RPTR MOLNAR

EDTR ROSEN

SECURING AMERICA'S ENERGY INFRASTRUCTURE: ADDRESSING CYBER AND PHYSICAL THREATS TO THE GRID

WEDNESDAY, DECEMBER 3, 2025,

House of Representatives,

Subcommittee on Energy,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:34 a.m., in Room 2141, Rayburn House Office Building, Hon. Robert E. Latta [chairman of the subcommittee] presiding.

Present: Representatives Latta, Weber, Palmer, Allen, Balderson, Pfluger, Harshbarger, Miller-Meeks, James, Fry, Lee, Langworthy, Evans, Goldman, Fedorchak, Guthrie (ex officio), Menendez, Mullin, McClellan, DeGette, Matsui, Tonko, Schrier, Fletcher, and Pallone (ex officio).

Staff Present: Clara Cargile, Professional Staff Member, Energy; Andrew Furman, Professional Staff Member, Energy; Sydney Greene, Director, Finance and Logistics; Calvin Huggins, Clerk, Energy; Megan Jackson, Staff Director; AT Johnson, Special Advisor; Sophie Khanahmadi, Deputy Staff Director; Brayden Lacefield, Special Assistant; Mary Martin, Chief

Counsel, Energy; Sarah Meier, Counsel and Parliamentarian; Peter Maris, Research Assistant, Oversight and Investigations; Mary Martin, Chief Counsel, Energy; Joel Miller, Chief Counsel; Ben Mullaney, Press Secretary, Press; Seth Ricketts, Special Assistant; Peter Spencer, Senior Professional Staff Member, Energy; Timothy Trimble, Staff Assistant; Matt VanHyfte, Communications Director; Jane Vickers, Press Assistant, Press; Katie West, Press Secretary, Press; Tiffany Guarascio, Minority Staff Director; Kristopher Pittard, Minority Professional Staff Member; Shae Reinberg, Minority Intern; Emma Roehrig, Minority Staff Assistant; Kylea Rogers, Minority Policy Analyst; Ella Seaman, Minority Press Intern; Andrew Souvall, Minority Director of Communications Outreach and Member Services; and Tuley Wright, Minority Staff Director, Energy.

Mr. Latta. Well, good morning, and I would like to call the Subcommittee on Energy to order. The chair now recognizes himself for 5 minutes for an opening statement.

Again, good morning again, and welcome to today's hearing. We will examine how the electric industry is adjusting cyber and physical threats to the electric grid, a key component of our Nation's energy infrastructure.

We will look at the challenges to securing this infrastructure at a time of tremendous growth and power demand. This hearing will inform the subcommittee on current initiatives and practices to secure our Nation's critical electric infrastructure from the various malicious threats to the delivery of power.

This year, we have frequently heard about the challenges to the reliable delivery of energy and power. Grid operators have testified about the massive premature loss of dispatchable baseload powering our electric grid without adequate replacement. As a result, an increased blackout risk in certain regions of the Nation during times of peak demand.

Addressing cyber and physical threats represents another challenge to the reliable delivery of energy and power, incapacitating the grid with some cyber or physical attacks will have widespread devastating impacts, which makes security particularly vital to our Nation's energy security, economy, our health, and our welfare.

Addressing these threats is difficult. The avenues for malicious attack only increase with the increased digitalization and growing linkages of gas pipelines, new generating resources, and expanded transmission.

These linkages have been rapidly increasing as the Nation works to meet growing power demand particularly from AI and manufacturing.

As the public security assessments note, the Nation faces an evolving landscape of

threats, from nation states to criminal and ideological motivated cyber attackers.

Russia has long been a persistent threat to our energy systems, yet China has become particularly worrisome. Even as we race with China on AI, the U.S. intelligence community reports, in its public assessments, that China remains the most active and persistent threat to American critical infrastructure networks.

China's proxies have pre-positioned attack capabilities in American infrastructure to be used during a major crisis or conflict.

More local risks relating to physical attacks also threaten communities and other important infrastructure. Just 2 years ago, this subcommittee held a field hearing in North Carolina to examine the threats surrounding an attack on electric substations. The attack in question left 30,000 people without power and exposed how targeted physical attacks can impact people and industry -- even the military -- in critical regions.

Addressing cyber and physical threats is made more complicated by individual utilities, particularly capabilities, resources, and access to threat intelligence and other information.

Our witnesses this morning will help us understand how the industry works to overcome these challenges. We will hear testimony from grid executives, representing both investor-owned utilities and nonprofit co-operatives which together cover the bulk of American electric infrastructure.

We will also hear from the head of the Electricity Information Sharing and Analysis Center, or E-ISAC. This operation, run by the North American Electric Reliability Corporation, or NERC, provides important information sharing services to assist industry with critical infrastructure threats.

Given that Congress has charged NERC with assuring reliability of the electric system, a perspective on what is necessary to coordinate grid security to effectively address growing

vulnerabilities will be important.

We will hear from a grid security expert at Carnegie Mellon, who has been active on the National Security Council. And finally, we will hear from the associate laboratory director for national security at Utah National Laboratory who will provide insights into threats and to how the U.S. Government is working to help industry be more informed about the most consequential risks, and to better plan and protect our grid.

Energy and Commerce has led on enactment of several laws over the past decade to ensure appropriate national attention to cyber and physical attacks in our Nation's critical energy infrastructure.

This work ranged from clarifying government authorities in the Federal Power Act to authorizing several technical assistance and information sharing programs to assist utilities of all sizes.

The hearing today should inform us as we seek to update and reauthorize various provisions that aim to make the Nation more secure.

And at this time, I will yield back the balance of my time, and I recognize the gentlelady from Florida's 14th District, the subcommittee ranking member for an opening statement.

Ms. Castor. Well, thank you, Mr. Chairman, thank you to our witnesses for being here today. The United States needs energy infrastructure and an electric grid that meets the needs of the 21st century. That means a modern, reliable, and resilient grid and tools for power providers to guard against malign attacks and extreme events.

Unfortunately, the Trump administration is taking us backwards, keeping us wedded to outdated technologies that are insufficient to meet modern threats, or power innovations, like artificial intelligence.

For example, the current Department of Energy terminated billions of dollars for

projects meant to reduce the frequency and durations of blackouts and help utilities restore power faster.

One energy expert who previously consulted for the Department recently criticized the administration for arbitrarily ending projects that sought to make the grid more reliable, and able to withstand storms, hackers, accidents, and other problems.

Some of the cancelled projects under the Grid Resilience and Innovation Partnerships Program would have upgraded grid management, including improved sensing of real-time voltage and frequency changes in the electricity sent to homes and businesses.

The Trump administration also slashed efforts to automate grid operations, and allow faster response to outages or changes in output from power plants, and develop microgrids, localized systems that can operate independently during outages, which really hit home for me last year when many businesses and neighbors went without power for days after Hurricanes Helene and Milton.

Cancelled grid modernization projects are estimated to total over $700 million across 24 States. For example, a $20 million project in the Upper Midwest would have installed smart sensors and software to detect overloaded power lines, or equipment failures, helping people respond faster to outages, and prevent blackouts.

A $50 million project in California would have boosted the capacity of existing sub transmission lines, improving power stability and grid flexibility, by installing a smart substation without needing new transmission corridors.

And microgrid projects in New York, Hawaii, and New Mexico, would have kept essential services running during disasters, cyber attacks, or planned outages.

Now, this committee could play a constructive role to get back on track, especially as it has focused a lot of attention on the power needs of AI. Electricity, the technologies that produce it cheaply and efficiently, and a grid that can deliver it where needed will determine

the future of AI.

In 2008, China and the United States were roughly on par in the deployment of emerging energy technologies, but not today. China dominates this sector.

They are electrifying while America recently has taken an off ramp.

Electrification in the U.S. is stuck at just over 20 percent. China is electrifying at 10 percentage points a decade. They are now at 30 percent and heading for 35 percent, and as a result they are reaping the geopolitical benefits of being able to sell these technologies abroad.

In August China exported $20 billion in clean technology exports, and for comparison, the U.S. exported about $1.3 billion in LNG that month.

We cannot win the AI race of the 21st century while limiting ourselves to a 20th century playbook. We need to rapidly deploy grid-enhancing technologies, scale energy efficiency, and support virtual power plants.

And while doing so, we can make our grid more flexible and resilient both to physical dangers and to malicious cyber threats.

Traditionally our grid was established with a few large-scale, fossil-based energy generators pushing out energy to customers, but that is changing to a much more flexible and interconnected model of distributed generation where electricity is moving in both directions across wires all the time.

The clean energy transition and broader energy expansion to meet AI electricity demand is an opportunity to counter cybersecurity threats, and if done properly, we can replace our outdated energy systems with software-enabled, clean-energy technologies, modern tools that allow the grid to recover more readily when harmed by a hurricane or a hacker that takes out a portion of the grid.

We can use smart inverters, grid-forming technologies, and batteries to restabilize,

or if necessary, quarantine a part of the grid.

Securing our electric grid should be a bipartisan national security imperative. Congress can do this. We did it in the Bipartisan Infrastructure Law. It is imperative that we strengthen what we did there.

So let's get back on track get back in the electrification race for the sake of our technological advancement and to put downward pressure on electric bills for consumers.

I look forward to hearing from the witnesses today, and I thank you.

Mr. Latta. The gentlelady yields back, and the chair now recognizes the chairman of the full committee, the gentleman from Kentucky, for 5 minutes for questions.

The Chair. Thank you. Thank you, Chairman Latta, for having this hearing, and thank you for all of our witnesses being here. And there is one specific one I will point out in just a few minutes.

And I also want to publicly thank Chairman Jordan for the opportunity to use this room today while our second room is being renovated.

So throughout our Nation's history, the affordable, reliable, and abundant supply of energy has underpinned our prosperity and security. Today's world is no different: a complex web of interwoven energy systems and networks of linear infrastructure power that facilities and technologies that Americans rely on for work, healthcare, or finance services, modern communications, and a myriad of everyday necessities.

Our society's ubiquitous reliance on digital systems to power all of these applications also makes the underlying energy systems a target for nefarious actors such as state-sponsored attacks from China, Russia, and Iran.

The committee has noted throughout this Congress that we are on the precipice of great technological advancements, and could reshape the next-generation economy.

But as these developments take root, our reliance on energy will continue to grow

and the surface area for potential threats will widen, potentially even equipping bad actors with sophisticated tools to cause harm and sew chaos in the lives of everyday Americans.

Ten years after Russia conducted the world's first large-scale cyber attack in Ukraine, that shut down the grid for 200,000 residents, we witnessed the first documented, large-scale, AI-driven cyber attack against governments, financial institutions, and businesses around the globe last month.

This attack served as a test case, demonstrating the capability of advanced computing models to conduct wide-ranging attacks with minimal human intervention.

But AI can also be deployed to promote security and resiliency on the cyberspace battlefield and equip operators with the tools they need to protect against attacks and respond in the case of disaster.

The witnesses before us today are on the frontline, protecting critical energy infrastructure in the efforts to address an evolving-threat landscape. One witness that I would particularly like to welcome is a friend of mine and from my area, Tim Lindahl, president and CEO of Kenergy Electric, a electric co-operative that serves several counties across western Kentucky.

I believe you serve 14 counties, and six of your 14 counties are among the best in the world. That is what I understand. They happen also to be in the Second District of Kentucky. Thank you for your service to them in places like Owensboro, Hawesville, McLean County. I don't think -- you're -- Muhlenberg and Breckenridge. I think I have hopefully got them all. Davies and Hancock are the counties for those cities I mentioned.

So co-operatives like Kenergy are a key partner in these efforts to protect reliability and security of the electric sector in our rural communities.

And it is just a note that I am glad you are here because we have, you know, big, large-scale investor utilities. We have cooperatives that are there to serve the members of

their co-op, and have the same requirement, that you have to have protection and security, you know, whatever scale you operate in.

And that is a daunting task. I know you take it seriously. I know the co-ops and all of our friends take it seriously, and we really appreciate you being here in this discussion.

As I said, I was thanking Chairman Jordan for this real estate because there is two -- another meeting going on. I am going to be back and forth, but I look forward to hearing as much testimony as I possibly can and engaging in this.

And, Mr. Chairman, I really appreciate you having this hearing, and I will yield back.

Mr. Latta. Thank you very much. The gentleman yields back the balance of his time. The chair now recognizes the gentleman from New Jersey, the ranking member of the full committee for 5 minutes for questions.

Mr. Pallone. Thank you, Chairman Latta. I am pleased the subcommittee is holding this important hearing today as cybersecurity is a critical issue that can impact energy affordability and reliability.

This is also the first energy subcommittee hearing this Congress that was put together in a bipartisan way -- and it is December. We should be having hearings like this regularly rather than just annually.

And securing our Nation's energy infrastructure from cyber and physical threats should be something we can all agree on. After all, threats to our energy system are only growing, whether it can be from nation-state actors such as Russia or China or domestic terrorists here at home whose capabilities are being enhanced every day by increasingly effective artificial intelligence tools.

And soon attacks that would have required the resources of a sophisticated opponent will be able to be carried out by a single person, and our adversaries with resources will be able to sow chaos on a much larger scale than we ever anticipated.

So these threats are not hypothetical. Earlier this year, we discovered that hackers, associated with the Chinese Government, unleashed an attack that compromised the systems of a Massachusetts utility for nearly a year.

And I don't have to tell anyone the disaster that this could cause both for the reliability of energy systems and for our mission to keep utility bills low.

And that is why today's hearing is so important, and why we have discussed the many threats facing energy reliability this year -- from President Trump's attack on clean, cheap energy, to threats brought by extreme, climate-fueled weather events, to challenges from data centers consuming enormous amounts of electricity.

Cyber threats to the grid involve an adversary who will seek to overcome any barriers that we can raise against them, so we have to be in a state of constant evolution.

Now, the interconnected nature of our energy systems means that any one threat cannot be viewed in isolation. Threats to a gas pipeline can quickly cascade into a threat to electric reliability.

And because of this interconnectivity, we must ensure that experts from the Department of Energy play a key role in our government's cybersecurity defenses for the energy sector.

And while agencies under the Department of Homeland Security can play an important, convening role, it is the DOE, the Department of Energy, not Homeland Security, that has the critical relationships with all the relevant actors in the industry, and has the expertise necessary to view threats in a holistic manner.

And we saw this in the aftermath of the Colonial Pipeline, a cyber attack when the Department of Energy took the lead on the Federal response.

I look forward to hearing about some of the work the DOE is doing in bringing together the energy industry to talk about threats that impact everyone.

However, none of this work at the Department of Energy, it is not going to work essentially, unless DOE is the agency that is properly staffed and has the resources to fulfill its mission.

Do you know we lost more than 3,500 staff this year as a result of Secretary Wright and DOGE's reckless and relentless attacks on Federal workers?

We need to ensure that we have sufficient staff working on the issue of cybersecurity, and that they get the resources at DOE and the funding that they need.

Now, I was the chair of this committee in 2021, and then we passed a law establishing a number of cybersecurity programs at the Department of Energy and the Federal Energy Regulatory Commission, and many of those programs are now coming up for reauthorization and are ripe for examination to see what worked, what didn't work, and lessons we should all learn as we look to potential legislative action.

So finally, I hope we can also discuss the security not only of our energy infrastructure but of the supply chain that creates that infrastructure.

During the last 10 months, the Trump tradition has hobbled our efforts to re-shore manufacturing in America, increasing tariffs, slashing tax credits that were designed to make American manufacturing competitive.

And as a result, we are more dependent than ever on foreign sources for critical infrastructure components, and that is a vulnerability that could turn into a devastating weakness if we don't work to reverse it.

So I hope to hear ideas on how we can turn this around today from all of you, and, again, I thank you, Chairman Latta, and I yield back the balance of my time. Thank you.

Mr. Latta. Well, thank you very much. The gentleman yields back the balance of his time, and this now concludes member opening statements.

The chair would like to remind members that pursuant to the committee rules, all

members' opening statements will be made part of the record.

Again, we want to thank our witnesses for being with us today and taking time to testify before the subcommittee. Each witness will have the opportunity to give an opening statement followed by a round of questions from our members.

Our witnesses for today are Mr. Michael Ball, CEO of the Electricity Information Sharing and Analysis Center, and senior vice president of the North American Electric Reliability Corporation; Ms. Sharla Artz, security and reliant -- pardon me -- security and resilience policy area vice president at Xcel Energy; Mr. Tim Lindahl, the president and CEO of Kenergy Corp; Mr. Harry Krejsa, the director of studies for the Carnegie Mellon Institute for Strategy and Technology; and Mr. Zach Tudor, the associate laboratory director at the Office of the National and Homeland Security at the Idaho National Laboratory.

We appreciate you all being here today, and before I recognize Mr. Ball for your 5 minutes, let me just mention, if you would pull the mics up close to you and press that button to make sure that that light has come on so we can hear you loud and clear.

And at 1 minute you will see the green light go to yellow, so you have 1 minute left in your opening statement. When the light goes red, we would like you to finish your opening statement.

So thank you again for being with us today, and, Mr. Ball, you are recognized for 5 minutes to give your opening statement. Thank you.

STATEMENTS OF MICHAEL BALL, SENIOR VICE PRESIDENT AND CEO, ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION; SHARLA ARTZ, SECURITY AND RESILIENCE POLICY AREA VICE PRESIDENT, XCEL ENERGY; HARRY KREJSA, DIRECTOR OF STUDIES, CARNEGIE MELLON INSTITUTE FOR STRATEGY & TECHNOLOGY; TIM LINDAHL, PRESIDENT AND CEO, KENERGY CORP; AND ZACH TUDOR, ASSOCIATE LABORATORY DIRECTOR, NATIONAL & HOMELAND SECURITY, IDAHO NATIONAL LABORATORY.

STATEMENT OF MICHAEL BALL

Mr. Ball. All right. Well, thank you, Chairman Latta, and ranking members, and members of the subcommittee for inviting me and convening this important discussion regarding threats to North America's electric grid.

My name is Michael Ball, and I served as the CEO of the Electricity Information Sharing and Analysis Center, or E-ISAC. The E-ISAC is a clearinghouse for security information for the electricity industry of North America. It is operated under NERC, the organization designated by FERC as the electric reliability organization for the United States.

Our mission is to reduce cyber and physical security risks to the electricity industry by providing unique insights, leadership, and collaboration across the United States and Canada.

We accomplish our mission by gathering, curating, and disseminating threat information in a timely and actionable manner. We do this with asset owners and operators to help mitigate the complex evolving threats of the grid.

The E-ISAC operates a 24/7 watch operation, develops analysis of ongoing incidents,

and provides a suite of analytical products and services accessible to over 1,900 member organizations.

E-ISAC membership represents more than 85 percent of the meters in North America, and includes a range of utilities of all sizes and types, some of which are represented here with us today.

The E-ISAC promotes cross-sector coordination and information sharing as well. This includes natural gas, communications, water, and finance. We work closely with our government partners, such as the Department of Energy, DHS, CISA, FERC, and the intelligence community. We maintain similar relationships with industry and government partners in Canada.

To support the connective tissue between the private sector and the government, NERC and the E-ISAC are members of the industry's Electricity Subsector Coordinating Council.

The ESCC, led by industry CEOs in partnership with senior government officials, seeks to operationalize security initiatives and coordinate around events that threaten grid reliability.

We do this because the threat landscape is complex. It includes continuously evolving threats from sophisticated and very capable adversaries. Among the most advanced are nation states, the state actors, which are very well-funded, and numerous public reports underscore how these adversaries focus on the electric sector.

China, Russia, Iran, and Korea are monitored closely. Currently, Chinese cyber activities pose one of the most dynamic threats to our critical infrastructure. The sheer scale and persistence of Chinese cyber activities are demonstrated in the various Typhoon campaigns that are widely reported on and lends credence to their ambition to target North American critical infrastructure.

In addition to nation-state threat actors, the E-ISAC monitors domestic and international hacktivists and criminal activities. Cyber criminals have access to a wide array of tools and techniques, supported by a stunning dark web ecosystem that fuels ransomware and other extortion campaigns that we see today.

And unfortunately, activists and extremists see destructive acts against critical infrastructure targets as an opportunity to create impact in a way that draws attention to their ideologies and beliefs.

The E-ISAC helps our industry counter these threats by fostering an active community of industry and government partners. A secure portal allows members to exchange and receive industry-recognized bulletin and alerts, regarding relevant cyber and physical threats to the industry.

Through this portal the E-ISAC provides analytical products with actionable content to support industry security teams.

In partnership with the Department of Energy, the E-ISAC operates CRISP, the Cybersecurity Risk Information Sharing Program. CRISP is a monitoring system that provides cyber threat intelligence and helps detect malicious activity and inform defensive measures.

We also partner with DOE on the ETAC, the Energy Threat Analysis Center. The ETAC is a collaboration between industry and government through CISA's Joint Cyber Defense Collaborative.

And ETAC partners work together to analyze threats, provide industry context and recommendations back to the sector, and it is an important example of how private sector is working with government to bolster the defense of critical infrastructure.

The E-ISAC also plays an important role in convening industry. We host GridSecCon, an annual, grid-security conference, which brings together nearly 1,000 security

professionals for training, education, and collaboration across industry.

And just 2 weeks ago, we conducted the eighth iteration of GridEx, the largest grid-security exercise in North America, and this is to tackle critical issues and identify ways to enhance our industry's readiness to respond to large-scale attacks.

And in conclusion, these are examples of how the E-ISAC operates around the clock to do our part to enable a reliable, resilient, and secure industry.

I look forward to today's discussion. Thank you.

[The prepared statement of Mr. Ball follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Thank you.

Ms. Artz, you are recognized for 5 minutes for your opening statement.

STATEMENT OF SHARLA ARTZ

Ms. Artz. Thank you. Chairman Latta, distinguished members of the subcommittee, thank you for holding this hearing.

I am Sharla Artz, and I serve as Xcel Energy's security and resilience policy area vice president. My testimony today is on behalf of Xcel Energy and Edison Electric Institute, or EEI.

Xcel Energy is a member of EEI, which represents all U.S. investor-owned electric companies. EEI's members provide electricity for nearly 250 million Americans, and operate in all 50 States and the District of Columbia.

Xcel Energy is a large investor-owned utility operating in eight western and midwestern States, serving 3.9 million electric customers, and 2.2 million natural gas customers.

For Xcel Energy and EEI's member companies, securing energy systems from all hazards, including cyber and physical threats, is a top priority.

As you just heard from Mr. Ball, the threat we face from nation-state adversaries is real, it is advanced, and it is persistent.

As the frontline defenders of the Nation's energy infrastructure, the private sector must be supported by the government to address national security risks. An essential component of that support is the timely sharing of actionable intelligence about our adversaries' tactics and their motivations.

Armed with this intelligence, private sector experts can proactively architect security into their systems, hunt for adversarial activity, and mitigate the risks from these threats.

An important example of this information-sharing, support, and partnership, is the Energy Threat Analysis Center, or ETAC, that Mr. Ball just described.

First piloted in 2023, and now consisting of 17 private sector entities, ETAC is an operational collaborative that convenes experts from our sector risk management agency, which is the Department of Energy, and private sector companies, to identify, analyze, and mitigate cyber threats in real time.

The uniqueness of ETAC is bidirectional exchange of information, private sector operational expertise, combined with government intelligence, that creates products that are specifically targeted to assist energy companies throughout the country reduce risk.

ETAC also facilitates collaboration with other Federal agency partners, including DHS, the military, and Federal law enforcement agencies, expanding cross-agency information sharing with the private sector.

Thousands of energy entities have accessed ETAC products, evidence of its importance to industry risk-reduction efforts.

In addition to initiatives like ETAC, industry and government are strategically assessing threats and prioritizing risk reduction at the executive level. The Electricity Subsector Coordinating Council, or ESCC, consists of CEOs who represents all segments of the electric sector and serves as the primary interface between government and industry to address national security issues.

Importantly, this convening mechanism exemplified by the ESCC unifies government and industry action on reducing systemic risk. A prime example of the effectiveness of the ESCC is the prioritization of industry efforts to support critical military installations and their energy-resilience needs during a time of increasing geopolitical conflicts.

At all levels of our industry, the commitment to countering nation-state actors is active, and it must be supported by Congress and our government partners.

To bolster these national security collaborative efforts, we ask Congress to do the following. First, Congress should authorize ETAC so that it can adapt to address evolving threats, allowing for the strategic advice from private sector partners.

Explicit recognition of this program allows industry partners and DOE to jointly shape sector risk-reduction priorities.

Second, Congress should continue to provide resources for ETAC so that private sector partners are armed with actionable information to defend their systems. Assured resources provide certainty for the private sector investment in this capability.

Third, continued recognition of the importance of the sector risk-management agencies for risk reduction is essential.

The energy system expertise contained within DOE and the National Lab complex assures that risk assessment is informed by system operational understanding. Having DOE lead interagency engagement minimizes duplicative or conflicting initiatives that tax private sector resources.

The security of energy infrastructure is essential to national security. Government and private industry both have roles to play, and we are committed to reducing national security risks.

Thank you again for including me in the hearing. I look forward to the questions.

[The prepared statement of Ms. Artz follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much for your testimony today, and, Mr. Lindahl, you are recognized for 5 minutes for an opening statement.

STATEMENT OF TIM LINDAHL

Mr. Lindahl. Thank you and good morning, Chairman Latta and Ranking Member Castor, and all the members of the committee.

Thank you for the opportunity to discuss how electric co-operatives are working to secure the grid against evolving cyber threats. My name is Tim Lindahl, and I serve as president and CEO of Kenergy Corp, a distribution utility in western Kentucky. I am testifying today on behalf of the National Rural Electric Cooperatives, otherwise known as NRECA, which represent nearly 900 co-operatives nationwide.

At Kenergy we serve about 60,000 homes and businesses across 14 counties. We also support a robust industrial base, and have built over 3,500 miles of fiber infrastructure to help evolve our grid and provide broadband to our rural economies.

Every day, America's electric grid faces thousands of cyber intrusion attempts. For rural electric co-operatives, these threats are not abstract. They are real, they are sophisticated, and they are growing.

Electric co-operatives are unique. We are private, independent businesses owned by the people we serve. We operate without profit incentive. We power over 42 million Americans, including critical infrastructure such as hospital, data centers, and more than 150 military installations.

However, securing this infrastructure presents distinct challenges. We operate in rural areas with lower population densities and fewer resources than many urban utilities.

We must secure lines in isolated substations that may be hours apart.

Because we have no shareholders, these costly investments are borne by our member consumers, many of whom live with modest incomes.

Despite these constraints, co-ops are rising to the occasion. We apply a risk-based, layered defense strategy to protect against all hazards, whether they are from severe storms or cyber attacks.

Our approach is built on the principle of cooperation. Because we are independent, we can innovate locally, but we can also pool our resources and gain strength in our collective defense.

But technology alone is not enough. 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 happened, or we never hear about the attack that never occurred.

To support these teams, we leverage cutting-edge tools and resources that are being developed through NRECA's cybersecurity program, like the Threat Analysis Center, a platform that helps co-ops identify, analyze, and communicate threats, while reducing alert fatigue so our teams can focus on high impact risks for the Co-Operative Cyber Goals Program, which also provides a structured framework designed specifically for co-operatives to advance cyber hygiene regardless of the utility's cyber maturity.

While co-operatives are doing their part, we cannot do this alone. Strong Federal partnerships are essential to closing this resource gap. Electric co-operatives utilize resources from various Federal agencies and departments, including the CISA, DHS, DOD, and the State intelligence fusion centers.

These all help co-ops better understand vulnerabilities, emerging threats, and mitigation efforts.

The Rural and Municipal Utility Cybersecurity Security Program, otherwise known as RMUC, is one example of these partnerships. RMUC represents the most significant opportunity for co-ops to bolster their readiness by providing $250 million to help us invest in the people, processes, and technologies needed to secure the grid.

However, we need your help to maximize its impact. While 80 million in the RMUC funding has been announced, much of the funding has yet to be released. We urge the Department of Energy to distribute these funds quickly so co-ops can put them into action.

With an estimated $160 million remaining and less than a year left in authorization, NRECA strongly urges Congress to reauthorize the NRECA program. This is critical to ensuring rural communities are not left behind.

Protecting the grid is a top priority for the Nation's electric co-ops. We are making smart investments, training our workforce, and sharing threat intelligence to keep the lights on.

With continued partnership and targeted Federal investment, we can strengthen our defenses and ensure the security of the energy infrastructure that powers our Nation. The electric grid is too critical to our existence for it to fail. We must get it right each time, every time, all the time.

Thank you for your leadership, and I look forward to your questions.

[The prepared statement of Mr. Lindahl follows:]

******** COMMITTEE INSERT ********

Mr. Latta. And thank you very much for your opening statement today.

Mr. Krejsa, you are recognized for 5 minutes for an opening statement.

STATEMENT OF HARRY KREJSA

Mr. Krejsa. Thank you, Chairman Latta and Ranking Member Castor, and members of the committee, for the opportunity to testify today. My name is Harry Krejsa, and I am the director of studies at the Carnegie Mellon Institute for Strategy and Technology.

My work focuses on U.S.-China competition and the national security implications of emerging technologies. I previously worked in both the Trump administration, at the Pentagon working on military doctrine for offensive cyber operations, and in the Biden administration at the White House, helping lead the development of the national cyber strategy.

In both of these roles I was confronted with wide-ranging efforts by the People's Republic of China to hold our critical infrastructure at risk. Beijing is preparing for conflict over Taiwan, potentially in the very near term.

Its theory of victory depends on preventing the United States from mounting a successful rescue mission in response. Both public and private sector cyber threat intelligence analysts have concluded that their strategy threat likely has two parts: first, to disrupt defense infrastructure to slow our ability to mobilize personnel and equipment; and second, to target civilian infrastructure, to sow panic and chaos among the panic at large.

Our aging infrastructure makes these threats easier, including in our energy ecosystem. Today's electricity grid is too often a hodgepodge of digital tools sitting atop an analog foundation, creating seams where adversaries can slip in.

Many cybersecurity specialists used to argue that the best way to handle this kind of challenge was to separate operational technologies from modern networks. In practice, we now know that is nearly impossible.

Digitization has swept our world so thoroughly that even national security networks that are believed to be air-gapped often are found to have accidental and unknown internet connections during regulatory security sweeps and efforts to ensure their ongoing defensibility from adversaries abroad.

The only way around this challenge will be through it, embracing modernization from top to bottom, as you have heard from many of the witnesses here today, to achieve that defense-in-depth that we need for our grid security and defensibility.

America's AI build-out, reindustrialization, and broader electrification are, in fact, already demonstrating the benefits of such an approach. The energy technologies powering this transition, from onsite generation and battery storage, to smart inverters and virtual power plants, were designed from the ground up with software at their core, enabling modern cybersecurity features and the ability to update and evolve in response to emerging threats.

They are also enabling a smarter, more distributed grid architecture, one that is more defensible, resilient, and even self-healing, capable of quarantining disruptions and preventing cascading blackouts.

These modern technologies are also opening a new frontier in energy security. Nuclear power, geothermal wells, and inverter-based resources, and battery storage, require little to no refueling, making them defensible against fuel disruptions, but also insulating homes and businesses from swings in commodity prices.

This transformation would be a valuable asset in any Indo-Pacific crisis as well. Our allies and partners in the region, upon whom our forward-deployed forces rely for electricity

and other infrastructure needs, are heavily dependent on maritime fuel shipments for their electricity.

Modern, digitally native energy systems can not only be more defensible against cyber attacks, but they can also be more defensible against the naval risks that fuel tankers will likely face in any such conflict.

But, of course, there is a catch. Even as we modernize, too many components that make these systems possible -- power electronics, precision magnets, batteries, and other building blocks, that some refer to in aggregate as electrotech -- are made in China.

Beijing's dominance of the very technologies that could make our grid more secure and resilient, and that are defining the future of innovation around the world as we speak, is a strategic and competitive threat.

We should treat these modern energy technologies the way we now treat semiconductors, as critical industries requiring greater visibility, investment, and control, by the United States and our allies.

I urge Congress to support more streamlined coordination between energy and national security stakeholders. Procurement frameworks that reward secure-by-design systems and sustain R&D in breakthrough technologies.

I also urge you to build on the manufacturing reshoring progress begun by the energy tax credits in the Inflation Reduction Act, and retained in the One Big Beautiful Bill Act. Doing so will ensure we have an energy system that is both more competitive and secure.

If we do it right, if we do the kinds of efforts described by my distinguished co-witnesses here today, we could pour a new foundation for our electrical grid that delivers on the energy expansion that we are working through today and guarantee American security and industrial leadership for the next 50 years.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Krejsa follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much for your testimony today, and Mr. Tudor, you are recognized for 5 minutes for your opening statement.

STATEMENT OF ZACH TUDOR

Mr. Tudor. Chairman Latta, Ranking Member Castor, and members of the committee, thank you for the opportunity to testify. I am Zach Tudor, associate laboratory director for national homeland security at Idaho National Laboratory, where I lead nearly 900 experts protecting U.S. critical infrastructure, including the power grid, from cyber and physical threats.

As has been mentioned more than once, America faces unprecedented cyber threats to our critical infrastructure. The 2025 Annual Threat Assessment of the intelligence community confirms adversarial states are prepositioning in U.S. networks to disrupt critical services at a time of their choosing.

China is the most persistent threat. Through Volt Typhoon, Salt Typhoon, Flax Typhoon, the Chinese Communist Party has embedded itself in our energy and communications and water systems to set conditions for destructive attacks during a Pacific conflict over Taiwan.

They are winning without fighting, attempting to undermine our infrastructure, and will to respond.

Russia continues aggressive operations despite constraints from the war in Ukraine. From 2015's BlackEnergy attacks on Ukraine's grid and to the 2021 Colonial Pipeline ransomware, Russian-affiliated actors have proven they can disrupt energy systems at will.

Recently Russian hackers targeted water systems in Norway and Poland and caused a

Texas water-treatment tank to overflow.

Iran has targeted our water, energy, and manufacturing sectors, forcing a Pennsylvania water utility to shut down portions of its system in 2023.

North Korea uses cybercrime to fund its regime, stealing over $1.3 billion in 2024, but has proven critical infrastructure capabilities through ransomware attacks that have disrupted hospitals, manufacturers, and energy companies worldwide.

The United States faces significant risk as our adversaries exploit fundamental vulnerabilities. Our infrastructure systems are interconnected. Disruption in one sector cascades across others.

We operate vast, digitized, privately owned infrastructure that is aging and underresourced against evolving cyber threats.

The electric grid is indispensable and a prime target. Russia and China are advancing capabilities to disable good segments during a crisis. China's Volt Typhoon has infiltrated U.S. utility networks with intent for long-term disruption.

Oil and gas infrastructure remains vulnerable. Colonial Pipeline showed how a ransomware intrusion in an IT network can trigger fuel shortages and panic-buying nationwide.

Iranian and Russian groups continue probing pipeline control systems.

Telecommunication networks are critical infrastructure's nervous system. China has embedded hardware vulnerability in routers and switches. In September, the Secret Service dismantled devices in New York, capable of disabling cell towers and the critical infrastructure dependent on real-time communication.

Water systems are particularly underresourced. EPA warns that over 70 percent of U.S. water systems fail basic, cybersecurity best practices. Many lack full-time cyber personnel or continuous monitoring, making water infrastructure vulnerable and high

stakes.

Addressing these threats requires specialized capabilities that the Department of Energy's National Laboratories can and have provided for many years. DOE operates 17 National Laboratories to advance national, economic, and energy security, while supporting other Federal agencies' security missions.

INL has defended critical infrastructure for over two decades. Our 890-square-mile site provides unique capabilities to test threats and solutions at scale. We lead national control system security efforts through programs, including cyber-informed engineering, that integrates cybersecurity into the design of infrastructure.

Our consequence-driven, cyber-informed engineering program strengthens system resilience through hands-on assessments. And the cyber testing for resilient industrial control systems, or CyTRICS, our program, is supported by six National Laboratories, to test energy-sector, supply chain components in coordination with the private sector.

Additionally, INL's test ranges offer unmatched infrastructure testing capabilities. We operate a utility-scale electric grid test bed and wireless communications test range.

We maintain over 150,000 square feet of control system lab space to safely test cyber and physical threats at full scale.

We work alongside DOE, DHS, and the Department of War, to support testing, training, and large-scale exercises.

Our new special activities office was established to bring coordinated focus across the lab complex and with our partners towards this critical mission.

In summary, America's adversaries are not waiting. They are already embedded in our systems. The threat is no longer hypothetical. It is a daily reality.

Congress must act decisively. We need to accelerate public-private partnerships to secure infrastructure. We should extend and expand the State and Local Cybersecurity

Grant Program. Passage of the PILLAR Act was a positive step.

We should expand National Laboratory investments to advance operational technology security.

At INL, we are concerned more than ever before, we face a defining test of resilience in national security. If we act decisively, we can safeguard the systems that power America's economy and protect our way of life.

Thank you and I look forward to your questions.

[The prepared statement of Mr. Tudor follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much for your testimony, and that will conclude our opening statements from our witnesses, and we will move into the question-and-answer portion of the hearing.

And it is very sobering what you have all been bringing before the committee, and with that, I am going to recognize myself for 5 minutes for questions.

If I could start, Mr. Ball, with you, you made some interesting statements, especially when you talk about the recommendations for Congress. And you talk about -- on the threat that is out there. You talk about the support for CRISP.

For northern Ohio, when I look at our utilities, you know, the question is, are we getting the information we need out there at our utilities, are the utilities getting information from Federal Government on existing threats that are occurring, or what is happening right now?

Mr. Ball. So it is a very good question. I would always err on the side that it is never enough. I would start with that. But I think what we are focused on is building a strong ecosystem of information sharing, and that part is built on relationships and is something that is built into, whether it be from an E-ISAC perspective, the members that we engage with that actually are recipients of all of the information that we push out. We serve as a conduit for that.

Programs like CRISP actually are programs that are -- you know, start out with a member-funded program, where they actually participate, and that information that goes from that actually is also shared with our government partners and the Department of Energy and the National Lab framework.

And what is important about that is, it starts to bring together our government and our industry.

I think also references to the ETAC is another great example of being able to provide information sharing. I think that I would -- I can't foot-stomp that enough, is bringing the awareness that our government partners have around threats. But the contextual understanding of what those threats represent to the industry become a really important part of that dialogue.

That is happening, but we need more of that. So I think anything that we can do to encourage engagement, information sharing, will actually help us drive towards a greater and more resilient grid, and certainly from a national security perspective, make us much more secure and resilient.

Mr. Latta. Well, thank you.

Ms. Artz, we have heard about the Communist Party and what they are doing out in the United States and to what their threats are.

You mentioned a defense-in-depth, because we got to protect ourselves, and so would you want to explain a little bit on what we should be doing on the defense-in-depth, because if already infiltrated, how are we going to protect ourselves?

Ms. Artz. Excellent question. Thank you for it. We take a multilayered approach to securing our systems. First, we are, as an industry, subject to mandatory cybersecurity regulations. Those are a part of the security controls that we implement, but we also really heavily rely on those partnerships that I described in my testimony and opening statement, so that we can ingest the intelligence our government partners have at the Federal level.

We also work very closely with our State and local partners as well to understand threats in those local areas, so that we can proactively implement security controls that will address those trends that we are seeing from these advanced, persistent threats.

Finally, a really critical component of defense-in-depth is being prepared. Mr. Ball

mentioned the GridEx exercise, but we also participate in exercises held by the Department of Energy, with our military partners, at the State and local level, so that we can respond to and recover from, very quickly, the incidents when they do occur.

Mr. Latta. Well, thank you.

Mr. Lindahl, I probably have more electric co-ops in my district than any other congressional district in Ohio. And when I go out and meet with them all the time, you know, I see what they have been investing, just to make sure on the cyber side, that they are protecting, not only, you know, their system but also all of their consumers out there, that they want to make sure that their power is always on.

The question, you know, do they have enough -- the information? Do they have, you know, the time, the money? What is happening out there? Unfortunately, I got about 44 seconds left.

Mr. Lindahl. We can always use more resources. As co-operatives, every dollar we spend is a dollar that goes into our rates and our members end up paying. So every resource we need, if we can partner and pool together our resources with the Federal Government, with State governments, with our other utility partners, with other co-operatives, we can help solve this problem without significant cost to the individual members.

There is always a need to evolve, and to have the tools we need, you know, we can't do this alone. We have got to do it together.

Mr. Latta. Well, thank you, and with my just remaining about 5 seconds, I have additional questions I will submit for you all, because these are really important questions that we have got to get resolved and make sure we protect the grid.

And with that, I yield back and recognize the gentleman from California, 50th District, for 5 minutes for questions.

Mr. Peters. Thank you, Chair Latta, for holding this important hearing. You know, I just want to say that what you have told us is very alarming, and I really appreciate you taking the time to come down here and tell us that.

And I would say to the chairman that American people will note someday that we have been warned today about this. They will have expected us to work on this, and I hope that we make this a priority in this committee.

Also just say parenthetically that I saw the -- you know, don't pay attention to this, but the congressional schedule this year again came out. I believe it has us on the plane more days than it has us in D.C.

I think that that really inhibits the ability of all committees, but including this committee, to work on important issues like this. And I was sorry to see again, despite our protests that we could do better, that the committee schedule itself will inhibit us from having enough meeting days to deal with important issues like this.

That is above our heads, but we see it again and again, and it is a frustration for me and I know for a lot of Members.

I do want to talk about one physical threat to the grid that is of particular interest to me and in San Diego, where catastrophic wildfire is the biggest physical threat to both our energy grid and energy affordability in California.

Wildfire-related costs, including proactive investments in post-disaster recovery, now represent 40 percent of Californians' utility rate increases -- 40 percent -- is wildfires. So it is clear we need to do a lot more in that bucket in terms of upfront mitigation.

The utility in my area, San Diego Gas & Electric, they are headquartered in my district. They have really done a, I think, commendable job. They have invested nearly $6 billion in wildfire preparedness, and they are innovators in wildfire mitigation and grid safety.

They have monitoring technologies to detect fire risk and respond to buried transmission lines underground to minimize the risk of ignition, and conduct extensive vegetation management to protect power lines from hazardous trees.

But this kind of investment is rare, as it is expensive, and a lot of our power grid is vulnerable to falling trees, catastrophic wildfire, and other threats. So there is a lot more that the Federal Government, that we, here, could do to improve coordination and information sharing between Federal agencies and State partners which would unlock the full potential of wildfire mitigation investments.

The Fix Our Forests Act, or FOFA, which we hope will pass the Senate this Congress, takes strong steps to address this. The House version of the bill called it the Fire Shed Center. The Senate version calls it the Wildfire Intelligence Center. But the goal is the same.

It is a one-stop shop for wildfire intelligence coordination and response. It would be empowered to work with States, utilities, and communities to mitigate fire risks.

Consolidating real-time information on wildfires and wildfire risk through this Federal hub will improve preparedness, real-time decisionmaking, and wildfire response, especially for utility infrastructure in fire-prone areas.

Now, Ms. Artz, Xcel Energy has a robust wildfire mitigation plan. Obviously, you work closely with many others to maintain the physical security of the grid.

Can you talk about the threat that catastrophic wildfire poses to the grid and how increased communication and coordination among Federal Government, utilities, and States could be helpful to mitigate those threats?

Ms. Artz. Thank you for the question, Congressman. We took a comprehensive approach to wildfire mitigation risk -- to all risks, physical hazards, that we face. We operate in eight States, and like in California, we have seen increased catastrophic wildfires

825 across all of our service territory.

826 Our wildfire-mitigation planning is comprehensive. It includes advanced
827 technologies. It includes improved operations and maintenance activity, all designed to
828 mitigate that wildfire risk.

829 Importantly because of this threat, the Electricity Subsector Coordinating Council has
830 a wildlife mitigation task force that is working very closely with our government partners in
831 the U.S. Forest Service, with Department of Energy, with the Bureau of Land Management,
832 to improve upon the consistency of the permits that are needed to conduct vegetation
833 management and other wildfire mitigation risks, to improve the information sharing and the
834 resource allocation to those coordinated efforts.

835 The last thing that I will say about that effort is -- and Mr. Lindahl and I were talking
836 prior to the hearing -- the benefit of this industry is the amount of information sharing we
837 do with each other, to expand understanding and best practices, so that we are all working
838 collectively to mitigate these risks. So thank you for the question.

839 Mr. Peters. Mr. Ball, quickly, I know E-ISAC works with industry to respond to
840 wildfire threats. How can Congress help that effort better? In 20 seconds.

841 Mr. Ball. Yes. So from the E-ISAC perspective, the wildfire threats aren't
842 specifically within the domain. However, as Ms. Artz references, the Electricity Subsector
843 Coordinating Council is very focused on this issue.

844 And in speaking from the NERC side of the House, you know, FERC has asked NERC to
845 conduct a study. They are in the process of bringing together stakeholders to produce a
846 report in May next year.

847 Mr. Peters. Thanks. We will look for that, and I yield back.

848 Mr. Latta. The gentleman's time is expired and yields back. The chair now
849 recognizes the gentleman from Kentucky, the chairman of the full committee, for 5 minutes

for questions.

The Chair. Thank you. I want to ask the gentleman from Kentucky a question here, Mr. Lindahl. Thank you for being here, and I appreciate you making the trip up.

So electric cooperatives serve over 42 million Americans across the country, including many service territories that are seeing significant energy demand due to AI data centers, and all that's in our area.

Very interested in AI data centers with the Ohio River, the water, and access to electricity that we have in Kentucky, and Kenergy is very particularly part of the middle that. And you have the large industrial loads, like in Hancock County and other places, and they are important economic drivers to our west Kentucky communities.

In the era of skyrocketing demand growth, can you discuss ways in which cooperatives like Kenergy are creatively addressing cyber threats to the system?

Mr. Lindahl. Yeah. One of the concerns we have, as we run the grid closer and closer to the edge, is, it becomes more and more critical to not have interruptions. Before, you know, we could have a small event, and it wouldn't have an impact, you know, on the reliability of the grid.

But as we push the grid to the limit, with new load -- data center load, or any kind of load, it just puts a microscope on any hiccup in the system that could happen.

So things we are doing, you know, we do a layered approach as well, and, you know, we are an all-of-the-above cooperative. You know, we like to diversify our resources, diversify how we serve things, diversify even the economics around how we serve things. So that is one way we get around it.

How we -- insight into our grid, so we can manage our grid much more officially and effectively by better management. So part of the reason we have invested in our fiber is to be able to have insight down within our distribution system, and we can leverage new tools

and new innovations to help thwart physical and cyber attacks that might come and help keep the lights on.

The Chair. So you mentioned getting close to the level of our grid can support, and my county has -- well, a municipal utility, but I have a family business that has a co-op one rule, and the power comes from TVA.

You know, TVA took out a coal plant, and 3 years ago during the polar vortex, we had blackouts in Kentucky, believe it or not. We are an energy-rich State. We had blackouts because of decisions to take out power.

And so I know that we have increasing demand for power and an incredible increased demand for these AI data centers, but just increased demand anyway because we are growing again and industrializing again, and taking energy offline.

And I know that has got to be a concern that -- I think Big Rivers is where you got some of the demands that they are having to look at maybe taking power offline because some of the requirements that have come down from Washington.

Is there any comment on that?

Mr. Lindahl. Yeah. You know, we are an all-of-the-above. We need to keep the resources we have, and then we also need to develop, you know, new resources and new ways to bring electricity in so that we can keep the grid alive, so -- and then we need fuel security. You know, a lot of our plants rely on, you know, natural gas, for instance. So we are indefinitely tied to the cybersecurity of the natural gas industry.

We roll our trucks with diesel fuel. We are heavily, you know, reliant on that network working. So cyber can have a cascading effect on a utility even if it doesn't directly impact us.

But we want the all-of-the-above.

RPTR HNATT

EDTR ROSEN

[11:34 a.m.]

The Chair. Thank you. I agree with you on all of the above. I am an all-of-the-above person as well. Thank you for that.

So Mr. Tudor, we recently witnessed the first documented AI large scale cyber attack using AI agents with minimal human intervention. AI innovation will create tools to protect critical infrastructure, but bad actors can use them, as we saw with China and Russia, or could see with China and Russia.

How might AI widen the attack landscape on our critical infrastructure, and how is INL working to foster innovation in AI development to address these risks? So what is the risk of AI, and what are you doing to counter with AI?

Mr. Tudor. Thank you for that question, Congressman. And, yeah, the risk of this really pervasive new tool hasn't been lost on us. And I will say that AI in its various forms has been used in critical infrastructure, you know, defense and operations for quite a long time. The onset of generative AI has really caught all of us as we go forward. But this new tool does, you know, allow adversaries to, you know, leverage the existing manpower they have, and China among those adversaries has a lot of manpower. It can also enable the defenders.

At the Idaho National Lab, and with other partners, such as Oak Ridge, Pacific Northwest, we have developed something that we call TAIGR, the testbed for AI grid resilience. I mentioned all of the infrastructure that we have. So understanding what adversaries can actually do with AI and how we can defend it is very important.

We are also building on our cyber testing for resilience and control systems program to make sure that we understand what it means when a control system, a vendor-provided

system has AI in it, and what critical vulnerabilities might be included in that and how we can mitigate them.

So we at INL are doing a lot, and so are the other national labs working with CESER and DOE and others.

The Chair. Well, thank you. Thank you for that.

Mr. Ball and Ms. Artz, we discussed at length in committee this Congress about how demand growth of electricity presents new risk to be managed by everyone.

So how is the industry approaching risk posed by an attack that causes the sudden loss of demand, such as from data centers, and what is -- what will that -- so you are looking at the overall grid stability and risk of this, how are you all -- how are you guys mitigating risk? I will start with Mr. Ball, and then Ms. Artz.

Mr. Ball. Okay. Well, thank you for the question. And, in fact, it is a pretty significant --

The Chair. I am sorry. I just noticed I am already negative on time. Maybe can we get the answer.

Mr. Latta. Go ahead and finish up quickly.

Mr. Ball. Okay. Just to say that, you know, we take that threat very seriously. In many ways, we have to explore the impacts of scenarios like that, and that is why we really focus on the ability to read and react to events in various scenarios, so very important topic.

Mr. Latta. Well, thank you. The gentleman yields back. And the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee, for 5 minutes for questions.

Mr. Pallone. Thank you, Chairman Latta. We often hear about the importance of a diversified grid and of not discriminating against any single resource type. Unfortunately, that is not the approach we have seen from the Trump administration and from

congressional Republicans, and I think that leaves us with real risk.

My question initially of Mr. Krejsa, I was struck by your written testimony, which said it was crucial that the United States not fall behind China in next generation technologies, like batteries, smart inverters for resources like wind and solar and virtual power plants. But could you talk about that importance, and do efforts to shut down the research and deployment of wind and solar technologies, for example, help or hurt the security of our energy system, if you will?

Mr. Krejsa. Absolutely, Congressman. The basket of technologies that many are beginning to refer to as electro-tech, or electro-industrial equipment, are increasingly forming the foundation of our economy today, and are going to infuse every part of it tomorrow.

Technologies that generate and store electricity that manipulate and move it that range from batteries, to advanced computes, to advanced sensors, autonomous vehicles, these are the technologies that are going to define the pace of industrial competition in the future. And they are critical not only to our electrical grid, but for many sources of innovation that we see on the horizon.

And it is, indeed, very troubling that the People's Republic of China has quite the head start on manufacturing many of these technologies, but the simple reason for that is that PRC had a head start on manufacturing smart phones and computers. Many of these key pieces of electro-tech machinery are downstream of those initial industrial investments. And so the bad news is we are quite behind now on a variety of critical strategic technologies, but the good news is that if we can make progress in some of them, we will have -- we will enjoy spillover benefits in other competitive areas because the truth is that a smart phone, a robotaxi, or a fusion reactor, all very different technologies, but are fundamentally made up of many of the same components.

Mr. Pallone. Thank you. I want to turn to Mr. Ball. I wanted to turn to the network of organizations that help keep our energy system secure, including the Electricity Information Sharing Analysis Center, the Electricity Subsector Coordinating Council, many of these entities are focused primarily on the utilities that handle the transmission and distribution of the electricity, and that is important. But in many parts of the country, including New Jersey, the actual generation of power is handled by different companies, separate from the utilities, but those companies are just as much an integral part of the power sector as any load-serving utility that owns wires or sells power to consumers.

So Mr. Ball, could you talk about the efforts by NERC, or that NERC has made to include independent power producers in the Electricity Information Sharing Analysis Center, and how can we ensure that those entities are getting the support they need to keep the system secure and online? About a minute because I want one more question to go.

Mr. Ball. So just to try to answer that very good question, one of the things we look at at the information-sharing fabric that we work with, it is a neuro network of resources. I talked about different ISACs, I talked about our membership. You know, one of the things we don't, from the E-ISAC perspective, all of entities have the ability to participate with the ISAC. In fact, we work with a lot of entities even within our NRECA who are, in fact, distribution organizations, and we channel information through to them as well. So we are not bound by necessarily those areas.

But I think we can always do better. And it is certainly an area that we are continuing to see growth, and not only in terms of engagement information sharing, but actually engagement. In the last GridEx exercise, we saw a 70 percent growth in small utilities participating, and that represents a lot of distribution as well. So I think we are seeing progress, sir. More to do.

Mr. Pallone. All right. Thank you. Let me just reiterate what I said in my

opening statement, which is that the Department of Energy plays a vital role in cybersecurity. Its expertise must be represented in any governmental conversations about the cybersecurity of the energy industry.

And I can just go down the line and ask if everyone here agrees. Quickly. Ms. Artz.

Ms. Artz. Yes, we heavily rely on the Department of Energy's expertise to enhance our national security efforts.

Mr. Pallone. Mr. Ball, quickly.

Mr. Ball. The answer is yes, and we are heavily engaged with them.

Mr. Pallone. Mr. Krejsa.

Mr. Krejsa. Yes.

Mr. Pallone. Mr. Lindahl.

Mr. Lindahl. Yes.

Mr. Pallone. And Mr. Tudor.

Mr. Tudor. Absolutely.

Mr. Pallone. All right. Thank you. And thank you, Mr. Chairman.

Mr. Latta. Thank you very much. The gentleman yields back. And the chair now recognizes the gentleman from Alabama's 6th District for 5 minutes for questions.

Mr. Palmer. Thank you. I am going to talk a little bit about the energy policies of the past administration and the emphasis on green and reliable and affordable, which I was just looking at some of the increases in energy costs just from 2021 to 2024, 2025 is up 34 percent. And I think a lot of it has to do with what NERC reported as the number one threat to the grid, the change in the fuel mix.

What doesn't often get reported is how much it is costing residential consumers, and that percentage that I quoted, 34 percent increase, is in residential energy costs. So it has

created an enormous problem for a lot of families around the country because of the investments that are made. And I am like Chairman Guthrie, I am, and the rest of my colleagues, I am for all of the above. But there is a hard truth that needs to be acknowledged that this transition is extremely expensive and it gets passed onto the consumers.

What we saw in Europe should be instructive to us. The economist magazine, nobody's idea of a right-wing publication, reported that in the winter of 2023, about 68,000 excess winter deaths. This was not people freezing to death. This was people who simply could not afford to adequately heat their homes. It is particularly problematic for people with respiratory illnesses, cardiovascular illnesses, but 68,000 excess winter deaths. That is more than died from COVID.

So when you take a look at these investments, and particularly in areas of the country where they have shut down so much hydrocarbon power generation, it has created, I think, a hazardous environment for a lot of people who simply can't afford to adequately heat their homes.

It has also, in my opinion, and I think the opinion of many, created an economic security issue, and a national security issue. We are in an arm's race for artificial intelligence with China. We are going to have to build massive data centers that cannot be powered with renewables, because they are -- it is intermittent power. You have to have a consistently high baseload to meet the demands of the data centers for us to be competitive.

When I talk about this arm's race in artificial intelligence and quantum computing, whoever wins that is not going to be a superpower. They will be the superpower. If you want to talk about power. Okay.

So just, Mr. Ball, in your experience at NERC, would you care to comment on this?

Mr. Ball. What I can say is, that is a, you know, it is a very big concern about the growth and the demand and trying to -- and balance out outcomes with that. I cannot speak expertly on that. However, I am always happy to come back with additional feedback. But I can tell you that NERC is very engaged.

Mr. Palmer. One of the things that I think we have got to address is supply-chain issues. We are not going to be able to build out renewable power until we -- as long as we are dependent on China for refined rare earth elements and critical minerals. That is a huge issue for us right now is securing our own supply chain domestically and collaboratively with allies in the Western Hemisphere. But it is also critical for us to build these data centers. It is one of the things that drives up cost is supply-chain issues.

Would you be interested in commenting on that, Mr. Lindahl?

Mr. Lindahl. Supply chain is a huge concern. You know, our system is built on three legs. When we make decisions on resource generation, resource delivery, we balance affordability, reliability and safety. So every decision we make has to balance between those three. And in some cases, renewables work, in some cases they don't, in some cases -- and that is why we say all of the above because, you know, we look at it all independently every single time. And you can't play economic affordability against reliability, or reliability against affordability.

Mr. Palmer. Well, since you brought up affordability, I want to touch on that very briefly. My colleagues across the aisle keep talking about that, but they created this problem with the legislation that they passed. And when you combine that with the supply-chain issues, we not only have an affordability crisis that is really hurting American families, I contend sincerely that this is an economic crisis and a national security crisis. Mr. Chairman, thank you for the opportunity. I yield back.

Mr. Latta. The gentleman yields back. The chair now recognizes the gentlelady

from Florida, the ranking member of the subcommittee, for 5 minutes for questions.

Ms. Castor. Well, thank you, Mr. Chairman. Mr. Krejsa, in your testimony you talk about virtual power plants as a linchpin technology that could be easier to secure against cybersecurity threats. Let's start with the basics, what is a virtual power plant?

Mr. Krejsa. Thank you, Congresswoman. A virtual power plant is essentially a network of small energy assets that have been stitched together by sophisticated software to function as though it is a single large dispatchable asset that the grid can turn up or down. Think of it in terms of home batteries, smart thermostats, even flexible industrial loads that can be aggregated together to function as though it were a dispatchable power plant.

Ms. Castor. That is a little bit different than the old-time power production that was like a single power plant with distributed systems. How was this technology developed?

Mr. Krejsa. Yes, ma'am. It is a benefit of a digitally native approach to a grid architecture which provides both flexibility, but also security and resilience benefits.

For a robust grid architecture, you probably want a combination of both centralized baseload resources, and flexible grid forming distributed resources that can be orchestrated with sophistication so they can play to each other's strengths and hedge against different kinds of risks.

Ms. Castor. And then how can VPPs help with grid security?

Mr. Krejsa. Absolutely. VPPs can provide an instantaneous and flexible response to forms of disruption. They enable models, like we call them graceful fail overs, into islanding and micro grids when certain parts of the grid gets disrupted. With this network of sensors and smaller energy assets, you have more flexibility to flow electricity to where it is needed and to quarantine disruptions from becoming cascading blackouts.

Ms. Castor. And is the U.S. leading in this technology, or are there other countries

that are in the lead on this?

Mr. Krejsa. It is early days. And I think that, like in many advanced modern electricity generation storage and orchestration technologies, we are in a race with China to define what right looks like and to develop secure supply chains, both in the software and hardware side.

Ms. Castor. Is there anything that the Congress can do on the regulatory side, or through legislation to support and assist with the deployment of VPPs?

Mr. Krejsa. Yes, ma'am. I believe that supply-chain security considerations, whether we are writing them into hardware sourcing or procurement guidelines should take into consideration the systemic impact of certain components of our electricity grid and --

Ms. Castor. All right. Get specific when you are talking about supply chains. What should this committee focus on on supply chains to bolster VPP technology and cybersecurity at the same time?

Mr. Krejsa. Absolutely. I think when writing foreign entity of concern legislation, or regulatory guidance, it should incorporate prioritization about what kinds of technologies have the most systemic impact, most high consequence. So virtual power plants are systemically influential and highly -- can have high consequence. The contrast would be to commodity equipment like a vanilla foldable TAIC, which is low consequence. So you would want to focus your efforts toward the systemically influential side rather than commodity less consequence side.

Ms. Castor. Ms. Artz, how does Xcel manage sourcing and procurement for some of these more cybersecurity sensitive components?

Ms. Artz. Thank you for the question. So Xcel Energy is a regulated entity, it has to adhere to the NERC's critical infrastructure protection regulations that require us to manage our supply-chain risk. We have a very robust process that we utilize that includes

assessing during the RFP process equipment manufactured in those countries of concern.

Importantly, we continue to urge our government partners to share specific intelligence information on manufacturers and/or specific components that we should be targeting in our assessment.

Finally, we are looking at remediating risk through removing equipment that is legacy in nature that might have been deployed prior to our understanding of some of these threats.

The last thing I will say, because I want to emphasize what Mr. Tudor shared about the CyTRICS program, the Department of Energy does, Idaho National Lab, where they are going in and looking at vulnerabilities in equipment, hardware, software, but importantly providing risk mitigations that industry can implement in the utilization of these technologies.

Ms. Castor. Thank you very much. I yield back.

Mr. Weber. [Presiding.] The gentlelady yields back. The Chair now recognizes the gentlelady from Tennessee for at least 5 minutes.

Mrs. Harshbarger. At least 5 minutes. Thank you, Mr. Chairman. And thank you to the witnesses for being here today.

Mr. Tudor, I will start with you. As you highlighted, our grid is the linchpin for multiple other dependent and interdependent sectors, including natural gas and communications. A physical or cyber incident impacting one of these interdependent sectors can have downstream impacts on the grid system, and, I guess, my question, because I represent east Tennessee, we have ORNL right down, you know, at Oak Ridge. Of course, we have TVA. How are you identifying and collaborating with interdependent sectors to further harden the electricity sector?

Mr. Tudor. Thank you for that question. Very good question. So number one,

yes, working with our partners like Oak Ridge National Lab and some of the utilities that are government-operated gives us access to a lot of information that we can use for our research.

But, also, you know, as I was taking notes, all of the different sector councils, the Electric Sect Coordinating Council, NERC, ETAC program, CRISP, these are all ways to get information.

You know, one thing I did want to point back to you is that, you know, we talk about information-sharing, I would say that every 4, and sometimes every 2 years there is an executive order that talks about critical infrastructure security, and information sharing is always one of the top three things and you would think that we had gotten -- well, I think we have gotten better at it, but not so much that Presidents would have to keep talking about it.

So information sharing, actual intelligence, context, all of these things are important. The national labs work with utilities organizations and others to try and get that context and that actual intelligence, but also use that to do research for mitigations for current threats, and hopefully mitigate upcoming threats.

So I guess what I want to say is partnership amongst all of us is key, working with CESER, the Office of Electricity, the Grid Deployment Office, our other agencies, you know, keeps us kind of at the forefront, and relationships really do matter.

Mrs. Harshbarger. Yeah, they certainly do. Thank you, sir.

Mr. Ball, I appreciate you highlighting the significance of GridEx and the Vendor Affiliate Program to strengthen the grid resilience. Do you happen to know if either program has ever been used to plan or protect against EMP attack on the grid?

Mr. Ball. So with regards to GridEx, in terms of the exercise, I am not aware of a specific scenario with that with regards to that particular exercise.

Mrs. Harshbarger. Well, if you haven't done it, what would be required to incorporate EMP scenarios in the future GridEx exercises?

Mr. Ball. Well, I would say, and certainly GridEx isn't the only mechanism by which we would do that, but I think by understanding the nature of the kinetic impacts of EMP to systems. Obviously there has been tremendous analysis done on that, EPRI has done a great body of work in partnership with industry on those, and really leveraging those, the understanding that has been developed out of that analysis, to apply those scenarios, and then explore the consequences of that, and then mitigation. So I believe that is a mechanism by which --

Mrs. Harshbarger. I always ask when I go visit TVA, What are you doing to EMP proof that, and even the nuclear facilities and things they are doing? They have new techniques and new things that they are doing to do that.

And I guess this question will be for Mr. Lindahl and Mr. Ball and Ms. Artz, the Federal Government relies on the private sector to provide not only mandatory, but also voluntary reporting of suspicious activity and minor incidents to improve overall analysis.

Additionally, the government depends upon industry through sector-based information sharing and analysis centers to identify threats, tactics, and provide material support for law-enforcement investigations. For its part in the private sector, it relies on the Federal Government's intelligence to sector -- to properly secure their assets from attack.

So from your perspective, what are the intelligence gaps in the public and private sector? And, Mr. Ball, we will start with you.

Mr. Ball. So I am sure there are gaps that we can focus on. However, I would say that there is actually a lot of dialogue occurring today. We referenced programs that identify mitigations, like for CyTRICS, for example, are conduits of information-gathering

that start to be able to be shared with our industry, and actually be able to deploy techniques to help mitigate the risks on that.

The other thing I think is really important is to recognize that, you know, our vendor community is a fundamental part of that ecosystem of information regarding threats. We find that industry, that suppliers that provide industry technologies oftentimes become aware of a vulnerability, or something is produced, we want to make sure that we are collecting that information, whether it is through government sources or not, but we want to be able to aggregate that, collate that, and get that out in actionable ways. That is an objective.

Mrs. Harshbarger. I am out of time, so you two will not get to answer my question, but you can give it to me in writing. Okay. Thank you all. I yield back.

Mr. Weber. The gentlelady yields back. The chair will recognize the gentleman, Mr. Menendez, for 5 minutes.

Mr. Menendez. Thank you, Chairman. To all of the panelists, are you familiar with President Trump's March 19th executive order titled, "Achieving Efficiency Through State and Local Preparedness"? Just a show of hands.

Mr. Menendez. Most of you aren't. Okay. I will read section one to you. "Commonsense approach and investments by State and local governments across American infrastructure will enhance national security and create a more resilient nation. Federal policy must rightly recognize that preparedness is most effectively owned and managed by the State, local, and even individual levels, supported by a competent, accessible, and efficient Federal Government." I am sorry that this administration has failed on the competency part.

But I just want to highlight two things from an article titled, "Five Ways the Trump Administration is Increasing The Risk of Blackouts." It states that in October the

administration canceled more than $2 billion worth of funding allocated to communities to harden their energy infrastructure against extreme weather threats through the Grid Resilience and Innovation Partnership Program administrated by the U.S. Department of Energy's Grid Deployment Office. Are you familiar with that program?

These cancellations included 26 grants across 25 States, and another 19 grants may also be cancelled according to an internal DOE list shared by POLITICO.

In addition to the cuts for DOE projects, the administration ended a major FEMA program for disaster resilience called the Building Resilient Infrastructure and Communities Program. BRIC provided funding to communities to reduce the risk of climate disasters and other natural hazards from damaging public infrastructure, such as energy, water and wastewater infrastructure. The elimination of the program revoked more than $3.6 billion in funding that was allocated for community projects across the country, including projects to upgrade the grid. Are you familiar with BRIC?

[No audible response.]

Mr. Menendez. Okay. Mr. Lindahl, in response to a question by Chairman Latta, you said, quote, "you can always use more resources"; is that correct?

Mr. Lindahl. That is correct.

Mr. Menendez. Does anybody disagree with that?

[No audible response.]

Mr. Menendez. Okay. So I am going to have you answer yes or no. Are these over $5.6 billion in cuts by the Trump administration to these two vital programs helpful to States' municipalities and utilities, yes or no?

Mr. Ball. No.

Ms. Artz. The cuts or the funds?

Mr. Menendez. The cuts to the funds.

Ms. Artz. No.

Mr. Menendez. Yes.

Mr. Lindahl. Depends.

Mr. Menendez. Depends on? You said you needed more resources, correct?

Mr. Lindahl. We do.

Mr. Menendez. So $5.6 billion is a significant amount of resources.

Mr. Lindahl. It is a significant amount, but, you know, we are going to continue to innovate and run the grid whether --

Mr. Menendez. I know you will do what you need to do, but you need us to be good partners.

Mr. Lindahl. That is right.

Mr. Menendez. The executive order says support, and that includes financial resources, including $5.6 billion in grants, yes or no?

Mr. Krejsa. No.

Mr. Tudor. No.

Mr. Menendez. So it is difficult to sit here in this committee room and have this conversation when Republican colleagues are silent when $5.6 billion are being cut from these essential programs and literally undermining the President's own executive order of supporting all of you.

But it just doesn't stop there. The administration has also fired over 1,000 cybersecurity and infrastructure agency staff. Does that make our country safer and more able to respond to these increasing cybersecurity attacks, yes or no? We will go down the line again.

Mr. Ball. No.

Ms. Artz. No.

Mr. Lindahl. No.

Mr. Krejsa. No.

Mr. Tudor. No.

Mr. Menendez. Yeah. So you understand the challenge that we feel here on this side. Right. Because we can diagnose the problem ad nauseam, but we have colleagues who refuse to lift their voices when the Trump administration is cutting $5.6 billion in funds, when they are cutting CISA, which is largely a vendetta, according to Project 2025, about what they think CISA did in the 2016 election. Crazy.

They are also moving CISA staff to other agencies like ICE, which has no connectivity to what their work has been. So this administration is weakening our community, is weakening the work that you need to do, they are weakening our cybersecurity capabilities.

And the last thing I will say is, Mr. Krejsa, you talk about China's awareness of our grid vulnerabilities and modernizing our grid for increased AI adoption can and should take future cyber threats into consideration. Right. Like AI is becoming more of an issue both from an offensive capability of our adversaries and needs to be a defensive capability. We had our first AI hearing in this committee on February 5th. All that they have done is try to roll back AI State laws. There is no Federal framework. There is no Federal approach to cybersecurity to AI, and we are all weaker and more vulnerable because of it. I look forward to our colleagues across the aisle actually doing the work and stepping up for our communities. I yield back.

Mr. Weber. The gentleman yields back. The chair now recognizes the gentleman from Georgia for no more than 5 minutes.

Mr. Allen. I thank the Chair, and I thank Chair Latta for holding this important hearing, securing our energy infrastructure. I thank the witnesses for being here to testify.

Protecting our critical infrastructure, I think we all agree, is paramount to our national security, especially from attacks from our adversaries. Electrical grid must be secured so that we can protect it from evolving threats and ensure reliable power can be dispatched. As part of securing our grid, cybersecurity plays a critical role in grid resiliency.

I am fortunate that adjacent to my district is the Savannah River site located in South Carolina. Located at SRS is the Savannah River National Lab. Researchers from Idaho National Laboratory and Savannah River National Laboratory participated through the Southeastern Regional Center for Cybersecurity Collaboration lead by Auburn University, and Oak Ridge National Laboratory in a first-of-its-kind lab demonstration of some of the challenges faced by electric utility companies, and the hardware suppliers to these utilities. The utility provided a scenario to demonstrate resiliency in the face of a cyber attack on a substation. To successfully show resilience, test ridge at INL and SRNL were virtually connected to each other.

An attack was perpetrated on a substation emulated at SRNL with resilient control falling back to control system at INL. This scenario demonstrated the challenges faced by utilities, a possible mitigation of this particular threat, and overcoming the technical challenges of long-distance command and control for grid equipment.

Mr. Tudor, often commercial industry threats, the cyber -- treats the cyber threat as an IT issue when it really is a problem for OT systems. How can national labs be leveraged to use their trained cyber operators to enhance security operating technologies?

Mr. Tudor. Thank you for your question, Congressman Allen. I am very happy to answer that. We have been partnering successfully with Savannah River National Lab since they have kind of joined the family, as well as Oak Ridge and the Southeast Regional Center. That is one of the things as we talk about the kind of, you know, shift in philosophy towards more regional preparedness with government response, we think that the SERC3 is a great

model, along with things like the Texas Cyber Command, Cyber Florida and others. So the national labs, for a long time, have worked to help people understand the meaning of convergence in IT and OT through both workforce development, training programs, demonstrations, appearances at conferences, and talks like this.

I think that there is the constant tension between IT and OT as the operational technology is becoming more and more computerized, the vulnerabilities from IT systems become more apparent in our critical infrastructure. I think that we are helping to grow a next generation of engineers in places like Auburn, Georgia Tech, and others that are working with us, to help spread that cyber informed engineering, that built-in resilience in programs. And I will stop there. Thank you.

Mr. Allen. Thank you. Mr. Tudor, what is Idaho National Laboratory doing to train utilities to identify and address risks to operation technology systems?

Mr. Tudor. Yeah. Thank you for that. INL is one of the leaders in training critical infrastructure security, utilities, and others that we work with from university partners, utility partners. We have a large-scale training program that has been ongoing for the last 17 years, it is called the Red/Blue Training, but people from across the industry and around the world come to learn about the threats and vulnerabilities against critical infrastructure and how to go about mitigating them and growing their capabilities.

The workforce is a very big issue for us. We know that places like NRECA and others may be underresourced, and larger companies, larger organizations, things, once again, NERC, FERC, the Xcels of the Nation, help to develop some of the capabilities that can then be given to the rest of the industry so they don't have to spend that kind of research dollar.

Mr. Allen. Thank you. Mr. Lindahl, rural electrical co-operatives play a huge role in my district in Georgia. You mentioned in your testimony industrial control system rural

electric co-operative initiative that helps with cyber monitoring. We have got 25 seconds, can you share how this has been impactful on helping rural communities protect critical infrastructure and enhance their cyber defense capabilities?

Mr. Lindahl. Yeah, the more we understand about how our systems operate, and the more we can kind of put protections in place to control them, the better we can respond to incidents out in the system.

Mr. Allen. Good. Great. Perfect. Mr. Chairman, I am two seconds early, and I yield back.

Mr. Weber. The braggadocios gentleman yields back, and the chair now recognizes the gentlelady from Virginia for at least 5 minutes.

Ms. McClellan. Thank you, Mr. Chair. And I want to thank ranking member -- the chair and ranking member for holding this very important hearing. And while this is not a hearing on clean energy or data centers, representing Virginia, which is both the clean energy capital of the south, and the data center capital of the globe, I can't let Mr. Palmer's false claims that clean energy doesn't power and can't power data centers go unanswered. And I would invite the gentleman from Alabama, and as a matter of fact, the entire subcommittee, or the full committee, even, to come to Virginia, to come to Henrico County, Sandston, specifically, to tour the Meta data center, which I toured during one of our many recesses.

The Meta Henrico data center is supplied with 100 percent renewable energy from new sources, from new projects specifically built to support the data centers' operations that -- and new solar projects that add more than 500 megawatts of reliable energy to Virginia's grid. And that is because the data center's campus itself was designed to be energy efficient, and they focused on both energy efficiency and clean and renewable sources, two things that the Trump administration, with the help of our Republican

colleagues, are trying to gut.

It is not just Meta, though. Amazon states that its data centers are powered by clean energy with 100 percent of the electricity consumed by its operations, including its data centers, matched with renewable energy in 2023.

So if anybody would like to come to Virginia and tour this 100 percent clean-energy powered, solar-powered data center, just let me know. I am happy to arrange a tour.

But let me get back to what we are supposed to be talking about today, which is grid security.

Now, as Chair Guthrie mentioned earlier, we have seen nation States use AI to enhance and automate cyber attacks against American corporations and entities.

Mr. Krejsa, with the explosion on availability of AI chat bots and large language models like the one we saw used in the attack that Anthropic revealed last month, how should we be prepared for the eventuality that an increasing number of non-state actors, including foreign terrorist organizations, will seek to leverage these now widely available technologies to target America's critical energy infrastructure, and how can we increase our adaptability of this threat?

Mr. Krejsa. Thank you, Congresswoman. Indeed, the explosion of AI technologies are lowering the bar for how many -- how much resources and expertise you need to mount a malicious cyber campaign. And as a result, we are going to need to take defense more seriously across the digital ecosystem, and in particular, in our critical infrastructure. And I think the answer is going to be modernization from top to bottom.

Ms. McClellan. Thank you. And as a follow-up, to what extent have we established a whole-of-government approach that ensures that government agencies and inner-agency entities are working with utilities and other private partners to monitor, prevent and react to cyber threats to the grid, and to what extent, if at all, should we be

looking to better leverage the resources of inner-agency efforts to bolster the security of the grid? And, again, Mr. Krejsa, this one is for you.

Mr. Krejsa. I think we are standing on a strong foundation built from the last few decades of hard-won lessens in defending our infrastructure from physical and cyber attacks, but it needs to continue to evolve to be flexible to the modern realities facing us in the years ahead.

Who makes up the energy stakeholder ecosystem is changing. We are getting more entrepreneurs, more diffuse and diverse sources of dynamic new inventive technologies that need to be folded into our existing information sharing and threat response ecosystem.

Ms. McClellan. And in your testimony, and in your response to one of my questions, you note that America's electric -- current electric grid is a hodgepodge of outdated analog technology, and more recent digital tools and components that create seams through which bad actors can gain access, compromise and attack the grid.

So I think we both agree we need to modernize and improve the grid. And I would argue one of the reasons for high electric costs is the fact that we have failed to invest in modernizing and expanding our grid for too long.

And so in 25 seconds or less, how would you recommend we in the Federal Government seek to steer the modernization of the grid to address both short-term vulnerabilities and create a grid that is both technologically advanced, secure and reliable?

Mr. Krejsa. Thank you, ma'am. The AI driven build-out of our energy ecosystem is a golden opportunity to focus the level of investment needed for that transformation to our electricity ecosystem that no other critical infrastructure sector allows. And so I think it will be ensuring that the hyper scalers, the various utilities and energy deployers of the country all have a similar idea of what right looks like, and we seize this moment to

distribute that understanding as far and wide as we can.

Ms. McClellan. Thank you. I yield back.

Mr. Weber. The gentlelady yields back. The chair now recognizes the gentleman from Texas for 5 minutes.

Mr. Pfluger. Thank you, Mr. Chairman. I think this is a really important topic. I serve on Homeland Security as well, and so the intersection of the grid, of the threats that we are facing, the things that you all are doing, how the government can help, what we need to be doing to help, the intelligence that you need, the sharing of information, those types of things are really important.

Before I get into questions, I want to submit a letter for the record, Mr. Chairman, that we have sent to the Department of Commerce, to Secretary Lutnick, that Mr. Balderson and I wrote.

Mr. Weber. Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Pfluger. And it has to do with the Chinese manufactured inverters and just the critical grid components that we are very concerned about. So we will get that for the record.

But I will just jump right into the questions. Mr. Ball, in your testimony you indicated that the PRC, the campaigns like Salt Typhoon and Volt Typhoon represent the most persistent and adaptive threats that are targeting our infrastructure. We know that the Chinese communist party is actively seeking to do damage and gather intelligence. But can you describe at an operational level what utilities are doing differently today than has been done to detect and to stop these campaigns, and then what gaps still exist that we need to be worried about?

Mr. Ball. So I think the best way to describe that is I think we see an industry that is evolving in its capabilities, and it is based on awareness. I think, you know, we have seen a significant awakening, and I am not saying it is enough, but we have seen a significant awakening to the threat with our industry.

And, you know, what it boils down to, despite the sophisticated capabilities that threat actors like the PRC has, you know, a lot of the things that make us resilient still boil down to basic practices and making ourselves -- and our utilities, and we need to continue to bolster that capability, our industry, whether it is large IOUs, or down to the municipals and cooperatives, I think you are hearing even today how they are -- this industry is awake to that, and I think we need to continue to empower them to be able to build a more resilient system.

Mr. Pfluger. Are you seeing that there are other State actors that are seeking to exploit the Chinese-made inverters?

Mr. Ball. That is a good question. I think that we don't see any -- from my

perspective, my purview, I necessarily can't comment or see any different threat actors utilizing the same core technologies to exploit it. But I would say that threat actors of all sorts, if there is a vulnerability in a technology, they will seek to exploit it. And that can range from sophisticated threat actors all the way down to criminals, folks that want to monetize vulnerability by attacking.

Mr. Pfluger. Mr. Lindahl, and Ms. Artz, I will get to you, a question here in a second, but same thing for you, we have a lot of rural cooperatives in my district. I think I overlap with something close to 15 or so. The gentleman behind you could probably answer that question for me. But what kind of threats or vulnerabilities or gaps are you seeing specifically in the rural cooperative?

Mr. Lindahl. We see the same threats, I think, that every other utility sees. I don't think -- you know, a threat actor doesn't differentiate between a small cooperative and a large all utility like an Xcel Energy. And we put the layers in place, and we don't necessarily care where the threat comes from, we care that we have things in place to prevent it from happening and be able to respond to it once it does happen.

However, with information sharing, we do need the tools so we understand what the threats are and we can develop the tools to mitigate them.

Mr. Pfluger. Are you getting what you need in the form of intelligence, information-sharing, and an awareness of the threat as our intelligence community sees it? Are you getting that in a timely manner?

Mr. Lindahl. It is a good foundation. I think it is working and it is working now, but we can always evolve and improve.

Mr. Pfluger. I will take that for we need to improve. Ms. Artz, you mentioned in your testimony that the Chinese State-sponsored actors have already compromised multiple U.S. critical infrastructure providers with the intent to disrupt operational controls. How

have the cybersecurity practices changed in response to these threats in these nation States?

Ms. Artz. Thank you for the question. I would say the information that we have received, particularly on Volt Typhoon and Salt Typhoon, resulted in the energy threat analysis center, which I mentioned, really honing in on that threat and developing capabilities, "capabilities" is maybe not the quite the right word, so that small, medium, large electric utilities could look for evidence of those cyber actors in their systems. Those threat-hunt memo guides that were produced by ETAC are an example of us as industry taking that intelligence, innovating and getting quick risk reduction priorities into the hands of those that need to use them to mitigate the risk.

Mr. Pfluger. Thank you. My time has expired. I yield back.

Mr. Weber. The gentleman yields back. The gentlelady from Colorado is now recognized for at least 5 minutes.

Ms. DeGette. Thank you, Mr. Chairman. First, I want to talk about sort of this principle I always keep hearing my Republican colleagues talk about every time we have an energy subcommittee hearing, and Mr. Palmer talked about it today, which is, he said, quote, "We all believe we should have an all-of-the-above energy strategy." I guess I just want to go down the panel, starting with you, Mr. Ball, do you believe we should have an all-of-the-above energy strategy? And each person can just answer yes or no.

Mr. Ball. Absolutely. You can see the complexity.

Ms. DeGette. Yeah. Ms. Artz.

Ms. Artz. Yes.

Ms. DeGette. Mr. Lindahl.

Mr. Lindahl. Yes.

Ms. DeGette. Mr. Krejsa.

Mr. Krejsa. Yes.

Mr. Tudor. Yes.

Mr. DeGette. Okay. So everybody thinks we should have an all-of-the-above energy policy.

Mr. Krejsa, I want to ask you, my staff and I tried to make an exhaustive list of what an all-of-the-above energy policy sources would contain, and here is what we came up with: Crude oil, natural gas, coal, solar, wind, nuclear, hydro, biofuels, geothermal, hydrogen. Does that sound about right?

Mr. Krejsa. That sounds about right, ma'am.

Ms. DeGette. So here is my concern is when we have these hearings, they say they support an all-of-the-above energy policy, but then they completely -- all the policies they advocate for completely only talk about those top three, crude oil, natural gas and oil. And I just want to ask all of you folks here who represent industry and others, are any of your industries or your businesses associated with you moving away from these other sources of energy to just go to these three because of cybersecurity issues?

Mr. Ball. No.

Ms. Artz. No.

Mr. Lindahl. No.

Mr. DeGette. Yeah. Okay. So I want to ask you, Mr. Krejsa, in terms of cybersecurity, is it inherently more dangerous to have an-all-of-the above energy approach and use these other things?

Mr. Krejsa. Thank you, Congresswoman. No, it is I would say more secure and resilient to have an all-of-the-above strategy.

Ms. DeGette. It is more secure and resilient to have an all-of-the-above strategy. So when we are talking about security, batteries and so on, it is not like these things are

going to go away, we have to figure out how to make these sources more secure; is that right?

Mr. Krejsa. Yes, ma'am.

Ms. DeGette. Now, in these lines, yesterday DOE announced that the National Renewable Energy Lab, which is just across the border from my district, will, quote, "Effectively be called the National Laboratory of the Rockies," which I am happy to have my beloved Rocky Mountains recognized, but I don't really know what this means. Does this mean that the administration doesn't want to have the iconic end route, which was established by President George W. Bush, Sr., in 1991 move away from renewable energy research. So thanks to the help of AI, I went online and I looked at their report for 2023, and they are talking about research fund opportunities for breakthrough battery designs, hydrogen blending as a pathway towards U.S. decarbonization, full steam ahead, unearthing the power of geothermal, and it goes on. You get my drift.

What I want to know is in this performative action by the administration yesterday of renaming the lab, are they now planning to move away from research that will actually help us make our grids more secure in the long run? And that is the problem I have with what is going on with the Trump administration and with my colleagues across the aisle.

Now, Ms. Artz, I do have to ask you a question because Xcel Energy, of course, is my local energy company, and I really do appreciate your testimony here today, given the presence of critical national security entities in the State like NORAD and Space Force and also, of course, of -- what is it called now, the National Laboratory of the Rockies, I wonder if you can talk to me briefly about how Xcel supports the security organizations, and how ETAC, the Energy Threat Analysis Center, can facilitate those relationships?

Ms. Artz. Thank you for the question. Xcel Energy collaborates very regularly with the national security partners we serve in the State to ensure that we are meeting their

energy resilience needs. We recently hosted NORAD and Northern Command at ETAC to exchange intelligence information. That complements the efforts we conduct in other venues with them. We look forward to continuing that collaboration on response and recovery efforts as well.

Ms. DeGette. Thank you. So the collaboration is really what is important here. Mr. Chairman, I yield back.

Mr. Weber. The gentlelady yields back. The chair now recognizes the gentleman from New York for 5 minutes.

Mr. Langworthy. Thank you very much, Mr. Chairman. Our witnesses know better than anyone how frequently adversaries test our defenses and target the operators who keep power flowing. But as we consider these vulnerabilities, we must also recognize a broader point, cyber and physical threats don't just expose weaknesses in the electrical system, they highlight the danger of relying on a single source of energy.

When States or cities adopt policies that eliminate natural gas or restrict access to other fuels, they don't just limit consumer choice, they reduce resiliency. Electricity is essential, but it only works when the grid is functioning. If a cyber attack or a physical incident takes the grid offline, everything that depends on electricity stops.

Natural gas and propane, however, can be delivered directly to the home or facility and continue to operate independently off the electrical grid. They provide heat, hot water, cooking capabilities, and even fuel for backup generators during an outage. These fuels don't replace electricity, but they give families, hospitals and emergency services a critical lifeline when the grid is down. Removing these options leaves communities with only one energy source to rely on, and one point of failure if that system is disrupted.

Mr. Tudor, if a cyber or physical attack takes down electrical services, what are the practical impacts on hospitals, water systems, emergency responders, and other critical

services, particularly in the areas without natural gas or other backup fuels?

Mr. Tudor. Thank you, Congressman. Obviously, you know, electricity is the lifeblood of almost all of these critical sectors, and so, anything that takes down the electric capacity in a region would definitely have a devastating effect to all those things you mentioned.

Mr. Langworthy. These aren't abstract concerns. In my home State of New York, policymakers are moving aggressively towards an all-electric mandate and rapidly increasing electric load without adding generation or transmission needed to support it. The New York independent system operator has repeatedly warned the grid is already strained during winter peaks and electrifying -- with electrifying for heat and transportation without backup options is creating serious reliability risks, and these are technical assessments, not political arguments.

Mr. Lindahl, when a cyber or physical incident knocks out electrical service, what does that mean for the hardworking families that you serve, especially those living paycheck to paycheck who can't afford long outages and don't have alternate heating or cooking options?

Mr. Lindahl. There is a significant cost to outages, and the longer term cost is to our general economy. If we have a negative impact on the reliability of our grid, that is going to force people to make decisions to go elsewhere. And it would be the same with affordability as well. And so we have got to get it right because we can't afford to lose what we have, and we can't afford to let our folks go cold in the wintertime, or hot in the summertime. Those are life-and-death matters.

Mr. Langworthy. Thank you very much, Mr. Lindahl. And when you combine a stressed grid with increased cyber threats, the increase becomes even clearer. If electrical demand keeps rising while natural gas is phased out, a single attack on a transmission line or

a control center doesn't just cause inconvenience, it threatens entire communities, hospitals without heat, seniors at risk from freezing temperatures, manufacturers forced offline, and emergency responders left without any kind of safety net. No redundancy.

True resilience requires multiple energy pathways, electricity, natural gas, propane, backup generation, and distributed resources so that a single disruption cannot shut down a community. And with that, Mr. Chairman, I yield back.

Mr. Weber. The gentleman yields back. The chair now recognizes the gentlelady from California for at least 5 minutes.

Ms. Matsui. Thank you very much, Mr. Chairman. And I want to thank the witnesses for being here today.

Mr. Krejsa, as ranking member of the Communications and Technology Subcommittee, I have led efforts to rip and replace insecure Huawei and GTE equipment from U.S. telecom networks. However, I am really concerned that we are facing a similar problem with Chinese-made grid equipment. It doesn't matter how strong our cyber defenses are if the Chinese military have direct back doors into Chinese-made inverters, transforms, battery systems across the U.S. electric grid. Mr. Krejsa, how big of a problem is this?

Mr. Krejsa. Thank you for that question, Congresswoman. And thank you for your efforts to secure our telecom infrastructure. This is indeed a big problem, but it is bigger than an electrical equipment problem. It is bigger than a telecom equipment problem. It is a modern society problem. Any piece of equipment that has a computer in it likely has a major Chinese dependency.

Ms. Matsui. So we can't just carry out a rip and replace program for Chinese-made grid equipment.

So let's say this, not everything made in China is spyware. Mr. Krejsa, how do we

identify with certainty what Chinese-made grid equipment poses a risk?

Mr. Krejsa. It is going to require a risk and consequence prioritization framework. We need to consider what kinds of electrical equipment has systemic impact, has the most digital exposure and focus our scrutiny on there, first.

Ms. Matsui. Okay. Now, Mr. Tudor, how are national labs helping to identify potential back doors or other vulnerabilities in Chinese-made grid equipment?

Mr. Tudor. Thank you for that question, ma'am. And, you know, we have been mentioning that PRC manufacturers, a majority of our power electronics, battery technology controlled equipment, at least 70 percent of the manufacturers are from the PRC, and probably 90 percent of our critical components have at least one critical component got from China, so it is a major problem. They have had a systemic 20-year strategy to make these things happen.

You know, we work with the Department of Energy, CESER and the DOE Grid Deployment Office to provide technical assistance to asset owners via the threat hunting.

And it is in response as already has been mentioned, we have worked with the integrators and other businesses that work to develop these different infrastructures to help them provide secure designs to cyber-informed engineering. And one of our similar programs, the consequence driven side of informed engineering helps utilities and others identify what the highest risk areas and highest risk components may be to be mitigated.

I wrote down, you know, you asked Mr. Krejsa, you know, how do we determine these things with certainty, and I don't know that I would ever be certain of these things until we could watch the manufacturer happen either in U.S. areas, or in partner areas. But reducing risk is what we are all working at and beginning to identify and recover.

Ms. Matsui. Okay. We have a lot of work to do here, then. Ultimately, we should reshore manufacturing for key components of our energy supply chain, and that is

why the Democrats included incentives in the Inflation and Reduction Act to manufacture inverters, batteries and other grid equipment in the U.S., and it was an incredible success with dozens of new factories planned here in this country, but the Republicans bill derailed that. No mention.

Mr. Krejsa, are you concerned that without a concerted government effort to boost U.S. manufacturing of key grid equipment, we can worsen our dependence on competitors like China?

Mr. Krejsa. Yes, ma'am. Thank you. I am very concerned, but I think that the -- our experience in securing our telecom infrastructure demonstrates that we need two primary tools to do so, a scalpel and a shovel. A scalpel to excise those high-consequence, high-risk pieces of technology, and a shovel to build those factories so they can produce the replacements.

Ms. Matsui. Okay. Thank you. I want to shift to talk about cyber threats to our local distribution system, the low voltage local transmission system that delivers power during the last mile to our homes and businesses. The local distribution system is vulnerable to cyber attacks and often receives less attention.

Mr. Krejsa, are you concerned that we are not paying enough attention to the local distribution system?

Mr. Krejsa. Yes, ma'am. It is estimated that 10 to 20 percent of the volt power system is under direct Federal oversight, but that is why we need the fantastic efforts of my co-witnesses here today to help make sure that those efforts get down to where they need to go.

Ms. Matsui. Absolutely. Mr. Ball, do you share Mr. Krejsa's concerns in looking forward?

Mr. Ball. I do. I do. And we are very focused on trying to fill any gaps thereby

really channeling information in actionable ways to the local companies that are running distribution systems.

Ms. Matsui. Realizing, of course, a lot of the States are more involved in that process, right?

Mr. Ball. Absolutely.

Ms. Matsui. Okay. I run out of time. I thank you very much. I yield back.

Mr. Weber. The gentlelady yields back. The chair now recognizes the gentleman from South Carolina for 5 minutes.

Mr. Fry. Thank you, Mr. Chairman. And thank you to our witnesses for being here today.

If the power goes out, everything stops, hospitals, water systems, communications network, everything. I think it is incredibly alarming, some of the testimony I have heard today about malign actors, state -- nation-states, and also others, China, Russia, Iran, North Korea, becoming more aggressive and sophisticated. I think reading, me personally, preparing for this hearing, reading about China's preparations if there was a conflict on how to target our grid. That is really alarming. Right. Like that is incredible stuff that we have to grapple with, and I am glad that this committee is taking a holistic and serious approach to identifying ways in which we can be more resilient. Right. That we can withstand these type of cyber attacks.

RPTR MOLNAR

EDTR CRYSTAL

[12:34 p.m.]

Mr. Fry. Mr. Ball, to you. What role do you think the E-ISAC plays in identifying and sharing threats coming from the pipeline sector that could affect power generation and power delivery?

Mr. Ball. Thank you. It is a very good question.

And I would have to say, you characterized the productive paranoia that I think all of us operate under.

And we, to that point, particularly with the natural gas sector, we have actually had partnership from an E-ISAC perspective that goes way back.

We have worked actually with the Downstream Natural Gas ISAC, what is now the ONE-ISAC. This is a network of information sharing that happens every day.

We believe that the trades also work very closely together, meaning AGA, INGAA, and our electric trades actually do work very close together and worry about the complex interdependencies between those different systems.

Mr. Fry. Do you think, in that same vein, though, that you have sufficient visibility into the pipeline sector threats, or are there any blind spots that Congress should consider for today's hearing?

Mr. Ball. Well, I think we certainly have lots of insights into the threats that are part of it. I think what is particularly challenging is the dynamics of those systems when it comes to natural gas and the operational realities of these assets when in need to supply the electric sector.

There is a lot of good -- in fact, there was an excellent exercise that EEI facilitated that actually brought leaders together to tackle some of those issues, like how do we deal

with these complexities when a very bad day happens.

Mr. Fry. What about Congress, are there blind spots that Congress needs to be aware of?

Mr. Ball. It is hard to speak to that. I actually have to believe we do not have perfect visibility. None of us should be able to claim that. And I think there is always an opportunity to improve there.

Mr. Fry. Thank you.

Ms. Artz, from the perspective of investor-owned utilities, do you think that the utilities are receiving actionable intelligence quick enough to prepare for threats that could move between sectors like gas and electricity?

Ms. Artz. Thank you for the question.

As one of my colleagues stated earlier, we can always do better. We are doing a lot of that improvement on sharing actionable intelligence out to the entire industry via the Energy Threat and Analysis Center and the regular information sharing that occurs between the E-ISAC and the Downstream Natural Gas ISAC.

We are very collaborative as an industry because we are interconnected, and we understand that. So sharing this information to all of our peers throughout the country, across the industry, is incredibly important to guarding against the threat.

Mr. Fry. Thank you for that.

Mr. Lindahl, rural electric cooperatives serve large geographic areas, less people, less resources oftentimes.

Does cross-sector information sharing provide sufficient visibility for rural systems, or are there gaps that make that job much harder to manage for smaller utilities?

Mr. Lindahl. It helps. There are always gaps because we don't know what we don't know, and we can always improve on that.

But the information we get, we react, and we have the same processes in place like the information that an Xcel Energy would get. We utilize the same tools, the same resources, the same opportunities.

Mr. Fry. Do you find that it is harder to manage from a rural electric perspective?

Mr. Lindahl. It is because our resources are sometimes very tried. It is hard to find the team, the staff that wants to live in rural America that has the expertise to do what we need to do.

So that is why we come together as cooperatives with, like, NRECA, and create programs like the RMUC, that we can actually bridge the gap and act like a larger entity even though we are 900 smaller entities.

Mr. Fry. Right. So you are taking -- I mean, you are taking sufficient steps then to bridge that gap --

Mr. Lindahl. That is right.

Mr. Fry. -- to use your term.

Mr. Lindahl. Yep.

Mr. Fry. Because that was always my concern, was investor-owned utilities, big things, a lot of money, maybe a lot of customers too, but the rural folks, they are kind of left on the sideline.

But you are taking, I would say, proactive steps to deal --

Mr. Lindahl. Yeah. One of the benefits we have, I think, in the cyber threat is we are many and we are diversified, but yet we cooperate among cooperatives and other utilities, and we come together to solve big problems.

Mr. Fry. Well, thank you for that.

Guess what, guys. I had questions for you too, but you are off the hook, especially you, Mr. Tudor. I had a really challenging one about our ability of Congress to understand

these threats. You are damned either way you answer that, quite frankly.

But anyway, Mr. Chairman, I yield back.

Mr. Weber. The gentleman is also off the hook. His time has expired.

The chair now recognizes the gentleman from New York for 5 minutes.

Mr. Tonko. Thank you, Mr. Chair.

I fully acknowledge that cyber attacks pose a real and serious threat to our energy system, but I also know that our constituents are dealing with major energy affordability challenges.

And every investment a utility makes, whether that is in generation, transmission, distribution, or security, will ultimately be paid for by their ratepayers.

What concerns me is there seems to be no limit to the amount of money that could be invested in well-meaning cybersecurity upgrades without ever being able to guarantee that our system is 100 percent secure.

Again, I don't want to downplay the risks we face from cyber threats, but I would like to understand the thought process that goes into evaluating whether a cybersecurity investment is a worthwhile use of ratepayers' money.

Mr. Lindahl, I know co-ops are conscientious of cost increases on their members. How do you think not-for-profit utilities, or even regulators who work on rate cases for other utility business models, should think about these issues?

Mr. Lindahl. From our perspective, how we look at it is we try and do things as efficient as we absolutely can. So a lot of times it makes no sense for maybe 900 of us to have a security expert on staff. But if we can pool together and hire one security expert to share amongst all 900, and leverage other tools, like RMUC or other things, to develop the innovation and the tools needed to fight this, that is a better use of the same dollar and less dollars used to achieve a bigger benefit.

Mr. Tonko. And how can they best balance the need for cybersecurity investments while also being mindful of that impact on people's rising utility bills?

Mr. Lindahl. We look at it from a risk perspective. You have the probability of something happening and the impact that it has. And we focus on those high-impact, high-probability events first, kind of the low-hanging fruit, and then we keep moving back, and we evaluate every risk of that decreasing return to determine what is the impact or what is the probability of that happening.

And we evaluate -- again, back to the three legs I talked about earlier -- the affordability, reliability, and safety of our system. That all has to be in balance. We can't put reliability at the expense of affordability.

Mr. Tonko. Well, I thank you for that.

And, Ms. Artz, how is Xcel thinking about finding this balance between, on one hand, protecting your customers from outages and other cyber-related disruptions, and on the other, the effects those investments will have on bills?

Ms. Artz. Thank you for the question.

Similar to my colleague, Mr. Lindahl, we take a very similar holistic risk-assessment approach, prioritize what we can get the most bang for our buck in terms of that risk reduction.

But I want to emphasize a point I made in my testimony that is vitally important, which is the timely and actionable sharing of intelligence so that we can build security in proactively versus bolting it on after the fact.

Bolting it on after the fact is much more costly. Building it in at the front end is very cost-effective. And that is why programs developed by Idaho National Labs, Department of Energy, such as the Cyber-Informed Engineering, really help us think through the architecture of our systems to achieve that cost-effectiveness and maintain affordability.

Mr. Tonko. So to Mr. Lindahl or Ms. Artz, are there simple, low-cost interventions or best practices that utilities could adopt to improve cybersecurity without adding a lot of costs to their customers?

Mr. Lindahl. Yeah. We have a Cyber Goals Program that we implement across all of our utilities that are the basic-level cyber-hygiene type practices -- and physical for that matter too. And those are low-cost, high-impact programs and kind of the base-level goals that everybody should abide by.

Ms. Artz. Another program that we implement is the training and situational awareness of the threat landscape for all of our employees.

We recognize that our employee base is our best defense, and so on a monthly basis our security team provides situational awareness on the threat landscape. We also test our employees so that they are better able to detect phishing attempts. They are our best line of defense.

Mr. Tonko. Thank you.

In April of 2023, FERC issued Order 893 to establish an incentive-based approach for qualified cybersecurity investments and participation in cybersecurity threat information-sharing programs. But my understanding is that utilities aren't really taking advantage of that incentive.

Mr. Ball, are you familiar with this FERC order?

Mr. Ball. I am.

Mr. Tonko. And do you have any insights as to why it hasn't proven to be as effective as the commission may have hoped?

Mr. Ball. For my current role, I do not. However, in my prior work certainly understood those programs to be available, but there is even a cost to try to gain funding. So it can be prohibitive.

Mr. Tonko. Well, with that, I ran out of time. But, Ms. Artz, I will have a question that I am sending your way in writing.

And again, Mr. Chair, I yield back, and thank you.

Mr. Weber. The gentleman yields back.

The chair now recognizes the gentlelady from Iowa, good doctor, for at least 5 minutes.

Mrs. Miller-Meeks. Thank you, Chair Weber and Ranking Member Castor, for holding this hearing on cyber and physical security of the grid.

The threat landscape we face today is unrecognizable compared to even 5 years ago. Our adversaries, specifically the Chinese Communist Party, are actively seeking vulnerabilities in our critical infrastructure. As we know, Russian hackers are doing so as well.

Grid security is national security, and it is the difference between keeping the lights on during a winter storm or facing catastrophic failure.

Iowa is leading both research and manufacturing. The Department of Energy selected Iowa State University to lead CyDERMS, a regional cybersecurity center focused on securing distributive energy resources.

As more renewables are brought online, we are introducing millions of new devices to our grid. Every connection point is a potential vulnerability.

CyDERMS is developing AI and machine-learning tools to detect attacks in real time while training the workforce needed to defend these systems, particularly for rural utilities that lack resources.

We must also address hardware. We cannot secure our grid if the components we

use are compromised by adversaries.

The reliance on Chinese technology in our supply chain is a glaring vulnerability. We must replace these components while being realistic about replacement speed and alternative availability.

This requires enhancing domestic manufacturing. If we want American companies to build the critical transformers and inverters we need, we must make it viable.

My bill, the Limiting Liability for Critical Infrastructure Manufacturers Act, provides domestic manufacturers legal certainty so they can invest in hiring American workers and expanding facilities, rather than hedging against frivolous legal risks.

Finally, I want to highlight the Energy Threat Analysis Center at NREL. ETAC solves the translation problem, converting classified intelligence into tactical operational guidance that utilities can actually use.

The tools to secure our grid exist. It is our job to ensure that they have the resources and authority to succeed.

Mr. Ball, the risk environment is intensifying. We are adding technology to the grid, expanding it to meet surging demand, modernizing aging infrastructure, while geopolitical tensions are rising.

We need coordination between the private sector and the Federal Government -- DOE, CISA, FERC, the White House, and others -- to move quickly and securely. Can you speak to how the coordination is working today and where you see gaps that need to be addressed.

Mr. Ball. So it is a very, very, very good question, and certainly a very important apparatus.

Speaking from the perspective of the E-ISAC, we see ourselves, and we are positioned, to be a conduit of information sharing.

So with these, our government partners, with our industry partners, we serve as a pathway and a bidirectional, multidirectional pathway for that information sharing.

So as curators of that information, we need to see that thriving. And so we certainly appreciate a great deal of engagement that we see today, but there is absolutely opportunity to empower that.

I think we need to see greater encouragement of information sharing and protection of information sharing from our members as they see incidents.

So these are areas we need to see improvement on.

Mrs. Miller-Meeks. Thank you.

Mr. Lindahl, Iowa has rural utilities that are already resource-strapped. When we tell them they need to replace outdated equipment and integrate new AI systems, what does that actually cost, and who is going to pay for it?

In that context, can you explain how CESER's Rural and Municipal Utility Advances Cybersecurity Grant and Technical Assistance Program support co-ops in strengthening their cybersecurity posture?

Mr. Lindahl. Yeah. For the specific costs, I can't necessarily address that for every co-op. But when we make investments in any tool we do a return-on-investment analysis, just like any good business would do, and we look at what it is going to provide us and what it costs us to make sure we get back out of it.

By pooling our resources together through programs like RMUC, we can develop these things collaboratively. So instead of, again, 900 of us developing an AI tool, let's say for an example, we can come together and develop one tool that works for all of us. And those are the ways we kind of have been working together to solve that problem.

Mrs. Miller-Meeks. Thank you.

Mr. Tudor, you mentioned that CyTRICS conducts rigorous testing of hardware and

software components in the energy supply chain.

Given that you have identified China's embedding of hardware vulnerabilities as a major structural risk, how effective are these testing programs?

And I know this is terrible, but I am going to ask you to respond in writing because I am running out of time.

But how effective are the testing programs at detecting back doors or vulnerabilities built into Chinese-manufactured equipment? And can these programs scale to address the volume of Chinese components currently in our infrastructure.

So if you would respond in writing to us, that would be greatly appreciated.

And with that, I yield.

Mr. Tudor. Thank you.

Mr. Weber. The gentlelady yields back.

The chair now recognizes the gentlelady from Washington for at least 5 minutes.

Ms. Schrier. Oh, I won't go over.

Thank you, Mr. Chairman.

And thank you very much to our witnesses today.

I am going to first talk about AI, because the new AI frontier has brought new vulnerabilities -- and benefits -- to the grid, and also to our broader society, both because of reliance on AI by virtually every industry out there and because AI can be used to foster resiliency in our grid. But it could also be used to sabotage our grid by bad actors.

Mr. Ball, NERC responded to the Department of Energy's request for information on the previous administration's executive order on the safe, secure, and trustworthy development of AI, and NERC noted that it was committed to identifying and monitoring the risks in implementing AI.

Things are moving quickly, it is a moving target, and I was just wondering if you could

quickly talk about what your observations are on the current risks associated with AI on the bulk power system.

Mr. Ball. Well, I think it is a great and actually very broad question. But I would say that I think you characterize it very well, that it is a prolific factor in managing information technology and certainly is within the energy sector.

I think that we are certainly learning how it can be misused. I think we heard a discussion a little bit about the recent demonstration of exploiting an AI tool that was for a large-scale attack. So I think we are seeing that emerge out.

I don't think we are ready yet to really handle all of the issues. I mean, it is an emerging and continually evolving problem.

We are monitoring it. In fact, with that threat I just referenced, from an E-ISAC perspective, which I can speak very discreetly, we were sharing information about that threat and actually things that you can do to help mitigate that risk.

So that, I think, is the best way I can describe what we are seeing and how we are trying to tackle it.

Ms. Schrier. Thank you. I appreciate that. It feels like we are going to just have to keep pace with this.

I am wondering, do you think that we should just have a fresh evaluation of NERC's Critical Infrastructure Protection standards in light of AI and the new threats and the quick evolution of those threats?

Mr. Ball. So what I can say is that while that is a specific threat area, that actually NERC is actively looking for ways to advance and renew the Critical Protection standards. In fact, there is an active effort underway today to try to find actionable ways to improve that.

So, in other words, there are opportunities, and NERC is actually working on.

Ms. Schrier. Great. It is already happening. That is good to know.

I am going to pivot a little bit actually to our infrastructure, and transformers in particular.

Many of you in your testimonies described or referenced the 2022 substation attacks in Washington State. Unfortunately, thousands of those affected were actually in my district. And while those Christmas Day attacks luckily only interrupted access to power for a few days, the large power transformers that were damaged in the incident were projected to take months to repair.

And I have been talking with utilities about what it takes to replace a transformer, and it is like finding a used one, making some modifications. It is not the way our grid should be functioning.

And, Ms. Artz, a question for you, representing a large utility. What is Xcel Energy's current capability to replace transformers and other critical electrical grid components that might be damaged in a physical or cybersecurity attack?

Ms. Artz. Yeah. Thank you for the question.

So we are very aware of the physical threats that are posed to our critical infrastructure. We have a very robust procurement process that assesses long lead times for important equipment so that we are prepared to have that equipment in hand.

Importantly, as an industry we have taken on a couple of initiatives to better provide availability of this critical equipment.

One example is the Electricity Subsector Coordinating Council, because of delays in equipment lead times, based on the pandemic, looked at the opportunity to reduce the number of specifications for individual transformers, thereby increasing the availability of that critical equipment.

Finally, we also have a spare transformer program that can be tapped into when

there are emergencies.

Ms. Schrier. Thank you.

I am over 5 minutes.

Just thank you for pointing that out because I think Mrs. Miller-Meeks pointed to this too. We rely on China, long lead times, too much individualization in what kinds of transformers can be used.

And so it is really hard to have a national stockpiling. That is something this committee is going to need to help figure out.

Thank you. I yield back.

Mr. Weber. The gentlelady yields back.

The chair now recognizes the gentlelady from Florida for at least 5 minutes.

Ms. Lee. Thank you, Chairman, and to our witnesses.

Cybersecurity is national security, and we must remain vigilant in maintaining the security of our grid and all of our critical infrastructure.

As cyber and physical threats continue to grow in scope and sophistication, it is essential that we evolve with the threat landscape and that we continue to leverage our public-private partnerships, foster information sharing, and build our cybersecurity workforce to be prepared to meet these challenges.

So I appreciate all of our witnesses here today sharing your substantial expertise and insight about the ways in which we can best strengthen the security of our energy infrastructure and proactively mitigate threats from adversaries and malicious actors.

Mr. Tudor, I would like to start with you.

In your written testimony, you noted the threat that Chinese state-sponsored cyber threats like Volt Typhoon pose to our electric grid.

I was pleased that a few weeks ago the House passed the Strengthening Cyber

Resilience Against State-Sponsored Threats Act to establish an interagency task force addressing these cybersecurity threats.

Can you describe for us how Volt Typhoon and similar actors attempt to infiltrate and disrupt our critical energy infrastructure or have the potential to lay dormant and do so at a future point?

Mr. Tudor. Yeah. Thank you, Ms. Lee, for your question, and it was encouraging to see that frank coordination at the Federal level being prescribed.

I think we are very concerned about the Chinese actors in particular. I mean, we note that the Russian-affiliated actors tend to be very active. They don't lay dormant. They go for the jugular in many different ways.

Volt Typhoon, Salt Typhoon, all of the things that we have designated there, have not been imminent threats, per se, to our infrastructure, but they are, as you said, lying dormant, waiting for appropriate times to be activated.

Across the interagency, the National Labs, CESER, and others are working on threat and incident-response capabilities, to be able to work with NRECA's other utilities to identify those threats and mitigate them where necessary and where possible.

And I think we are also developing tools that can be applied across the industry to help with those hunt and threat activities. Understanding where the adversary may be is critical.

One of the things that we also work on is something called Consequence-driven Cyber-informed Engineering, to try to understand not just what might happen, but what are the most important, impactful things that might happen and help the government understand where they might invest to mitigate those.

Ms. Lee. Mr. Ball, on the subject of information sharing and incident sharing within the E-ISAC, you mentioned just a moment ago protection for members.

Would you elaborate on whether there are obstacles or reticence that might exist for private partners sharing information about specific suspicious activity or incidents within the E-ISAC?

If so, how can we overcome those? Or do you feel at this point that there is, in fact, a very open sharing of incident information within the E-ISAC?

Mr. Ball. So it is a very good question. Certainly information sharing, we see a tremendous -- this industry is exceptional at sharing information, and I think we can continue to leverage that.

One thing we see concerns about, you saw some of the liability protections that were in CISA 2015. It was issued out with that expiring but subsequently being extended for a period -- little bit period -- small period of time.

Those provide some confidence to members to say, "I can share." When we start to see erosion of that protection, then we -- I am worried about the atrophy of it.

What I need to see is the opposite. We need to see increased sharing information, and the speed in which we do that needs to be based on trust and confidence.

And that is something we, I think, have a challenge for. But the good news is we have a tremendous base of capability right now that is working well. We just need it to work better and faster.

Ms. Lee. And, Ms. Artz, you just mentioned something that is so important. It had to do with internal employee education.

Would you elaborate on why training about things like phishing and social engineering is both critical to cybersecurity and also low cost in many cases?

Ms. Artz. Thank you for the question.

As I said, our employees are our best line of defense. We are being targeted because we provide essential energy services, both natural gas and electricity. We need

our employees to understand that they will be targeted, and therefore we provide them briefs on the threat landscape so they can understand how China and others are targeting us, that they are aware of how clever bad actors are in their attempts to steal credentials that would then allow them to access our system.

So I mentioned the phishing training that we do. So the testing that we do, so if you see it, you report it, and don't click on it, robust training practices to help them protect our infrastructure.

Ms. Lee. Thank you, Mr. Chairman. I yield back.

Mr. Weber. The gentlelady yields back.

The chair now recognizes the gentlelady from our beloved Texas for at least 5 minutes.

Mrs. Fletcher. Well, thank you so much, Mr. Chairman.

And thank you to all of our witnesses today for your testimony. It has been alarming and very important. And as we have heard today, the cybersecurity threats to our energy infrastructure are becoming more and more common and more and more dangerous every year.

Someone said earlier in this hearing that this year looks different than even 5 years ago. I think that might be the understatement of the year on all fronts.

What is happening is really unrecognizable to many of us who were here 5 years ago, and it really is absolutely essential that Congress assert its authority and work to address the challenges that we face, especially now.

We know, for example, just in 2023, Texans were shocked to learn that hackers that were backed by the Chinese Government attempted to access the computer systems used to maintain our power grid in Texas.

And fortunately there is no evidence that those hackers gained entry. But if

successful, attacks like these could be devastating, causing rolling blackouts for people who live across the State -- and obviously across the country in other systems -- as well as cutting off power for emergency services, something we are all too familiar with in our region along the Gulf Coast and someplace where long-term grid stability is absolutely a priority and a deep concern.

So as grid operators work to expand our energy infrastructure in response to growing demand from AI development, which we have also covered a little bit today, we really have to expand our ability to address these cybersecurity threats.

It is crucial that Congress takes up transmission permitting reform so that operators can expand and modernize the grid on pace with demand.

And while we talk about permitting reform, and I am hopeful that we are going to see some coming out of our committee and out of this Congress, I really hope that this committee can come together to find solutions to this problem and to address transmission.

When I hear from our independent grid operator, ERCOT, about security issues, CRISP stands out as an exemplary partnership that is driving real results, and so I want to acknowledge that.

And everyone here knows, of course, that it facilitates information sharing among asset owners and operators about cybersecurity threats and leverages the National Labs' expertise to analyze the threats and provide program participants with the information they need.

I think a lot of people who aren't in this space don't necessarily know and understand the importance of this partnership, but I think it is really critical that we are sharing with the people that we represent and people across the country these examples of these successful partnerships between the government, industry, academia, research institutions.

That is something that when Mr. Weber and I served on the Science, Space, and Technology Committee, I was always struck by how well and effective these collaborative partnerships are.

And so I think it is just really important to point that out and to emphasize that when we work together, we can work to get things done and to address challenges like these.

But as many of us know, things are not working very well in Washington these days. And I hope that Congress will take your testimony to heart and will move quickly on several of the recommendations that you have made.

I do have a couple of questions to ask before my time is up.

Mr. Krejsa, you mentioned the need for information sharing and analysis organizations, like E-ISAC, to ensure that membership includes a broad set of energy stakeholders.

What can Congress do to help expand access and utilization of programs like CRISP, give energy stakeholders greater insight into the threat environment? And obviously always a question, do we need additional funding from Congress to ensure adequate participation?

Mr. Krejsa. Thank you, Congresswoman.

I think that we have talked a lot about the ETAC today and its efforts at figuring out new models of turning threat intelligence into practical, helpful advice for different kinds of consumers.

And I think whether it is ensuring that ETAC has the authorities and funding it needs, or if we need different variants of it for different subsectors along the way, I think that is something that would be very impactful, especially as our energy ecosystem moves toward one that is more diverse, diffuse, and distributed and has more different kinds of actors in it.

Mrs. Fletcher. And just as a quick follow-up to that, because this is an issue we

have dealt with in this committee in this Congress, can you speak to the importance of adequately funding and staffing the National Labs to analyze CRISP's data and help keep our communities safe?

Mr. Krejsa. Absolutely. The National Labs are jewels of this Nation's ability to do the kinds of technical research, forensic analysis that gives us the information we need to make risk-informed prioritization decisions.

Mrs. Fletcher. Great. Thank you so much.

And, Mr. Chairman, I see I have gone over my time. I appreciate it. And I will yield back. Thank you.

Mr. Weber. The lady yields back.

The gentlelady now from North Dakota is recognized for at least 5 minutes.

Mrs. Fedorchak. Excellent. Thank you, Mr. Chairman.

Thank you, panel, for your time here today and for sharing your expertise with us on this really important subject matter.

I want to focus in on the utilities -- no shock there as a former utility regulator -- starting with Xcel.

You mentioned, Ms. Artz, Xcel's coordination with RTOs and ISOs and participation in the regional planning and resource-sharing arrangements.

Can you briefly, kind of in an overview, describe how these relationships address not necessarily the prevention but the restoration of power in the event that we do have a cyber attack?

Ms. Artz. Thank you for the question.

We recently just hosted the 8th annual GridEx exercise. Xcel Energy had 316 participants this year. Sixty-four of those were external stakeholders that are critical to looking at how we quickly respond and recover from really bad days.

The scenarios that we infuse into the exercise are pretty extreme to get us really thinking about what if we are not able to rely on our traditional tools, the importance of the collaboration in advance of the incidents, and then making sure that we are exercising the actual execution of those response capabilities.

Mrs. Fedorchak. And can you share with me what is different about responding to a cyber attack versus, like, a bad snowstorm or weather-related blackouts and impacts?

Ms. Artz. So I think there are two things.

First, a cyber attack probably is not going to be forecasted. We might get some intelligence from our government partners that there are imminent attacks, but likely the actual occurrence of the attack is not going to be forecasted for us.

Secondly, the cyber attack can render the destruction of equipment similarly to a storm, but then it means that we are not maybe able to trust the device once we get it back into operational mode.

That is why we need information and assistance on ensuring the backups of our systems, that we have access to equipment.

And then I will just note that we, as a company, an industry, are really looking more and more at zero-trust types of environments, knowing that we have to be maybe suspicious of the device, the communication that is coming from it, so that we are operating in a mode or manner that allows us to continue to provide those reliable services.

Mrs. Fedorchak. Then how does Xcel prioritize baseload units in emergency response drills?

Ms. Artz. Congresswoman, I would probably have to get back to you on the exact answer for that question, but we do include all of our energy sources in our security drills.

Mrs. Fedorchak. Sure. Okay. No worries.

Are there emerging AI-related vulnerabilities? And how are you using AI to both

detect and recover? And what other vulnerabilities are being created by AI? Both you and Mr. Lindahl, if you could address that.

Ms. Artz. So we are working with the National Lab complex, with the Department of Energy, on understanding the threats that are posed by AI. We are utilizing AI in our business environments to create efficiencies.

But as with any new technology, in the actual operational environments, we are slow to implement because we want to understand the impact on reliability from these new technologies.

Mr. Lindahl. And the only thing I will add is we are working with vendors independently, but we are also working together with folks like NRECA to develop the AI tools to enhance our grid.

Mrs. Fedorchak. Okay. Very good.

With 1 minute -- well, 30 seconds -- remaining, Mr. Tudor, can you talk about how adversaries are using trusted vendors or software-updated channels to gain access to critical systems? In 20 seconds.

Mr. Tudor. Yeah. Thank you for that question.

So the software-update process, some of the various ways that technologies can be improved can also be another vector for malicious actors.

I believe some of our programs, such as CyTRICS, that will identify those update paths and make sure that they are more secure themselves.

Also several of the different, as I mentioned before, hunt and incident response-type capabilities that the National Labs bring together can also look for some suspicious or malicious update sites and try to take them off and, once again, provide the information to many of the people that are represented here.

Mrs. Fedorchak. Excellent. Thank you all.

Mr. Chairman, I yield back.

Mr. Weber. The gentlelady yields back.

The chair now recognizes the gentleman from California for 5 minutes.

Mr. Mullin. Thank you, Mr. Chair.

And thank you to our witnesses for your testimony today.

Our electric grid is in a moment of generational transformation. After decades of stable energy usage, the rapid growth of data centers and adoption of electric vehicles and appliances are driving a sharp increase in energy demand.

We need to expand our energy infrastructure while ensuring it remains resilient and secure. This moment presents both an enormous opportunity and a significant national security challenge. I believe American innovation can help us seize the opportunity and mitigate the risks.

As digital technologies become more embedded in the grid, it is also exposing our aging infrastructure to increasingly sophisticated threats, such as China's Volt Typhoon, campaign, which many of you have discussed today.

Congress anticipated these challenges when it created the Grid Resilience and Innovation Partnerships, or GRIP, at the Department of Energy, and the Bipartisan Infrastructure Law.

Yet the current administration has said it would cut more than $2 billion, disproportionately targeting Democratic States. At the same time, it proposed a 15 percent budget cut to the Cybersecurity and Infrastructure Security Agency, undermining our collective goal of achieving a more secure and more resilient grid.

With these constraints, we need to ensure faster returns on our national investments in research and development.

Our National Labs are leading groundbreaking work to identify and mitigate security

risks in the energy system. My staff has seen these projects firsthand at Idaho and Lawrence Berkeley National Labs in the Bay Area, but too often there is a gap between lab innovation and commercial deployment on the grid.

So, Mr. Tudor, based on your experience at the Idaho National Lab, what are the most significant barriers preventing grid security innovations from moving quickly from the lab into commercial use by utilities and manufacturers.

Mr. Tudor. Yeah. Thank you for that question. I have worked a very long time on some of the different commercialization aspects in the valley of death that we all experience.

I think that it is hard for National Laboratories, whose primary missions focus around research but also those partnerships, to be able to do the marketing necessary to make commercialization possible, but we do work with some of the new programs within the Department of Energy, the technology transition programs, et cetera, who are providing grants to help those technologies move forward.

We also bring partners in, like the NRECA members, other utilities, to come help us beta test these programs and see for themselves, so we have an advocate that has seen the benefit of one of these programs.

Right now one of the tools that we have developed, called Malcolm, which is an intrusion detection and monitoring and analysis capability that is open source, has been tested and sponsored by many of the utilities, and so we have been able to get that out and make a big impact, I think.

So we have to practice more about how we can do transition, the Department, but also we have to work with our partners to make sure they understand the capabilities we might be able to give them.

Mr. Mullin. Appreciate that, Mr. Tudor.

My next question is, Mr. Krejsa, a bunch of your testimony outlines how China's dominance in manufacturing components like smart inverters and batteries poses a national security risk.

To build long-term American industrial leadership, how should Congress prioritize and sequence its efforts between the near-term need to on-shore existing components and the longer-term investments in next-generation energy technologies?

Mr. Krejsa. Thank you for that question, Congressman. That is, I think, the key question underpinning a lot of this.

I think it is instructive to take a look at the case of the F-35, which does not have zero Chinese-made components. The defense industrial base instead makes a risk-informed prioritization decision about where the cut line is for components sourced from anywhere you can get it, or from the United States, from our allies and partners.

And I think Congress could play an important role in helping catalyze that kind of prioritization among the broader electricity equipment and electrotech field and advanced manufacturing more generally, to help us focus on what the highest-consequence, highest-risk priorities should be that need that urgent scrutiny, and what kinds of sustained industrial investments are going to be necessary to patch those risks.

Mr. Mullin. Appreciate that. Thank you.

And thank you all for your testimony.

And, Mr. Chairman, I yield back.

Mr. Weber. The gentleman yields back.

The chair now recognizes the gentleman from Ohio for 5 minutes.

Mr. Balderson. Thank you, Mr. Chairman.

Thank you all for being here today and how we can secure our critical energy infrastructure. So appreciate your time here.

Two weeks ago, the U.S.-China Economic and Security Review Commission released their 2025 report to Congress. In this report the commission stated: "The extensive use of Chinese components in the U.S. grid creates risks for cyber espionage and sabotage."

As our Nation looks to increase grid resiliency and reliability in the face of historic electricity demand growth, Congress and all relevant energy stakeholders must work to reduce our reliance on foreign adversaries, such as China, to meet our energy needs.

My first question is for Mr. Tudor.

In regards to China, Russia, Iran, and North Korea, you note: "Although the United States is not the only nation in the crosshairs of these advanced, persistent cyber actors, the unique makeup of our critical infrastructures and key resources make us particularly vulnerable."

Can you discuss why the United States is uniquely vulnerable to cyber attacks on our grid.

Mr. Tudor. Yeah. Thank you for that question, Congressman.

I think the first thing is that one of the first major countries to have an electric grid like this -- and we sometimes say that it is the most complex and complete machine in the world -- has been built up over decades and decades, almost a century.

And so as we keep adding new components and keeping old components, those interfaces, as have mentioned before, sometimes become vectors for attack.

Understanding how to and where to update some of these equipments with new technologies which help digitize and provide different benefits, but also may contain some of those components that we are concerned about, also puts us at risk.

I think that we are the leader in understanding cyber risks internationally, and I think that is the other aspect that makes us more of a target. And also, as the number one economy in the world, obviously we are a rich adversary to go after.

Because of the infrastructure not being owned by the Federal Government, by any one entity, but being owned across different types of asset owners, different asset types, also provides a little bit higher risk, and that we all work on protecting all of those different types of assets.

Mr. Balderson. Okay. Thank you for that answer, Mr. Tudor.

You also mentioned that the emergence of AI has shown promise in the ability to enhance grid operations and defend the grid from cyber attacks, but it also introduces risks that could be exploited by cyber attacks.

Can you expand on some of those risks? And how is the Idaho National Lab working with AI stakeholders to address those risks.

Mr. Tudor. Yeah. Thank you again.

AI is not the worst thing that we have seen happen, but it is a powerful new tool for both malicious actors but also for defenders.

As Ms. Artz mentioned before, adapting some of the new technologies is not without risk itself. And so we are working with utilities to understand what actually AI-enabled defensive capabilities that come from vendors may actually do and how they might be subverted; looking at how AI-enabled offensive tools might identify risks in our critical infrastructure, something that we and other National Labs work on as well.

We can't necessarily defend something that we don't understand or don't know where it is coming from. So we are looking at all the capabilities of our adversaries to see where they might apply AI.

And it is a continuous battle. We work on developing understanding of the adversary as well as developing new technologies to work to defend the grid and to reduce risk.

Mr. Balderson. Thank you. Well done.

My last question is for Mr. Lindahl.

As you mentioned, rural electric cooperatives face unique challenges as your infrastructure often covers thousands of square miles with few customers per mile.

Can you discuss the difficulties co-ops might face protecting your rural and remote infrastructure? And how can Congress and relevant Federal agencies support your efforts to protect against physical and cyber attacks to your infrastructures?

Thirty seconds, sir, please. Thank you.

Mr. Lindahl. Yeah. It is a difficult challenge because we are so spread out. But how Congress can help is to continue to fund things that allow the innovation to address these challenges.

So like the RMUC program and other programs like that, Congress can fund those and come together and allow the industry to identify the unique challenges they face and work together to solve those problems.

Mr. Balderson. Thank you very much.

Mr. Chairman, I yield back.

Mr. Weber. The gentleman yields back.

The chair now recognizes the good doctor from Colorado for 5 minutes. Doctor or not, we recognize you.

Mr. Evans. Thank you, Mr. Chair. I am glad to be upgraded to doctor even though I am not, of course, the ranking member.

And then thanks to our witnesses for taking the time today.

My first question will be to Mr. Krejsa.

Did I say that right?

Mr. Krejsa. Krejsa, sir. Thank you.

Mr. Evans. Krejsa. Got it.

You talk about in your testimony how important it is to organize the disparate modern energy and national security stakeholders across public and private sectors. And so I think we have talked about a couple of different facets of that so far in the testimony.

One thing that I wanted to hone in on a little bit, in a previous life I spent 12 years in the U.S. Army in Colorado Army National Guard as a helicopter pilot fighting wildfires.

And so we know that wildfire risk, especially in States like Colorado, which is one of the most at-risk States, has a direct impact on critical infrastructure like energy distribution systems.

And so I would just love to hear your thoughts on things that the Federal Government can do to bring together some of those different actors that are in the immediate response to natural disasters, and then the long-term follow-up, specifically when entities may be facing lawsuits or any other sort of liability that potentially has the capacity to bankrupt, for instance, a rural electric provider.

Mr. Krejsa. Thank you, Congressman, and thank you for your service. I think that is a very important question.

I like to think about the steps we can take, be it the technology, resources, information sharing, to ensure the security and resilience of our infrastructure. Often looks very similar, whether we are talking about a hurricane, a hacker, or a wildfire.

And that is ensuring that we are practicing how to respond, how to anticipate, with the right stakeholders at the Federal, State, and local level along the way.

And the critical role that institutions like the E-ISAC and ETAC and that their sector risk management agencies at Department of Energy, CISA, and elsewhere play in convening all those stakeholders can't be overstated.

This is a complex -- as Mr. Tudor just said -- this is one of the most complex and complete machines in the world that is manned and operated by just many, many

thousands of people with all different kinds of resources, all different kinds of backgrounds and level of expertise.

And the convening power and national leadership function that the Federal Government plays is absolutely critical, just in terms of information but also resourcing and information sharing.

Mr. Evans. Thank you.

Same question to Mr. Lindahl.

I know you represent some of these rural electric co-ops. Natural disasters, immediate response, and then longer term, specifically with thought to, like, some of the insurance and liability questions that emerge in this space.

Mr. Lindahl. Yeah. We deal with equipment. It took us over nearly a hundred years -- or 80 years in our case -- to build our grid. We can't afford to rebuild it overnight.

So we adapt and prepare. And like Mr. Krejsa said, it really makes no difference what the threat is. We need to respond the same, whether it is a wildfire, cybersecurity, physical security incident.

So part of it is we prepare and we have things ready and in place to go should something like that happen.

But then the second part is we really identify how can we get ahead of it, how can we learn from the past and really learn how to mitigate these costs in the future so we don't have those significant costs.

Mr. Evans. Great.

So along kind of similar lines, being able to have that preplanning, to be able to mitigate any sort of major disasters, we just talked about it. I want to switch a little bit to supply chains now.

How can we make sure -- as you said, the grid is 80 to a hundred years old -- how can

we make sure that we are prioritizing either new components or new technology and we also have the supply chain to be able to roll those things out, specifically focusing on things like permitting reform -- that has been a big emphasis of mine -- to make sure that we just have the manufacturing capacity to be able to do things like get newer modern transformers, generating turbines, things of those natures?

Can you speak to the supply chain component of this and what Congress should be focusing on to do that triaging and the prioritization that we previously discussed in the context of F-35s? Thirty-five seconds.

Mr. Lindahl. Yeah. One of the things that we are doing as cooperatives is we partner together, like we do with many things, and we have our own suppliers, and we self-source a lot of our stuff that we actually utilize. And that keeps it in the family. It allows us to have the full control over it.

As far as the government helping us, is really vetting those components that are coming in. We don't have the ability to really understand the threats that are coming in from overseas or the threats even from within our own walls.

How can Congress put into place, through the National Labs and other partners, to do that vetting on our behalf? Because we don't have the ability to do that ourselves.

Mr. Evans. Thank you. Yield back.

Mr. Weber. The gentleman yields back.

Now the chair recognizes the good doctor from Pennsylvania for 5 minutes.

Mr. Joyce. Thank you, Mr. Chairman, and thank you for holding this important hearing today.

This year our committee has discussed at length how critical an affordable and reliable grid actually is. Much of this conversation has been focused on how we can improve the generation, the transmission, and the distribution of electricity to support all of

America's energy needs and to spur the economic and technologic growth necessary to compete with our adversaries.

As electricity and the demand for it continues to grow, and as we build out more infrastructure to support this demand, securing the grid against both cyber and physical threats, these will both become even more challenging.

Building up necessary energy infrastructure is the first step in reliability, but keeping it operational, in spite of numerous State and criminal actors who see our electrical grid as a target, will be a continuous and an ongoing challenge.

Each technological advancement used to enhance the grid or new piece of infrastructure that is brought online represents a new vulnerability for threat actors to target the political or financial gain that might be achieved.

I represent an incredibly beautiful rural area in Pennsylvania which provides unique challenges to both cyber and physical grid security.

Mr. Lindahl, how can we ensure that we are utilizing the more limited resources in rural areas to identify and secure the infrastructure which is most vulnerable to attack and most critical to keep online?

Mr. Lindahl. I think through partnerships. One of the things we do well as cooperatives is we proactively take a look at what we can do to solve it, but then we also have the reactive approach.

So we work, and it is quite evident when you see a hurricane come through Florida, let's say. We have a mutual aid system set up, that we send folks down and help restore power in Florida.

We have similar things set up with a lot of our equipment manufacturers and transformers and things like that nature.

So that helps us mitigate when stuff does happen.

Mr. Joyce. In central Pennsylvania, we see that cooperation with our rural electric co-ops. They are incredibly interactive and incredibly cooperative, whether in the face of emergency or in the day-to-day activities that they provide.

Mr. Lindahl. That is right.

Mr. Joyce. How can the coordination and information sharing that you talk about between rural electric co-ops, like yours, help those with limited resources to function more effectively?

Mr. Lindahl. So one of the things that we have talked about and I talked about in my testimony was funding programs like RMUC, the Rural Municipal Cybersecurity Program, because that helps us develop collectively the tools that we can. And we can share the knowledge and information from the larger cooperatives down to the smaller cooperatives, and it really allows us to share those resources among, no matter your size.

Mr. Joyce. Do you feel that any regulatory or knowledge barriers currently exist that make proactive coordination that you are talking about in advance of threats more difficult? And is there action that this committee specifically, or Congress in general, should take to remedy such barriers?

Mr. Lindahl. My caution would be, as we develop the regulatory environment, especially around physical and cyber, that we don't stifle the innovation to address the threat today and tomorrow.

Mr. Joyce. Boy, I am so glad you teed up innovation because I think that is so important. So I am going to move my questioning to Mr. Tudor.

In your testimony, you referred to unmanned aerial systems and the testing of that. At Johnstown Airport in Pennsylvania, in my district, Dr. Larry Nulton, through his group Aerium, is working to grow the UAS pilot workforce and advance UAS innovation. You and I recognize how important that can be.

Can you elaborate on how you see UAS integration as a way to improve grid security, and how the training of a UAS workforce can prepare individuals for these security applications, as is currently going on right now in Johnstown, Pennsylvania.

Mr. Tudor. Thank you for your question, Congressman Joyce.

So training in all of these critical areas is something that is near and dear to my heart, as well as innovation, as you mentioned.

We have a UAS and counter-UAS capability at the Idaho National Lab in that 890-square mile, working with such as those, to help look at specific use cases. And one of those is the ability to look at different critical infrastructures and whether it is for overgrown vegetation or concentration.

So having those capabilities, using those UASs to help protect critical infrastructure is one of the early use cases, and I think it will continue to be a use case for them.

Mr. Joyce. Securing our electrical grid against threats, we all recognize, is critical, and we need to explore that even further.

I look forward to working with this committee to ensure that America maintains the most reliable grid, the safest grid that is possible.

Thank you, Mr. Chairman, and I yield.

Mr. Weber. The gentleman yields back.

And the chair now recognizes himself for at least 5 minutes.

Thank you all for being here.

Moore County, North Carolina, attack in December of 2022, you all are familiar with that. We were out there with the committee. We saw 27 shell casings on the ground. You are talking about a high-powered rifle.

And we watched, we looked at it very carefully and very closely. Every single round was put in this far down from the transformer so they could drain the oil. Then they had

an oil tank that held, I don't know what the -- 250 gallons -- had two rounds put in it.

They knew exactly what they were doing. They didn't go there and just start shooting the place up.

So when we talk about hardening the grid, are we talking about higher walls? Are we talking about getting that facility off away from the beaten path, as the poet once wrote? Are we talking about having security there 24/7? Ideas to protect these substations?

Mr. Ball, we will start with you.

Mr. Ball. Well, thank you for that question, and certainly that concern has plagued us for many years. Our industry has seen it even with vandalism for that matter.

But just all the way back to the Metcalf Substation attack where there was a very purposeful and knowledgeable attack on -- physical attack on a substation, which had some significant implications, and I think we saw that flare up.

I think what we need -- I don't think you can build a wall tall enough. I don't think we can afford the costs necessary to harden that infrastructure to prevent against ballistic attacks when there are other attack scenarios such as drones.

RPTR HNATT

EDTR CRYSTAL

[1:34 p.m.]

Mr. Weber. You can shoot those down if you have the experts there.

Mr. Ball. If you have the expert and the authority.

Mr. Weber. You can get those experts from Texas, by the way.

Mr. Ball. Yeah. Yeah. Yeah.

I couldn't foot stomp enough, but I think we just -- there are a lot of different threats to -- physical threats to a substation.

And, again, while you have ballistic attacks as a legitimate concern, also drones do pose a real concern for industry. And I think that is another area where we need to put some focus on, which is unlocking the capabilities.

Mr. Weber. Mr. Lindahl, since you are in the business you are in, what say you?

Mr. Lindahl. Yeah. So I think there is a lot of low-hanging fruit that we can do before we build walls to actually stop everything, and a wall won't stop absolutely everything either.

Mr. Weber. Sure.

Mr. Lindahl. Things we are looking at from a policy perspective, really not putting our infrastructure out there where people can easily access what it is and where it is and what it does, those are some simple things we can do.

What we are doing at Kenergy is part of the reason we are building our fiber network, is so that we have better insight, better monitoring of our system, and we can have quicker and more accurate response and maybe hopefully catch things sooner than later.

Mr. Weber. Last I heard there was a move for a different kind of transformer that

was in very, very short supply. Is that still the case where the government is mandating different transformers, or was that just under Biden?

Not ringing a bell?

Mr. Lindahl. Yeah. There was a push to use a different type of steel that was going to kind of struggle for us to keep up with manufacturing on the smaller transformers, in particular.

For the ones that take the actual time, we are talking about the big substation transformers, those I don't believe were in that bill.

Mr. Weber. Okay. But smaller transformers still all good. Okay.

Mr. Lindahl. We are good.

Mr. Weber. Good.

A couple things we have been talking about, when Mr. Peters was here doing his 5 minutes he talked about wildfire risks.

So, Ms. Artz, I am going to come to you.

Wildfires can't just be in California. There have got to be other areas. How widespread is that?

Ms. Artz. So we are seeing increased risks from wildfire across our entire service territory. Being here in Washington, D.C., we saw the smoke from the Canadian wildfires a couple summers ago.

So it is something that all utilities are working collectively on, risk mitigation best practices, sharing that information. We are investing in technologies to better detect when fires are ignited.

And then we are actively working with our government partners on access to the rights of way to do the vegetation management we need to do to minimize those risks.

Mr. Weber. Okay. Thank you.

Now, the next question I have is about data centers.

Has anybody come up with a concise guesstimate of how much power is going to be needed?

I will start with you, Mister -- is it -- say your last name.

Mr. Krejsa. Krejsa, sir.

Mr. Weber. That is what I would have said.

Mr. Krejsa. It is a very large amount. I think there is some question about precisely how much, but we are going to need more power than we have now, and more flexibility than our grid currently provides.

Mr. Weber. Okay. Then I am going to go one more place before I yield to the gentleman from Michigan in just a minute, and that is this.

Is anybody calculating what the United States population is going to look like in 4 to 5 years when all this stuff comes to fruition? Anybody? Do we know what the population is going to be? Are there any guesstimates that have been kind of mixed in with this discussion?

Mr. Ball?

Mr. Ball. I can't say that I have.

Mr. Weber. There is time.

Ms. Artz?

Ms. Artz. We work very closely as a regulated utility with our State regulators and other stakeholders and inject a lot of information in thinking through that resource planning that we need to do, but I don't know off the top of my head if it includes population.

Mr. Weber. Mr. Lindahl?

Mr. Lindahl. I don't have that information.

Mr. Weber. Mr. Krejsa.

Mr. Krejsa. I can speculate that it is probably not vastly different in 5 years, but potentially more after that.

Mr. Weber. I think you are on to something there. It is going to be a lot more.

Mr. Tudor?

Mr. Tudor. No, I don't believe from -- I don't know that number, but I know that in a lot of the calculations and the answer is a very large number. The growing population is also included in that.

Mr. Weber. Just an interesting thought that popped up into my head listening to all this, all the discussion we are having.

Thank you all for being here.

Now the gentleman from Michigan is recognized for 5 minutes.

Mr. James. Thank you, Mr. Chairman.

Michigan families are already paying the price for an energy policy that is based more on fantasy than on physics. Reserve margins are tightening, reliability warnings are increasing, and we are watching generational assets that were scheduled for retirement get pulled back into service because Democrats were more focused on solar and wind than nuclear and natural gas. The system cannot absorb the loss.

The Campbell plant in Michigan is a perfect example. It was slated to shut down, but Americans could not afford to lose that reliable, dispatchable power.

Now FERC is reviewing whether Michigan ratepayers should be compensated for the burdens of cost created by keeping this plant open and avoiding unavoidable brownouts for the rest of the region. We are continuing to work with those organizations here to make sure that Michiganders do not shoulder that burden alone.

That tells us something very clear despite these facts. We are not transitioning from strength. We are backfilling reliability gaps created by policy decisions that ignored

the operational realities of the grid.

Yet Governor Gretchen Whitmer continues to push aggressive net-zero mandates that force early retirement of dependable baseload generation, increased dependence on weather-driven imports, and accelerate deployment of complex digital systems that add new vulnerabilities without strengthening the backbone of the grid.

At the same time, the technologies being deployed under these mandates -- solar inverters, EV chargers, battery systems -- are far more digitally connected than traditional generation.

They increase the number of access points adversaries like the PRC can exploit, and they expand the cyber attack surface at the moment when the threat environment is becoming ever more aggressive, not less.

So my concern today is straightforward. Michigan is being pushed into a high-cost, high-risk energy future before the grid is ready, before cybersecurity standards have caught up, and before consumers have real protections in place.

We need clear answers on reliability impact, the cyber vulnerability, and the financial burden being placed on families.

Mr. Ball, in your view, are these rushed net-zero polices creating both higher costs for families and greater cyber exposure for the grid and at the very moment that we are changing course?

Mr. Ball. To be candid, I don't have enough contextual understanding to be able to give an affirmative or negative answer to that, but I admit that it is a very significant issue.

Mr. James. Okay. Well, then a net-zero technology such as solar inverters, EV chargers, battery systems, and similar technologies, does accelerated deployment of these devices expand the attack services for adversaries such as the PRC?

Mr. Ball. Absolutely.

Mr. James. And based on current threat levels, are today's NERC standards sufficient to manage this increased digital exposure, or are we adding technology faster than we can secure it?

Mr. Ball. Well, I can say that you can't look at the regulations or the standards to be completely comprehensive, but I can say that NERC on that side of the house is actively looking for more agile and adaptive standards-writing to adapt to the changes that are happening.

So I know there is attention to that, but I would have to provide additional detail at a later time on what they are doing.

Mr. James. Thank you.

Continuing to strive toward a greater, more sustainable, and affordable energy future is in all of our best interests, but we must remain focused on the reality at hand while we strive toward a brighter future.

Mr. Chairman, I will cede the balance of my time.

Mr. Weber. The gentleman yields back.

I would like to thank all of the witnesses for being here today. Members may have additional written questions for you all. That is a Texas term.

I will remind members they have 10 business days to submit additional questions for the record, and I ask that witnesses please do your best to submit responses within 10 business days upon receipt of the questions.

So I ask unanimous consent to insert into the record the documents included on the staff hearing documents list.

Without objection, so ordered.

[The information follows:]

2700 ******** COMMITTEE INSERT ********

Mr. Weber. Without objection, the subcommittee is adjourned.

[Whereupon, at 1:42 p.m., the subcommittee was adjourned.]