Testimony of Tim Lindahl
President and Chief Executive Officer
Kenergy Corp

To the United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Energy

"*Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid*"

Tuesday, December 2, 2025

Introduction

Chairman Latta, Ranking Member Castor, and Members of the Committee: Thank you for the opportunity to discuss how electric cooperatives are working to secure the grid against evolving cyber threats. Every day, America's electric grid faces thousands of cyber intrusion attempts. For rural electric cooperatives, these threats are not abstract; they are real and growing more sophisticated. My name is Tim Lindahl, and I serve as President and CEO of Kenergy. I am testifying today on behalf of the National Rural Electric Cooperative Association (NRECA), which represents nearly 900 electric cooperatives nationwide. As a co-op leader with over 30 years of experience in the technology and energy industries, I look forward to sharing my perspective on how electric cooperatives are securing the grid.

Kenergy is a distribution electric cooperative that serves over 60,000 homes and businesses across 14 counties in Western Kentucky with more than 7,200 miles of power lines. Kenergy has a long, proud history of serving our communities. Our co-op supports a robust industrial base in paper, metals, food, manufacturing, and energy. In 1937, our predecessor, Henderson-Union RECC, was the first electric cooperative in Kentucky to supply power to a member. Today, we also provide fiber optic services that have enabled broadband service to over 13,600 homes and businesses, having built out over 3,500 miles of fiber infrastructure. This will be instrumental in evolving our grid to meet changing needs, including the safety and security of our grid.

NRECA is the national trade association representing America's 900 rural electric cooperatives. Electric co-ops are not-for-profit, at-cost electric utility providers focused on delivering affordable, reliable, and secure electricity to over 42 million Americans in 48 states. We are unique in the electric utility sector in that we are private, independent businesses that operate without profit incentives and are owned and governed by the people we serve.

Electric co-ops were created with a mission to address the distinct challenges associated with providing electric service to rural communities, which typically have lower population densities, are more residential, and are less affluent than the industry average. This means that cooperatives are constantly asked to do more with less, and they deliver.

Electric co-ops are owners and operators of some of our nation's most critical infrastructure, such as power plants, electrical substations, and transmission and distribution lines. This also includes infrastructure to generate or provide power for more than 150 military facilities and installations across the United States. We also serve as economic drivers and lifelines for critical industries and services in rural communities, helping power data centers, hospitals, emergency services, and food and agriculture production.

Protecting America's electric grid from cyber and physical threats is a top priority for the nation's electric cooperatives. Achieving this vital goal presents its own set of challenges. The same conditions that made it difficult to electrify rural America nearly a hundred years ago still exist today. These obstacles make it harder to secure the grid in rural communities.

Co-ops across the country are coming together and thinking innovatively to overcome these challenges. The seven cooperative principles, like concern for community and cooperation among cooperatives, are the driving force behind what we do. Additionally, our national trade association, NRECA, is leveraging private and public dollars to develop cybersecurity tools and resources to improve information sharing, deploy new technologies, and build a capable workforce.

The Department of Energy (DOE) is also a strong partner in efforts to improve co-op cyber defenses. DOE's Rural and Municipal Utility Cybersecurity Program (RMUC) represents the most significant opportunity for electric cooperatives to bolster their cyber readiness and close the rural resource gap. This program helps co-ops invest in the people, processes, and technologies needed to help co-ops secure the grid. DOE must act more swiftly to fund critical RMUC cyber initiatives, and Congress to continue to support and reauthorize this program.

Threat Landscape

Cyber threats jeopardize electric reliability and pose a serious risk to the nation's safety, security, and economic well-being. The threat landscape for electric utilities is becoming more complex and dangerous. Electric cooperatives and other electric utilities are primary targets for cyberattacks because of their crucial role in national security and everyday life. Threat actors, ranging from state-sponsored groups to cybercriminals, exploit vulnerabilities for geopolitical or financial reasons, with the potential of cascading impacts on critical infrastructure. These attacks could disrupt the power supply, leading to widespread outages, causing societal panic, public health concerns, and economic harm. The emergence of advanced malware, ransomware, and phishing attacks further increases the risks and impacts.

Additionally, smart grids, distributed energy resources (DER), and Internet of Things (IoT) devices, while improving efficiency, introduce new targets. Defending our infrastructure against

new challenges and evolving cybersecurity threats requires strong cybersecurity measures, continuous monitoring, proactive threat intelligence, and a skilled workforce capable of safeguarding these critical assets against increasingly sophisticated attacks.

While cyber events often grab the headlines, physical threats to the electric grid remain persistent and evolving. Electric cooperatives face unique challenges in this regard. Our infrastructure is geographically dispersed, often covering thousands of square miles with relatively few customers per mile of line. Unlike urban utilities with dense infrastructure and centralized control, rural electric co-ops must secure long stretches of transmission or distribution lines, isolated substations, and facilities that may be hours apart, all with limited resources.

Securing the Grid

Electric cooperatives place absolute importance on maintaining an affordable, reliable, and secure electric grid for our members. Co-ops apply a risk-based, layered defense strategy to protect critical assets, including power plants, transmission infrastructure that carries electricity long distances, and substations and distribution lines that provide electricity to local users. This approach is designed to ensure protection against all hazards – severe storms, vandalism, physical, and cyber incidents. The task of providing a reliable and secure electric grid is continuously evolving. Electric cooperatives use long-term strategies and various measures to adjust to emerging threats and conditions to ensure their cyber and physical security. Co-ops employ a range of measures, including risk assessments, technology and telecommunication deployments, data backups, response and continuity planning, tabletop exercises, and workforce development.

I joined the utility industry in 2005, when, for most organizations, cybersecurity was not at the forefront of their minds. Seeing the significant need to secure our digital assets, at a time when new technologies were quickly being implemented and grid operations were changing, resulted in several initiatives to bring security to the forefront of decision-making, at our local utility and across the nation. Programs and opportunities were leveraged to raise awareness across all functions of the utilities, which led to the development of partnerships and tools to make cyber a foundational part of our operations. The most critical piece of a security culture is the teams that work tirelessly day in and day out to ensure that when the switch is flipped, the light comes on. Countless unsung heroes work quietly and anonymously in the background, monitoring and evolving our security. We never see the event that never happens or hear about the attack that did not occur.

The commitment to the community principle that cooperatives hold includes making sure our local economies stay robust. A cyber event on a business or industry in our community can have grave consequences to the local economy and even to the viability of the electric cooperative. Beyond securing our systems, we have led community-level education sessions to help our rural small businesses ensure they are aware of their risks and can adapt to stay secure and viable.

Additionally, the sharing of threat information is the backbone of industry efforts to protect the grid and mitigate risk. Many electric cooperatives actively monitor and share information with organizations like the Electricity Information Sharing and Analysis Center (E-ISAC). The analysis and rapid sharing of security information from E-ISAC to the electric sector and back helps the industry to more clearly understand threats to the electric grid, which inform electric cooperatives' decisions on everything from technologies and mitigation efforts to tabletop exercise scenarios and workforce development strategies. Following the 2022 substation attacks in North Carolina, the industry worked through E-ISAC to update physical security risk management options for the electric system to better assess and manage risk at critical facilities.

Electric cooperatives, however, face unique challenges in securing the electric grid due to their geographical and operational characteristics. Smart investments in infrastructure cybersecurity can help ensure the security of, and prevent catastrophic damage to, the nation's electric grid, but often require high upfront costs and persistent funding to maintain capabilities. Because cooperatives operate without shareholders or profit incentives, financing costly investments often requires reliance on debt, which must be approved by their Boards and is ultimately paid back through rates paid by their members. Boards are careful stewards of their members' resources and mindful of the economic impact of rate increases to end-of-line consumer-members, particularly given that one in four households served by cooperatives has an annual income below $35,000. These resource constraints can make it difficult to invest in advanced technologies and recruit and retain a skilled cyber workforce necessary to defend against increasingly sophisticated cyberattacks, especially those from nation-state actors.

Overcoming Challenges

One of electric cooperatives' greatest strengths is their autonomy and independence, each with its own networks, software, and systems, yet interconnected to provide resiliency. Although independent, electric cooperatives across the country also work together to think innovatively, improving collaboration, pooling resources, sharing knowledge, and implementing new technologies that help co-ops protect against emerging threats. In some states, large generation and transmission cooperatives, statewide associations, and distribution co-ops are developing partnerships to share tools, equipment, and expertise across shared electric systems to strengthen their collective cyber defenses. We recognize that we are greater than the sum of our parts, and these efforts embody one of our core principles of cooperation among cooperatives.

Kenergy and other cooperatives are building fiber networks deep within our electric networks. These win-win builds help solve the digital divide by providing broadband access to our rural members, but also allow us a foundational platform to build our next-generation physical and cyber security platforms

Kenergy partners with NRECA and other institutions, such as the B.E.T.H Institute (Broadband, Energy, Technology, and Home), a foundation that brings funding and partners together in each of the named categories at the community level to innovate solutions for enhancing our grid, ensuring reliability, and improving affordability.

Additionally, NRECA is building a robust cybersecurity program designed to continue to provide co-ops with the most up to date tools tailored to their needs to improve their cybersecurity posture. The program creates products and services that help co-ops prepare for existing and potential threats to their reliability and security.

Threat Analysis Center

The NRECA Threat Analysis Center (TAC) is a secure technology platform that helps the co-op community detect, analyze, and communicate cybersecurity threats. In the cybersecurity landscape, electric cooperatives rely on multiple sources of threat intelligence and alerting systems to protect their infrastructure. These alerts can be filled with false positives, low-priority, or irrelevant notifications, which can desensitize analysts, leading to slower response times, missed threats, and increased risk of breaches. TAC helps reduce alert fatigue, allowing cybersecurity professionals to focus on high-impact cyber threats and respond more quickly. Additionally, TAC works closely with federal partners and industry stakeholders to ensure co-ops have access to timely intelligence without compromising privacy. Even the smallest and most remote cooperatives gain access to expert analysis, training, and a national network of support, helping level the playing field in the face of increasingly sophisticated cyber threats.

Co-op Cyber Goals Program

There are numerous cybersecurity frameworks to help organizations improve their cybersecurity posture, each designed to address different needs, industries, and regulatory requirements. For electric cooperatives with limited resources and staff, understanding where to begin can be a daunting task. That's why NRECA launched the Co-op Cyber Goals Program in 2023. This initiative provides a structured framework of 20 achievable cybersecurity goals tailored to rural electric utilities and adaptable to any cyber maturity level. The program is designed to foster a culture of security across the organization, guiding co-ops through cyber hygiene from the most basic practices to the most advanced. More than 400 co-ops are part of the program, demonstrating the high priority placed on furthering and evolving our cyber resilience. By aligning cybersecurity efforts with practical, measurable goals, the program empowers co-ops to prioritize investments, engage staff at all levels, and build confidence.

Co-op Cyber Tech Conference

NRECA's Co-op Cyber Tech conference serves as a premier event for electric cooperatives to engage in technical training, share best practices, and collaborate on emerging cybersecurity challenges. This annual event brings together co-op cybersecurity professionals, utility leaders, and federal partners to discuss threat trends, showcase innovative tools, and conduct tabletop exercises that simulate real-world cyber incidents. The conference reinforces the importance of continuous learning and peer-to-peer engagement, especially for smaller co-ops that may lack access to specialized expertise.

Cyber Risk Quantification Pilot

NRECA recently launched a program to help electric cooperatives better understand cyber risks as a business decision. Participating co-ops can model the potential financial impact of cyber

threats on their operations and assess how implementing NRECA's Co-op Cyber Goals program, a set of high-priority cybersecurity measures designed to help electric cooperatives build a strong security foundation, reduces that exposure. By translating technical vulnerabilities into financial terms, cooperatives gain a clearer understanding of the potential business impact of cyber threats. This analysis helps shift the conversation from abstract threats to tangible consequences, such as potential service disruptions, financial losses, or reputational damage.

Federal Partnerships

While co-ops are strengthening their cyber posture through collaboration and shared services, they cannot meet these challenges alone. Smart, targeted federal support through funding, workforce development, and improved threat intelligence sharing is essential. This will help close the resource gap and ensure rural communities are not left behind in the national effort to secure our energy infrastructure.

Leveraging our federal partnerships has been critical in evolving our security posture by hardening our physical and cyber systems. Electric cooperatives have a long history of federal partnerships and responsible management of taxpayer dollars. The Rural Cooperative Cybersecurity Capabilities Program, or RC3, was an initial collaborative partnership between NRECA and the Department of Energy to provide resources to the co-op community. RC3 has now grown into a broader NRECA cybersecurity program aimed at helping co-ops advance their cybersecurity posture. Additionally, electric cooperatives utilize resources from various federal agencies and departments, like CISA, DHS, DOE, DoD, and state fusion centers, to better understand vulnerabilities, emerging threats, and mitigation efforts. Public-private partnerships are essential in addressing cybersecurity challenges faced by co-ops, thereby enhancing the energy resilience of the communities they serve.

Rural and Municipal Utility Cybersecurity Program

Nowhere is this more immediate than with the Rural and Municipal Utility Cybersecurity Program, or RMUC. This $250 million program, authorized through FY 2026, is a generational opportunity to improve the cybersecurity posture of electric cooperatives and municipally owned electric utilities. RMUC prioritizes co-ops with the greatest need of support that serve the nation's most critical infrastructure, including military installations, to help them make the necessary investment to secure the grid.

The Department of Energy (DOE) announced last fall $80 million in RMUC funding that will directly support more than 400 cooperatives' cybersecurity programs. Much of that funding has yet to be released to the award winners. We encourage DOE to move expeditiously to distribute the awarded funds so that electric cooperatives can put them into action to defend their critical infrastructure

While co-ops await the lion's share of funds, DOE has utilized RMUC funds to host multiple advanced utility training sessions across the country. These intensive, three-day programs, which were attended by more than 200 individuals from 123 electric cooperatives, were designed to

help cyber personnel improve the security of industrial control systems and operational technology.

Additionally, NRECA was awarded $4 million cooperative agreement to launch the Project Guardian program. NRECA's Project Guardian is a multifaceted program focused on ensuring that no co-op is left behind and developing frameworks for four key focus areas: Cyber Champions; Threat Analysis Center Expansion; Cyber Resilience Initiative; and Education, Training, and Workforce Development. These focus areas will allow NRECA to target cooperative cybersecurity needs to develop self-assessment tools, tabletop exercises, and expand access to experienced cybersecurity personnel who can strengthen defenses and improve planning and incident response.

There is an estimated $160 million left in RMUC with less than a year left in its authorization. Given the importance this program represents to electric cooperatives and our nation's security, NRECA is strongly urging Congress to reauthorize this program. RMUC is helping move the needle for electric co-ops to improve their cybersecurity protections, but there is still more to be done.

Industrial Control System for Rural Electric Cooperatives

Another federally funded initiative utilized by electric cooperatives is the Industrial Control Systems – Rural Electric Cooperative (ICS-REC). This program is focused on strengthening cybersecurity for operational technology (OT) environments by helping member co-ops expand their cyber monitoring capabilities of their industrial control facilities. In September, ICS-REC, originally funded at $15 million, was awarded an additional $5 million by DOE, recognizing the success and need for the program. NRECA is partnering with member co-ops to identify and deploy industrial control system monitoring technologies that will provide cyber visibility, detection, and response capabilities for energy delivery systems. Sophisticated cyber actors increasingly target these systems because of their role in maintaining reliability and safety. Through ICS-REC, cooperatives gain access to best practices for network segmentation, vulnerability management, and incident response specific to OT assets. The program also fosters collaboration among co-ops and federal partners to develop practical solutions that address the unique challenges of rural infrastructure.

Conclusion

Securing America's electric grid is essential to our national security, economic stability, and the well-being of every community we serve. Electric cooperatives are committed to doing their part, but we cannot do it alone. While electric cooperatives are making smart investments and building strategic partnerships to strengthen our cyber readiness, more work can be done. RMUC reauthorization and the timely release of remaining funds from this program are critical steps to ensure rural communities are not left behind. With continued partnership and targeted investment, we can strengthen our defenses, protect critical infrastructure, and keep the lights on

for 42 million Americans. The last two decades have seen significant advancement in how electric cooperatives secure our grid, but there is much more work still to do.

I thank the Committee for the chance to highlight the challenges and opportunities to securing our grid and look forward to answering your questions.