Dr. Nate Melby QFR Responses
March 17, 2026

Questions from the Honorable Brett Guthrie, Chairman, House Energy and Commerce Committee

1. DOE is the energy sector authority and must work with other agencies and States. To do this effectively, it must have a culture of constant learning and improvement, which will benefit the whole federal approach to support the energy sector.

a. Would you speak to the importance of a culture of constant learning and constant improvement for the stakeholders you represent?

In cybersecurity, especially when safeguarding the grid, fostering a culture of constant learning is essential. Threats evolve daily, and only teams committed to continuous improvement can stay ahead of adversaries seeking to exploit vulnerabilities. Encouraging ongoing education not only strengthens technical capabilities but also empowers organizations to anticipate and adapt to emerging risks. By embracing this mindset, we build a more resilient, secure grid to defend against current and future challenges.

Questions from the Honorable Mariannette Miller-Meeks, Member, Subcommittee on Energy, House Energy and Commerce Committee

1. You mentioned that cooperatives are asked to 'do more with less' and that one in four co-ops has annual income below $35,000. This creates unique challenges when funding cybersecurity investments through member rates. Can you help the Committee understand:

a. What does the resource gap between electric cooperatives and investor-owned utilities actually look like in practical terms? For example, when a large IOU faces a cybersecurity threat, what resources can they deploy that a rural cooperative simply doesn't have access to?

Investor-owned utilities (IOUs) typically have far greater access to capital and benefit from economies of scale, enabling them to invest in advanced technologies, sophisticated monitoring tools, and larger, dedicated cybersecurity teams. When a major IOU encounters a cybersecurity threat, it can rapidly mobilize specialized in-house experts, contract with external incident response firms, and deploy cutting-edge detection and mitigation systems. Resources that many rural cooperatives are unable to access due to financial constraints.

Conversely, electric cooperatives are not-for-profit, at-cost electric utility providers that predominantly serve rural and lower-density communities, including roughly 92% of the nation’s persistent poverty counties. While each cooperative is different in its unique circumstances, generally, their limited financial and human resources make it far more challenging to invest in modern cybersecurity technologies or to recruit and retain the specialized talent needed to respond to increasingly complex cyber threats. Because of

this, financing costly investments often requires reliance on debt, which must be approved by each cooperative's Board of Directors and ultimately paid back through rates paid by its members. Boards are careful stewards of their members' resources and mindful of the economic impact of rate increases to end-of-line consumer-members in their communities.

b. How do the approaches differ, not just in budget, but in available expertise, technology, and vendor relationships?

Because of limited financial resources, investing in the most sophisticated security technologies and competing for skilled cyber professionals can be a challenge. Recruitment and retention of cyber professionals are complicated by competitive salaries and benefits offered by larger, urban-based firms, which can lure away skilled workers. Many cooperatives operate in rural areas that may be less attractive to cybersecurity specialists, making it even more difficult to build and sustain a deep talent pipeline. Rural areas also face significant challenges in developing a robust cybersecurity talent pool. Smaller electric cooperatives often have a small number of staff, meaning that whether it's IT, cyber, or non-technical roles, co-op employees often wear multiple hats within the organization. Additionally, electric cooperatives also face inherent disadvantages in vendor relationships because limited budgets, smaller staff, and constrained cybersecurity capabilities make it difficult to thoroughly assess vendor risks or demand stronger contractual protections.

c. Why is federal support through programs like RMUC not just helpful, but essential for bridging this gap?

Federal support through programs like RMUC is essential for closing the widening cybersecurity resource gap between electric cooperatives and larger utilities. Electric cooperatives are innovating and collaborating to meet modern cyber threats, but RMUC accelerates this work by providing direct technical assistance, targeted tools, and capacity building resources that many co-ops could not otherwise afford. This program represents the most significant opportunity to ensure that rural utilities can meet national cybersecurity expectations, helping them strengthen defenses at a pace and scale that matches today's threat environment. By helping co-ops to build robust, modern security capabilities, RMUC ensures that the cybersecurity posture of rural America is as strong and resilient as any other part of the national grid.

2. You mentioned that RMUC helps cooperatives invest in 'the people, processes, and technologies' needed to secure the grid. Can you be more specific about the workforce development component?

a. What specific cybersecurity roles and skills do cooperatives most urgently need to hire or develop?

There is a significant nationwide shortage of cybersecurity professionals across nearly all sectors, including the electric industry. The United States currently faces an estimated 500,000 unfilled cybersecurity positions. Although every region struggles to recruit and retain skilled cyber personnel, these challenges are amplified for electric cooperatives,

particularly those serving rural communities with limited populations, constrained budgets, and difficulty competing with other private sector compensation.

While each cooperative's staffing needs vary based on size, systems, and risk profile, several cybersecurity roles and skill sets consistently emerge as the most urgent to hire or develop. Generally, cooperatives need professionals at every skill and career level, from IT cybersecurity analysts to operation technology (OT) and industrial control system (ICS) specialists to cybersecurity leaders and program managers. These needs are particularly critical in OT security, where specialized expertise is scarce but essential to protecting energy infrastructure.

b. How do training programs funded by RMUC differ from traditional utility workforce development?

The cybersecurity training programs funded through RMUC are not fundamentally different from those already available on the market. What makes RMUC essential is that it places these advanced, high-quality training courses within reach of electric cooperatives by providing customized content to co-ops that would otherwise be unable to afford them. Many leading cyber workforce development courses cost several thousand dollars per participant, creating a barrier that RMUC funding helps cooperatives overcome. By removing this financial hurdle, RMUC ensures that co-ops can access the same level of cutting-edge training.

c. What role do you see for community colleges, universities, and programs like Iowa State's CyDERMS in building the rural utility cybersecurity workforce?

Developing a strong cybersecurity talent pipeline with clear pathways into rural communities is essential for protecting critical infrastructure. Community colleges, universities, and technical programs are uniquely positioned to help build this workforce pipeline.

These institutions can provide accessible, high-quality training in cybersecurity while partnering directly with rural critical infrastructure operators, including electric cooperatives, to offer hands-on experience with operational technology and real-world utility environments. Such partnerships both strengthen workforce readiness and increase awareness of viable, long-term cybersecurity career pathways in rural areas.

NRECA has long supported efforts to expand these opportunities, including the Cyber PIVOTT Act, which would extend cybersecurity internship programs to rural critical infrastructure providers through participating educational institutions. Expanding these kinds of initiatives can help ensure that rural utilities have access to the skilled cybersecurity professionals needed to meet today's evolving threats.

3. You mentioned that Dairyland was awarded $3.5 million under RMUC to work with 20 distribution cooperatives, but that much of the $80 million in announced funding hasn't yet been released by DOE, including funding for Iowa.

a. How long have you been waiting for your awarded funds?

Dairyland has waited over a year for these funds to be released. We are encouraged, however, by the recent notification from the Department of Energy that award negotiations are proceeding and are actively engaging with DOE to maintain momentum and ensure that project work can commence as quickly as possible

b. What specific cybersecurity improvements are you unable to implement until those funds are released?

This funding 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.

c. What message would you send to DOE about the urgency of getting these dollars out to utilities that are defending critical infrastructure every day?

We are encouraged to see DOE begin to advance these funds, but timely distribution remains essential. The threats continue to move fast, and we have to meet them with the speed of our defense. Moving these dollars out of the pipeline and into the hands of electric cooperatives will directly enhance our ability to defend the grid and protect the nation's critical infrastructure against escalating cyber threats.

4. Iowa State University is leading CyDERMS, a regional cybersecurity center focused on securing Distributed Energy Resources. As we integrate millions of new devices we're dramatically expanding the attack surface of our grid. At the same time, we're deploying AI and machine learning tools to detect attacks and manage these distributed systems. This creates a paradox: we're using high-tech AI solutions to secure increasingly complex systems, but that technology itself could be a vulnerability.

a. How do you think about this balance?

Electric cooperatives, particularly the generation and transmission (G&T) cooperatives, have been utilizing artificial intelligence for some time now for grid management, predictive maintenance, customer service, and cybersecurity. From a security perspective, Artificial Intelligence (AI) and machine learning tools help us detect anomalies across this expanding attack surface far more effectively than manual monitoring alone. As our adversaries leverage AI to accelerate attacks, AI can also accelerate defense. At the same time, any technology that ingests data, makes autonomous recommendations, or interfaces with operational technology (OT) systems introduces new dependencies and cyber risk.

Our approach is to treat AI systems as high-value assets in their own right and employ strict boundaries around these systems, like maintaining a "human-in-the-loop" decision-making or strict boundaries between AI and OT control equipment. AI can enhance grid defense, but it does not replace proven engineering protections or operational discipline. For a G&T, reliability comes first; technological sophistication must always be evaluated against the operational consequences of failure.

b. Are there certain applications where simpler, lower-tech approaches might actually be more secure?

Many of the most critical G&T functions are intentionally kept simple, deterministic, and isolated because they must continue operating reliably during emergencies or cyber incidents. In these areas, lower tech or traditional engineering approaches can offer stronger security by reducing exposure and limiting the number of potential failure points.

Some examples of where these approaches offer superior security are: out-of-band communications and manual switching procedures that allow operations to continue if digital systems are compromised; air gapped or highly segmented OT networks where complexity adds risk rather than reducing it, or mechanical or analog failsafe that do not depend on software or firmware integrity. In some cases, low-tech does not necessarily mean outdated. In many cases, this approach is a deliberate security control, not a limitation.

c. How do we ensure that the AI tools we're deploying to defend the grid don't become the vector for attack?

AI can greatly enhance situational awareness and threat detection, but it must never become a single point of failure. We apply the same level of rigor to securing AI systems as we do to any tool that interacts with grid-relevant data or operations.

Our guiding principle is that AI can inform decisions and improve efficiency, but it should not directly control generation or transmission assets. Today, AI is best suited for anomaly detection, trend analysis, and advisory functions, not autonomous operational decision-making.

To prevent AI from becoming an attack vector, we rely on strong architectural separation, human-in-the-loop oversight, strict access controls, and continuous monitoring of both the models and the data feeding them. These safeguards ensure that if an AI system is compromised or produces misleading outputs, it does not undermine grid reliability or operator authority.