Five Critical Challenges Facing America's Electric Grid

Introduction: The Converging Crisis Demanding Strategic Action

The American electric grid is at an inflection point, facing an unprecedented convergence of challenges that demand immediate strategic attention and comprehensive, innovative solutions. Rural electric cooperatives and municipal utilities are grappling with aging infrastructure, evolving security threats, cost pressures, and fundamentally shifting demand patterns. These challenges are not independent problems that can be solved sequentially—they are deeply interconnected, creating a complex system where solving one challenge may exacerbate another if not approached holistically.

As rural electric cooperatives testified before Congress, electric cooperatives are committed to innovation but cannot address these challenges alone. Federal support, state coordination, and industry partnerships are essential. The five challenges examined in this analysis represent the most significant pressures facing utilities and the electric grid system in the coming decade.

According to testimony presented to the House Energy and Commerce Subcommittee, electric cooperatives and their federal partners are actively seeking solutions to secure the nation's grid while managing costs and maintaining service quality. However, the complexity of addressing these challenges simultaneously requires unprecedented coordination, investment, and innovation. Industry analysts have identified five interconnected issues that will define the future of the electric grid: cybersecurity vulnerabilities, volatile peak pricing, affordability pressures, operational cost management, and the explosive growth in data center demand.

Each of these challenges presents distinct obstacles, yet they are fundamentally interrelated, creating a complex puzzle that requires holistic solutions rather than isolated fixes. Addressing one without considering implications for others will result in suboptimal outcomes and potentially worsen overall grid performance.

Challenge One: Cybersecurity—The Most Immediate and Persistent Threat

Cybersecurity has emerged as the most pressing immediate threat to America's energy infrastructure. Electric cooperatives and municipal utilities operate systems that are increasingly digitized and interconnected, yet many were designed with legacy infrastructure that predates modern cyber threats. The paradox is stark: the very technologies that enable more efficient grid management also create new vulnerability points that adversaries—including nation-state actors—continuously exploit.

The challenge is particularly acute for electric cooperatives serving America's most rural and remote areas. These utilities operate on tight budgets with limited resources for specialized IT staff. As cooperative leaders testified to Congress, "Smart, targeted federal support through funding, workforce development and improved threat intelligence sharing is essential." This assessment reflects a sobering reality: rural utilities cannot address cybersecurity challenges through market mechanisms alone.

The Department of Energy's Rural and Municipal Utility Cybersecurity Program (RMUC) represents a $250 million, five-year federal commitment to address this gap. However, even with significant federal investment, the challenge remains formidable. Electric cooperatives face cybersecurity pressures simultaneously: they must defend against increasingly sophisticated state-sponsored cyberattacks, protect aging systems not designed with modern security in mind, compete for limited cybersecurity talent in competitive job markets, and maintain service reliability to rural communities.

The Workforce Development Crisis in Cybersecurity

The workforce development component of any cybersecurity solution is critical. There is a severe shortage of skilled cybersecurity professionals, and rural areas are particularly disadvantaged in recruiting and retaining this talent. Cybersecurity professionals in major metropolitan areas command starting salaries from $80,000 to $120,000 annually, with experienced professionals earning $150,000 or more. For a rural cooperative operating at break-even

margins and serving communities where one in four households earns less than $35,000 annually, competing for this talent becomes nearly impossible without substantial outside support.

The shortage extends beyond entry-level positions. There is a critical shortage of mid-career and senior professionals with utility-sector cybersecurity expertise. These specialized professionals understand not just cybersecurity principles but operational technology, power system operations, legacy systems, and utility-specific constraints. Developing this expertise requires years of experience within the utility sector. Once developed, these professionals are highly sought after by larger utilities with bigger budgets, technology vendors offering higher compensation, federal agencies, and cybersecurity consulting firms.

This creates a self-reinforcing cycle. Without experienced cybersecurity personnel, utilities cannot effectively implement sophisticated security measures or train newer personnel. This makes positions at rural utilities less attractive to talented professionals seeking to develop expertise in challenging, well-resourced environments with mentoring from experienced security professionals. Over time, utilities that cannot attract security talent fall further behind in security posture, making them increasingly attractive targets for attackers while less attractive to potential security professionals.

Continuous Evolution of Threats and Required Adaptation

Cybersecurity is not a static problem—it evolves continuously. Threat actors develop new attack vectors, employ more sophisticated social engineering techniques, and adapt strategies in response to defensive measures. The cybersecurity landscape changes in weeks and days. A vulnerability discovered Monday might be actively exploited Wednesday. New attack techniques emerge constantly, often combining multiple vectors in sophisticated campaigns.

Utilities must maintain organizational capacity to evolve defenses constantly. This burden falls particularly heavily on smaller organizations with limited dedicated cybersecurity staff. A utility with a single IT director managing the billing system, helpdesk, network infrastructure, and industrial control systems cannot maintain the vigilance required to stay ahead of evolving threats.

Federal agencies and large utilities dedicate significant resources to threat monitoring, vulnerability assessment, and defensive adaptation. They employ dedicated security operations centers staffed twenty-four hours daily. They participate in information sharing networks providing early warning of emerging threats. They subscribe to threat intelligence services identifying and analyzing emerging techniques. Smaller utilities, operating on constrained budgets, often cannot afford these services and must rely on publicly available information—which by definition attackers already know.

Nation-State Actors and Critical Infrastructure Threats

The threat landscape has shifted to include nation-state actors explicitly targeting electrical infrastructure. Intelligence agencies have documented cyberattacks by Russia, China, North Korea, and Iran against electrical infrastructure in the United States and allied countries. These nation-state actors have demonstrated sophisticated capabilities including malware specifically targeting industrial control systems, maintaining persistence in victim networks for months or years, and coordinating attacks across multiple targets.

Nation-state actors have resources, expertise, and time horizons fundamentally different from criminal actors. Where criminals conduct quick attacks to extract data or money, nation-state actors conduct sophisticated multi-year campaigns, building deep knowledge of utility systems and positioning for potential future attacks.

For rural cooperatives, nation-state threats might seem irrelevant—surely no country would target a cooperative serving 50,000 rural customers. However, critical infrastructure is interconnected at national and international levels. A successful attack on a rural utility might provide access to systems eventually connecting to larger utilities, military installations, or defense contractors. Attackers might target rural utilities not for themselves but for access they provide to larger systems. Additionally, disruption of electricity supply to rural areas affects national security by affecting agricultural production, supply chains, and economic viability of rural regions.

Challenge Two: Managing Drastic Peak Prices—Economics and Grid Stability

The second major challenge is managing increasingly severe peak pricing volatility. This issue has become more acute as demand patterns have fundamentally shifted. Traditional baseload generation has given way to more variable renewable energy sources, while consumer demand has become less predictable and more concentrated during certain times of day.

Peak pricing volatility creates complex economic problems for utilities and customers. When demand spikes—often during extreme weather events when air conditioning or heating demand skyrockets—wholesale electricity prices can increase exponentially. A cooperative that must serve all customers regardless of price must absorb these costs, which then flow through as rate increases. This creates a vicious cycle: higher rates discourage consumption during peak times for affluent customers, but low-income customers have less flexibility and end up paying more per unit of electricity.

Extreme Weather Events and Intensifying Peak Demand

The challenge is particularly severe during extreme weather events. A heat wave in summer or cold snap in winter can drive demand far beyond normal levels, pushing electricity prices to unsustainable levels if maintained. Utilities must manage not just their own generation and distribution assets but their participation in wholesale markets and ability to manage demand during peak periods.

Several dynamics are making peak pricing management more difficult. First, increasing air conditioning penetration in previously unequipped areas, particularly in southern and southwestern states, means peak demand is becoming more concentrated and intense. Second, the transition to electric vehicles means utilities must prepare for concentrated charging demand during certain times of day. Third, climate change is making extreme weather events more frequent and severe, extending and intensifying peak demand periods.

The operational strategy of managing peak demand involves multiple components: investing in load flexibility to shift demand away from peak times, improving forecasting capabilities to predict demand more accurately, participating in demand response programs, and maintaining adequate generation or storage capacity to meet peak demand. Each requires capital investment and operational expertise that smaller utilities struggle to maintain.

Geographic Challenges for Rural Cooperatives

The distributed nature of rural electric cooperatives means they often lack the geographic and load diversity that helps larger utilities manage peaks. A large utility serving multiple climate zones and customer types can use diversity to offset peak demand in one region with lower demand in another. Rural cooperatives serving primarily agricultural or single-industry communities often face more correlated demand patterns, making peaks more pronounced.

A rural cooperative serving primarily agricultural customers experiences peak demand during growing season when irrigation systems operate simultaneously. A cooperative serving a manufacturing hub experiences peak demand when all facilities operate at full capacity. A cooperative with significant tourism experiences peaks during vacation seasons. Without geographic or customer-type diversity, these peaks become extreme and difficult to manage.

Challenge Three: Delivering Affordable Electricity—The Equity Imperative

Affordability represents the third critical challenge, fundamentally intertwined with other issues discussed here. Electric cooperatives have statutory missions to serve entire territories regardless of profitability. This universal service obligation ensures rural communities have reliable electricity but creates financial constraints that urban utilities don't face.

The economics of rural electrification are fundamentally different from urban electrification. In urban areas, utility assets serve thousands of customers per mile of distribution line. In rural areas, that same mile of line might serve only dozens of customers. Capital costs per customer are significantly higher in rural areas, and fixed costs must be spread across fewer customers. Rural cooperatives therefore face unavoidable cost pressures that urban utilities can mitigate through density.

Demographic and Income Considerations

Adding to these structural challenges is the demographic reality of rural America. As noted in testimony to Congress, one in four households served by electric cooperatives earns less than $35,000 annually. These households are particularly vulnerable to even modest rate increases, and energy costs consume larger percentages of total household budgets. Rate increases that might represent minor inconveniences to affluent households represent genuine hardships for low-income rural families.

The interconnection of affordability with other challenges is significant. Cybersecurity investments require capital that ultimately funds through customer rates. Peak pricing volatility can drive spot prices to levels that utilities must absorb and recover through rates. Investments in grid modernization and reliability require capital flowing through to customers. Each challenge therefore creates pressure on affordability.

The challenge for policymakers and utility leaders is finding ways to address necessary investments while maintaining electricity affordability for rural communities. Federal support programs, targeted infrastructure investments, and thoughtful regulatory policies all play roles. However, the fundamental challenge remains: how to invest adequately in grid security, reliability, and modernization while keeping electricity affordable for low-income households.

Strategies involve leveraging federal and state grant programs to fund necessary investments without creating disproportionate rate impacts. Another involves improving operational efficiency to reduce costs. A third involves strategic use of grid modernization technologies that can simultaneously improve security, reliability, and efficiency. But all strategies require coordination, expertise, and capital that smaller utilities may struggle to access without external support.

Challenge Four: Reducing Operational Costs—Efficiency and Innovation

The fourth challenge involves operational cost reduction—finding ways to deliver the same or better service while reducing operational expenses flowing through to customer rates. This challenge is particularly acute for cooperatives because they operate on margin-based economics. Unlike investor-owned utilities that can pass costs through to shareholders, cooperatives must recover all costs through customer rates or through efficiency improvements.

Primary Levers for Operational Cost Reduction

Primary levers for operational cost reduction involve several areas: labor productivity, technology deployment, supply chain optimization, and strategic asset management. Each presents opportunities but also requires investment and expertise.

Labor productivity is sensitive in rural areas where utility jobs represent good-paying, stable employment opportunities. However, changing workforce demographics mean many utilities are facing retirements of experienced staff without equivalent replacement hiring. This is partly due to changing career preferences—fewer young people are entering utility trades—and partly due to competitive disadvantages rural utilities face in recruiting young talent. Addressing this requires strategies such as apprenticeship programs, technical training partnerships with educational institutions, and competitive compensation that rural utilities may struggle to maintain.

Technology deployment offers significant promise for reducing operational costs. Advanced metering infrastructure (AMI) can reduce meter reading labor and provide better visibility into usage patterns. Predictive maintenance technologies can reduce emergency repair costs by identifying equipment failures before they occur. Geographic information systems (GIS) and asset management software can optimize resource allocation. However, implementing these technologies requires substantial upfront capital investment and staff retraining.

Supply chain optimization involves ensuring utilities can procure materials, equipment, and services at competitive prices. Rural utilities often suffer disadvantages in supply chain negotiations due to smaller size and geographic isolation. Some have addressed this through cooperative purchasing consortiums that pool demand to achieve better pricing. Others have invested in vertical integration or strategic partnerships with equipment suppliers and service providers.

Strategic asset management involves making deliberate decisions about which assets to maintain, upgrade, or retire. This requires sophisticated planning and forecasting capabilities that smaller utilities may lack. A utility that replaces aging infrastructure too slowly faces increasing failure rates and emergency repair costs. A utility that replaces infrastructure too quickly wastes capital usable elsewhere. Optimizing this balance requires data analytics, financial modeling, and strategic thinking.

Challenge Five: Increasing Data Center Demand—Hyperbolic Growth

The fifth critical challenge facing the electric grid is perhaps the most surprising and least anticipated by many utility planners: explosive growth in data center demand. Proliferation of artificial intelligence, cloud computing, high-performance computing for research and advanced applications, and data-intensive business applications is driving unprecedented electricity demand growth, particularly in regions with favorable geography, climate, and regulatory environments.

Data centers are not typical electricity consumers. A large hyperscale data center can consume as much electricity as a small city—potentially 100 to 500 megawatts or more for a single facility. These facilities require not just adequate electrical supply but also high reliability and clean power characteristics. A brief power interruption or voltage fluctuation that might be tolerable for residential and small business customers can cause cascading failures in data center operations, resulting in hundreds of thousands of dollars in losses per minute.

Geographic Concentration and Regional Impacts

The geographic concentration of data center development is creating acute challenges for some utilities while leaving others unaffected. Data centers tend to cluster around fiber optic hubs, in regions with cool climates to reduce cooling costs, and in areas with abundant, relatively inexpensive electricity. Some regions have experienced explosive growth in data center demand while others have seen minimal impact. This geographic variation means the challenge is particularly acute for utilities in favorable locations but less immediately pressing for others.

The demand growth is staggering. In regions experiencing data center clustering, electricity demand forecasts that looked reasonable five years ago are already being revised upward significantly. Utility planners must now grapple with demand growth rates that were previously considered impossible, requiring massive new generation and transmission capacity. A utility in a data center hotspot might need to add as much new generation capacity in five years as it previously expected to add in twenty years.

This explosive demand growth creates multiple cascading challenges. First, it requires massive capital investment in new generation and transmission infrastructure. Second, it puts pressure on fuel supply chains—whether for natural gas, coal, or nuclear fuel. Third, it accelerates the need for grid modernization and digitalization. Fourth, it creates opportunities for but significant challenges in integrating renewable energy sources at the scale and speed required.

Ripple Effects Through the Interconnected Grid

For a rural electric cooperative serving primarily agricultural and residential load, the data center challenge might seem irrelevant. However, even utilities not directly serving data centers are affected through wholesale electricity markets. As data center demand concentrates in certain regions, it drives up wholesale electricity prices in those regions, which then affects the cost of wholesale power for utilities in nearby regions. This means the data center challenge has ripple effects throughout the interconnected grid.

The challenge for utility planners and federal policymakers is managing this explosive demand growth responsibly. Demand must be met with adequate supply, but the supply should come from sources that are economically efficient, environmentally sustainable, and strategically resilient. This requires coordinated planning at regional and national levels, significant capital investment, and thoughtful management of energy resources.

Interconnections and Systemic Complexity: The Real Challenge

These five challenges do not exist in isolation. They are deeply interconnected, and addressing one often exacerbates the others. Cybersecurity investments require capital that increases operational costs and puts pressure on

affordability. Peak pricing management might require demand response programs that put burdens on low-income households. Data center demand might drive wholesale price increases that make affordable electricity harder to deliver.

This systemic complexity means solutions must be holistic and coordinated. A utility cannot simply invest in cybersecurity while ignoring affordability challenges. A federal program cannot address peak pricing without considering its impact on operational costs and cybersecurity capacity. Policymakers must consider how infrastructure investments to accommodate data center demand affect the financial viability of rural utilities serving less lucrative customer bases.

Real-World Examples: How Utilities Are Addressing These Challenges

Electric utilities across the country are implementing strategies to address these five interconnected challenges, providing case studies for how others might approach similar problems.

Case Study: Rural Cooperative Addressing Cybersecurity and Affordability

One multi-state rural electric cooperative with approximately 300,000 members faced significant cybersecurity vulnerabilities while struggling with affordability pressures. The cooperative's average member household income was well below the national average, making rate increases particularly sensitive.

The cooperative received federal grant funding through the RMUC program to conduct a comprehensive cybersecurity assessment. Working with federal support, the cooperative identified critical vulnerabilities in their aging SCADA systems and distribution management systems. However, replacement of these systems would have cost millions of dollars and would have required significant rate increases that would have been politically and socially difficult.

The cooperative worked with federal technical assistance to develop a layered security approach. Rather than replacing systems immediately, they implemented network segmentation to isolate critical control systems, deployed enhanced monitoring and intrusion detection capabilities, implemented strong authentication requirements, and trained personnel on security awareness and best practices. These measures provided substantial security improvements at a fraction of the cost of system replacement.

The cooperative then developed a multi-year modernization plan to systematically replace legacy systems as they reached end of life, ensuring that replacements included modern security features. Federal grants supported the initial assessments and training. The cooperative recovered costs for ongoing cybersecurity measures through operational efficiency improvements and modest rate increases that were spread over many years, managing affordability impacts.

Case Study: Small Utility Managing Peak Pricing Through Demand Response

A small municipal utility serving approximately 40,000 customers experienced severe peak pricing challenges during summer months when air conditioning demand spiked. The utility's costs during peak periods were driving wholesale prices to unsustainable levels and creating rate pressure.

Working with federal technical assistance and industry partners, the utility developed a comprehensive demand response program. The program included smart thermostat rebates for residential customers, interruptible rate options for commercial and industrial customers, and real-time pricing information enabling customers to shift consumption away from peak periods.

The utility also invested in battery storage systems that could absorb excess generation during off-peak periods and discharge during peak periods, smoothing the utility's load profile. These investments were funded through a combination of federal grants, state incentives, and utility revenues. The demand response program and storage system substantially reduced the utility's peak demand, moderating wholesale price exposure and reducing the need for rate increases.

Case Study: Cooperative Managing Data Center Demand

One electric cooperative located in a region experiencing rapid data center development faced explosive demand growth that threatened to overwhelm its generation and transmission capacity. The cooperative's forecasts for the next five years showed demand growth rates that would have required massive capital investments.

Rather than simply trying to meet explosive demand through infrastructure expansion, the cooperative worked with data center operators to understand their specific power needs and requirements. The cooperative discovered that data centers had specific power quality requirements but that they were willing to pay premium rates for guaranteed service levels.

The cooperative developed tiered service offerings with different prices and service levels. Standard service was available at moderate rates. Premium service with guaranteed uptime and minimal outages was available at higher rates. This enabled the cooperative to recover the costs of investments necessary to serve data center loads while offering affordable service to traditional customers.

The cooperative also worked with renewable energy developers to bring solar and wind resources online specifically to serve data center loads. This enabled the cooperative to meet the growing demand with renewable energy while also positioning the cooperative as a leader in clean energy transition. These renewable resources provided additional benefits of improving reliability and reducing overall system costs.

Recommendations for Strategic Action

Addressing these five critical challenges requires a multi-faceted approach including federal policy support, technical assistance, collaborative industry initiatives, and thoughtful capital investment.

Federal support programs like the Department of Energy's Rural and Municipal Utility Cybersecurity Program must be reauthorized and adequately funded. According to congressional testimony, the RMUC program represents a generational opportunity to improve cybersecurity posture of electric cooperatives and municipally owned electric utilities. The program was authorized at $250 million over five years but not all funding has been released. Congress should ensure that all authorized funding is appropriated and that the program is reauthorized beyond the current 2026 authorization.

Additionally, federal programs should address the full spectrum of challenges identified in this analysis, not just cybersecurity. While cybersecurity is critical, utilities also need support addressing peak pricing management, affordability, operational efficiency, and data center demand. A comprehensive federal strategy would address all these interconnected challenges rather than treating them as separate policy domains.

Workforce Development and Education

Workforce development programs should prioritize the electric utility sector, particularly in rural areas. The shortage of skilled utility workers—including cybersecurity professionals, distribution technicians, and system operators—threatens the ability of utilities to effectively operate and maintain infrastructure. Federal and state workforce development programs should include support for utility apprenticeships, technical training partnerships with community colleges and vocational schools, and loan forgiveness programs for utility professionals committing to rural service.

Community colleges in rural areas should receive federal support to develop training programs focused on utility sector skills. These programs should include not just technical training but also education on cybersecurity, grid modernization, and advanced operational practices. By developing this training locally, rural areas can build workforce capacity while retaining young people who might otherwise leave rural communities for urban areas with more job opportunities.

Partnerships between utilities, schools, and community colleges should be incentivized through federal grants. These partnerships can create apprenticeship programs where students earn while learning, combining classroom instruction with on-the-job training. Such programs have proven highly effective at developing skilled workers while providing utilities with a pipeline of trained personnel.

Regional Technical Assistance

Smaller utilities need access to technical expertise they cannot afford to employ directly. Regional technical assistance centers funded by federal or state resources could provide consulting support to utilities addressing cybersecurity challenges, grid modernization, demand management, and other issues. These centers could serve as hubs bringing together expertise across multiple utilities and making that expertise available to utilities that otherwise could not access it.

Technical assistance programs should be designed to build utility capacity rather than create dependency on external consultants. A technical assistance model might involve a consultant working with a utility to identify challenges and develop solutions, then training utility personnel to implement and maintain solutions, rather than the consultant simply implementing solutions on behalf of the utility.

Information Sharing and Coordination

Federal agencies should invest in systems and processes enabling rapid threat intelligence sharing, load forecasting collaboration, and best practices communication among utilities of all sizes. While large utilities participate in information sharing consortiums, smaller utilities often lack access to timely threat intelligence and best practices information.

A federal threat intelligence sharing system could collect and analyze cybersecurity threats across utilities, identifying patterns and emerging threats, and then rapidly disseminate this information to all utilities. Such a system might operate similar to how public health agencies track disease outbreaks, enabling early warning and coordinated response.

Similarly, federal agencies could facilitate load forecasting collaboration where utilities share forecasting models and methodologies, enabling smaller utilities to benefit from more sophisticated forecasting approaches than they could develop independently.

Capital Investment Programs

Federal grant and loan programs should help smaller utilities make necessary investments in cybersecurity, grid modernization, demand management, and renewable energy integration. Grants should be structured to address the capital constraints that smaller utilities face, recognizing that utilities operating on thin margins cannot self-finance major infrastructure investments.

Loan programs should offer favorable interest rates and long repayment periods enabling utilities to finance investments while managing affordability impacts. A utility that must finance $50 million in grid modernization investments over 20 years can spread costs more evenly than one that must pay for investments over shorter timeframes.

Regulatory Reform

State and federal regulators should review whether current regulatory frameworks adequately incentivize utilities to address these challenges while maintaining affordability and reliability. In some cases, regulatory structures may discourage needed investments. For example, if regulatory structures penalize utilities for peak demand spikes, utilities might invest in expensive peaking generation rather than in demand management that would be less expensive and more sustainable.

Regulators should consider regulatory reforms enabling utilities to recover costs for investments in cybersecurity, grid modernization, and demand management. Utilities are more likely to invest in these areas if confident that costs will be recoverable through rates rather than absorbed by utility shareholders.

Conclusion: The Path Forward

The American electric grid faces five critical, interconnected challenges demanding immediate attention and significant resources. These challenges threaten the reliability, affordability, and security of electricity supply for all Americans, but particularly for rural communities served by electric cooperatives and municipal utilities.

Cybersecurity vulnerabilities threaten the integrity of critical infrastructure upon which American prosperity depends. Peak pricing volatility threatens affordability and creates financial stress on utilities. Affordability pressures threaten the ability of low-income households to meet basic electricity needs. Operational cost pressures threaten the financial viability of smaller utilities. And explosive data center demand threatens to overwhelm grid infrastructure in some regions while leaving others underutilized.

These challenges are interconnected—addressing one often affects the others. Cybersecurity investments that increase costs threaten affordability. Peak pricing management that shifts consumption to certain times of day affects both operational planning and affordability. Data center demand in some regions drives wholesale price increases affecting all regions. Operational efficiency improvements require capital investment that must be recovered through rates, affecting affordability.

The stakes are high. Reliable, affordable electricity is foundational to economic opportunity and quality of life for all Americans. Failure to adequately address these challenges will result in less reliable service, higher costs, and increased vulnerability to threats. The challenges are real and urgent.

However, the challenges are not insurmountable. With appropriate support, coordinated policy, technical assistance, and collaborative industry initiatives, the American electric grid can navigate this critical period and emerge stronger, more secure, and more resilient. Federal leadership, state coordination, utility innovation, and community support can combine to address these challenges comprehensively.

The nation has successfully addressed major infrastructure challenges before. The rural electrification programs of the 1930s brought electricity to communities that markets alone would not have served. The interstate highway system connected the nation's regions. Modern broadband deployment is extending connectivity to rural communities. Similar commitment to ensuring that all communities benefit from secure, reliable, affordable electricity can address the challenges identified in this analysis.

The time for action is now. Utilities understand the challenges and are committed to addressing them. Federal support programs are in place but need adequate funding and coordination. The technology and expertise to address these challenges exist. What is required is sustained commitment from policymakers, utilities, industry partners, and communities to work together to ensure that America's electric grid serves all people effectively.