Testimony of Mr. Chris Jones
President and Chief Executive Officer
Middle Tennessee Electric

To the United States House of Representatives, Committee on Homeland Security

"Preparing the Pipeline: Examining the State of America's Cyber Workforce"

Wednesday, February 5, 2025

Introduction

Chairman Green, Ranking Member Thompson, and Members of this Committee: Thank you for the opportunity to testify before you today. My name is Chris Jones, and I serve as President and CEO of Middle Tennessee Electric (MTE). I am testifying today to provide my own insights as a co-op leader, but also representing the National Rural Electric Cooperative Association (NRECA) and nearly 900 electric cooperatives across the country.

MTE is the largest electric cooperative in the Tennessee Valley Authority (TVA) region and the second largest in the United States, serving more than 750,000 Tennesseans. Our service territory includes 15,000 miles of distribution lines over 2,200 square miles – or more than double the landmass of Rhode Island – across 11 Middle Tennessee counties, primarily Rutherford, Cannon, Williamson, and Wilson. MTE employs around 540 people in six local offices and its Murfreesboro headquarters.

NRECA is the national trade association representing nearly 900 rural electric cooperatives across the country. 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 sector, 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 less affluent than the industry average. This means that cooperatives are constantly asked to do more with less, and they deliver. Cooperative members give their utilities the highest customer satisfaction scores, on average, in the electric sector.

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, including hospitals, schools, 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. Accomplishing this important task presents its own set of challenges. The same circumstances that made it difficult to invest in electrifying rural America nearly a hundred years ago, including being isolated from the larger customer bases and diverse talent pools available in urban areas, persist today. These challenges add difficulty in investing in the people, processes, and technologies needed to secure the grid in rural communities.

We have a saying in our industry: If you have met one electric co-op, then you have met exactly one electric co-op. The nearly 900 electric co-ops across the country all come in different shapes and sizes. Although MTE does not fit the profile of the typical electric cooperative, all our challenges share similar themes. MTE is fortunate to not have to wrestle with some of the more intense challenges of the rural cyber workforce issue. However, with my over two decades of experience working for the cooperative, I have seen how MTE has tackled those issues and can share how co-ops are impacted across the broader community.

I will share some of the challenges electric co-ops face in securing the grid, specifically in recruiting, retaining, and developing cybersecurity professionals. I also will highlight how electric cooperatives are overcoming these challenges through the help of resources developed by NRECA and the smart investment of federal dollars.

Threat Landscape

Cyber threats jeopardize electric reliability and pose a significant risk to the nation's safety, security, and economic well-being.

The cybersecurity threat landscape for electric utilities is increasingly complex and perilous. Electric utilities are prime targets for cyberattacks due to their pivotal role in both national security and daily life. Threat actors, ranging from state-sponsored groups to cybercriminals, exploit vulnerabilities for geopolitical or monetary gains. These attacks have the potential to disrupt the power supply, causing widespread outages and economic damage. The rise of sophisticated malware, ransomware, and phishing attacks further exacerbates the risk.

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.

Workforce Challenge

As cyber threats grow more complex and prevalent, particularly those targeting critical infrastructure like electric utilities, the demand for cybersecurity professionals will continue to grow. In 2023, the National Institute of Standards and Technology (NIST) reported that only 20% of business leaders at energy utilities surveyed felt confident that they had the cyber talent they needed. These experts are essential for developing and implementing advanced security measures, conducting threat assessments, and responding to incidents swiftly and effectively.

Despite the evolving and complex threat environment, there are still around 450,000 cybersecurity vacancies in the United States. We need more cyber professionals to safeguard critical infrastructure across the country. While no sector or region is immune to the underlying difficulties of recruiting and retaining skilled cyber professionals, these challenges are exacerbated by the unique and inherent characteristics of electric cooperatives and rural areas.

Electric cooperatives are not-for-profit, at-cost utility providers, meaning we operate without a profit incentive. This model allows co-ops to serve more remote areas with low population density, averaging only 25% of the customers and revenue per mile of line, compared with the rest of the industry. Unlike investor-owned utilities, electric cooperatives operate without shareholders. 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 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 cooperatives provide service to 92% of the nation's persistent poverty counties.

Therefore, investing in the most sophisticated security technologies and competing for skilled cyber professionals can be a challenge. Recruitment and retention for these professionals are complicated by competitive salaries and benefits offered by larger, urban-based firms, which can lure away skilled workers. Cooperative staff, whether in IT, cyber, or non-technical roles, often wear multiple hats within the organization.

Since electric cooperative service areas are often largely rural, they can be seen as less attractive to professionals seeking vibrant social and professional networks, further complicating recruitment efforts. Rural areas also face significant challenges in developing a robust cybersecurity talent pool. One of the primary issues is the limited access to specialized education and training programs. Many rural regions lack institutions that offer advanced cybersecurity courses, making it difficult for residents to acquire, and keep up to date on, the necessary skills and changing techniques and tactics locally. Additionally, the overall awareness of cybersecurity careers is often lower in these areas, leading to fewer individuals pursuing this field.

Cyber PIVOTT Act

We want to thank and acknowledge Chairman Green's leadership on introducing the Cyber PIVOTT Act during the last Congress. This proposed legislation was a positive step toward addressing the complex and multifaceted difficulties surrounding the cyber workforce in general, and particularly in rural areas.

NRECA was particularly pleased with the inclusion of language that would extend cybersecurity internship opportunities to critical infrastructure providers in rural communities. We hope this provision will raise the visibility of electric co-ops as a viable and rewarding career path in cyber. Developing a talent pipeline with off-ramps into rural communities will help grow a local, skilled cybersecurity workforce to protect critical infrastructure in these communities. The Cyber PIVOTT Act will bridge the skills gap, enabling rural communities to strengthen their cyber defenses and secure their critical infrastructure.

Electric Cooperatives Solutions

Electric cooperatives are identifying innovative ways to address cyber workforce challenges. Co-ops are increasingly focused on building local talent through partnerships with educational institutions and providing opportunities for remote work and professional development. We are also seeing partnerships between large generation and transmission cooperatives, statewide associations, and distribution co-ops to share tools, equipment, and expertise across shared systems to bolster cyber defenses. In the Tennessee Valley, we have a long history of collaboration and partnership among TVA and its 153 local power companies, which are electric cooperatives and municipally owned electric systems. This partnership extends into the cybersecurity arena. Our state and Valley wide associations have made cybersecurity a top priority, from conferences and training to work groups and webinars.

Additionally, NRECA is leveraging members' fees and federal dollars to build a robust cybersecurity program to assist cooperatives in attracting cybersecurity talent, building professional and mentoring networks, and providing skill development and training opportunities.

The Rural Cooperative Cybersecurity Capabilities (RC3) Handbook is a series of comprehensive guides designed for specific roles within cooperatives to help enhance their cybersecurity posture. Last year, NRECA published the final handbook in the series targeted toward HR managers to provide practical advice on implementing recruitment and retention strategies and employing ongoing professional development.

NRECA and electric cooperatives are also utilizing funds through the Department of Energy's (DOE) Rural and Municipal Utility Cybersecurity Program, or RMUC, to make investments in cybersecurity technology, training, and educational opportunities. RMUC is a generational opportunity to improve the cybersecurity posture of electric cooperatives by providing resources to critical infrastructure operators with the greatest need of support.

Through RMUC, more than 200 personnel from 123 cooperatives participated in an intensive, three-day training program last year, hosted by DOE. The program was designed to advise attendees on how to improve cybersecurity for industrial control systems and operational technology.

Additionally, NRECA was awarded $9 million in RMUC funds to strengthen peer-to-peer information sharing, boost mutual assistance, promote cybersecurity awareness, and build

internal expertise through the expansion of the NRECA Threat Analysis Center (TAC) and the development of the Cyber Champions Program.

Finally, NRECA hosts an annual technical conference, known as Co-op Cyber Tech, that brings together cybersecurity professionals from rural electric cooperatives to collaborate, share knowledge, and develop skills. The event features hands-on content and sessions on the latest cybersecurity trends and technologies.

Conclusion

Cyber threats endanger electric reliability and present a major risk to the nation's safety, security, and economic stability. Electric cooperatives have a mission to safeguard the electric grid of the communities we serve and live in ourselves.

While electric cooperatives are making smart investments and building strategic partnerships to develop our cyber professionals, more work needs to be done. Initiatives like those in the Cyber PIVOT Act bring much-needed focus to the cyber workforce needs of rural America. Creating a talent pipeline that includes pathways into rural areas will foster a local, skilled cybersecurity workforce to safeguard critical infrastructure in these regions. Co-ops and our rural communities have a lot to offer in protecting America's critical infrastructure.

I thank the Committee for its bipartisan work on this issue and look forward to answering your questions.