones. A basic financial health check may be necessary.

Application & Review Process

The background of the slide features a blurred industrial scene, likely an oil or gas refinery, with various towers, pipes, and structures. A semi-transparent purple filter is applied over the entire image. On the right side, there are several white, concentric, angular lines that resemble a stylized arrow or a series of nested chevrons pointing towards the right.

Application

File Title	Max Pages	File Type
Project Overview & Plan	6 (Times New Roman 12 font, which includes graphs and pictures on all PDFs)	PDF
Project Schedule & Gantt Chart		PDF
Cost Proposal/Project Budget	1 page per period of performance (submitted as one file)	XLS
Key Personnel (Resumes)	2 pages per person (submitted as one file)	PDF
Letters of Support	5	PDF

Application Timeline

Milestones to Consider:	Target Date:
- Project Application Period Open: DOE begins accepting applications - Informational “Office Hours” presentation available	Sep 30, 2026
Deadline for Questions	Oct 13, 2026
Submissions Close	Oct 20, 2026 (2PM ET)

Review Criteria

1. **Statutory Priority and Need:** The extent to which the proposed utility beneficiaries have limited cybersecurity resources, own assets critical to bulk-power system reliability, and/or own defense critical electric infrastructure.
2. **Breadth of Eligible Utility Reach and Sector Impact:** The number and diversity of eligible utilities that will receive substantive services and the expected sector-wide impact. Proposals capable of effectively serving a larger number of eligible utilities may receive more favorable consideration when the proposed level of service remains meaningful, achievable, and adequately supported.
3. **Technical Merit and RMUC Alignment:** The strength of the proposed approach to deploy advanced cybersecurity technologies and/or increase participation in cybersecurity threat information-sharing programs, including alignment with the applicable Focus Area.
4. **Implementation Readiness and Feasibility:** The credibility of the work plan, utility engagement strategy, staffing, schedule, vendor or technology approach, and ability to initiate and sustain performance.
5. **Measurable Cybersecurity Improvement:** The quality of proposed baselines, metrics, outcomes, and methods for demonstrating improvements in utilities' ability to protect against, detect, respond to, and recover from cybersecurity threats.

Review Criteria

6. **Organizational Capability and Partnerships:** The applicant's relevant cybersecurity expertise, experience serving RMUC eligible utilities, strength of formal utility partnerships, and ability to manage technical assistance, vendors, sensitive information, and required reporting.
7. **Cost Effectiveness and Scalability:** The reasonableness of proposed costs in relation to the number of utilities served, level of service, expected cybersecurity benefit, and potential to scale or replicate successful approaches.
8. **Verification and Validation:** The extent to which the proposed approach includes appropriate post-implementation verification and validation to demonstrate that funded cybersecurity improvements, technologies, practices, or capabilities have been successfully implemented and are achieving their intended cybersecurity outcomes. Applicants should describe methods for testing or otherwise validating effectiveness, documenting results, addressing identified deficiencies, and providing follow-up support, as appropriate to the proposed activities and utility environment.
9. **Sustainability and Durability of Benefits:** The extent to which the proposed approach demonstrates a credible and feasible strategy for sustaining RMUC-funded cybersecurity improvements and capabilities beyond the period of performance. This may include, but is not limited to, utility ownership and maintenance of implemented capabilities, workforce development and knowledge transfer, ongoing service or funding models where feasible, partnerships, shared-service approaches, or other strategies appropriate to the participating utilities and proposed activities.



CWX-028-CESER

Q&A

How to Participate

1. Review details on eligibility, evaluation criteria, and how to apply.
2. Review the Informational “Office Hours” presentation and submit questions [here](#).
3. Download the Project Overview & Plan and Project Schedule & Gantt Chart templates.
4. [Register in AMP](#), and complete the online application and upload completed required documents in the application for CWX-028-CESER.

Submissions are due no later than Tuesday, October 20, 2026 at 2 PM ET.