Testimony of Dr. Nathaniel J. Melby

Vice President and Chief Information Officer

Dairyland Power Cooperative

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

"*Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape.*"

January 13, 2026

The Electric Cooperative Mission and Landscape

Chairman Latta, Ranking Member Castor, and Members of the Committee: Thank you for this committee's diligent and comprehensive work to provide the tools electric cooperatives need to stay ahead of an evolving cyber threat landscape and strengthen our nation's grid security. I appreciate the opportunity to discuss the draft legislation before the committee, particularly the reauthorization of the Rural and Municipal Utility Cybersecurity Program. My name is Nate Melby, and I am the Vice President and Chief Information Officer at Dairyland Power Cooperative in La Crosse, Wisconsin. In my role, I lead the strategy, development, and implementation of information technology initiatives and systems. I am testifying today as a cooperative leader and on behalf of the National Rural Electric Cooperative Association (NRECA), the national trade association that represents nearly 900 electric cooperatives nationwide.

Dairyland is a generation and transmission electric cooperative that provides wholesale electricity for 24 distribution cooperatives and 27 municipal utilities who, in turn, supply the energy needs of over 750,000 members and consumers across western Wisconsin and parts of Minnesota, Iowa, and Illinois. Dairyland generates electricity using an all-of-the-above strategy and delivers it through over 3,700 miles of transmission lines to 400 distribution substations located throughout the system's 44,500 square mile service area.

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 within 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 we 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 hospitals, emergency services, schools, data centers, and food and agriculture production.

Co-ops support the Administration's goals, as outlined in the 2025 National Security Strategy, of ensuring "resilient national infrastructure that can withstand natural disasters, resist and thwart foreign threats, and prevent or mitigate any events that might harm the American people or disrupt the American economy". However, 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 innovating to overcome these challenges. But 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.

The Department of Energy's (DOE) 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. RMUC is a public-private partnership that's helping co-ops invest in the people, processes, and technologies needed to help co-ops secure the grid.

Defending Critical Infrastructure in Rural America

Electric cooperatives are dedicated to maintaining an affordable, reliable, and secure grid through a risk-based, layered defense strategy. We employ an 'all-hazards' approach that protects critical infrastructure against a full range of threats, including everything from severe weather to cyberattacks. To stay ahead of evolving risks, co-ops employ comprehensive measures including continuous risk assessments, advanced technology deployment, and rigorous workforce training.

Collaboration is central to our defense. Through partnerships with the Electricity Information Sharing and Analysis Center (E-ISAC), co-ops share real-time threat intelligence that shapes our mitigation strategies. For instance, following the 2022 North Carolina substation attacks, industry-wide collaboration through E-ISAC led to updated physical security protocols for critical facilities.

However, securing the grid in rural areas presents unique financial challenges. As not-for-profit entities without shareholders, co-ops must fund costly security investments through member rates. This is particularly difficult when one in four co-op households has an annual income below $35,000. These resource constraints make it challenging to fund the advanced

technologies and skilled workforce needed to defend the grid. For electric cooperatives, the most effective federal role is one that helps us overcome these hurdles through strong partnerships, collaboration, voluntary information-sharing, and workforce development.

The Rural and Municipal Utility Cybersecurity Program

Leveraging our federal partnerships has been imperative to overcoming fiscal constraints to harden 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 partnership between NRECA and the Department of Energy that demonstrated how co-ops can successfully leverage public resources to improve security while keeping electric rates affordable.

The support provided through the Rural and Municipal Utility Cybersecurity Program builds on the work of the RC3 program by providing direct support to electric cooperatives. This $250 million program prioritizes co-ops with the greatest need for support and those that serve the nation's most critical infrastructure, including military installations. Cybersecurity investment is not just about defense; it is about deterrence. Foreign nations, such as the People's Republic of China, and cyber criminals are among the most active and persistent threats to critical infrastructure networks. Bad actors can disrupt the delivery of critical services, threatening American national and economic security. RMUC bridges the rural resource gap, ensuring that the security posture in rural America is as robust and formidable as anywhere else in the nation. This is accomplished by helping electric cooperatives make critical investments into three key areas: the people, processes, and technologies necessary to secure the grid.

DOE has created several funding streams to support electric cooperatives in these key areas. The Department used RMUC funds to host multiple advanced utility training sessions across different regions. These intensive, three-day programs were attended by more than 200 people from 123 electric cooperatives to help improve industrial control systems and operational technology security.

Furthermore, DOE designed the $8.9 million RMUC Advanced Cybersecurity Technology (ACT) Prize series to empower under-resourced utilities by lowering traditional barriers to entry. By prioritizing flexibility over rigid and complex application requirements, the prize structure significantly reduced administrative burdens, making it practical for resource-constrained cooperatives to apply directly and implement actionable cybersecurity enhancements.

Last fall, DOE announced $80 million in RMUC awards that would directly support more than 400 cooperatives' cybersecurity programs across the country. This funding includes $3.5 million for Dairyland Power Cooperative, which will allow us to work with 20 of our distribution co-ops to invest in technologies that will boost cyber defenses across our shared systems. These investments will ensure that we no longer see pockets of strength, but substantial cybersecurity improvement across our member co-ops' systems and infrastructure.

Unfortunately, much of the $80 million in funding, including Dairyland's, has yet to be released by DOE to the award winners. We encourage DOE to move expeditiously to distribute the awarded funds so that electric cooperatives can use it to defend their critical infrastructure. These funds will expand and expedite the collaborative work to improve cyber defenses that is already being done between co-ops, statewide associations, and NRECA. We will be able to hire cyber professionals, conduct more assessments, improve internal processes, strengthen information-sharing, and use more advanced cyber technologies.

Additionally, our national trade association, NRECA, was awarded a $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 by focusing on four key areas: Cyber Champions; Cyber Resource Development; Cyber Resilience Initiative; and Education, Training, and Workforce Development. These focus areas will allow NRECA 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 remaining in its authorization. Given the importance of this program to electric cooperatives and our nation's security, NRECA is strongly urging Congress to reauthorize this program and update the legislation to improve program access for co-ops with limited resources.

Unlocking the Full Potential of RMUC

The RMUC program represents the most significant opportunity for electric cooperatives to bolster their cyber readiness, yet its full potential has not yet been realized due to hurdles that have slowed its impact. While some RMUC funds are moving, implementation has been sluggish, and a significant portion of announced funding is yet to be released to award winners, leaving critical resources stuck in the pipeline rather than defending the grid.

Furthermore, the program has been constrained by a lack of flexibility and statutory language that requires electric cooperatives to compete not only for grant funding but also for technical assistance. Technical assistance is routinely provided outside of a competitive process across other federal agencies because its goal is to build capacity, not reward the strength of entities that are already prepared. Although DOE has worked creatively to overcome these challenges, like the ACT Prize, the primary funding mechanisms still involve complex requirements that create barriers to entry for smaller co-ops who lack the dedicated resources to navigate the burdensome application process.

Despite these concerns, the promise of RMUC is undeniable. NRECA and its members strongly support the draft reauthorization legislation because it directly addresses these obstacles by removing the requirement to compete for technical assistance. By streamlining the distribution process and authorizing additional time and resources, this bill will unlock the full potential of the RMUC partnership and ensure that rural communities are not left behind.

Strengthening the Broader Energy Security Landscape

Beyond the RMUC program, we thank the Committee for its comprehensive approach to grid security reflected in the other measures before us today. We support the *Energy Threat Analysis Center Act*. ETAC has already proven to benefit the greater information-sharing environment through enhanced collaboration, and we look forward to working with DOE to improve electric cooperative participation in ETAC. Similarly, the *Energy Emergency Leadership Act* rightly elevates energy security and cybersecurity concerns to the Assistant Secretary level, ensuring that these critical issues receive the high-level attention they deserve within the Department and across federal partnerships. Finally, we appreciate the Committee's diligence with proposals, including the *SECURE Grid Act* and the *Pipeline Cybersecurity Preparedness Act,* which underscores the importance of a holistic strategy to ensure every segment of the energy sector is moving toward a more resilient posture.

Conclusion

Securing the grid is essential to national security, but the threat landscape is evolving faster than ever. While cooperatives are committed to this fight, we cannot confront sophisticated nation-state actors alone. We appreciate the Committee's focus on this shared responsibility, particularly through the RMUC program, which remains our most vital tool for closing the rural resource gap. Because co-ops operate on thin margins in difficult terrain, effective policy must be paired with resources, not burdens and bureaucracy. Every dollar we spend comes directly from our members' pockets, so we need solutions that empower us to protect our communities without adding financial strain. We strongly urge the Committee to advance the RMUC reauthorization to ensure we can keep the lights on for 42 million Americans. Thank you for your leadership, and I look forward to your questions.