

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

---

## HEARING BEFORE THE SUBCOMMITTEE ON ENERGY OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED NINETEENTH CONGRESS FIRST SESSION

DECEMBER 2, 2025

**Serial No. 119–45**



Published for the use of the Committee on Energy and Commerce  
[govinfo.gov/committee/house-energy](https://govinfo.gov/committee/house-energy)  
[energycommerce.house.gov](https://energycommerce.house.gov)

U.S. GOVERNMENT PUBLISHING OFFICE

62–367 PDF

WASHINGTON : 2026

## COMMITTEE ON ENERGY AND COMMERCE

BRETT GUTHRIE, Kentucky  
*Chairman*

|                                             |                                    |
|---------------------------------------------|------------------------------------|
| ROBERT E. LATTA, Ohio                       | FRANK PALLONE, JR., New Jersey     |
| H. MORGAN GRIFFITH, Virginia                | <i>Ranking Member</i>              |
| GUS M. BILIRAKIS, Florida                   | DIANA DeGETTE, Colorado            |
| RICHARD HUDSON, North Carolina              | JAN SCHAKOWSKY, Illinois           |
| EARL L. "BUDDY" CARTER, Georgia             | DORIS O. MATSUI, California        |
| GARY J. PALMER, Alabama                     | KATHY CASTOR, Florida              |
| NEAL P. DUNN, Florida, <i>Vice Chairman</i> | PAUL TONKO, New York               |
| DAN CRENSHAW, Texas                         | YVETTE D. CLARKE, New York         |
| JOHN JOYCE, Pennsylvania                    | RAUL RUIZ, California              |
| RANDY K. WEBER, SR., TEXAS                  | SCOTT H. PETERS, California        |
| RICK W. ALLEN, Georgia                      | DEBBIE DINGELL, Michigan           |
| TROY BALDERSON, Ohio                        | MARC A. VEASEY, Texas              |
| RUSS FULCHER, Idaho                         | ROBIN L. KELLY, Illinois           |
| AUGUST PFLUGER, Texas                       | NANETTE DIAZ BARRAGÁN, California  |
| DIANA HARSHBARGER, Tennessee                | DARREN SOTO, Florida               |
| MARIANNETTE MILLER-MEEKS, Iowa              | KIM SCHRIER, Washington            |
| KAT CAMMACK, Florida                        | LORI TRAHAN, Massachusetts         |
| JAY OBERNOLTE, California                   | LIZZIE FLETCHER, Texas             |
| JOHN JAMES, Michigan                        | ALEXANDRIA OCASIO-CORTEZ, New York |
| CLIFF BENTZ, Oregon                         | JAKE AUCHINCLOSS, Massachusetts    |
| ERIN HOUCHIN, Indiana                       | TROY A. CARTER, Louisiana          |
| RUSSELL FRY, South Carolina                 | ROBERT MENENDEZ, New Jersey        |
| LAUREL M. LEE, Florida                      | KEVIN MULLIN, California           |
| NICHOLAS A. LANGWORTHY, New York            | GREG LANDSMAN, Ohio                |
| THOMAS H. KEAN, JR., New Jersey             | JENNIFER L. McCLELLAN, Virginia    |
| MICHAEL A. RULLI, Ohio                      |                                    |
| GABE EVANS, Colorado                        |                                    |
| CRAIG A. GOLDMAN, Texas                     |                                    |
| JULIE FEDORCHAK, North Dakota               |                                    |

---

### PROFESSIONAL STAFF

MEGAN JACKSON, *Staff Director*  
SOPHIE KHANAHMADI, *Deputy Staff Director*  
TIFFANY GUARASCIO, *Minority Staff Director*



SUBCOMMITTEE ON ENERGY

ROBERT E. LATTA, Ohio

*Chairman*

RANDY K. WEBER, SR., TEXAS, *Vice*  
*Chairman*

GARY J. PALMER, Alabama

RICK W. ALLEN, Georgia

TROY BALDERSON, Ohio

AUGUST PFLUGER, Texas

DIANA HARSHBARGER, Tennessee

MARIANNETTE MILLER-MEEKS, Iowa

JOHN JAMES, Michigan

CLIFF BENTZ, Oregon

RUSSELL FRY, South Carolina

LAUREL M. LEE, Florida

NICHOLAS A. LANGWORTHY, New York

MICHAEL A. RULLI, Ohio

GABE EVANS, Colorado

CRAIG A. GOLDMAN, Texas

JULIE FEDORCHAK, North Dakota

BRETT GUTHRIE, Kentucky (ex officio)

KATHY CASTOR, Florida

*Ranking Member*

SCOTT H. PETERS, California

ROBERT MENENDEZ, New Jersey

KEVIN MULLIN, California

JENNIFER L. McCLELLAN, Virginia

DIANA DeGETTE, Colorado

DORIS O. MATSUI, California

PAUL TONKO, New York

MARC A. VEASEY, Texas

KIM SCHRIER, Washington

LIZZIE FLETCHER, Texas

ALEXANDRIA OCASIO-CORTEZ, New York

JAKE AUCHINCLOSS, Massachusetts

FRANK PALLONE, JR., New Jersey (*ex*  
*officio*)



## C O N T E N T S

|                                                                            | Page |
|----------------------------------------------------------------------------|------|
| Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, |      |
| opening statement .....                                                    | 1    |
| Prepared statement .....                                                   | 4    |
| Hon. Kathy Castor, a Representative in Congress from the State of Florida, |      |
| opening statement .....                                                    | 6    |
| Prepared statement .....                                                   | 8    |
| Hon. Brett Guthrie, a Representative in Congress from the Commonwealth     |      |
| of Kentucky, opening statement .....                                       | 10   |
| Prepared statement .....                                                   | 12   |
| Hon. Frank Pallone, Jr., a Representative in Congress from the State of    |      |
| New Jersey, opening statement .....                                        | 14   |
| Prepared statement .....                                                   | 16   |

### WITNESSES

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Michael Ball, Chief Executive Officer, Electricity Information Sharing and    |     |
| Analysis Center, and Senior Vice President, North American Electric Reli-     |     |
| ability Corporation .....                                                     | 18  |
| Prepared statement .....                                                      | 21  |
| Answers to submitted questions .....                                          | 218 |
| Sharla B. Artz, Area Vice President, Security and Resilience Policy, Xcel     |     |
| Energy .....                                                                  | 40  |
| Prepared statement .....                                                      | 42  |
| Answers to submitted questions .....                                          | 222 |
| Tim Lindahl, President and Chief Executive Officer, Kenergy Corp. ....        | 54  |
| Prepared statement .....                                                      | 56  |
| Answers to submitted questions .....                                          | 225 |
| Harry Krejsa, Director of Studies, Carnegie Mellon Institute for Strategy     |     |
| & Technology .....                                                            | 64  |
| Prepared statement .....                                                      | 66  |
| Answers to submitted questions .....                                          | 226 |
| Zachary Tudor, Associate Laboratory Director, Idaho National Laboratory ..... | 76  |
| Prepared statement .....                                                      | 78  |
| Answers to submitted questions .....                                          | 229 |

### SUBMITTED MATERIAL

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| <i>Inclusion of the following was approved by unanimous consent.</i>          |     |
| List of documents submitted for the record .....                              | 145 |
| Letter of November 14, 2025, from Mr. Pfluger, et al., to Howard Lutnick,     |     |
| Secretary of Commerce .....                                                   | 146 |
| Letter of December 2, 2025, from Digital Power Network to Mr. Guthrie,        |     |
| et al. ....                                                                   | 152 |
| Letter of December 1, 2025, from Desmarie Waterhouse, Senior Vice Presi-      |     |
| dent, Advocacy and Communications and General Counsel, American Public        |     |
| Power Association, to Mr. Latta, et al. ....                                  | 155 |
| Report of ANTHROPIC, “Disrupting the first reported AI-orchestrated cyber     |     |
| espionage campaign,” November 2025 .....                                      | 160 |
| Article of October 20, 2025, “As cyber threats grow, utilities say lapsed     |     |
| information-sharing law stymies security,” by Robert Walton, Utility Dive ..  | 174 |
| Report of the Office of the Director of National Intelligence, “Annual Threat |     |
| Assessment of the U.S. Intelligence Community,” March 2025 .....              | 178 |
| Article of February 18, 2024, “FBI Director Says China Cyberattacks on        |     |
| U.S. Infrastructure Now at Unprecedented Scale,” by Joe Parkinson and         |     |
| Drew Hinshaw, The Wall Street Journal .....                                   | 209 |

# VI

|                                                                                                                               | Page |
|-------------------------------------------------------------------------------------------------------------------------------|------|
| Article of November 23, 2025, “The First Large-Scale Cyberattack by AI,”<br>by Nury Turkel, The Wall Street Journal .....     | 212  |
| Letter of December 2, 2025, from Desmond Wheatley, Chief Executive Officer,<br>Beam Global, to Mr. Latta and Ms. Castor ..... | 215  |

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

**TUESDAY, DECEMBER 2, 2025,**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON ENERGY,  
COMMITTEE ON ENERGY AND COMMERCE,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:33 a.m., in room 2141, Rayburn House Office Building, Hon. Robert E. Latta (chairman of the subcommittee) presiding.

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

Also present: Representative Joyce.

Staff present: Clara Cargile, Professional Staff Member, Energy; Andrew Furman, Professional Staff Member, Energy; Sydney Greene, Director of 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; Joel Miller, Chief Counsel; Ben Mullaney, Press Secretary; 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; 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.

### **OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO**

Again, good morning again, and welcome to today's hearing. We will examine how the electric industry is adjusting cyber and phys-

ical 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 prepositioned 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 cooperatives 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, pro-

vides 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.

[The prepared statement of Mr. Latta follows:]

**Chairman Robert Latta**  
**Opening Statement—Subcommittee on Energy**  
**“Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid”**  
**December 2, 2025**  
*As prepared for delivery*

Good morning and welcome to today’s hearing. We will examine how the electric industry is addressing cyber and physical threats to the electric grid—a key component of our nation’s critical energy infrastructure.

We will look at the challenges to securing this infrastructure at a time of tremendous growth in power demand.

This hearing will help 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 power in our electric grid without adequate replacement. This has resulted in increased blackout risks 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 cyber or physical attacks can have widespread, devastating impacts, which makes security particularly vital to our nation’s security, economy, our health, and welfare.

Addressing these threats is difficult. The avenues for malicious attack only increase with increased digitization, and the 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.

As the public security assessments note, the nation faces an evolving landscape of threats – from nation states to criminal and ideologically 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 two 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' particular capabilities, resources, and access to threat intelligence and other information.

Our witnesses this morning can help us understand how the industry works to overcome these challenges.

We'll hear testimony from grid executives representing both investor-owned utilities and the nonprofit Cooperatives—which together cover the bulk of American electric infrastructure.

We'll 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'll hear from a grid security expert at Carnegie Mellon who has been active on the National Security Council.

And, finally, we'll hear from the Associate Laboratory Director for national security at Idaho National Laboratory. He can provide insights into threats and into 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 risks 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.

Mr. LATTA. 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.

**OPENING STATEMENT OF HON. KATHY CASTOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA**

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 canceled 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.

Canceled 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 subtransmission 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.

[The prepared statement of Ms. Castor follows:]

**Committee on Energy and Commerce**

**Opening Statement as Prepared for Delivery  
of  
Subcommittee on Energy  
Ranking Member Kathy Castor**

***Hearing on “Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid”***

**December 2, 2025**

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. Unfortunately, the Trump Administration is taking us backwards, keeping us wedded to the technologies of the past that are insufficient to meet modern threats, or power next-generation innovations like artificial intelligence.

For example, the current Department of Energy terminated billions of dollars for projects meant to reduce the frequency and duration of blackouts and help utilities restore power faster. One energy expert who previously consulted with the DOE 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 canceled 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, allowing faster response to outages or changes in output from power plants, and developing microgrids – localized systems that can operate independently during outages – which really hit home last year when many businesses and neighbors went without power for days after hurricanes Helene and Milton.

Canceled projects are estimated to total \$724.6 million in 24 states. For example, a \$19.5 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. Microgrid projects in New York, New Mexico and Hawaii would have kept essential services running during disasters, cyberattacks and planned power outages.

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. Today, China dominates this sector – they are electrifying, while America recently has taken an offramp. Electrification in the U.S. is stuck at just over 20%. China is electrifying at 10

December 2, 2025

Page 2

percentage points a decade. They're now at 30% and heading for 35%. And as a result, they're reaping the geopolitical benefits of being able to sell these technologies abroad. In August, China exported \$20 billion in clean technology exports. For comparison, the US exported about \$1.3 billion in liquified natural gas that month.

We cannot win the AI race of the 21st century while limiting ourselves to a 20th century energy policy playbook. As this committee has heard from witnesses repeatedly, we need to rapidly deploy grid-enhancing technologies, scale energy efficiency, and support virtual power plants. While doing so, we can make our grid more flexible and resilient, both to physical dangers and malicious cyber threats. Traditionally, our grid was established with a few, large-scale fossil-based electricity 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. If done properly, we can replace our outdated energy systems with software-enabled clean energy technologies. Modern tools allow the grid to recover more readily when harmed by a hurricane or a hacker that takes down a portion of the grid. We can use smart inverters, grid-forming technologies, and batteries to restabilize, or if necessary, quarantine a portion of the grid.

During Hurricane Milton last year, more than 600 well pumps failed in Hillsborough County due to the loss of power, leaving neighborhoods underwater. While parts of our grid took weeks to restore, solar and storage-equipped households never lost power. Good investments don't just make our grid stronger – they also make it smarter. We need more than stronger poles and wires. We need a more intelligent system that uses smart switches, sensors, and digital twins.

To support our utilities and co-ops that are deploying these technologies, we need modern regulatory structures and standards. We need better visibility into local grid architecture to optimize grid planning. And we need to prioritize the parts of our energy supply chain that pose the biggest security risks – like software management systems and inverters.

Securing our electric grid is a bipartisan national security imperative. Congress created several cybersecurity programs at DOE through the Bipartisan Infrastructure Law. It's imperative that we continue to support these efforts with sufficient funds and robust staffing. Plus, let's 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 our witnesses today about how we can get the United States back on track – so we can deliver the safer, cheaper, and cleaner energy.

I yield back.

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.

**OPENING STATEMENT OF HON. BRETT GUTHRIE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY**

Mr. GUTHRIE. 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, the facilities and technologies that Americans rely on for work, healthcare, or financial 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 sow 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, an electric cooperative 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 to also 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. Daviess and Hancock are the counties for those cities I mentioned.

So cooperatives 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.

[The prepared statement of Mr. Guthrie follows:]

**Chairman Brett Guthrie**  
**Opening Statement—Subcommittee on Energy**  
**“Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid”**  
**December 2, 2025**  
*As prepared for delivery*

Good morning and welcome to today’s hearing. We will examine how the electric industry is addressing cyber and physical threats to the electric grid—a key component of our nation’s critical energy infrastructure.

We will look at the challenges to securing this infrastructure at a time of tremendous growth in power demand.

This hearing will help 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 power in our electric grid without adequate replacement. This has resulted in increased blackout risks 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 cyber or physical attacks can have widespread, devastating impacts, which makes security particularly vital to our nation’s security, economy, our health, and welfare.

Addressing these threats is difficult. The avenues for malicious attack only increase with increased digitization, and the 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.

As the public security assessments note, the nation faces an evolving landscape of threats – from nation states to criminal and ideologically 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 two 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' particular capabilities, resources, and access to threat intelligence and other information.

Our witnesses this morning can help us understand how the industry works to overcome these challenges.

We'll hear testimony from grid executives representing both investor-owned utilities and the nonprofit Cooperatives—which together cover the bulk of American electric infrastructure.

We'll 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'll hear from a grid security expert at Carnegie Mellon who has been active on the National Security Council.

And, finally, we'll hear from the Associate Laboratory Director for national security at Idaho National Laboratory. He can provide insights into threats and into 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 risks 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.

Mr. GUTHRIE. 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.

**OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY**

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 rela-

tionships 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 administration has hobbled our efforts to reshore 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.

[The prepared statement of Mr. Pallone follows:]

**Committee on Energy and Commerce**

**Opening Statement as Prepared for Delivery  
of  
Full Committee Ranking Member Frank Pallone, Jr.**

***Hearing on “Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid”***

**December 2, 2025**

I’m 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. It is December – we should be having hearings like this regularly rather than annually.

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 systems are only growing, whether it 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. 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.

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. 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.

That is why today’s hearing is so important. While 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 we can raise against them. We must be in a state of constant evolution.

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.

While agencies under the Department of Homeland Security can play an important convening role, it is DOE, 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. We saw this in the aftermath of the Colonial Pipeline cyberattack when DOE took the lead on the federal response. I look forward to hearing about some of the work that DOE is doing in bringing together the energy industry to talk about threats that impact everyone.

However, none of this works at DOE unless the agency is properly staffed and has the resources to fulfill its mission. DOE lost more than 3,500 staff this year as a result of Secretary Wright and DOGE’s

December 2, 2025

Page 2

reckless and relentless attacks on federal workers. We need to ensure that we have sufficient staff working on cybersecurity at DOE, and that they get the resources and funding they need.

When I was Chair of this Committee in 2021, we passed a law establishing a number of cybersecurity programs at DOE and the Federal Energy Regulatory Commission (FERC). 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.

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 ten months, the Trump Administration has hobbled our efforts to reshore manufacturing in America, increasing tariffs and slashing tax credits that were designed to make American manufacturing competitive. As a result, we are more dependent than ever on foreign sources for critical infrastructure components – a vulnerability that could turn into a devastating weakness if we do not work to reverse it. I hope to hear ideas on how we can turn this around today.

Thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. LATTI. 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 resilient—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, CHIEF EXECUTIVE OFFICER, ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER, AND SENIOR VICE PRESIDENT, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION; SHARLA B. ARTZ, AREA VICE PRESIDENT, SECURITY AND RESILIENCE POLICY, XCEL ENERGY; TIM LINDAHL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, KENERGY CORP.; HARRY KREJSA, DIRECTOR OF STUDIES, CARNEGIE MELLON INSTITUTE FOR STRATEGY & TECHNOLOGY; AND ZACHARY TUDOR, ASSOCIATE LABORATORY DIRECTOR, 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 bulletins 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:]



Testimony of Michael Ball  
Chief Executive Officer, Electricity Information Sharing and Analysis Center,  
and Senior Vice President, North American Electric Reliability Corporation

Before the Subcommittee on Energy,  
U.S. House Committee on Energy and Commerce

“Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid”  
December 2, 2025

#### **SUMMARY OF TESTIMONY**

##### **E-ISAC Role and Mission**

The E-ISAC, operated by NERC since 1999, serves as the central clearinghouse for security information for the North American electricity industry. Its mission is to reduce cyber and physical security risks by sharing trusted, timely, credible, and actionable information and analysis with over 1,900 member and partner organizations. The E-ISAC operates a 24/7 watch operation and collaborates closely with various U.S. government departments (DOE, DHS, FERC, FBI) and cross-sector partners (oil, natural gas, water).

The E-ISAC's information sharing is voluntary and organizationally isolated from NERC's enforcement programs to maintain trust. NERC also enforces mandatory Critical Infrastructure Protection (CIP) standards, which complement E-ISAC activities by providing a universal foundation for security measures such as access controls, malware prevention, incident response, physical protections, and supply chain risk management.

##### **Key Programs and Partnerships**

The E-ISAC utilizes several programs to enhance grid security and situational awareness:

- **E-ISAC Portal, Bulletins, and Alerts:** A secure portal and alert system communicate threat warnings, mitigations, and analytical products, sometimes requiring mandatory industry responses to implementing mitigations.
- **Cybersecurity Risk Information Sharing Program (CRISP):** A premier partnership with DOE that leverages national laboratory analysis to provide unique, government-informed cyber threat intelligence, with participants covering over 90% of U.S. customers.
- **Energy Threat Analysis Center (ETAC):** A new DOE-led initiative where E-ISAC partners meet regularly to collaborate on operational intelligence and industry context for the intelligence community.
- **Training and Exercises:** The E-ISAC hosts workshops on physical security methodologies, the biennial GridEx exercise (largest grid security exercise in North America), and GridSecCon, an annual conference for industry and government experts.
- **Vendor Affiliate Program:** A program bringing original equipment manufacturers and security solution providers into the community to facilitate information sharing regarding supply chain risks.

### The Threat Landscape

While no loss of load has been attributed to a cyberattack to date, the threat landscape is dynamic and requires continuous vigilance. Nation states, sophisticated criminal actors, and hacktivists pose persistent and evolving threats.

- **Nation-State Actors:**
  - **China:** Salt Typhoon and Volt Typhoon are some of the largest and most dynamic threats, focusing on persistent access and espionage with the potential for future disruption.
  - **Russia:** Focus remains primarily on Ukraine and NATO affiliates, utilizing hacktivist groups and cyber espionage, but tactics could be adapted for North America.
  - **Iran:** Monitored for potential retaliation against U.S. infrastructure amid tensions, often using DDoS attacks.
  - **North Korea:** Deploys thousands of IT operatives using fabricated personas and AI tools to secure remote jobs in North American companies to gain high-level network access.
- **Other Threats:** The E-ISAC monitors domestic hacktivists mentioning physical attacks and persistent ransomware operations.

### Recommendations for Congress

- **Authorize ETAC:** Provide congressional authorization for the DOE-led Energy Threat Analysis Center to establish the partnership and advance its mission.
- **Support Funding for CRISP +30 and ONG Programs:** Ensure sufficient funding for programs that help smaller utilities and oil/natural gas companies access critical intelligence and improve situational awareness.
- **Reauthorize CISA 2015:** Reauthorize the Cybersecurity Information Sharing Act of 2015 to support the broader information sharing ecosystem between the private sector and government.

### INTRODUCTION

Thank you, Chairman Latta, Ranking Member Castor, and members of the subcommittee. I am pleased to testify today concerning threats to the security of the nation's electric grid. As chief executive officer of the Electricity Information Sharing and Analysis Center (E-ISAC), a division of the North American Electric Reliability Corporation<sup>1</sup> (NERC), I appreciate the subcommittee's

---

<sup>1</sup> NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system (BPS) through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight in the United States by the Federal Energy Regulatory

interest in examining the highly complex and continuously evolving threat environment, and actions to address security risks. Reliable delivery of electricity is essential to every aspect of life in the United States. While there has been no loss of load to date in North America that can be attributed to a cyber attack, grid security requires continuous vigilance and agility. The E-ISAC plays an important role in helping protect the grid from malicious cyber and physical threats. This testimony will summarize these E-ISAC activities and the current threat landscape.

**About the E-ISAC – Key Programs and Partnerships**

Operated by the NERC and created in 1999, the E-ISAC serves as the clearinghouse for security information for the electricity industry in North America. The mission of the E-ISAC is to reduce cyber and physical security risk to the electricity industry across the continent by providing unique insights, leadership, and collaboration. It accomplishes this mission by sharing trusted information and quality analysis in a timely, credible, and actionable manner with asset owners and operators across the continent to mitigate complex, constantly evolving threats to the grid.

The E-ISAC operates a 24/7 watch operation, develops expert in-house analysis of ongoing incidents, and provides a suite of analytical products and services accessible through the secure E-ISAC Portal to over 1,900 member and partner organizations. E-ISAC membership represents more than 85% of the meters in North America and includes a range of utilities of all sizes and types. The E-ISAC plays a key role in cross-sector coordination, engaging with sectors and their ISACs that have a critical interdependence with electricity, including oil, natural gas, and water,

---

Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves nearly 400 million people.

and other critical infrastructure sectors, such as finance and communications. We work in collaboration with these cross-sector partners to break down information sharing silos between industry and government to promote broad awareness of threats and mitigations.

We collaborate closely with the Department of Energy (DOE), the Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the National Counterterrorism Center (NCTC), the Department of Defense (DoD), and the Federal Bureau of Investigation (FBI). NERC also works closely with the Electricity Subsector Coordinating Council<sup>2</sup> (ESCC) to further partnerships that are vital to addressing security.

The E-ISAC is organizationally isolated from NERC's enforcement program to facilitate and maintain a culture of voluntary information sharing and trust. NERC and the E-ISAC adhere to a strict Code of Conduct. NERC's regulatory programs complement the E-ISAC's activities to strengthen grid security. North America's high voltage electric transmission system is subject to a suite of mandatory cyber and physical security standards, known as the Critical Infrastructure Protection (CIP) standards, enforced by NERC and FERC. The CIP standards provide a common, universal foundation for security, covering a wide range of priorities and threat vectors. These include:

- Categorizing cyber systems based on impact
- Controlling electronic and physical access
- Managing system security, including malware prevention and patching
- Training personnel on security procedures

---

<sup>2</sup> The CEO-led [Electricity Subsector Coordinating Council](#) (ESCC) serves as the principal liaison between the federal government and the electric power industry on efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC works across the sector, and with the E-ISAC, to develop actions and strategies that help protect the North American energy grid and prevent a spectrum of threats from disrupting electricity service.

- Implementing plans for incident response and recovery
- Physical security protections for critical transmission substations and control centers
- Managing supply chain risks

Given the dynamic nature of the threat environment, standards must be complemented with the analysis and sharing of threat and vulnerability information to enhance situational awareness and share mitigation tactics. The E-ISAC provides the type of timely, actionable information needed to complement the regulatory framework and strengthen the security posture of the electricity sector. General insights and trends observed by the E-ISAC can also inform improvements to mandatory standards, as warranted.

Key E-ISAC activities, programs, and partnerships include:

**E-ISAC Portal** – E-ISAC members and partners access information on cyber, physical, geopolitical threats, news and events through a secure Portal. Information shared with the E-ISAC is voluntary and can be shared anonymously or with attribution. The E-ISAC analyzes, enriches, curates, and shares information with the community in accordance with the Traffic Light Protocol (or TLP) system. The E-ISAC also uses the Portal to communicate threat warnings and mitigations, and provide analytical products that provide actionable context to support industry security personnel. Many products posted to the Portal are a collaborative effort between E-ISAC analysts and industry.

**Bulletins and Alerts** – In addition to the secure E-ISAC Portal, NERC Alerts are an industry-recognized program to provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. Depending on the Alert level, NERC can require industry participants to respond concerning their progress in implementing mitigation measures. Recent security-related Alerts have covered such topics as supply chain risks, such as the SolarWinds incident, cross-border remote access to bulk power system elements, preparation for potential Russian cyber activities, communication of a prohibition order securing critical defense facilities, and the Log4j vulnerability. For rapid, elevated, industry-wide awareness requiring immediate action, the E-ISAC also issues All-Points Bulletins and conducts Critical Broadcast Program calls, often within hours of a major event or incident. Examples include the recent U.S. Government and Microsoft report on Volt Typhoon. This suite of bulletins and alerts ensures industry is aware of the most significant threats and the mitigations necessary to defend the grid.

**Cyber Threat Analysis Programs** – The E-ISAC provides a suite of capabilities tailored to the industry's cyber analysis needs. The Cybersecurity Risk Information Sharing Program (CRISP) is a premier example of the E-ISAC's partnership with DOE. Managed by the E-ISAC, CRISP uses unique technology, leveraging DOE and its National Laboratory System's analytical capability to provide cyber threat intelligence and government-informed reporting to help North American asset owners and operators detect threats that utilities cannot get anywhere else. CRISP participants cover more than 90 percent of U.S. customers, who receive timely bi-directional sharing of unclassified and classified threat information. Utilities use this critical situational awareness tool

to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. CRISP information is further shared in a secure fashion through the E-ISAC Portal and allows non-CRISP companies to benefit from the shared indicators and threat actor activity captured by the program. In the nine years since its inception, CRISP has continued to grow its capabilities, and we are working closely with the participating utilities, national laboratories, and DOE to grow and evolve the program to face expanding threats from nation-states like China and Russia. E-ISAC analysts, in turn, conduct proactive threat hunting in CRISP data and other data sets to identify additional threats based on the tools and information available. These threat hunts have helped identify additional gaps and enabled industry to apply mitigation strategies. This analysis is complemented by partnerships with cross-sector and international organizations including the Canadian Independent Electricity System Operator (IESO), Canadian Gas Association, Danish SektorCERT, Financial Services ISAC, and Oil and Natural Energy ISAC, among others. The E-ISAC also collaborates with cyber security firms to bolster information sharing and analytical capabilities, ensuring industry has access to best-in-class IT and OT information.

**Energy Threat Analysis Center (ETAC) and Government Engagement** – The E-ISAC is part of the newly established Energy Threat Analysis Center (ETAC), a DOE-led initiative that features collaboration between electric industry partners and government agencies through DHS Cybersecurity & Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative. ETAC will serve as a spoke to the Joint Cyber Defense Collaborative hub and enable operational intelligence collaboration for the entire energy sector, and the E-ISAC is proud to be part of the pilot to stand up this capability. ETAC partners meet regularly in classified and unclassified

environments to discuss threats and to provide industry context to the intelligence community. ETAC participants have collaborated on threats emanating from the Russian war in Ukraine, supply chain events, and operational technology vulnerabilities. ETAC is an important example of how the private sector is working with government to defend critical infrastructure.

**Trainings, Briefings, and Workshops** – To help industry understand the evolving threat environment and mitigations, the E-ISAC provides members and partners with regular trainings, briefings, and workshops. In addition to cyber-focused engagements, in response to the emerging and diverse physical security threats to the bulk power system (BPS), the E-ISAC has conducted specific and actionable workshops on physical security to provide utilities with mitigation strategies that lead to upgrades at their facilities, thereby enhancing protective measures in defense of physical security attacks.

E-ISAC workshops teach the design basis threat methodology (DBT). DBT is a scenario-based methodology that focuses on detection, assessment, and response. It helps utilities identify unacceptable consequences and leads to determining specific upgrades to ensure those consequences do not occur. The E-ISAC has conducted over 25 of these workshops since 2017 across a diverse subset of our membership. The E-ISAC will host three more workshops in 2025.

**GridEx** – The largest grid security exercise in North America, GridEx is hosted every two years by the E-ISAC. The exercise gives E-ISAC member and partner organizations a forum in which to practice how they would respond to and recover from coordinated cyber and physical security threats and incidents. The eighth GridEx concluded two weeks ago.



**GridSecCon** – GridSecCon is one of the industry’s premier events that convenes hundreds of grid security experts each year from industry and government to participate for a week of training, conference, threat briefings, and networking. Participants engage in discussions on critical energy security topics such as incident response, risk management, resilience, identifying indicators of compromise, and cross-sector risk – to name a few.

CRISP, GridEx, and GridSecCon also provide opportunities for hands-on cyber security training, using realistic scenarios based off real world events.

**Industry and Vendor Engagement** – The E-ISAC also recognizes the increased interdependencies and complexities in the supply chain among security, vendors, and the electricity industry, and is addressing this issue through the Vendor Affiliate Program (VAP). This program brings OEM vendors and security solution providers into the E-ISAC community as partners to facilitate information sharing and best practices, leveraging subject matter expertise and thought leadership of some of the biggest suppliers to industry. VAP currently has 22 members representing manufacturers and security firms widely used by the electricity community. We expect continued growth within this community and will continue to leverage it to help mitigate the supply chain threat.

**Resilient Communications** – The E-ISAC is also focused on building enhanced resilience across the industry. After-action reports from previous GridEx cycles highlighted opportunities to further strengthen communication technology planning and ensure seamless coordination across

the electric sector during major events. In response to these insights, the E-ISAC, in collaboration with the ESCC Secretariat and other partners, conducted an in-depth review of the processes and tools that support the ESCC's emergency procedures. This thorough review informed the development of actionable recommendations and tools to enhance communication resilience across the sector.

#### **The Threat Landscape**

**The E-ISAC is not aware of any specific, credible and imminent cyber or physical security threats to the North American electric grid at this time.** The E-ISAC continues to monitor threat activity and intelligence bulletins provides stakeholders with insights into the tradecraft of politically motivated hacktivists, ransomware operators, and state-sponsored threat actors.

The threat landscape includes continuously evolving and persistent threats from sophisticated, capable, and diverse adversaries. Among the most pernicious are nation states, which possess the capability to disrupt critical infrastructure in North America. Numerous reports issued by the U.S. and Canadian governments, including the U.S. Intelligence Community's Annual Threat Assessment, underscore the severity of the threat faced by critical infrastructure from nation-state and transnational criminal actors. Aided by a significant increase in software and hardware vulnerabilities, adversaries are constantly looking for ways to exploit electricity sector participants.

As discussed further below, the E-ISAC continues to monitor threats from China, Iran, North Korea and Russia. Chinese cyber activities are one of the largest and most dynamic cyber threats to critical

infrastructure and continue to demonstrate an increasing sophistication, including new and adaptive techniques to gain access to networks and conduct espionage. The sheer scale and persistence of Chinese cyber activities demonstrated in the various Typhoon campaigns lends credence to their ambition to hold North American critical infrastructure at risk. Iran's growing expertise and willingness to conduct aggressive cyber operations make it a threat to the security of U.S. and its allies, however, their regional neighbors such as Israel are more likely to experience cyber impacts. North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat, especially in the use of the thousands of cyber operatives across the world they utilize to gain access to North American critical infrastructure as remote workers. Russia remains a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Its focus currently remains primarily on its regional neighbors and Ukraine. Finally, the E-ISAC continues to monitor and report on physical and cyber domestic and foreign hacktivist, criminal, and ransomware threats to the sector.

***People's Republic of China (PRC) Cyber Threats***

Salt Typhoon is a state sponsored threat group attributed to the People's Republic of China (PRC), believed to be operated by the PRC's Ministry of State Security (MSS). They have been active since 2019 and have targeted the telecommunications, health, and hospitality sectors in the United States, Canada, and Asia. In late 2024, Salt Typhoon compromised the networks of nine U.S. telecommunications companies. In June 2025, the Canadian Centre for Cyber Security attributed Salt Typhoon to a breach at a Canadian telecommunications company in February 2025.

Salt Typhoon commonly exploited unpatched vulnerabilities in public-facing network devices including routers, firewalls, and virtual private network (VPN) solutions to gain initial access to a target network. They utilized living-off-the-land (LOTL) techniques and custom malware to go undetected for years. The activities of the Salt Typhoon extend beyond mere technical weaknesses and represent a profound strategic intelligence threat. The technologies targeted by Salt Typhoon are prolific across critical infrastructure sectors, including the electric sector, which makes repurposing tactics, techniques, and procedures learned targeting one sector easier when targeting the next.

The compromise of large data centers could lead to infiltrations in shared cloud environments and the compromise of cloud tenant data as in the case reported by NEXTGOV/FCW on June 9, 2025 where Digital Realty, a large data center operator, and Comcast report as victims of Salt Typhoon's espionage activities.<sup>3</sup> The service disruption and sudden disconnection of a large data center could also have impacts on grid reliability. In a report published in January of 2025, NERC identified the risks that would be present with the growth of large data center loads.<sup>4</sup>

Volt Typhoon was reported by Microsoft and CISA in May 2023 and has remained active since. CRISP began reporting to both DOE and the CRISP community on Volt Typhoon in October 2022, prior to public release in May 2023. This threat actor exhibits a sophisticated and stealthy

---

<sup>3</sup> See <https://www.nextgov.com/cybersecurity/2025/06/us-agencies-assessed-chinese-telecom-hackers-likely-hit-data-center-and-residential-internet-providers/405920/>

<sup>4</sup> See [https://www.nerc.com/pa/rrm/ea/Documents/Incident\\_Review\\_Large\\_Load\\_Loss.pdf](https://www.nerc.com/pa/rrm/ea/Documents/Incident_Review_Large_Load_Loss.pdf).

approach to cyber espionage targeting U.S. critical infrastructure. Active since mid-2021, its focus is not on immediate data exfiltration but rather on maintaining persistent access for potential future disruptions. Volt Typhoon operations leverage compromised small office/home office (SOHO) routers and network devices, often utilizing publicly known exploits for initial access. Once they have gained access, they employ extensive LOTL techniques. Additionally, they employ techniques to bypass multifactor authentication (MFA) when possible and maintain persistence through scheduled tasks or registry modifications.

***The Democratic People’s Republic of Korea Cyber Threat***

The Democratic People’s Republic of Korea (DPRK) has systematically deployed thousands of IT operatives who have applied for jobs throughout North America. The targeted jobs are designated as “remote” and are technology focused – such as Data Scientist, Software Engineer, Business Intelligence Engineer, Stack Engineer, and Data Engineer. The job roles and responsibilities usually require high-level access to include administrative access to fulfill the job requirements. The workers use fabricated personas, along with deepfakes and other artificial intelligence tools, to secure legitimate roles in IT and other technical functions.

The E-ISAC has shared numerous personas and network indicators associated with DPRK IT workers, and we have received reports from members that have received applications from these personas. The E-ISAC recommends requiring stringent background checks, implementing careful interview processes, training human resources departments to spot inconsistencies in behavior or AI deepfakes. Network security should monitor the installation of unauthorized remote administration tools and the use of VPN services to connect to corporate infrastructure.

***Iranian Cyber Threats***

The E-ISAC is tracking ongoing Israel-Iran tensions. Specifically, the E-ISAC continues to monitor open-source intelligence and CRISP data for any cyber activity against North American electrical infrastructure for possible retaliation of Iranian cyber actors targeting vulnerable U.S. networks and entities of interest.<sup>5</sup> The E-ISAC encountered upticks in activity by pro-Iran hacktivist groups claiming to carry out attacks, primarily DDoS attacks, against U.S. and Israeli organizations across numerous sectors. Though DDoS activity remains the routine standard for hacktivist activity in general, the E-ISAC continues to observe some hacktivists claiming to breach industrial control systems (ICS) in specifically targeted victim countries – most typical are pro-Russia operations targeting European sectors.

***Russian Cyber Threats***

We continue to monitor for Russian cyber activity in North America. Reporting suggests their cyber focus area currently remains on Ukraine and NATO affiliated countries in Europe. Russian hacktivist groups, such as NoName057(16), leveraged disruptive Denial of Service attacks to knock victim websites offline across various critical infrastructure sectors. Russian hacktivist groups can also be thought of as cyber privateers, state-sponsored actors operating as cyber criminals and geopolitical ideologues. Russian cyber actors continued their cyberespionage activity against organizations of interest to the Russian government, including in government, defense, transportation, media, non-governmental organizations, and healthcare sectors primarily in Europe and North America. We will continue to monitor this situation as Russian tactics, techniques, and procedures (TTPs) used in infrastructure in those companies could later

---

<sup>5</sup> See DHS notice: [Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest](#).

be tailored for use against North American electric utilities.

#### **Hacktivist, Criminal, and Ransomware Threats**

Public protests have been exploited to promote violent rhetoric. For example, protests in Los Angeles resulted in several online users mentioning specific targets and tactics, such as using a specific caliber firearm against transformers and promoting “drone bombing” of a substation. The E-ISAC also observed claims of sabotage incidents targeting the electricity and broader energy sector outside of North America. For example, a series of sabotage incidents on May 24-25 in France involved downing a power pylon, an arson attack on a substation, and an arson attack on a transformer in close geographic proximity, for which two French anarchist groups claimed credit. Media attention to incidents such as these can raise visibility of various TTPs that can be used against the grid. Cyber threats focused on espionage, crime, and hacktivism will continue to evolve, led by the tensions related to the geopolitical landscape in the European, Mideast, and Asia Pacific regions.

Ransomware cyber-criminals continue to pursue common tactics that impact victims with encrypted files and assets, sensitive information exfiltrated from the victims’ environment, and holding impacted technology and information for ransom while naming and shaming victims. Ransomware tactics have evolved to where groups impersonate legitimate network administrators to steal login credentials, leading to subsequent malicious activity.

Threat actors on ransomware sites and cybercrime forums monitored by the E-ISAC continue to make claims of cyberattacks against alleged energy sector victims, including energy sector

vendors, oil and gas companies, and electric utilities. Cybercrime forums often help facilitate ransomware attacks by providing platforms where threat actors can buy and sell initial/unauthorized access to victim networks, which can then be utilized for more severe follow-on attacks. Cybercrime forum activities also involve the sale or leaking of stolen data, credentials, and other illegal digital goods and services.

The E-ISAC observed a temporary drop in the number of tracked claims of cyberattacks against energy sector entities when the most prominent English-language cybercrime forum, Breach Forums, was shut down in April. However, other English-language forums seek to become a replacement for Breach Forums, and Russian-language cybercrime forums continue to operate unimpeded and now constitute all the “top-tier” forums in terms of selling or leaking victim network accesses and stolen data.

#### **Recommendations**

As the subcommittee continues its examination of threats to grid security, Congress could consider the following actions:

**Authorize ETAC** – As discussed above, DOE’s ETAC pilot led by the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), is a public-private partnership that convenes experts from the federal government and the U.S. energy sector, joining analytic capabilities from the national laboratories with real-world threat insights to secure critical infrastructure and support the nation’s response to energy system threats. Congressional authorization of the ETAC will further establish this important partnership, enabling advancement of its important mission in collaboration



with the energy sector.

**Support Funding for CRISP +30 and DOE Oil and Natural Gas (ONG) Programs** – DOE’s CRISP +30 and Oil and Natural Gas pilots provide critical intelligence value to both the Department of Energy and the CRISP community utility members. Begun in 2018, CRISP +30 is a DOE program supporting the participation of electricity providers with smaller customer bases, mostly cooperative and municipal utilities. A goal of the program is to facilitate participation of smaller companies that otherwise lack sufficient resources. While smaller in size, some utilities serve critical defense critical infrastructure in remote, rural areas. Their contributions are often significant. Previous funding for CRISP +30 was approximately \$3 million annually, and any increase would benefit the program by adding additional defense critical energy infrastructure utilities. For example, CRISP identified and reported on malicious nation state activity attributed to Chinese nation state actors prior to publication by CISA and Microsoft. This early reporting informed DOE CESER and the sector of an emerging threat, enabling the sector to undertake proactive mitigations to better defend against new malicious cyber tactics, techniques, and procedures. Sufficient funding for the CRISP +30 expansion will enable stability and growth of this valuable partnership.

DOE’S ONG program began in 2018 in an effort to add CRISP technologies to ONG companies to increase the data set and monitor for anomalous and/or malicious activity. Maintenance or even expansion of DOE’s ONG program would benefit the national security of the nation by providing cyber situational awareness to ONG participants and DOE, and providing domestic coverage of infrastructure. As malicious cyber actors continue to target ONG infrastructure, funding to maintain and potentially expand the ONG pilot would bring increased visibility and CRISP support to ONG

companies.

**Reauthorize CISA 2015** – The Cybersecurity Information Sharing Act of 2015 (CISA 2015) expired on September 30, 2025, while most recently given a short-term extension to January 30, 2026. CISA 2015 was enacted to facilitate voluntary information sharing between the private sector and government. Industry sources report that the law has enhanced response capabilities to cyber incidents and meaningfully advanced information sharing and cyber defense. As a private entity, expiration of the law has no immediate negative consequences on E-ISAC operations. However, the law does encourage information sharing with ISACs and other sharing relationships. Reauthorization would support the broader information sharing ecosystem and preserve a highly valued framework for the private sector.

#### **Conclusion**

Grid security is inextricably linked to reliability. To date, there has not been any loss of load in North America that can be attributed to a cyber attack. Yet the security landscape is dynamic, requiring constant vigilance and agility to help prevent and mitigate the impact of any such attacks. Recent physical attacks show that these types of attacks can disrupt electric service, even as the impact of those experienced thus far were localized. NERC and the E-ISAC address cyber threats through a comprehensive range of complementary strategies. Partnerships with DOE and other agencies are critical. Mandatory CIP standards provide a universal foundation for security and is a shared priority with FERC and industry. Through the E-ISAC, NERC provides situational awareness, and sharing of timely, actionable intelligence with industry and government. Strong collaboration with industry is key to successful information sharing within the electricity sector and across sectors. Harmonizing reporting requirements and encouraging information sharing,

especially automated sharing, will help utilities and government better protect critical infrastructure. NERC and the E-ISAC remain keenly focused on our mission to assure reliability of the BPS.

The electricity industry has taken a defense-in-depth approach for decades. Its culture of mutual assistance and aid emphasizes sharing resources and expertise to ensure the lights stay on or get back on as safely and quickly as possible. Cyber and physical security are no different. The ESCC, in partnership with DOE, CISA, and the White House, continue to emphasize collective defense, and have developed concepts like cyber mutual assistance, response playbooks, and the development of resilient communications activities to help the industry prepare for and respond to these types of incidents. NERC, the E-ISAC, and the industry are working 24/7 to ensure a secure and reliable grid in the face of significant threats.

Mr. LATTA. Thank you.

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

#### **STATEMENT OF SHARLA B. 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 8 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 realtime.

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 ESSC, consists of CEOs who represents all segments of the elec-

tric 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:]

**TESTIMONY OF SHARLA B. ARTZ  
SECURITY AND RESILIENCE POLICY, AREA VICE PRESIDENT  
XCEL ENERGY**

**BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE  
SUBCOMMITTEE ON ENERGY**

**HEARING TITLED “SECURING AMERICA’S ENERGY INFRASTRUCTURE:  
ADDRESSING CYBER AND PHYSICAL THREATS TO THE GRID”**

**DECEMBER 2, 2025**

**Introduction**

Chairman Latta, Ranking Member Castor, and members of the Subcommittee, thank you for the invitation to testify on this important topic. My name is Sharla Artz, and I am the Security and Resilience Policy Area Vice President for Xcel Energy. 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. Xcel Energy is a member of certain national trade associations, including the Edison Electric Institute (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. My testimony today is on behalf of both Xcel Energy and EEI more broadly. For Xcel Energy and EEI's member companies, securing the energy grid from all hazards, including cyber threats, is a top priority.

The energy grid is critical to America's national security and economic competitiveness. With electricity demand growing dramatically to support critical technologies like artificial intelligence and the proliferation of data centers that fuel our digital lives, electricity is more essential than ever to our nation's energy dominance. Ensuring a secure, reliable, and resilient energy grid is a responsibility Xcel Energy and the electric power sector take extremely seriously.

As the grid continues to modernize, so too do the threat actors who seek to undermine U.S. critical infrastructure. For years, the U.S. intelligence community<sup>1</sup> has warned of the potential for malicious nation-state exploitation of U.S. critical infrastructure. Today, we know from our federal partners that Chinese state-sponsored cyber actors known as Volt Typhoon have compromised multiple U.S. critical infrastructure providers with the intent of disrupting

---

<sup>1</sup> [2025 Annual Threat Assessment of the U.S. Intelligence Community](#)

operational controls. With the increasingly complex geopolitical threat landscape, sophistication of ransomware operations by transnational organized criminals, and the use of artificial intelligence (AI) to conduct cyber attacks<sup>2</sup>, we have seen an uptick in threats to critical infrastructure organizations across all sectors. The threat is real, it is advanced and it is persistent. Thus, Xcel Energy and our industry partners work constantly to mitigate these threats and provide resilient power to our communities and those we serve.

Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, government at all levels can and must play a role in protecting it, especially when it comes to defending against nation-state actors. Because of this shared responsibility, investor-owned utilities work collaboratively with our federal, state and local partners, with each other, with rural cooperatives, public power and with other critical infrastructure sectors to achieve this vital national security mission.

Our national security lines of effort are rooted in a “defense-in-depth” approach with several layers of security strategies designed to eliminate single points of failure. There are three main components to our defense-in-depth approach:

1. Adherence to mandatory and enforceable reliability, physical, and cybersecurity regulations;
2. Partnerships among industry and government for proactive defense; and
3. Preparing for and exercising recovery plans against all hazards.

### **Resilience for National Security**

Private sector critical infrastructure asset owners and operators are on the front lines of defending our nation’s essential services from rapidly evolving threat actors on a daily basis. The attacks by Russia against Ukraine’s power system solidified the importance of creatively, constructively and collaboratively addressing threats to critical infrastructure. For this reason, the energy sector has

---

<sup>2</sup> [AI firm claims Chinese spies used its tech to automate cyber attacks](#)



been actively implementing security risk mitigation programs and engaged with our government partners to develop tools, technologies and processes that enhance visibility into critical control systems, improve situational awareness and information sharing for emerging threats, and make sure we have comprehensive plans in place to respond and recover quickly when incidents occur.

### **Security Standards**

Under the Federal Power Act and Federal Energy Regulatory Commission (FERC) oversight, the electric power sector is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed \$1 million per violation per day. The standards cover key components of effective risk management including supply chain risk management and physical security. For over 15 years, these mandatory standards continue to evolve using the process created by Congress to allow for input from subject matter experts across the industry and government. That process ensures utility owner and operator expertise from across the stakeholder community informs the security controls that most effectively reduce prioritized risks.

In addition to NERC CIP, companies like Xcel Energy are subject to the TSA Security Directives. First issued in 2021, industry and TSA have worked together to enhance the existing security controls implemented to secure natural gas infrastructure systems. Since their issuance, the collaboration between TSA and industry has resulted in requirements that allow asset owners and operators to tackle priority risks with controls that achieve the desired outcomes.

The industry also uses voluntary standards and maturity frameworks to improve the security of their systems. Examples include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Department of Energy's (DOE's) Cybersecurity Capability Maturity Model (C2M2) and the DOE's Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources (DER) that are being developed in partnership with state regulatory bodies through the National Association of Regulatory Utility Commissioners

(NARUC). The frameworks and guidance provided in these efforts allow utilities of all shapes and sizes to assess their current maturity, identify areas for improvement, and benchmark against existing known best practices.

In addition to complying with standards, the sector strongly believes in advancing a culture of security. Thanks to leadership from the chief executives of all U.S. investor-owned electric companies, EEI developed a “Culture of Security” initiative that has provided tools to improve security culture for individual electric companies and a venue for sharing practices across the industry.<sup>3</sup>

Self-assessments are now conducted by companies annually. In addition to demonstrating that security is a priority for our executives, this yearly exercise provides a venue for security teams and leaders across business units to address corporate security culture and to better align efforts.

When it comes to securing specific systems like operational technology for power delivery, much of the expertise is in the sector. To leverage this expertise, the Culture of Security initiative now includes peer reviews. The peer reviews cover topics ranging from physical security processes, training of personnel, and cybersecurity architectures. Participating electric companies invite security professionals from other electric companies to review their peers, identify opportunities for improvement, and socialize best practices. The process is extensive, builds strong relationships across industries, and identifies security-enhancing opportunities that can be shared more broadly across the industry.

The commitment from industry operators to participate in these programs highlights both the shared responsibility felt across the sector and the desire to learn from each other. While culture alone does not improve security posture, it is the foundation on which new efforts are built and ensures that today’s imperatives remain tomorrow’s priorities.

---

<sup>3</sup>Scott Aaronson, Edison Electric Institute, Protecting the energy grid is a team sport (October 2021), <https://www.securitymagazine.com/articles/96231-protecting-the-energy-grid-is-a-team-sport>.

Through these standards and voluntary regimes, the bulk power system and other critical grid components benefit from a baseline level of security. While these standards are important, given the dynamic threat environment regulations alone are insufficient and must be supplemented by industry-government partnerships and coordinated response and recovery efforts.

### **Partnerships**

As threats evolve, the value of industry-government partnership and the need to remain vigilant cannot be overstated. We appreciate the continued partnership of our Sector Risk Management Agency, the Department of Energy, as they have the sector-specific expertise and relationships to understand our risks and mitigation strategies.

The electric power sector has worked with DOE and other government partners to develop and deploy sophisticated threat monitoring tools and to create an environment where threat intelligence is shared in near real-time and where operational collaboration among asset owners and government operators is the norm. This gets information into the hands of system operators quickly to better protect and defend their critical systems against rapidly evolving threats. Understanding the adversaries' tactics, techniques, procedures and motivations also helps asset owners plan their infrastructure with security and resilience to these threats in mind. While the sector values current coordination efforts through partnerships like the Energy Threat Analysis Center, the Cybersecurity Risk Information Sharing Program (CRISP), and the Electricity Subsector Coordinating Council (ESCC), there is opportunity to continue to enhance these partnerships.

Industry and government have long understood the importance of actionable intelligence tailored to address sector specific threats and impacts. The Energy Threat Analysis Center, or "ETAC," was created to address this need. First piloted in 2023 and now consisting of 17 private sector entities including Xcel Energy, ETAC is an operational collaborative that convenes experts from the DOE and the U.S. energy sector to identify, analyze, and mitigate cyber threats to America's critical energy infrastructure. The ETAC integrates industry data and context with government

intelligence to reduce risk to the energy sector writ large. Housed at the National Renewable Energy Laboratory (NREL) in Colorado and including representatives from multiple national labs, ETAC analysts from public power utilities, rural cooperatives, investor owned utilities, and oil and natural gas entities are able to review threat intelligence in real time, assess impact to the energy sector and develop risk mitigations that are shared via the Electricity Information Sharing and Analysis Center (E-ISAC) and the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC) to energy providers across the country. In addition to DOE, ETAC facilitates industry collaboration with other federal partners, including DHS, the military and federal security and law enforcement agencies expanding cross agency information sharing with the private sector.

As an example of the positive impact ETAC has made, after the public disclosure of PRC-linked Salt Typhoon's compromise of major U.S. telecommunications providers in late 2024, ETAC issued four threat memos (March-August 2025) that took government information, injected private sector data and provided specific, actionable best practices to mitigate the identified threat. These products garnered 1000+ views on the E-ISAC portal demonstrating strong industry interest and utilization.

In addition to ETAC, Xcel Energy and our industry utilize other government partnerships to enhance system security. For example, private sector owners and operators participate in the DHS's Joint Cyber Defense Collaborative (JCDC), TSA's Surface Information Sharing Cell (SISC's) industry briefings, the NSA's Cybersecurity Collaboration Center and the FBI's Cybersecurity Action Team. Xcel Energy actively engages our state partners as well, participating in the Minnesota Fusion Center, the Texas Fusion Center and holding a permanent seat at the Colorado Information Analysis Center. Our Threat Intelligence team uses these partnerships to further our understanding and our partners' understanding of the threat and corresponding operational risk.

Identifying threats encompasses more than people to people interaction but also involves the deployment of technology that rapidly detects threats. A prime example of an effort that brings the expertise of national labs, the voluntary efforts of industry, the reach of the E-ISAC, and the intelligence apparatus of government is the Cyber Risk Intelligence Sharing Program, or “CRISP.” The CRISP program includes DOE, the Pacific Northwest National Laboratories, and the E-ISAC, which manages the program. Participants in the program deploy unique sensors on their networks and share that data with intelligence analysts. The sensors monitor network traffic, send the data to the national lab for analysis for potential adversarial activity. Participants are then alerted to potential threats so that they can take action to protect their systems. More than 90 percent of U.S. electric customers are served by a company that has deployed CRISP sensors. The information gleaned from the sensors and the associated analysis has proven extremely valuable to identifying and addressing cybersecurity risks.

In addition to the information sharing initiatives described above, industry and government are strategically assessing threats to energy infrastructure at the executive level. The Electricity Subsector Coordinating Council or “ESCC,” consists of electric company CEOs and trade association leaders who represent all segments of the electric sector, and serves as the primary interface between government leaders and the private sector to address national security priorities, leveraging the strengths government and industry each provide. Together, the ESCC executives and government partners proactively prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. Our CEOs and Senior Officials from the federal government sit at the same table and work through the key risks that impact our sector. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort and unity of message among participating organizations. The concerted collaboration creates efficiencies needed for effective and rapid threat remediation efforts. This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-

sector coordination. The ESCC has been seen as a model across critical infrastructure sectors due to its CEO-level engagement and prioritization of security and preparedness for all hazards.

### **Preparedness, Response and Recovery**

Preparing for incidents is a regular component of our security and resilience practices and exercises help us improve the effectiveness of our individual and collective response to various incidents. Industry-government exercises, such as the biennial GridEx, sharpen the industry's skill set, ensuring that when incidents happen our playbook has been tested before it is put into action. The first GridEx was conducted in 2011 at the direction of NERC and industry and has grown every time it has occurred. Most recently, GridEx VIII saw increased participation and included thousands of participants from across the U.S. and Canada. At Xcel Energy, our two days of distributed play included over 316 participants, including 64 participants from external partnering organizations, such as state emergency managers and homeland security advisors.

At the end of distributed play, the E-ISAC brings together ESCC CEOs, Canadian Cybersecurity officials, cross sector participants and leaders from the U.S. government to review the coordination and communication processes between industry and government in responding to a hypothetical coordinated attack by a nation state. These discussions help us identify needed improvements to facilitate resilience during a time of crisis.

While GridEx is one of the largest exercises, industry participates in many additional exercises across the state and federal level to enhance our shared understanding of processes, priorities and opportunities for improvement. In Wisconsin, for example, the Wisconsin National Guard, the state emergency operations center and utilities exercise regularly. Similarly, in Colorado, utilities in the state exercised with NORAD and Northern Command to enhance response capability mutual understanding. In Virginia, the 91<sup>st</sup> Cyber Brigade recently hosted Cyber Fortress 2025, a joint, interagency, intergovernmental, multinational exercise focused on electric utilities. The 2-week exercise allowed federal, state, and local entities to coordinate directly with electric industry leaders and plan for future collective response and resiliency activities. The Department of Energy also hosts regionally-based exercises focused on response to natural and man-made

threats, such as Liberty Eclipse and Clear Path. Next year, the American Gas Association will host the biennial Natural Gas Exercise, an exercise in which operators test and validate response/recovery plans for cybersecurity and physical security threats that stress gas control and corporate business continuity. These drills sharpen not just the unity of effort between energy industry companies and government agencies but also practice unity of message to ensure that we speak with one voice to our customers and your constituents during incidents.

The electric power sector is proud of its record on reliability, but outages and incidents do occur. When these happen, many key investments help companies restore power safely and as quickly as possible. EEI's members are forecast to spend more than \$200 billion this year — and more than \$1.1 trillion over the next five years — to make the energy grid stronger, smarter, more dynamic, and more secure. The industry's culture of mutual assistance deploys a world-class workforce amidst the toughest conditions to restore power for customers safely.

More recently, we have supplemented that traditional response and recovery with a 21<sup>st</sup>-century addition: cyber mutual assistance. The same surge capacity that rushes to companies in need during hurricanes, winter storms, and wildfires stands ready to assist and share resources in the face of a potential cyber incident. So far, more than 190 entities including investor-owned natural gas and power companies, cooperatives, municipalities, Canadian power companies, and Regional Transmission Organizations/Independent System Operators (RTOs/ISOs), are participating in the program. EEI manages these efforts and has determined that these entities cover more than 80 percent of U.S. electricity customers, roughly 75 percent of U.S. domestic natural gas customers, and 74 percent of natural gas distribution pipelines.

#### **How Government Can Help**

Government should continue to fund information sharing collaboration initiatives, like ETAC, so they can build upon the strong foundation established in this unique environment. Expanding programs like CRISP enhances industry and government understanding of the threat landscape and thus needs additional government funding to accomplish that expansion.

Congress should authorize ETAC so that this unique public private partnership can adapt and grow to address evolving threats. Explicit recognition of this program allows industry partners and DOE to shape the joint effort to address the evolving risk landscape and to incorporate needed partners in the work effort.

Continued support and recognition of the importance of Sector Risk Management Agencies for sector risk reduction efforts is essential to critical infrastructure protection. The energy system expertise contained within DOE and the national lab complex assures that risk assessment is informed by system operational understanding. Supporting DOE leading government engagement with industry is most efficient and effective while minimizing duplication or conflicting initiatives.

It is equally critical to recognize that certain information about the energy grid—such as detailed operational data and security protocols—must be protected from public disclosure. The release of such sensitive information could inadvertently aid malicious actors and undermine the security of our infrastructure. Although some state-level initiatives seek to increase public access to grid information, we continue to urge policymakers and regulators to carefully balance transparency with the imperative to safeguard details that, if disclosed, could pose risks to national security and public safety. Protecting this information is essential to maintaining the resilience and reliability of the grid in the face of evolving threats.

### **Conclusion**

Thank you again for holding this hearing. As evidenced in my testimony, the industry's commitment to security and our willingness to work with both public and private partners across all sectors to address all hazards is a constant effort. We appreciate the bipartisan support that grid security legislation historically has enjoyed in Congress and the work you have done to enhance the energy sector's security posture. We look forward to working together to continue to



build critical infrastructure security and resilience for the safety, security, and well-being of all Americans.

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 cooperatives 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 cooperatives 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 cooperatives, these threats are not abstract. They are real, they are sophisticated, and they are growing.

Electric cooperatives 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 struc-

tured framework designed specifically for cooperatives to advance cyber hygiene regardless of the utility's cyber maturity.

While cooperatives are doing their part, we cannot do this alone. Strong Federal partnerships are essential to closing this resource gap. Electric cooperatives 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:]



**Testimony of Tim Lindahl  
President and Chief Executive Officer  
Kenergy Corp**

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

***“Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the  
Grid”***

**Tuesday, December 2, 2025**

#### **Introduction**

Chairman Latta, Ranking Member Castor, and Members of the Committee: Thank you for the opportunity to discuss how electric cooperatives are working to secure the grid against evolving cyber threats. Every day, America’s electric grid faces thousands of cyber intrusion attempts. For rural electric cooperatives, these threats are not abstract; they are real and growing more sophisticated. My name is Tim Lindahl, and I serve as President and CEO of Kenergy. I am testifying today on behalf of the National Rural Electric Cooperative Association (NRECA), which represents nearly 900 electric cooperatives nationwide. As a co-op leader with over 30 years of experience in the technology and energy industries, I look forward to sharing my perspective on how electric cooperatives are securing the grid.

Kenergy is a distribution electric cooperative that serves over 60,000 homes and businesses across 14 counties in Western Kentucky with more than 7,200 miles of power lines. Kenergy has a long, proud history of serving our communities. Our co-op supports a robust industrial base in paper, metals, food, manufacturing, and energy. In 1937, our predecessor, Henderson-Union RECC, was the first electric cooperative in Kentucky to supply power to a member. Today, we also provide fiber optic services that have enabled broadband service to over 13,600 homes and businesses, having built out over 3,500 miles of fiber infrastructure. This will be instrumental in evolving our grid to meet changing needs, including the safety and security of our grid.

NRECA is the national trade association representing America’s 900 rural electric cooperatives. Electric co-ops are not-for-profit, at-cost electric utility providers focused on delivering affordable, reliable, and secure electricity to over 42 million Americans in 48 states. We are unique in the electric utility sector in that we are private, independent businesses that operate without profit incentives and are owned and governed by the people we serve.

Electric co-ops were created with a mission to address the distinct challenges associated with providing electric service to rural communities, which typically have lower population densities, are more residential, and are less affluent than the industry average. This means that cooperatives are constantly asked to do more with less, and they deliver.

Electric co-ops are owners and operators of some of our nation's most critical infrastructure, such as power plants, electrical substations, and transmission and distribution lines. This also includes infrastructure to generate or provide power for more than 150 military facilities and installations across the United States. We also serve as economic drivers and lifelines for critical industries and services in rural communities, helping power data centers, hospitals, emergency services, and food and agriculture production.

Protecting America's electric grid from cyber and physical threats is a top priority for the nation's electric cooperatives. Achieving this vital goal presents its own set of challenges. The same conditions that made it difficult to electrify rural America nearly a hundred years ago still exist today. These obstacles make it harder to secure the grid in rural communities.

Co-ops across the country are coming together and thinking innovatively to overcome these challenges. The seven cooperative principles, like concern for community and cooperation among cooperatives, are the driving force behind what we do. Additionally, our national trade association, NRECA, is leveraging private and public dollars to develop cybersecurity tools and resources to improve information sharing, deploy new technologies, and build a capable workforce.

The Department of Energy (DOE) is also a strong partner in efforts to improve co-op cyber defenses. DOE's Rural and Municipal Utility Cybersecurity Program (RMUC) represents the most significant opportunity for electric cooperatives to bolster their cyber readiness and close the rural resource gap. This program helps co-ops invest in the people, processes, and technologies needed to help co-ops secure the grid. DOE must act more swiftly to fund critical RMUC cyber initiatives, and Congress to continue to support and reauthorize this program.

### **Threat Landscape**

Cyber threats jeopardize electric reliability and pose a serious risk to the nation's safety, security, and economic well-being. The threat landscape for electric utilities is becoming more complex and dangerous. Electric cooperatives and other electric utilities are primary targets for cyberattacks because of their crucial role in national security and everyday life. Threat actors, ranging from state-sponsored groups to cybercriminals, exploit vulnerabilities for geopolitical or financial reasons, with the potential of cascading impacts on critical infrastructure. These attacks could disrupt the power supply, leading to widespread outages, causing societal panic, public health concerns, and economic harm. The emergence of advanced malware, ransomware, and phishing attacks further increases the risks and impacts.

Additionally, smart grids, distributed energy resources (DER), and Internet of Things (IoT) devices, while improving efficiency, introduce new targets. Defending our infrastructure against

new challenges and evolving cybersecurity threats requires strong cybersecurity measures, continuous monitoring, proactive threat intelligence, and a skilled workforce capable of safeguarding these critical assets against increasingly sophisticated attacks.

While cyber events often grab the headlines, physical threats to the electric grid remain persistent and evolving. Electric cooperatives face unique challenges in this regard. Our infrastructure is geographically dispersed, often covering thousands of square miles with relatively few customers per mile of line. Unlike urban utilities with dense infrastructure and centralized control, rural electric co-ops must secure long stretches of transmission or distribution lines, isolated substations, and facilities that may be hours apart, all with limited resources.

### **Securing the Grid**

Electric cooperatives place absolute importance on maintaining an affordable, reliable, and secure electric grid for our members. Co-ops apply a risk-based, layered defense strategy to protect critical assets, including power plants, transmission infrastructure that carries electricity long distances, and substations and distribution lines that provide electricity to local users. This approach is designed to ensure protection against all hazards – severe storms, vandalism, physical, and cyber incidents. The task of providing a reliable and secure electric grid is continuously evolving. Electric cooperatives use long-term strategies and various measures to adjust to emerging threats and conditions to ensure their cyber and physical security. Co-ops employ a range of measures, including risk assessments, technology and telecommunication deployments, data backups, response and continuity planning, tabletop exercises, and workforce development.

I joined the utility industry in 2005, when, for most organizations, cybersecurity was not at the forefront of their minds. Seeing the significant need to secure our digital assets, at a time when new technologies were quickly being implemented and grid operations were changing, resulted in several initiatives to bring security to the forefront of decision-making, at our local utility and across the nation. Programs and opportunities were leveraged to raise awareness across all functions of the utilities, which led to the development of partnerships and tools to make cyber a foundational part of our operations. 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 happens or hear about the attack that did not occur.

The commitment to the community principle that cooperatives hold includes making sure our local economies stay robust. A cyber event on a business or industry in our community can have grave consequences to the local economy and even to the viability of the electric cooperative. Beyond securing our systems, we have led community-level education sessions to help our rural small businesses ensure they are aware of their risks and can adapt to stay secure and viable.

Additionally, the sharing of threat information is the backbone of industry efforts to protect the grid and mitigate risk. Many electric cooperatives actively monitor and share information with organizations like the Electricity Information Sharing and Analysis Center (E-ISAC). The analysis and rapid sharing of security information from E-ISAC to the electric sector and back helps the industry to more clearly understand threats to the electric grid, which inform electric cooperatives' decisions on everything from technologies and mitigation efforts to tabletop exercise scenarios and workforce development strategies. Following the 2022 substation attacks in North Carolina, the industry worked through E-ISAC to update physical security risk management options for the electric system to better assess and manage risk at critical facilities.

Electric cooperatives, however, face unique challenges in securing the electric grid due to their geographical and operational characteristics. Smart investments in infrastructure cybersecurity can help ensure the security of, and prevent catastrophic damage to, the nation's electric grid, but often require high upfront costs and persistent funding to maintain capabilities. Because cooperatives operate without shareholders or profit incentives, financing costly investments often requires reliance on debt, which must be approved by their Boards and is ultimately paid back through rates paid by their members. Boards are careful stewards of their members' resources and mindful of the economic impact of rate increases to end-of-line consumer-members, particularly given that one in four households served by cooperatives has an annual income below \$35,000. These resource constraints can make it difficult to invest in advanced technologies and recruit and retain a skilled cyber workforce necessary to defend against increasingly sophisticated cyberattacks, especially those from nation-state actors.

### **Overcoming Challenges**

One of electric cooperatives' greatest strengths is their autonomy and independence, each with its own networks, software, and systems, yet interconnected to provide resiliency. Although independent, electric cooperatives across the country also work together to think innovatively, improving collaboration, pooling resources, sharing knowledge, and implementing new technologies that help co-ops protect against emerging threats. In some states, large generation and transmission cooperatives, statewide associations, and distribution co-ops are developing partnerships to share tools, equipment, and expertise across shared electric systems to strengthen their collective cyber defenses. We recognize that we are greater than the sum of our parts, and these efforts embody one of our core principles of cooperation among cooperatives.

Kenergy and other cooperatives are building fiber networks deep within our electric networks. These win-win builds help solve the digital divide by providing broadband access to our rural members, but also allow us a foundational platform to build our next-generation physical and cyber security platforms.

Kenergy partners with NRECA and other institutions, such as the B.E.T.H Institute (Broadband, Energy, Technology, and Home), a foundation that brings funding and partners together in each of the named categories at the community level to innovate solutions for enhancing our grid, ensuring reliability, and improving affordability.

Additionally, NRECA is building a robust cybersecurity program designed to continue to provide co-ops with the most up to date tools tailored to their needs to improve their cybersecurity posture. The program creates products and services that help co-ops prepare for existing and potential threats to their reliability and security.

#### *Threat Analysis Center*

The NRECA Threat Analysis Center (TAC) is a secure technology platform that helps the co-op community detect, analyze, and communicate cybersecurity threats. In the cybersecurity landscape, electric cooperatives rely on multiple sources of threat intelligence and alerting systems to protect their infrastructure. These alerts can be filled with false positives, low-priority, or irrelevant notifications, which can desensitize analysts, leading to slower response times, missed threats, and increased risk of breaches. TAC helps reduce alert fatigue, allowing cybersecurity professionals to focus on high-impact cyber threats and respond more quickly. Additionally, TAC works closely with federal partners and industry stakeholders to ensure co-ops have access to timely intelligence without compromising privacy. Even the smallest and most remote cooperatives gain access to expert analysis, training, and a national network of support, helping level the playing field in the face of increasingly sophisticated cyber threats.

#### *Co-op Cyber Goals Program*

There are numerous cybersecurity frameworks to help organizations improve their cybersecurity posture, each designed to address different needs, industries, and regulatory requirements. For electric cooperatives with limited resources and staff, understanding where to begin can be a daunting task. That's why NRECA launched the Co-op Cyber Goals Program in 2023. This initiative provides a structured framework of 20 achievable cybersecurity goals tailored to rural electric utilities and adaptable to any cyber maturity level. The program is designed to foster a culture of security across the organization, guiding co-ops through cyber hygiene from the most basic practices to the most advanced. More than 400 co-ops are part of the program, demonstrating the high priority placed on furthering and evolving our cyber resilience. By aligning cybersecurity efforts with practical, measurable goals, the program empowers co-ops to prioritize investments, engage staff at all levels, and build confidence.

#### *Co-op Cyber Tech Conference*

NRECA's Co-op Cyber Tech conference serves as a premier event for electric cooperatives to engage in technical training, share best practices, and collaborate on emerging cybersecurity challenges. This annual event brings together co-op cybersecurity professionals, utility leaders, and federal partners to discuss threat trends, showcase innovative tools, and conduct tabletop exercises that simulate real-world cyber incidents. The conference reinforces the importance of continuous learning and peer-to-peer engagement, especially for smaller co-ops that may lack access to specialized expertise.

#### *Cyber Risk Quantification Pilot*

NRECA recently launched a program to help electric cooperatives better understand cyber risks as a business decision. Participating co-ops can model the potential financial impact of cyber



threats on their operations and assess how implementing NRECA's Co-op Cyber Goals program, a set of high-priority cybersecurity measures designed to help electric cooperatives build a strong security foundation, reduces that exposure. By translating technical vulnerabilities into financial terms, cooperatives gain a clearer understanding of the potential business impact of cyber threats. This analysis helps shift the conversation from abstract threats to tangible consequences, such as potential service disruptions, financial losses, or reputational damage.

### **Federal Partnerships**

While co-ops are strengthening their cyber posture through collaboration and shared services, they cannot meet these challenges alone. Smart, targeted federal support through funding, workforce development, and improved threat intelligence sharing is essential. This will help close the resource gap and ensure rural communities are not left behind in the national effort to secure our energy infrastructure.

Leveraging our federal partnerships has been critical in evolving our security posture by hardening our physical and cyber systems. Electric cooperatives have a long history of federal partnerships and responsible management of taxpayer dollars. The Rural Cooperative Cybersecurity Capabilities Program, or RC3, was an initial collaborative partnership between NRECA and the Department of Energy to provide resources to the co-op community. RC3 has now grown into a broader NRECA cybersecurity program aimed at helping co-ops advance their cybersecurity posture. Additionally, electric cooperatives utilize resources from various federal agencies and departments, like CISA, DHS, DOE, DoD, and state fusion centers, to better understand vulnerabilities, emerging threats, and mitigation efforts. Public-private partnerships are essential in addressing cybersecurity challenges faced by co-ops, thereby enhancing the energy resilience of the communities they serve.

#### **Rural and Municipal Utility Cybersecurity Program**

Nowhere is this more immediate than with the Rural and Municipal Utility Cybersecurity Program, or RMUC. This \$250 million program, authorized through FY 2026, is a generational opportunity to improve the cybersecurity posture of electric cooperatives and municipally owned electric utilities. RMUC prioritizes co-ops with the greatest need of support that serve the nation's most critical infrastructure, including military installations, to help them make the necessary investment to secure the grid.

The Department of Energy (DOE) announced last fall \$80 million in RMUC funding that will directly support more than 400 cooperatives' cybersecurity programs. Much of that funding has yet to be released to the award winners. We encourage DOE to move expeditiously to distribute the awarded funds so that electric cooperatives can put them into action to defend their critical infrastructure.

While co-ops await the lion's share of funds, DOE has utilized RMUC funds to host multiple advanced utility training sessions across the country. These intensive, three-day programs, which were attended by more than 200 individuals from 123 electric cooperatives, were designed to

help cyber personnel improve the security of industrial control systems and operational technology.

Additionally, NRECA was awarded \$4 million cooperative agreement to launch the Project Guardian program. NRECA's Project Guardian is a multifaceted program focused on ensuring that no co-op is left behind and developing frameworks for four key focus areas: Cyber Champions; Threat Analysis Center Expansion; Cyber Resilience Initiative; and Education, Training, and Workforce Development. These focus areas will allow NRECA to target cooperative cybersecurity needs to develop self-assessment tools, tabletop exercises, and expand access to experienced cybersecurity personnel who can strengthen defenses and improve planning and incident response.

There is an estimated \$160 million left in RMUC with less than a year left in its authorization. Given the importance this program represents to electric cooperatives and our nation's security, NRECA is strongly urging Congress to reauthorize this program. RMUC is helping move the needle for electric co-ops to improve their cybersecurity protections, but there is still more to be done.

#### Industrial Control System for Rural Electric Cooperatives

Another federally funded initiative utilized by electric cooperatives is the Industrial Control Systems – Rural Electric Cooperative (ICS-REC). This program is focused on strengthening cybersecurity for operational technology (OT) environments by helping member co-ops expand their cyber monitoring capabilities of their industrial control facilities. In September, ICS-REC, originally funded at \$15 million, was awarded an additional \$5 million by DOE, recognizing the success and need for the program. NRECA is partnering with member co-ops to identify and deploy industrial control system monitoring technologies that will provide cyber visibility, detection, and response capabilities for energy delivery systems. Sophisticated cyber actors increasingly target these systems because of their role in maintaining reliability and safety. Through ICS-REC, cooperatives gain access to best practices for network segmentation, vulnerability management, and incident response specific to OT assets. The program also fosters collaboration among co-ops and federal partners to develop practical solutions that address the unique challenges of rural infrastructure.

#### **Conclusion**

Securing America's electric grid is essential to our national security, economic stability, and the well-being of every community we serve. Electric cooperatives are committed to doing their part, but we cannot do it alone. While electric cooperatives are making smart investments and building strategic partnerships to strengthen our cyber readiness, more work can be done. RMUC reauthorization and the timely release of remaining funds from this program are critical steps to ensure rural communities are not left behind. With continued partnership and targeted investment, we can strengthen our defenses, protect critical infrastructure, and keep the lights on

for 42 million Americans. The last two decades have seen significant advancement in how electric cooperatives secure our grid, but there is much more work still to do.

I thank the Committee for the chance to highlight the challenges and opportunities to securing our grid and look forward to answering your questions.

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 public 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 cowitnesses 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:]

**TESTIMONY OF**

**Harry Krejsa**  
**Director of Studies**  
**Carnegie Mellon Institute for Strategy & Technology**

**BEFORE**

**The House Energy & Commerce Committee, Energy Subcommittee**

**ON**

**Securing America's Energy Infrastructure:**  
**Addressing Cyber and Physical Threats to the Grid**

**December 2, 2025**  
**Washington, DC**

**Summary Points**

- The AI boom is creating unprecedented demand for electricity, driving a massive and digitally-native expansion of the U.S. power grid. This transformation could either bring vital security and resilience advantages with it, or merely paper over our grid's vulnerability to attack, particularly from China, whose hackers have already infiltrated our aging infrastructure.
- Defending our energy ecosystem—and the AI race it is powering—will require a whole-of-nation approach that integrates new, modern energy stakeholders with traditional national security leaders. Only by leveraging both perspectives can the United States simultaneously capitalize on the abundance and security potential of modern energy technologies, mitigate their sources of technical risk, and retake industrial leadership from China's early advantage in the field.
- Speed and adaptability must define our response. The convergence of AI and advanced energy infrastructure is evolving faster than our governance structures can keep up. Success will require:
  - Rethinking existing industry convening and coordination structures;
  - Adopting more dynamic risk and reward assessments to identify critical "linchpin technologies" (like batteries, smart inverters, or virtual power plants);
  - Combining public-sector threat intelligence with private-sector purchasing power to drive secure-by-design practices and streamline secure deployment; and
  - Accelerating R&D priorities on "leap ahead" technologies that can break our dependence on Chinese-controlled supply chains, like next-generation batteries, enhanced geothermal, advanced nuclear, or fusion energy.

Thank you Chairman Latta, Ranking Member Castor, and Members of the Committee for the opportunity to talk to you today about why the AI-driven transformation of our energy infrastructure is both our greatest near-term vulnerability and our best opportunity to build a more defensible grid. I am the research director for the Carnegie Mellon Institute for Strategy & Technology, and a specialist in US-China technological competition. I came to Carnegie Mellon from a tour in government spanning both the Trump Pentagon and the Biden White House, where I helped devise new military doctrine for offensive cyber operations, and then led the development of the National Cyber Strategy. That experience left me convinced that the People's Republic of China views our grid as a strategic target—and that the technologies now reshaping our energy system have become a new front in great power competition.

**The Opportunity: The AI Infrastructure Buildout is a Golden Opportunity to Simultaneously Secure Our Grid and Power Our Future**

Artificial intelligence's explosive growth is driving a historic transformation of America's energy infrastructure. The booming expansion of data centers across the country is creating unprecedented electricity demand, and with it, historic levels of investment in our power grid that no other critical infrastructure sector enjoys.

Yet this AI-driven buildout is also arriving at a moment of profound vulnerability. Our aging grid is a hodgepodge of digital tools sitting atop an analog foundation that was never designed for modern levels of connectivity. The U.S. government has warned consistently that the PRC is seeking to exploit this tension. Chinese President Xi Jinping reportedly has directed the People's Liberation Army (PLA)—China's military—to be prepared to do just that in a conflict over Taiwan by the year 2027.<sup>1</sup> In anticipation of such a conflict, Beijing has been investing in cyber capabilities and operations intended to disrupt our critical infrastructure. Our inconsistent mix of older, insecure infrastructure and highly interconnected computer systems is creating “seams” in technology that are too easy for cyber actors to exploit.

Exploiting these “seams” during a crisis would have both military and civilian costs. Leaders from the Cybersecurity and Infrastructure Security Agency (CISA) have testified to Congress<sup>2</sup> that PRC cyber actors are seeking to preposition disruptive cyber effects on U.S. infrastructure to stymie Washington's ability to project power abroad while sowing societal chaos at home.<sup>3</sup> FBI leaders have similarly warned that these malicious cyber campaigns are “broad and unrelenting,” and that Beijing's “plan is to land low blows against civilian infrastructure to try and induce panic and break America's will to resist.”<sup>4</sup> Recent research into cyberattacks against hospitals by criminal ransomware gangs suggests that even simple disruptions to computer services can meaningfully raise patient mortality rates; if paired with disruptions to water or power, it is easy to imagine how human consequences could worsen quickly within and beyond the healthcare system.<sup>5</sup>

Microsoft in 2023 publicly exposed one PRC state-backed hacking group responsible for a variety of critical infrastructure intrusions, issuing them the taxonomic moniker “Volt Typhoon<sup>6</sup>.” Volt Typhoon was notable for its stealth, using a variety of means to secure a user’s valid credentials and then wielding those credentials so that their nefarious activities blended into legitimate network traffic (cyber tradecraft known as “living-off-the-land techniques”). Volt Typhoon apparently has been active on U.S. systems since 2021 and motivated some of the federal government’s most urgent recent warnings about the vulnerability of Americans’ infrastructure.<sup>7</sup> With only 10-20% of our electricity system under federal cybersecurity oversight, a rapidly-diversifying industry ecosystem, and an outdated governance apparatus too fragmented to address systemic vulnerabilities, the status quo is dangerously untenable for both the AI race and our critical services.<sup>8</sup>

Yet this crisis presents us with a golden opportunity to pour a stronger foundation for both our public safety and our energy ambitions alike. The energy technologies overwhelmingly powering our recent grid expansion are far more digitally-native than what has come before, from on-site co-generation and battery storage to smart inverters and virtual power plants. These modern systems 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. These technologies are also shepherding a smarter, more distributed grid architecture—one that is not only more defensible, but also resilient and self-healing, capable of quarantining disruptions and preventing cascading blackouts.

Many of these modern technologies also promise a new frontier in energy security. Nuclear power, geothermal wells, inverter-based resources, and battery storage—the preferred energy sources for most tech giants, and the source of most new electricity being added to the grid—either require no or infrequent refueling, and in some cases even approach near-zero-marginal-cost electricity generation.<sup>9</sup> Being liberated from the ups and downs of commodity fuel prices would be a significant benefit for American energy consumers, who are facing significant increases in their utility bills. But this transformation would also be a valuable defense against a US-PRC contingency in the Indo-Pacific. Our allies and partners in the region, upon whose grids our own forward-deployed forces rely, are heavily dependent on maritime fuel shipments for their electricity. Modern and digitally-native energy technologies promise to be not only more defensible against the kinds of cyberattacks we know Beijing is planning against our allies, but also more resilient against blockades and other naval risks that fragile oil and gas tankers will likely face in any such conflict.

### **The Urgency: AI Competition is Taking Center Stage in US-China Competition – and Painting A Target On Our Grid**

But as the AI boom brings more opportunities to harden our grid against attack, it may also increase the interest of potential attackers. Compute power is directly and increasingly tied to



electricity availability, making our grid the strategic chokepoint in the race for artificial intelligence advantage. As Beijing recognizes the strategic implications—especially after tools like DeepSeek, Qwen, and Kimi demonstrated China's formidable AI capabilities—it will likely paint an even bigger target on our energy infrastructure and increase their and others' risk tolerance for more aggressive cyber operations. The shift from training-intensive to inference-intensive AI compounds this challenge, as compute requirements diffuse from remote mega-centers to more distributed, latency-sensitive facilities closer to everyday Americans—and potentially growing our compute infrastructure's attack surface in the process.

While the United States has a narrow lead in the AI race for now, China has secured an advantage in the swift, cheap deployment of electricity that will power the race into the future. Beijing has used its early capture of smartphone and electronics manufacturing to dominate what some are calling the "electrotech stack"—the foundational components that underpin modern energy systems, AI infrastructure, robotics, and many other technologies that will likely be key to future innovation and growth.<sup>10</sup> Beijing controls the majority of global battery production, precision magnets, power electronics, and other critical components that were refined and miniaturized during the smartphone revolution and now define the digitally-native energy future. These cascading advantages mean that even as the United States races to deploy modern energy technologies to power our AI ambitions, we remain dangerously dependent on the very actor from whom we need to defend our grid. While federal investments retained in the One Big Beautiful Bill Act continue to support the standup of domestic battery manufacturing, advanced nuclear, and enhanced geothermal development, we are still playing catch-up in a game where China already has secured a considerable lead.

The convergence of energy and compute infrastructure around this shared electrotech heritage means that securing our AI future will require not just building more data centers or power plants, but fundamentally reconceptualizing, securing, and—where risk prioritization requires it—reshoring the component technologies that make both possible. Our policy and governance frameworks are dangerously unprepared for this convergence of opportunities and challenges accompanying the AI-driven grid transformation. Traditional infrastructure protection bodies have been slow to incorporate modern energy stakeholders, new market entrants are too often naive about security risks and supply chain dependencies, and no unified approach exists for the convergence of digital and legacy technologies that are reshaping our grid.

In my testimony today, I want to make the case that success requires urgent action and national leadership across three lines of effort:

- Unifying strategic priorities for the security, availability, and swift deployability of modern energy technologies;
- Organizing disparate modern energy and national security stakeholders across the public and private sectors; and

- Maintaining vigilance over fast-moving developments in both AI architectures and energy systems that could rapidly shift our security posture.

Taking these steps will ensure the public and private sectors are prepared to collaboratively secure the energy foundation for America's future while denying our adversaries the leverage to disrupt it.

**The United States Needs unified, Strategic Priorities for the Security, Availability, and Swift Deployment of Modern Energy Technologies**

Beijing clearly views its early lead in modern energy manufacturing, and its ability to rapidly deliver resilient and abundant electricity, as a strategic asset worth protecting. Chinese President Xi Jinping has repeatedly emphasized the need to coordinate "new energy" development alongside broader national security considerations, fusing its national security and economic impacts.<sup>11</sup> As global investment in these digitally-native technologies approaches \$2 trillion annually, China has positioned itself at the center of one of history's largest capital opportunities—insulating itself from economic isolation while maintaining leverage over critical supply chains.<sup>12</sup> The United States must signal an equally serious political, financial, and security commitment to leadership in these technologies.

While Washington shouldn't reactively mirror Beijing's every move, it must recognize when our competitors are right: Modern, digitally-native energy technologies are not just trendy nice-to-haves, but strategic imperatives for maintaining competitiveness in both the AI race and the broader contest for technological leadership.

Recommendation

The Committee should consider how to ensure the U.S. government adopts a whole-of-nation strategy to guarantee the security, availability, and vendor trustworthiness of the modern energy technologies that will be key to powering the AI race and subsequent engines of innovation.

- This strategy should focus in the near term on the cybersecurity of key modern energy technologies (especially those with high dependence on PRC supply chains) and scalable solutions to promote the faster deployment of secure and resilient electricity.
- For the medium term, it should adapt lessons learned from U.S. and allied semiconductor supply chain diversification efforts, including maintaining both leading-edge innovative engines to maintain advantage as well as trailing-edge production capacities to hedge against supply disruption.
- This strategy should prioritize maintaining U.S. and allied leadership in international energy technology financing. This should ensure that cyber-secure and trusted technology is accessible to emerging markets, that those markets' demand can contribute to scaling U.S. and allied manufacturing capacity, and in so doing, balance PRC influence over the

future of those markets' energy security so we avoid another Huawei-and-5G-style setback.<sup>13</sup>

### **We Need Federal Leadership to Organize Disparate Modern Energy and National Security Stakeholders Across the Public and Private Sectors**

The development, security, and deployment of modern energy technologies is increasingly intertwined with US-China competition, but the communities driving each remain dangerously siloed. Traditional energy and security stakeholders possess decades of experience mitigating national security threats, but are poorly integrated with the entrepreneurs and innovators deploying digitally-native technologies that now make up the majority of new electricity generation. Meanwhile, modern energy developers—often smaller, more numerous, and less security-sophisticated than their traditional counterparts—are racing to deploy sophisticated software-defined systems without adequate access to threat intelligence or security frameworks. This disconnect extends throughout our governance structures: Public-private critical infrastructure protection bodies have not updated their frameworks to address the fundamentally distinct way modern energy technologies interact with digital connectivity, while energy policy processes deploy grid-transforming technologies with minimal integration of national security expertise.

The convergence of AI compute and rapidly-digitizing energy infrastructure demands a more integrated community of practice around the risk of Chinese tech dependencies that can transform sources of potential technical vulnerability into strategic advantage, but will require leadership from the federal government and industry executives to succeed.

#### Recommendation

The Committee should consider how to ensure the U.S. government intentionally integrates relevant national security and modern energy policymaking processes and frameworks.

- Given the rapidly growing importance of modern, digitally-native technologies to our grid, the National Energy Dominance Council—and other relevant energy-focused policymaking bodies and processes—should include CISA and the National Security Agency in its membership.
- The next National Infrastructure Risk Management Plan, a White House-directed policy update coordinated by CISA, should explicitly incorporate the novel considerations introduced by modern energy technologies.

#### Recommendation

The Committee should consider how to ensure industry coordination and intelligence distribution bodies, like Information Sharing and Analysis Organizations and Centers (ISAOs/ISACs),

update their membership and processes to incorporate and engage with the modern energy ecosystem and its structural novelties.

- ISAOs/ISACs should review a) their membership to ensure they reflect the modern, digitally-native energy influence in their marketplaces, and b) restructure their coordination mechanisms to better integrate with smaller, more numerous, and less risk-sophisticated modern energy stakeholders.
- ISAOs/ISACs and sector-specific coordinating councils should adapt security and resilience resources for modern energy stakeholders' unique considerations, including those on secure-by-design principles, technical standards implementation, and open-source software security.

#### Recommendation

The Committee should consider how electricity sector stakeholders, from utilities to the tech industry, can drive coordinated cybersecurity practices that are tailored to and scalable among the broader modern energy marketplace.

- The country's energy utilities and infrastructure operators should coordinate on shared guidance for "what right looks like" for the unique cybersecurity considerations of integrating digitally-native energy technologies into their grids. This will make it easier for more modern energy vendors to scale their contributions to security and resilience across different regional regulatory jurisdictions and integrate into different regional grids more quickly, all while helping mitigate broad regulatory gaps in electricity infrastructure cybersecurity.
- Cloud computing hyperscalers, whose next-generation AI training and inference data centers are helping to propel historic increases in electricity demand, should use their purchasing power to inform and drive new modern energy cybersecurity practices. As some of the few actors in the U.S. economy possessing deep expertise in both energy economics and PRC exploitation of flawed software, today's AI-driven hyperscalers should use their influence over the next generation of energy deployment to inform and drive the development of modern energy-specific security practices.

#### **Industry and Government Must Remain Nimble to – and Vigilant of – Fast-Moving Developments in Both AI architectures and Energy Systems That Could Rapidly Shift Our Security Posture**

The convergence of AI and modern energy infrastructure is evolving at unprecedented speed, demanding frameworks that can adapt as quickly as the technologies they govern. Just years ago, batteries were peripheral to grid planning—today they keep entire states' grids operational during peak demand.<sup>14</sup> The shift from training-intensive to inference-intensive AI is similarly upending assumptions about data center geography, latency requirements, and co-located generation needs. Our prioritization frameworks must be equally dynamic, capable of rapidly

reassessing which technologies pose the greatest systemic influence—and bring the most digital risk—as the landscape shifts. Virtual power plants, for example, are entirely software-defined with massive systemic impact, yet their digital nature may make them easier to secure through established software validation practices—if we act quickly. Batteries present a more complex challenge: digitally sophisticated enough to pose risk, systemically critical to grid stability, yet often dependent on Chinese supply chains that challenge traditional security controls. Meanwhile, breakthroughs in solid-state batteries, enhanced geothermal, or fusion reactors could suddenly offer leap-ahead opportunities to break supply chain dependencies—but only if policymakers are watching for them.

As specific technologies and threats evolve, certain principles must endure: prioritizing the security of our most systemically critical infrastructure, maintaining vendor trust and supply chain awareness, and ensuring that every new deployment enhances rather than undermines our grid's defensibility against adversary attack. But in this current environment, our greatest risk may be fighting yesterday's war with outdated assumptions about where threats and opportunities lie. To operationalize this balance between enduring priorities and adaptive flexibility, we need assessment frameworks that are rigorous enough to guide billion-dollar infrastructure investments yet nimble enough to evolve with the rapidly shifting AI-energy landscape. These frameworks must evaluate both relative risk—assessing digital exposure and systemic influence across technologies—and difficulty of remediation—identifying which vulnerabilities can be addressed through scalable interventions, versus those requiring bespoke solutions.

This will require a more nimble approach to risk assessment and technology development—one that can identify which emerging technologies pose the greatest security exposure while simultaneously spotting opportunities to break free from geopolitically risky dependencies. We need frameworks agile enough to continuously reassess the threat landscape as new technologies achieve critical mass, yet rigorous enough to guide major infrastructure investments. Equally important, we must actively cultivate breakthrough alternatives—like in solid-state batteries, enhanced geothermal, or advanced nuclear and fusion—that could provide leap-ahead substitutes for the PRC-dominated components that define our energy supply chains. The U.S. government should work with industry to establish assessment mechanisms to track this evolving landscape, and R&D priorities to shape it in America's favor.

#### Recommendation

The Committee should consider how to ensure the Office of the National Cyber Director, Department of Energy, CISA, and the National Security Agency develop a joint risk and

remediation framework for modern energy technologies that can inform legislative priorities for onshoring initiatives and sourcing from Foreign Entities of Concern.

- The assessment should recognize “linchpin technologies” key to our AI-driven grid buildout according to digital exposure, systemic impact, and relevant threat intelligence. It should identify areas of scalable interventions for swifter and more secure deployment—such as with broader adoption of certain secure software development practices—and areas where bespoke interventions may be required.
- The assessment should consider near-term cybersecurity considerations as well as longer-term supply chain dependencies that may impede greater certainty in relevant technologies’ security and resilience. These can better inform investment and manufacturing tax credits and other Congressional actions to shape our evolving energy technology ecosystem.

#### Recommendation

The Committee should consider how to ensure the Office of Science & Technology Policy, the Department of Energy, and the Department of Commerce establish an R&D strategy for modern energy technologies that not only are game-changing generation and storage tools, but also provide “leap-ahead” substitution opportunities for U.S. and allied manufacturers currently dependent on PRC supply chains and electrotech advantages.

- This R&D strategy should identify and accelerate emerging technologies that could help break U.S. and allied dependence on vulnerable or insecure supply chains.
- This strategy should adjudicate for which technologies the United States is willing to tolerate relative PRC dominance—perhaps including, for example, relatively “dumb” and commodity energy components—and those that are more systemically impactful and over which the United States should seek to retain influence and Congress can legislate such inducements, such as in battery storage or other more digitally-native platforms.

#### **Conclusion**

Chairman Latta, Ranking Member Castor, and Members of the Committee: the question before us is not simply how to defend an aging grid against cyber and physical threats—it is whether the United States will seize a once-in-a-generation opportunity to build something stronger in its place. The AI-driven transformation of our energy infrastructure is happening now, with or without deliberate security leadership. Left unguided, this buildout risks entrenching our dependence on adversary-controlled supply chains and expanding our attack surface at the very moment Beijing is positioning to exploit it. But approached strategically—with unified priorities, organized stakeholders, and adaptive vigilance—this same transformation can yield an energy foundation that is not only more abundant and affordable, but fundamentally more defensible than what came before. The technologies powering the AI race were designed for the digital age;



our governance and security frameworks must be as well. Thank you for the opportunity to discuss these issues before the Committee today.<sup>15</sup>

<sup>1</sup> “Statement of Admiral John C. Aquilino, U.S. Indo-Pacific Command, on U.S. Indo-Pacific Command Posture, to the U.S. House Armed Services Committee,” Congress.gov, 20 March 2024, <https://www.congress.gov/118/meeting/house/116960/witnesses/HHRG-118-AS00-Wstate-AquilinoJ-20240320.pdf>.

<sup>2</sup> Formally, “Select Committee on Strategic Competition Between the United States and the Chinese Communist Party.”

<sup>3</sup> “Testimony of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, on the CCP Cyber Threat to the American Homeland and National Security, to the Select Committee on Strategic Competition Between the United States and the Chinese Communist Party,” Congress.gov, 31 January 2024, <https://docs.house.gov/meetings/ZS/ZS00/20240131/116776/HHRG-118-ZS00-Wstate-EasterlyJ-20240131.pdf>.

<sup>4</sup> “Wray: Chinese government poses ‘broad and unrelenting’ threat to U.S. critical infrastructure,” FBI, 18 April 2024, <https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says>.

<sup>5</sup> Zac Amos, “The Link Between Health Care Cyberattacks and Patient Mortality,” The Journal of mHealth, 8 January 2024, <https://thejournalofmhealth.com/the-link-between-health-care-cyberattacks-and-patient-mortality/>.

<sup>6</sup> “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques,” Microsoft Security Insider, 25 May 2023, <https://www.microsoft.com/en-us/security/security-insider/emerging-threats/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques>.

<sup>7</sup> Julian E. Barnes, “China Could Threaten Critical Infrastructure in a Conflict, N.S.A. Chief Says,” The New York Times, 17 April 2024, <https://www.nytimes.com/2024/04/17/us/politics/china-cyber-us-infrastructure.html>.

<sup>8</sup> “Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems,” Government Accountability Office, March 2021, GAO-21-81, <https://www.gao.gov/assets/gao-21-81.pdf>; “Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid,” Government Accountability Office, August 2019, GAO-19-332, <https://www.gao.gov/products/gao-19-332>.

<sup>9</sup> Dan McCarthy, “Chart: 96 percent of new US power capacity was carbon-free in 2024,” Canary Media, January 2025, <https://www.canarymedia.com/articles/clean-energy/chart-96-percent-of-new-us-power-capacity-was-carbon-free-in-2024>.

<sup>10</sup> Daan Walter, Sam Butler-Sloss, and Kingsmill Bond, “Rewiring the Energy Debate,” The Electrotech Revolution, May 2025, <https://electrotechrevolution.substack.com/p/rewiring-the-energy-debate>.

<sup>11</sup> “Xi Jinping Emphasizes Vigorously Promoting High-Quality Development of New Energy in China to Make Greater Contributions to Building a Clean and Beautiful World during the 12th Collective Study Session of the CCP Central Politburo,” CSIS Interpret: China policy document translation, published by Xinhua News Agency, 29 February 2024, <https://interpret.csis.org/translations/xi-jinping-emphasizes-vigorously-promoting-high-quality-development-of-new-energy-in-china-to-make-greater-contributions-to-building-a-clean-and-beautiful-world-during-the-12th-collective-study-session/>.

<sup>12</sup> Executive Summary of the World Energy Outlook 2024, International Energy Agency, October 2024, <https://www.iea.org/reports/world-energy-outlook-2024/executive-summary>.

<sup>13</sup> Brian Deese, “The Case for a Clean Energy Marshall Plan: How the Fight Against Climate Change Can Renew American Leadership,” Foreign Affairs, 20 August 2024, <https://www.foreignaffairs.com/united-states/case-clean-energy-marshallplan-deese>.

<sup>14</sup> Robert Walton, “Batteries are making the grid more reliable: NERC,” Utility Dive, June 2025, <https://www.utilitydive.com/news/batteries-grid-state-of-reliability-nerc/750649/>; Garrett Golding, “Solar, battery capacity saved the Texas grid last summer, an uncertain future awaits,” Federal Reserve Bank of Dallas, January 2025, <https://www.dallasfed.org/research/economics/2025/0114>.

<sup>15</sup> This testimony was adapted from recent research for the Carnegie Mellon Institute for Strategy & Technology.

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 ZACHARY 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:]

TESTIMONY OF Mr. Zachary Tudor  
Associate Laboratory Director, IDAHO NATIONAL LABORATORY

*before the*

UNITED STATES HOUSE OF REPRESENTATIVES  
COMMITTEE ON ENERGY AND COMMERCE  
SUBCOMMITTEE ON ENERGY

*concerning*

*“Securing America’s Energy Infrastructure:  
Addressing Cyber and Physical Threats to the Grid”*

December 2, 2025

Chairman Latta, ranking member Castor, and members of the committee, thank you for the opportunity to testify on a topic critical to our nation’s security. My name is Zach Tudor, and I am the associate laboratory director for National and Homeland Security at the Idaho National Laboratory (INL). I am a cybersecurity expert by education and trade, and I have spent most of my professional and military careers focused primarily on operational technology (OT) cybersecurity and the protection of United States (U.S.) critical infrastructure. The directorate I lead consists of nearly 900 scientists, engineers, cyber researchers, analysts, and staff dedicated to safeguarding the United States from the most consequential foreign and domestic threats, including cybersecurity threats that aim to disrupt our nation’s energy supply, clean water, telecommunications, and other critical functions. We are among the best in the world at understanding threats to critical infrastructure and, more importantly, developing solutions that protect our nation’s critical functions from attacks.

INL, managed by Battelle Energy Alliance, LLC, is one of 17 U.S. Department of Energy (DOE) national laboratories. Located in Idaho Falls, Idaho, INL employs more than 6,100 researchers and support staff with a common vision: to change the world’s energy future and secure our nation’s critical infrastructure. The national security mission I lead focuses on protecting the

nation's critical infrastructure, preventing the proliferation of weapons of mass destruction, and providing direct support to America's warfighters. Our decades of nuclear innovation—52 reactors built and tested, with next-generation demonstrations underway—forged INL's distinctive approach to securing critical systems distinctive for a deep understanding of OT and of the cybersecurity and engineering needed to secure systems and provide critical function assurance. INL's 890-square mile Site provides unique infrastructure to test threats and mitigations to our critical systems at scale.

#### **Lay of the Land: Cyber Threats to U.S. Critical Infrastructure**

The United States faces an unprecedented wave of cyber threats directed at our critical infrastructure. The 2025 Annual Threat Assessment of the U.S. Intelligence Community underscores this reality: Adversarial states are conducting aggressive campaigns to pre-position themselves within U.S. networks, with the goal of breaking our resolve and limiting our response options at a time of their choosing. Among these adversarial states, China, Russia, Iran, and North Korea stand out as key actors with distinct capabilities and motivations.

China is the most persistent and capable threat, embedding itself into OT networks across sectors. According to recent analysis from the Foundation for Defense of Democracies, China has significantly escalated its cyber-enabled economic warfare operations, targeting the U.S. through intellectual property theft, critical infrastructure intrusions, and mass collection of personally identifiable information.<sup>1</sup> Beijing's strategy aims to control global information and communications technology infrastructure, leveraging technology to manipulate vast amounts of

---

<sup>1</sup> Ravish, S., M. Montgomery. 2022. "China's Accelerating CEEW Campaign." Foundation for Defense of Democracies, CEEW Campaign. Last modified October 28, 2022.  
<https://www.fdd.org/analysis/2022/10/28/chinas-accelerating-ceew-campaign/>

data and disrupt essential services. This ambition is further supported by aggressive industrial policies and extensive legal frameworks that merge commercial ventures with intelligence collection, allowing China to access information from firms under its jurisdiction and blurring the lines between economic activity and espionage.<sup>2</sup> This multifaceted cyber and technological offensive poses a severe threat, underscoring China's intent to undermine U.S. economic stability and national security without direct military confrontation. As such, it is imperative for the United States to bolster its defenses and regulatory mechanisms against these insidious attacks.

Similarly, Russia seeks disruptive capabilities, demonstrated by its attacks against Ukraine's energy infrastructure, supply-chain assaults, and constant probing of U.S. industry and infrastructure. Iran has shown willingness to cause disruption for political leverage, particularly against water and oil resources. North Korea remains financially motivated but opportunistic, with capabilities extending into energy and telecommunication targets.

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 makes us particularly vulnerable. Our interdependent systems and heavy reliance on technology amplify the potential impact these threat actors pose. The modern-day risk environment in the United States is extensive and evolving because our critical infrastructures include:

---

<sup>2</sup> Burnham, J., J. Yang. 2025. "Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control." Foundation for Defense of Democracies, Public Comment. October 6, 2025. <https://www.fdd.org/analysis/2025/10/06/protecting-our-communications-networks-by-promoting-transparency-regarding-foreign-adversary-control-2/>

- **Interconnected Systems** – Energy, telecommunications, transportation, and water systems are deeply interdependent. A disruption in one sector often cascades across others, worsening the potential damage and complicating response efforts.
- **Unique U.S. Exposure** – Unlike other nations, the U.S. operates vast, digitized, and largely privately owned infrastructure. The sheer size and intricacy of our critical infrastructure systems and networks create significant challenges in implementing unified security measures across all sectors, increasing the potential for gaps in protection.
- **Aging Infrastructure** – Much of the critical infrastructure in the U.S. is aging, with many systems operating well past their intended life cycle. Consequently, many of these systems remain vulnerable to cyberattacks.
- **Lag in Security Upgrades** – The long lifecycle of industrial control systems, often operating for 30–40 years, ensures simplicity and efficiency. However, this results in a lag in adopting modern security technologies and standards. Consequently, these systems are more vulnerable to advanced cyberattacks, leaving critical infrastructure exposed to evolving threats.
- **Attractive Targets** – Infrastructure assets are both symbolic and practical targets. Disruption in these areas can have a significant impact on human health and safety, economic stability, and national security, making them highly attractive to adversarial actors.

Given that foreign adversaries are likely to continue their persistent use of cyberattacks against our critical infrastructure, it is essential for policymakers to understand their methods and distinct motivations.

### Key State Actors

The cybersecurity landscape is dominated by several key state actors, each with unique capabilities and objectives. China, Russia, Iran, and North Korea are routinely identified as the primary adversaries targeting U.S. critical infrastructure. Their actions range from espionage and intelligence gathering to disruptive attacks and financial extortion, posing significant risks to national security, economic stability, and human health and safety.

**China** – The People’s Republic of China (PRC) pursues long-term, stealthy cyber operations to collect intelligence, pre-position access, and prepare options for disruptive effects in the event of a crisis. The PRC favors a strategy denoted by asymmetrical actions, including winning without fighting, or achieving strategic objectives by undermining an adversary’s confidence and capabilities without engaging in direct conflict. This approach is a key aspect of irregular warfare, defined as a form of warfare in which states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities.<sup>3</sup>

In recent years, the U.S. has been the victim of this strategic approach as hacking campaigns<sup>4</sup> like Salt, Volt, and Flax Typhoon demonstrate how state-sponsored entities are infiltrating our digital ecosystems to steal sensitive data and embed themselves in our communications, industrial, and defense networks. Prominent organizations, including Microsoft,<sup>5</sup> Tenable,<sup>6</sup> and

---

<sup>3</sup> Theohary, C. A. 2024. “Defense Primer: What Is Irregular Warfare?” Congressional Research Service, Product Number IF12565. November 29, 2024. <https://www.congress.gov/crs-product/IF12565>

<sup>4</sup> Singleton, C., et al. 2025. “Countering Threats Posed by the Chinese Communist Party to U.S. National Security.” Foundation for Defense of Democracies, Congressional Testimony. March 5, 2025. <https://www.fdd.org/wp-content/uploads/2025/03/03-05-25-Singleton-Written-Testimony-Final-1.pdf>

<sup>5</sup> Microsoft Threat Intelligence. 2023. “Volt Typhoon Targets U.S. Critical Infrastructure with Living-Off-The-Land Techniques.” Microsoft, Research. Last modified May 24, 2023. <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

<sup>6</sup> Caveza, S. 2025. “Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor.” Tenable, Blog, Cyber Exposure Alerts. Last modified January 23, 2025. <https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor>

Dragos,<sup>7</sup> along with government agencies, such as the Cybersecurity and Infrastructure Security Agency,<sup>8</sup> the Federal Bureau of Investigation,<sup>9</sup> and the National Security Agency,<sup>10</sup> have confirmed that these campaigns remain active and continue to target critical infrastructure and key resources across the United States. Through these campaigns, the Chinese Communist Party is setting the conditions<sup>11</sup> to execute destructive cyberattacks against the United States should there be a regional conflict in the Pacific over Taiwan. These efforts are part of China's broader strategy to weaken our infrastructure and undermine our willingness to engage in a prolonged conflict.

Most concerning, China's aim is to conduct espionage and pre-position themselves on the IT networks of U.S. critical infrastructure while remaining undetected for as long as possible, providing them with a rapid capability to disrupt or destroy our critical infrastructure at the time and place of their choosing. These sophisticated campaigns have knowingly impacted critical infrastructure sectors, including energy, communications, manufacturing, utilities, transportation, construction, maritime, government, information technology, and education.

---

<sup>7</sup> Hanrahan, J. 2024. "VOLTZITE Espionage Operations Targeting U.S. Critical Systems." Dragos Safeguarding Civilization, Intelligence Brief. Last modified February 2024. [https://hub.dragos.com/hubfs/116-Datasheets/Dragos\\_SB\\_IntelVOLTZITE\\_Feb24\\_FINAL\\_r4.pdf?hsLang=en](https://hub.dragos.com/hubfs/116-Datasheets/Dragos_SB_IntelVOLTZITE_Feb24_FINAL_r4.pdf?hsLang=en)

<sup>8</sup> CISA. 2024. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." News & Events, Cybersecurity Advisory. Last modified February 7, 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

<sup>9</sup> Leatherman, B. 2025. "FBI Announces Joint Cybersecurity Advisory Related to Salt Typhoon." U.S. Federal Bureau of Investigation. Video, August 27, 2025. <https://www.fbi.gov/video-repository/salttyphoon082725.mp4/view>

<sup>10</sup> National Security Agency/Central Security Service. 2025. "NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical Infrastructure Organizations." Press Release, August 27, 2025. <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/>

<sup>11</sup> Harper, J. 2025. "Air Force Cyber Leader Warns Threats Like Volt Typhoon Could Enable China to Wage 'Total War' Against US." DefenseScoop. Last modified September 23, 2025. <https://defensescoop.com/2025/09/23/volt-typhoon-china-us-air-force-cyber-defensive-operations/>

**Russia** – Russia continues to pose a credible threat to the U.S. across the cyber domain despite the current constraints they face from the war in Ukraine. Russian state-sponsored cyber actors routinely engage in espionage, pre-positioning access, campaigns that compromise supply chains, and sabotage. The Russian cyber threat is multifaceted, blending state-sponsored actors like military and intelligence services with hacktivist groups, and more traditional criminal organizations.<sup>12</sup>

From ransomware attacks that extort millions of dollars to major supply-chain attacks for covert intelligence gathering, the Kremlin’s cyber strategy integrates technical and psychological operations within its concept of information confrontation<sup>13</sup> to achieve strategic objectives, often below the threshold of armed conflict, sometimes referred to as irregular warfare. They combine offensive measures like infrastructure attacks with defensive efforts such as “digital sovereignty,” leveraging state actors, proxies, and false flags to exploit open systems and obscure attribution.<sup>14</sup> Furthermore, a recent Atlantic Council report thoroughly examined Russia’s intensifying bilateral ties with China, Iran, and North Korea. The report conveys the particularly close relationship between Russia and China, particularly related to critical military capabilities including artificial intelligence, quantum computing, and space technology.<sup>15</sup>

---

<sup>12</sup> Sherman, J. 2022. “Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior.” Atlantic Council, Cyber Statecraft Initiative, Issue Brief, September 2022. <https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Untangling-the-Russian-Web-Spies-Proxies-and-Spectrums-of-Russian-Cyber-Behavior-1.pdf>

<sup>13</sup> Voo, J., Singh, V. V. 2025. “Russia’s Information Confrontation Ecosystem.” IISS, Charting Cyberspace. Last modified June 26, 2025. <https://www.iiss.org/charting-cyberspace/2025/06/russias-information-confrontation-ecosystem/>

<sup>14</sup> Hakala, J., J. Melnychuk. 2021. “Russia’s Strategy in Cyberspace.” 978-9934-564-90-1, NATO Strategic Communications Centre of Excellence.

<sup>15</sup> Stent, A. 2025. “THE CRINK: Inside the New Bloc Supporting Russia’s War Against Ukraine.” Atlantic Council, Eurasia Center. <https://www.atlanticcouncil.org/wp-content/uploads/2025/10/the-crink-inside-the-new-bloc-supporting-russias-war-against-ukraine.pdf>



In the last decade, Russia has emerged as a major source of cyberattacks against global critical infrastructure, both through state-sponsored operations and cybercriminal groups operating from Russian territory. Notable attacks include the 2015 BlackEnergy and 2016 Industroyer campaigns against Ukrainian power companies, the 2017 NotPetya attack that began in Ukraine and spread globally causing billions in damages, the Triton malware attack on a Saudi Aramco petrochemical plant, the 2020 SolarWinds supply-chain compromise, and the 2021 Colonial Pipeline ransomware attack by the Russia-based DarkSide group. Many of these attacks initiated in information technology (IT) networks and then propagated to OT systems through their interconnections.

With the war in Ukraine, Russian cyber activity has only increased with the FBI warning that a Russian cyber-espionage group has targeting a known vulnerability in CISCO equipment to go after telecommunications, higher education, and manufacturing sectors across North America, Asia, Africa, and Europe. In 2024, Russian-linked hacking groups carried out a cyberattack against a Texas water treatment facility that caused a tank to overflow. The incident led national security agencies to issue a stark warning to the more than 170,000 private U.S. water and wastewater treatment facilities to shore up their cyber defenses. Two months ago, European leaders were briefed on two cyberattacks that targeted water systems in Norway and Poland, both linked to Russian hackers.

**Iran** – According to the Institute for National Security Studies, Iran’s cyber capabilities can disrupt, sabotage, and destroy civil and commercial targets, critical national infrastructure, and military capabilities.<sup>16</sup> Their cyber espionage and information operations have grown over time

---

<sup>16</sup> Freilich, C. 2024. “The Iranian Cyber Threat.” The Institute for National Security Studies. Accessed November 20, 2025. <https://www.inss.org.il/publication/iranian-cyber/>

and represent a significant threat, particularly to the United States, Israel, and Saudi Arabia. They have steadily improved their cyber warfare capabilities, with espionage, sabotage, and revenge as core motivations. Experts characterize Iran's cyber ambitions as asymmetrical, clandestine, and focused on plausible deniability, mixing state-sponsored actions with sympathetic hacktivist organizations that together complement the well-understood proxy and shadow operations the Islamic Republic has favored for decades.<sup>17</sup>

Regarding specific critical infrastructure threats, Iran has in recent years actively targeted U.S. water, energy, manufacturing, and healthcare organizations after finding success executing similar campaigns against Israel in response to the Israel-Hamas conflict.<sup>18</sup> In 2023, a water authority near Pittsburgh, Pennsylvania, was breached by state-sponsored Iranian hackers and forced to shut down parts of their IT and OT networks. Though the water supply remained safely available to customers, the hackers managed to shut down a pump on a supply line that provided drinking water from the plant to local communities.<sup>19</sup> Reports of similar compromises affecting Unitronics Vision Series programmable logic controllers were reported by companies operating energy, food, beverage manufacturing, and healthcare equipment in several states.

In 2024, an international contingent of national security organizations issued an updated advisory to warn critical infrastructure equipment owners and operators of continued malicious cyber

---

<sup>17</sup> Daragahi, B. 2023. "Iran is Using its Cyber Capabilities to Kidnap its Foes in the Real World." Atlantic Council, IranSource. Last modified May 24, 2023. <https://www.atlanticcouncil.org/blogs/iransource/iran-cyber-warfare-kidnappings/>

<sup>18</sup> CISA. 2025. "Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest." Accessed November 20, 2025. <https://www.ic3.gov/CSA/2025/250630.pdf>

<sup>19</sup> Counter Threat Unit Research Team. 2023. "Iranian Cyber Av3ngers Compromise Unitronics Systems." Last modified December 7, 2023. <https://www.secureworks.com/blog/iranian-cyber-av3ngers-compromise-unitronics-systems>

activity by Iranian-affiliated cyber actors.<sup>20</sup> This joint advisory was informed by recent FBI investigations and included new information on likely tactics, techniques, and procedures the Islamic Republic could use against U.S. critical infrastructure. This year, several U.S. national security organizations published an updated factsheet detailing increased cyber threats and risks against U.S. critical infrastructure by Iranian state-sponsored or affiliated threat actors.<sup>21</sup> Of particular concern, the agencies noted that defense industrial base companies with relationships in or with Israeli research and defense firms were at greater risk.

**North Korea** – North Korea has emerged as a persistent player in the cyber domain, leveraging its capabilities to conduct espionage, theft, and disruptive attacks against its perceived enemies. While their tactics often lack the scale of more sophisticated adversaries like China and Russia, they frequently deploy harassment and nuisance strategies designed to sow confusion, frustration, and financial loss. The regime’s state-sponsored hackers often target financial institutions, critical infrastructure, and government agencies.

North Korea is known for aggressive cyber operations, including the 2014 Sony Pictures hack and the 2017 WannaCry ransomware attack.<sup>22</sup> These attacks demonstrate their capability for cyber warfare and use of cybercriminal activities to fund their regime. In 2024, global companies lost \$1.34 billion<sup>23</sup> to North Korean cyberattacks. Earlier this year, North Korean hackers stole

---

<sup>20</sup> CISA. 2024. “IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities.” Last modified December 18, 2025. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

<sup>21</sup> CISA. 2025. “Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest.” Accessed November 20, 2025. <https://www.ic3.gov/CSA/2025/250630.pdf>

<sup>22</sup> U.S. Department of Justice. 2018. “North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.” Archives, Press Release, September 6, 2018. <https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>

<sup>23</sup> Chainalysis Team. 2024. “\$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July.” Chainalysis. Last modified December 19, 2024. <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>

\$1.5 billion in cryptocurrency through the ByBit exchange.<sup>24</sup> Beyond financial theft, the North Korean regime has been linked to various cyber intrusions aimed at gathering intelligence on military capabilities and critical infrastructure in adversarial nations, particularly the U.S. and South Korea.

Cybersecurity firms like Mandiant<sup>25</sup> and CrowdStrike<sup>26</sup> have reported on North Korean cyber tactics, revealing a focus on stealth and deception designed to evade detection. As geopolitical tensions continue, North Korea is expected to further employ its cyber capabilities to conduct disruptive operations and espionage, posing an ongoing threat to U.S. and allied national security.

### **Sector-Specific Threats**

Conducting a cyberattack against the specialized computer systems controlling critical infrastructure is difficult. Such attacks usually require significant resources and months or years of preparation. However, our adversaries have learned that they can degrade or destroy critical infrastructure by targeting the easier-to-compromise IT networks that support these systems. Because IT and OT systems are intertwined across every critical infrastructure sector, this approach provides adversaries with widespread opportunities for disruption.<sup>27</sup> Adversaries have recognized these vulnerabilities, and they are adapting their strategies accordingly. Cyber threats

---

<sup>24</sup> CSIS. 2025. "The ByBit Heist and the Future of U.S. Crypto Regulation." Last modified March 18, 2025. <https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation>

<sup>25</sup> Fraser, N., et al. 2018. "APT38: Details on New North Korean Regime-Backed Threat Group." Google Cloud, Threat Intelligence. <https://cloud.google.com/blog/topics/threat-intelligence/apt38-details-on-new-north-korean-regime-backed-threat-group>

<sup>26</sup> Kapko, M. 2025. "CrowdStrike Investigated 320 North Korean IT Worker Cases in the Past Year." Cyberscoop. Last modified August 4, 2025. <https://cyberscoop.com/crowdstrike-north-korean-operatives/>

<sup>27</sup> Brumfield, C. 2025. "Foreign Hackers Breached a US Nuclear Weapons Plant via SharePoint Flaws." CSO, News Analysis. Last modified October 20, 2025. <https://www.csoonline.com/article/4074962/foreign-hackers-breached-a-us-nuclear-weapons-plant-via-sharepoint-flaws.html>

are a function of both adversary capability and intent. Not only are adversary capabilities becoming stronger and more sophisticated each year, but we are also seeing changes in their intent to use those capabilities against critical infrastructure. While the nation has developed better resilience, we have not kept pace with this growing threat, leaving us more vulnerable than ever before.

### **Electric Power Grid**

The U.S. electric grid is indispensable. It is the foundation for healthcare, communications, national defense, and societal functioning, but also a prime target. Russian cyber operations against Ukraine's grid in 2015 and 2016 proved that remote power disruption is viable. More recently, the emergence of the Industroyer2 malware in 2022 confirmed our adversaries continued tool development for grid attacks.<sup>28</sup> In 2023, analysts disclosed that China's Volt Typhoon group had infiltrated U.S. utility networks with the intent of long-term positioning for disruption. The previously mentioned 2025 Annual Threat Assessment of the U.S. Intelligence Community warns Russia and China are advancing capabilities that could disable segments of the U.S. grid during a major crisis. The emergence of artificial intelligence (AI) has shown promise in both the ability to enhance grid operations and defend the grid from cyberattacks, but it also introduces risks and conditions that could be exploited by adversarial cyber actors.<sup>29</sup>

### **Oil and Natural Gas**

The 2021 Colonial Pipeline ransomware attack showed how crippling an energy infrastructure

---

<sup>28</sup> Tidy, J. 2022. "Ukrainian Power Grid 'Lucky' To Withstand Russian Cyber-Attack." BBC. Last modified April 12, 2022. <https://www.bbc.com/news/technology-61085480>

<sup>29</sup> Industrial Cyber. 2025. "INL's TAIGR Initiative Confronts AI Hallucinations, Cyberattacks, Other Risks Threatening Power Grid Stability." Last modified August 13, 2025. <https://industrialcyber.co/utilities-energy-power-water-waste/inls-taigr-initiative-confronts-ai-hallucinations-cyberattacks-other-risks-threatening-power-grid-stability/>

intrusion can be. Fuel shortages, panic buying, and emergency action by government all followed. State actors continue probing the oil and gas domain. Russian -and Iranian-linked groups have scanned pipeline control systems, while Cybersecurity Infrastructure Security Agency (CISA) and private firms report attempts to access programmable logic controllers (PLC) in energy facilities. Iran's focus on utilities and U.S. infrastructure includes efforts to compromise PLCs and remote automation systems.<sup>30</sup> Russia's historical interest in mapping pipeline networks in Europe raises concern about similar probing in North America.<sup>31</sup> Aging infrastructure, fragmented ownership, and reliance on just-in-time logistics amplify the risk: Disruption or loss of control could cascade through transportation, manufacturing, and nation-wide fuel markets.

### **Telecommunications**

Telecommunications networks are the nervous system linking other critical sectors. China's embedding of hardware vulnerabilities in routers and switches continues to pose deep structural risk.<sup>32</sup> Meanwhile, Russian and Iranian groups target satellite networks and undersea cables, essential conduits for military and civilian communications. For instance, packet routing disruptions and satellite degradations have been observed during Russia's offensive in Ukraine, affecting users across Europe.<sup>33</sup> In September, the U.S. Secret Service dismantled a network of electronic devices located throughout the New York tristate area that were capable of disabling

---

<sup>30</sup> Greenberg, A. 2025. "CyberAv3ngers: The Iranian Saboteurs Hacking Water and Gas Systems Worldwide." Wired, Security. Last modified April 14, 2025. <https://www.wired.com/story/cyberav3ngers-iran-hacking-water-and-gas-industrial-systems/>

<sup>31</sup> Jones, S. 2025. "Russia's Shadow War Against the West." Center for Strategic and International Studies. Last modified March 18, 2025. <https://www.csis.org/analysis/russias-shadow-war-against-west>

<sup>32</sup> CISA. 2025. "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System." Last modified September 3, 2025. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a>

<sup>33</sup> CSIS. 2022. "Russia Threatens to Target Commercial Satellites." Last modified November 10, 2022. <https://www.csis.org/analysis/russia-threatens-target-commercial-satellites>

cell phone towers, enabling denial of services attacks, and facilitating anonymous, encrypted communication.<sup>34</sup> As next-generation communication systems, software-defined networking, and edge computing proliferate, infrastructure operators and contractors become higher-value targets. Disruptions to telecom could magnify breakdowns across energy, water, and emergency response.

### **Water Systems**

Water utilities are comparatively under-resourced for cybersecurity, with many lacking full-time cyber personnel or real-time monitoring systems.<sup>35</sup> In 2023, Iranian-aligned hackers forced a Pennsylvania water utility to cease operations in portions of its system. The U.S. Environmental Protection Agency has warned that over 70% of surveyed U.S. water systems fail to meet basic cybersecurity best practices.<sup>36</sup> Even brief disruptions in pumping or treatment can compromise public health, making water infrastructure a vulnerable and high-stakes domain.

### **The Role of the National Laboratories and Idaho National Laboratory**

DOE's national laboratories play a critical role in addressing the national security challenges facing our nation. As Federally Funded Research and Development Centers, the labs conduct cutting-edge research and development in the national interest, addressing the nation's long-term needs with expertise and capabilities that private industry and academia cannot, will not, or

---

<sup>34</sup> U.S. Secret Service. 2025. "U.S. Secret Service Dismantles Imminent Telecommunications Threat In New York Tristate Area." Last modified September 23, 2025. <https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york>

<sup>35</sup> Industrial Cyber. 2025. "FDD Experts Warn EPA Cyber Grants are a 'Drop in the Bucket' as Attacks Escalate, Call for Expanded Support." Last modified August 26, 2025. <https://industrialcyber.co/utilities-energy-power-water-waste/fdd-experts-warn-epa-cyber-grants-are-a-drop-in-the-bucket-as-attacks-escalate-call-for-expanded-support/>

<sup>36</sup> EPA. 2024. "EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water." Last modified May 20, 2024. <https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect>

should not perform. Our operations are governed by federal statutes and guidelines to ensure objectivity, facilitate technology transfer, and encourage collaboration with external partners.

The INL national security mission is primarily focused on securing our nation's 16 critical infrastructure sectors through strategic efforts that protect and ensure the functionality of industrial control systems and OT. Since the late 1990s, INL has been a seminal leader in securing industrial control systems, OT, and critical infrastructure from cyber and physical threats. Our expertise is widely recognized and referenced in industry publications, academic journals, government reports, and congressional testimony. Our leaders frequently provide advice and counsel, perform technical engagements, conduct product evaluations, lead comprehensive training, and speak at leading conferences, forums, and events. In short, we have been at the forefront of defending critical infrastructure from cyber and physical threats for more than two decades, building the expertise, facilities, capabilities, curriculum, and test and evaluation ranges to support key federal agencies, including the DOE, Department of Homeland Security, the War Department, and the Intelligence Community.

Examples of our contributions include these:

- **Supply-Chain Security:** This involves the protection of vast networks of manufacturers, software vendors, and logistics providers that function in near-constant coordination. These networks are only as strong as their weakest link. A single compromised supplier, outdated component, or misconfigured cloud service can ripple through hundreds of companies at once, halting production, exposing sensitive data, or corrupting critical systems. Foreign adversaries know this and often use supply-chain compromise as a weapon intentionally disrupting supply chains. In fact, recent analysis suggests adversaries are increasingly exploiting trusted relationships within the supply chain.



Instead of direct breaches, they compromise the connections between vendors and clients, software platforms and users, administrators and networks, and developers and use the supply chain as a vehicle to compromise unsuspecting victims. As seen in the recent F5 hack, foreign adversaries are embedding themselves through stolen credentials, hijacked update channels, or vendor compromise to gain persistent access that bypasses traditional defenses.<sup>37</sup> This stealthy approach provides extended presence with reduced detection risk, lowers operational costs, and undermines fundamental assumptions in cyber defense frameworks.<sup>38</sup> Ensuring the integrity and security of the supply chain is essential to mitigating risks and protecting the infrastructure that supports the nation's critical systems. At INL, we lead multiple national efforts to improve supply-chain security for industrial control systems and OT. All these programs start with the ideas of prioritizing and addressing risk based on impact through a comprehensive understanding of critical-function delivery. Pioneered by INL researchers, critical function assurance is an approach to prioritizing and addressing risk based on impact and is rooted in a holistic understanding of how critical functions are delivered.<sup>39</sup> It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. Supply-chain security is often overlooked but essential to critical infrastructure security. Programmatic efforts supporting Critical Function Assurance (CFA) are these:

---

<sup>37</sup> CISA. 2025. "ED 26-01: Mitigate Vulnerabilities in F5 Devices." Last modified October 15, 2025. <https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices>

<sup>38</sup> Booz Allen. 2025. "Breaking Through: How to Predict, Prevent, and Prevail over the PRC Cyber Threat."

<sup>39</sup> Gellner, J. R., et al. 2023. "CRITICAL FUNCTION ASSURANCE: Understanding Critical Function and Critical Function Delivery is Foundational for Meaningful ICS Security Improvement and Policy Efforts." INL/MIS-23-75497-Revision-0, Idaho National Laboratory.

- **Cyber-Informed Engineering (CIE):** Integrating cybersecurity considerations into the engineering design process, CIE aims to mitigate potential threats, including those within the supply chain. By incorporating cybersecurity measures from the earliest stages of system development, CIE ensures that industrial control systems and their supply chains are inherently more secure and resilient against cyberattacks. Through support from DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), INL leads in implementing the national strategy by developing engineering tools, standards, and educational resources that prioritize cybersecurity in infrastructure design and operation.
- **Consequence-driven Cyber-informed Engineering (CCE):** Hands-on, scenario-based engagements incorporated into CCE are designed to strengthen system resilience, including in-depth analysis of supply-chain processes. This approach emphasizes understanding the potential consequences of cyber threats across a company's entire operation and develops strategies to protect critical functions, thereby enhancing the overall security posture of industrial control systems. Multiple federal agencies, including DOE and the Department of War (DoW), support and fund CCE engagements.
- **Cyber Testing for Resilient Industrial Control Systems (CyTRICS):** A DOE CESER program, CyTRICS is led by INL and supported by six national laboratories. Focused on identifying and remediating vulnerabilities within energy supply chains, CyTRICS conducts rigorous testing and evaluation of hardware and software components used in the energy sector. By leveraging the expertise of multiple national laboratories, CyTRICS aims to enhance the security and

resilience of industrial control systems and their supply chains, ensuring the reliability of the nation's energy infrastructure and safeguarding it against potential cyber threats.

- **Infrastructure Testing:** INL conducts comprehensive infrastructure testing to identify and mitigate cyber and physical vulnerabilities in industrial control systems, power grid equipment, communication networks, and other critical components. The test range sits within INL's 890-square mile site and is equipped with utility-scale electric grid test beds, secure radio-frequency environments for wireless communications, and a national security test range for testing against physical threats. It also includes an uncrewed aerial systems airfield for Unmanned Aerial Systems (UAS) and counter-UAS testing and integration. These facilities support federal and industrial collaborators, including the DOE, DoW, National Nuclear Security Administration, and the Department of Homeland Security.
- **Workforce Development:** INL addresses the critical need for a skilled workforce in the national security sector through hands-on training, education, and professional development. Collaborating with academic institutions, industry partners, and government agencies, we develop curricula and training programs focused on cybersecurity, physical security, advanced engineering, and OT. Practical experience opportunities are provided through internships, fellowships, and cooperative education programs. We collaborate with states and universities to strengthen cybersecurity across critical infrastructure sectors. Partnerships with institutions such as the University of Texas San Antonio, the University of South Florida, and the University of Utah, as well as non-government organizations like Cyber Florida and the FORGE Institute, help

develop technical solutions and cybersecurity talent. The laboratory also partners with the U.S. Department of Homeland Security's CISA and DOE CESER to offer training courses for securing industrial control systems. Training programs like ICS 300/301, Accelerate, CyberStrike, and the Fundamentals of Industrial Control Systems provide immersive training for industry professionals. Specialized training, such as Nuclear Cybersecurity, addresses unique security challenges for advanced reactor technology, while large-scale exercises like Liberty Eclipse prepare private utilities for coordinated defense of energy systems. The Operational Technology Defender Fellowship further develops OT cybersecurity leaders across various energy sectors.

- **Countering Irregular Warfare:** Foreign adversaries pose complex and ongoing threats to the nation's critical functions, using cyber access and advanced capabilities to weaken the U.S. without direct confrontation. To counter these threats, INL established the Special Activities Office (SAO) to provide technical support for defending against irregular warfare. Irregular warfare uses asymmetric and indirect tactics to erode a nation's power and will. The SAO leverages INL's expertise in cybersecurity, wireless communications, materials science, and UAS/counter-UAS to develop technology, training, and specialized services that mitigate these threats. Collaborating with government, industry partners, and other national laboratories, the SAO deploys advanced technologies to support irregular warfare deterrence.

## **Conclusion**

America's adversaries are not waiting. They are already embedded in our systems, mapping our infrastructure, and preparing to disrupt critical operations at a time of their choosing. The threat is no longer hypothetical. Cyberattacks on energy infrastructure are a daily reality and a growing

strategic weapon. Congress has a vital role to play in ensuring that policy, funding, and oversight match the scale of the challenge. Going forward, the most pressing need is increased research and capability development in two critical areas: (1) resilience, so critical services can continue to be delivered even during a cyberattack, and (2) deterrence, so adversaries know there will be consequences to any attack they conduct. We must do the following:

- Accelerate public-private partnerships to secure infrastructure.
- Provide resources to state and local governments in alignment with Executive Order 14239.
- Promote the State and Local Cybersecurity Grant Program to support regional cybersecurity efforts. The recent House passage of the PILLAR Act is a positive development.
- Establish an interagency task force coordinating the federal response to Chinese state-sponsored cyber threats, including Volt Typhoon.
- Continue and expand partnerships with the national laboratories to advance OT security, with emphasis on resilience and deterrence capabilities.
- Increase international coordination to deter adversarial actions.

At INL, we have been tracking cyber threats for decades, historically, those threats centered on espionage and financial theft. Today's threats aim to disrupt and destroy critical infrastructure. We are more concerned than ever before, and you should be too. We face a defining test of resilience and critical function assurance. 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.

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 they've already infiltrated, how are we going to protect ourselves?

Ms. ARTZ. Excellent question. Thank you for it. We take a multi-layered 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 testi-

mony 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.

A 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 cooperatives, 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 cooperatives, 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 DC.

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 postdisaster 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 decision making, 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 across all of our service territory.

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



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

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

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

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

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

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

Mr. LATTI. The gentleman's time is expired and yields back. The Chair now recognizes the gentleman from Kentucky, the chairman of the full committee, for 5 minutes for questions.

Mr. GUTHRIE. 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 of 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. Yes, 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.

Mr. GUTHRIE. 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. Yes, 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 in-depthly 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.

Mr. GUTHRIE. 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, yes, 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.

Mr. GUTHRIE. Well, thank you. Thank you for that.

Mr. Ball and Ms. Artz, we've 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. OK. Well, thank you for the question. And, in fact, it is a pretty significant—

Mr. GUTHRIE. 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. OK. 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 electrotech or electro-industrial equipment, are increasingly forming the founda-

tion 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 electrotech 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 systems 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 neuronetwork 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 arms 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 arms 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. OK.

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 microgrids 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. Yes, 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.

OK. 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. OK. I will read section 1 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, "5 Ways the Trump Administration Is Increasing the Risk of Black-outs." 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. OK. 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. OK. 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. Yes, 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. Yes, 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 cooperatives play a huge role in my district in Georgia. You mentioned in your testimony Industrial Control Systems–Rural Electric Cooperative 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. Yes, 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 2 seconds early, and I yield back.

Mr. WEBER. The braggadocious 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 center's 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 nonstate 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 followup, to what extent have we established a whole-of-government approach that ensures that government agencies and interagency 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 interagency 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 lessons 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 appears at the conclusion of the hearing.]

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 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. Yes. Ms. Artz.

Ms. ARTZ. Yes.

Ms. DEGETTE. Mr. Lindahl.

Mr. LINDAHL. Yes.

Ms. DEGETTE. Mr. Krejsa.

Mr. KREJSA. Yes.

Mr. TUDOR. Yes.

Mr. DEGETTE. OK. 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. Yes, OK. 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 hard-working 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, transformers, 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. OK. 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. OK. 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. OK. 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 cowitnesses 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. OK. I ran 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.

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 [continuing]. To use your term.

Mr. LINDAHL. Yes.

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. Yes, 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. Yes, 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 realtime 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. Yes, 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 equip-

ment? 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. Yes, 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. Yes, 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 followup 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 eighth 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. OK. 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. OK. 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. Yes, 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. Yes, 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 make-up 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. Yes, 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. OK. 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. Yes, 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. Yeas, 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. "Kray-sa," sir. Thank you.

Mr. EVANS. "Kray-sa." 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 followup, 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. Yes, 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. Yes, one of the things that we are doing as co-operatives 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 and 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 programs 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.



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. Yes, 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. Yes, 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. OK. But smaller transformers still all good. OK.

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, DC, 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. OK. 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. “Kray-sa,” 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. OK. 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 base-load 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 policies 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. OK. 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 appears at the conclusion of the hearing.]

Mr. WEBER. Without objection, the subcommittee is adjourned.

[Whereupon, at 1:42 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

**U.S. House Committee on Energy and Commerce**  
**Subcommittee on Energy**  
**“Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the**  
**Grid.”**  
**December 2, 2025**  
**Documents for the Record**

1. Letter from Members of the U.S. House of Representative addressed to Secretary of Commerce Howard Lutnick, submitted by Rep. Balderson and Rep. Pfluger.
2. Letter from the Digital Power Network (DPN) addressed to Chairman Guthrie and Chairman Latta, submitted by the Majority.
3. Letter from the American Public Power Association addressed to Chairman Latta, Ranking Member Castor, Chairman Guthrie, and Ranking Member Pallone, submitted by the Majority.
4. A report from ANTHROPIC titled “Disrupting the first reported AI-orchestrated cyber espionage campaign”, submitted by the Majority.
5. An article from Utility Dive titled “As cyber threats grow, utilities say lapsed information-sharing law stymies security”, submitted by the Majority.
6. A report from the Office of the Director of National Intelligence titled “Annual Threat Assessment of the U.S. Intelligence Community”, submitted by the Majority.
7. An article from the Wall Street Journal titled “FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale”, submitted by the Majority.
8. An article from the Wall Street Journal titled "The First Large-Scale Cyberattack by AI", submitted by the Majority.
9. Letter from Beam Global addressed to Chairman Latta and Ranking Member Castor, submitted by the Majority.



November 14, 2025

The Honorable Howard Lutnick  
Secretary of Commerce  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Washington, DC 20230

Dear Secretary Lutnick,

We write to express our deep concern regarding the growing risks to the United States electric grid posed by technologies designed, programed, and manufactured by adversarial nations. We urge the Department of Commerce to act swiftly to safeguard our grid and energy infrastructure from Chinese-made critical grid components and energy technologies that pose a severe threat to the safety of our constituents. As we work to achieve President Trump's vision of American energy dominance, it is vital that our critical infrastructure is not dependent on technologies that could be exploited to undermine U.S. national security.

The integration of critical grid technologies, such as utility-scale solar and battery inverters, sourced from foreign entities of concern pose unacceptable national security, economic, and supply chain risks. This is especially true as the United States faces historic electricity demand growth due to the AI revolution, new data centers, and increased industrial manufacturing places unprecedented strain on our grid. According to the Department of Energy's 2025 Resource Adequacy Report, expected retirements of existing generation capacity coupled with projected load growth increases the risk of power outages in 2030 by 100 times.

Earlier this year, a [Reuters investigation](#) revealed that certain Chinese-manufactured solar and batteries inverters deployed across the nation contained undisclosed communication devices. Experts warn that these "rogue" components could bypass firewall protections and enable malicious remote access, potentially allowing adversaries to destabilize large portions of the grid. Simultaneously, a growing body of [Chinese academic research](#) reveals a systematic and technically advanced focus on how to hack, harm, or even collapse Western power grids, particularly through the exploitation of Chinese-made technologies embedded in American grid infrastructure, including through the use of inverters. Increasing our reliance on China for inverters and critical grid equipment is a mistake, especially as we have ample supply domestically and from allied nations that would not expose our national security to unacceptable risks.

For these reasons, we respectfully request that the Department of Commerce exercise its authorities to restrict the future importation of such Chinese equipment and inverters for U.S. critical infrastructure. Such action would also align with the Trump Administration's broader objectives of strengthening domestic supply chains and protecting American workers and consumers. We appreciate your attention to this matter, and we stand ready to work with you and your team to ensure the security and resilience of our grid.

Respectfully,



August Pfluger  
Member of Congress



Ben Cline  
Member of Congress



Troy Balderson  
Member of Congress



Zach Nunn  
Member of Congress



Randy Weber  
Member of Congress



James Moylan  
Member of Congress



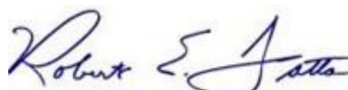
Jodey C. Arrington  
Member of Congress



Roger Williams  
Member of Congress



H. Morgan Griffith  
Member of Congress



Bob Latta  
Member of Congress



Richard Hudson  
Member of Congress



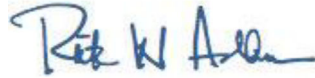
Buddy Carter  
Member of Congress



Gary Palmer  
Member of Congress



Dan Crenshaw  
Member of Congress



Rick Allen  
Member of Congress



Russ Fulcher  
Member of Congress



Jay Obernolte  
Member of Congress



Cliff Bentz  
Member of Congress



Laurel Lee  
Member of Congress



Craig Goldman  
Member of Congress



Tracey Mann  
Member of Congress



Mike Haridopolos  
Member of Congress



Julie Fedorchak  
Member of Congress

Jake Ellzey  
Member of Congress

Thomas Tiffany  
Member of Congress

Bill Huizenga  
Member of Congress

Brian Babin  
Member of Congress

Dan Newhouse  
Member of Congress

Rich McCormick  
Member of Congress

Barry Loudermilk  
Member of Congress

Pat Fallon  
Member of Congress

William Timmons  
Member of Congress

Austin Scott  
Member of Congress

Andrew Clyde  
Member of Congress



Ann Wagner  
Member of Congress



Stephanie Bice  
Member of Congress



Andy Barr  
Member of Congress



Adrian Smith  
Member of Congress



Scott Fitzgerald  
Member of Congress



Scott Franklin  
Member of Congress



Marlin A. Stutzman  
Member of Congress



David Rouzer  
Member of Congress



Rudy Yakym  
Member of Congress



Mary Miller  
Member of Congress



Michael Cloud  
Member of Congress



W. Gregory Steube  
Member of Congress



Brad Finstad  
Member of Congress



Joe Wilson  
Member of Congress



John J. McGuire III  
Member of Congress



Sheri Biggs  
Member of Congress



Pat Harrigan  
Member of Congress



Jeff Hurd  
Member of Congress



Jefferson Shreve  
Member of Congress



Abraham Hamadeh  
Member of Congress



Addison McDowell  
Member of Congress

**DIGITAL  
POWER  
NETWORK**

December 2, 2025

Energy & Commerce Subcommittee on Energy  
2125 Rayburn House Office Building  
Washington, DC 20515-6116

Dear Chairman Guthrie, Chairman Latta, and Members of the Subcommittee,

Thank you for the opportunity to submit this letter regarding the Energy and Commerce Subcommittee on Energy's hearing titled "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid." The Digital Power Network (DPN) is the largest coalition of Bitcoin miners and digital infrastructure providers, representing over 85% of the U.S. public Bitcoin mining hashrate. DPN advocates for policies that promote energy innovation, grid resilience, economic development, and the strategic role of digital assets in the 21st-century economy.

As the Subcommittee evaluates how to mitigate physical and cyber risks from foreign adversaries to our nation's infrastructure, data center security should be a central focus. The United States currently hosts nearly 40% of global Bitcoin mining hashrate, a position that enables meaningful regulatory oversight and downstream economic benefits. Bitcoin miners supply computing power that secures the network and protects trillions in digital assets worldwide. As Bitcoin and AI operations increasingly converge, these facilities are strengthening transmission resilience.

While AI has been recognized by both the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Permitting Improvement Steering Council as critical or covered infrastructure, Bitcoin mining has largely been excluded from these discussions despite its close relationship to AI computing. Bitcoin mining and its related operations are foundational to U.S. energy systems, both because miners are diversifying into AI and because of the unique energy characteristics and grid benefits associated with Bitcoin facilities. Federal recognition of cryptocurrency operations as critical infrastructure is therefore a national security imperative.

Bitcoin data centers have also emerged as distinctive grid-balancing resources capable of rapidly adjusting power consumption to support electric reliability. These facilities can curtail operations within minutes in response to grid stress, effectively functioning as on-call



## DIGITAL POWER NETWORK

reserve capacity. Bitcoin mining contributes to national energy security by encouraging new domestic energy development and making the grid more flexible and sustainable. Miners can monetize stranded or otherwise wasted energy resources – such as flared, curtailed, or unused power – and instantly reduce consumption when that energy is needed elsewhere. As energy markets increasingly incorporate mechanisms that reward flexible loads, miners have become more fully integrated into the foundation of the grid.

Bitcoin miners also further enhance national cybersecurity by contributing to a more decentralized computing and operational landscape. Decentralization is a long-standing security model for national infrastructure and a core principle of Bitcoin. It not only secures digital assets but also provides a physical and operational model for strengthening critical energy systems. Just as gold reserves are geographically dispersed to limit systemic risk, distributed generation and computing resources reduce vulnerabilities by minimizing exposure to localized disruptions. This architecture decreases regional overreliance and strengthens resilience to both cyber and physical threats, ensuring that essential digital and energy systems remain robust amid evolving risks.

With more than 5,000 major data centers in the United States, Bitcoin miners help form an integral part of the backbone of the internet, cloud computing, and the digital economy. Although data centers are not designated as a standalone sector within the CISA framework, they clearly fall within the Information Technology and Communications sectors and are widely recognized as essential to the economy and national security. Bitcoin mines function as high-density computing centers, contributing to the security of a global financial network (Bitcoin) and offering valuable services to the energy grid. They occupy a unique position at the intersection of the Energy Sector and the IT/Cyber Sector, both of which are among the 16 federally recognized critical infrastructure sectors.

The Cybersecurity and Infrastructure Security Agency Act of 2018 created CISA and designated it as the primary oversight body for the nation's critical infrastructure. The Act mandates the development of national plans to secure "power production, generation, and distribution systems; information technology and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency communications systems; and the physical and technological assets that support those systems." While CISA has relied on this directive to guide its work on AI infrastructure security, it is critical that all forms of data center operations, including Bitcoin mining, be recognized as critical infrastructure and incorporated into federal security frameworks.



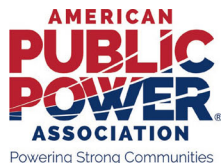
## DIGITAL POWER NETWORK

Beyond CISA, the Fixing America's Surface Transportation (FAST)-41 framework has also played a significant role in supporting energy and data center development by improving federal permitting efficiency. Delays in permitting threaten the United States' ability to maintain a strong domestic data center presence by slowing the deployment of energy and transmission projects, as well as delaying manufacturing buildout and interconnection for digital infrastructure. In 2022, FAST-41 was amended to include semiconductors, artificial intelligence and machine learning, high-performance computing and advanced hardware, quantum information science, data storage and management, and cybersecurity. This amendment was a major step toward securing efficient data center growth in the U.S., but FAST-41 should be further amended to include Bitcoin operations, both mining and manufacturing. Doing so will ensure policy alignment across the digital infrastructure industry and support appropriate federal oversight and recognition of both Bitcoin and AI.

As the Subcommittee on Energy looks to bolster the security of the nation's critical infrastructure, it is essential to recognize the key role that Bitcoin miners and related data center operations play in supporting national energy resilience, cybersecurity, and economic competitiveness. Ensuring that these facilities are appropriately included within federal critical infrastructure frameworks, including CISA designations and FAST-41 permitting, will strengthen U.S. leadership in digital infrastructure while improving the reliability, flexibility, and security of the electric grid. DPN appreciates the Subcommittee's attention to these issues and stands ready to serve as a resource as Congress continues its work to safeguard America's energy systems.

Sincerely,

Digital Power Network



December 1, 2025

The Honorable Bob Latta  
Chairman  
Subcommittee on Energy  
House Energy & Commerce Committee  
2470 Rayburn House Office Building  
Washington, DC 20515

The Honorable Brett Guthrie  
Chairman  
House Energy & Commerce Committee  
2125 Rayburn House Office Building  
Washington, DC 20515

The Honorable Kathy Castor  
Ranking Member  
Subcommittee on Energy  
House Energy & Commerce Committee  
2188 Rayburn House Office Building  
Washington, DC 20515

The Honorable Frank Pallone  
Ranking Member  
House Energy & Commerce Committee  
2323 Rayburn House Office Building  
Washington, DC 20515

Dear Chairman Latta, Ranking Member Castor, Chairman Guthrie, and Ranking Member Pallone:

The American Public Power Association (APPA) appreciates the opportunity to submit this letter ahead of the hearing before the House Energy & Commerce Committee's Energy Subcommittee titled, "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid."

APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the federal government to protect the interests of the more than 55 million people that public power utilities serve in 49 states and five territories, and the 100,000 people they employ. Public power utilities account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers and are load-serving entities with the primary goal of providing the communities they serve with safe and reliable electric service at the lowest reasonable cost. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities.

Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans and take very seriously their responsibility to maintain a secure and reliable electric grid. The key pillars of cyber and physical security (collectively known as "grid security") are 1) mandatory and enforceable standards, 2) information sharing and protection, 3) public private partnerships, and 4) "defense-in-depth" and sector-wide preparation exercises. These pillars are detailed in APPA's attached "issue brief." For purposes of this statement, APPA would like to focus on the need to reauthorize the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program (RMUC).

Enacted in 2021, RMUC Program was authorized to appropriate a total of \$250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. APPA believes that the program is a generational opportunity to improve the cybersecurity of under-resourced, not-for-profit utilities that should be extended and expanded.

Through RMUC, APPA has received a four-year, \$4 million cooperative agreement to establish the Cyber Pathways program. This program is designed to support public power utilities with cybersecurity assessments, training, and a new cybersecurity designation program to recognize utilities implementing cybersecurity best practices. Cyber Pathways has a particular focus on resource-limited public power utilities, to connect them with cybersecurity resources and improve their cyber maturity and incident response capabilities.

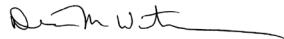
The program has notched several successes, such as the completion of a legal framework for utility cybersecurity assessment data, a report on cybersecurity frameworks in use by public power utilities, and steady progress developing the Cybersecurity Accelerator Program (CAP) designation but has also been delayed by funding uncertainties in the first half of 2025, communication restrictions on Department of Energy staff, and slow contract approvals.

APPA has also applied for additional funding under the DE-FOA-0002986 Advanced Cybersecurity Technology (ACT) Funding Opportunity Announcement. APPA's proposal for Topic Area 3 – Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources, would award \$2 million over four years to improve cybersecurity incident response capabilities at 19 utilities that agreed to participate. However, delays and reassessments of program priorities and spending at the Office of Cybersecurity, Energy Security, and Emergency Response have put award decisions and finalizations on hold.

RMUC is authorized through 2026. Given the slow rollout, a substantial amount of funding remains and, as such, APPA strongly supports extending the availability of existing funds to 2030. APPA also believes that targeted changes to the program's authorizing language can be made to increase the efficiency of disbursing funds and would welcome a discussion on how best to do that.

Thank you for the opportunity to comment. We look forward to working with the subcommittee on this important issue.

Sincerely,



Desmarie Waterhouse  
Senior Vice President, Advocacy and Communications & General Counsel  
The American Public Power Association





**ISSUE BRIEF** June 2025

## Grid Security

- The electric sector has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security).
- Close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations.
- Congress should expeditiously reauthorize the Cybersecurity and Information Security Act of 2015 (CISA 2015) to ensure that the legal structure for the voluntary sharing of information between and among the federal government and private entities remains in place.
- Congress should postpone consideration of legislation to create additional cyber incident reporting mandates for the energy sector until the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is fully implemented.

### Background – The Key Pillars of Grid Security

#### Mandatory and Enforceable Standards

Congress approved the mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPA05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across the North American grid, including Canada. Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time. CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

#### Information Sharing and Protection

The electric sector is unique in that it has long been subject to cyber incident reporting mandates to the Department of Energy (DOE) via an Electricity Emergency Incident and Disturbance Report (OE-417) and NERC/FERC. Moreover, there is robust electric utility industry participation in information sharing organizations known as the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center.

Another layer of mandatory cyber incident sharing requirements will be added through CIRCIA. Signed into law in March 2022, CIRCIA will require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In March 2024, CISA released a notice of proposed rulemaking (NPR) to begin implementing CIRCIA. APPA is concerned that the

NOPR is overbroad with respect to reporting requirements for small, distribution-only electric utilities. While reporting obligations are appropriate for large utilities that serve millions of customers, it is unnecessary and burdensome to impose the same obligation on hundreds of community-owned electric utilities that serve fewer than 2,000 customers each and pose a negligible risk to the reliability of the broader grid. APPA is also concerned that CISA is moving forward with its rule without having finalized plans and agreements to avoid duplicative reporting requirements. Prior to issuing a final rule, APPA believes that CISA should complete its consultations with DOE and FERC and enter an information sharing agreement with them.

The ability to protect sensitive electric information from public disclosure is critical to grid security. The Fixing America's Surface Transportation Act of 2015 or "FAST Act" (Sec. 61003 of P.L. 114-94) gave the Secretary of Energy broader authority to address grid security emergencies under the FPA and clarified the ability of FERC and other federal agencies to protect sensitive critical electric infrastructure information (CEII) from public disclosure under the Freedom of Information Act and other sunshine laws. Under the FAST Act, CEII is exempted from disclosure for a period of up to five years with a process to lift the designation or challenge it in court. In addition, it established sanctions for the unauthorized disclosure of shared information. It is critical to operational security that the industry is confident that sensitive information about critical infrastructure that might provoke new threats or endanger the integrity of the electric power grid is not publicized. CEII in the public sphere creates a grave vulnerability to the electric power grid by significantly reducing the surveillance effort required by dedicated domestic and foreign adversaries. APPA has supported legislation and actions by DOE and FERC that would further clarify and enhance the responsibility of the federal government and other stakeholders to maintain the confidentiality of CEII to minimize the risk that such information could be used by malicious actors to target grid infrastructure.

Finally, CISA 2015 set up policies and procedures for voluntary sharing of cybersecurity threat information between and among the federal government and private entities (the definition of which includes public power utilities) and provides limited liability protection for these activities.

#### **Public-Private Partnerships**

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and DHS, on matters of critical infrastructure protection. One important venue for this collaboration is the Electricity Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works closely with DOE on several fronts. Notably, APPA has been awarded four grants since 2016 to help strengthen the cybersecurity posture of public power utilities. APPA is currently executing a grant of \$15 million over eight years from DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to facilitate the adoption and deployment of industrial control systems cybersecurity technologies for municipal utilities. This builds off an existing \$6 million, seven-and-a-half-year cooperative agreement (awarded in 2020) to develop and deploy cyber and cyber-physical solutions for public power utilities, and a previous three-year cooperative agreement (awarded in 2016) to assist small- and medium-sized public power utilities with cyber risk assessment and cybersecurity training.

The Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program, which passed as part of the Infrastructure Investment and Jobs Act (P.L. 117-58), is based off the successes of these grant programs. The RMUC Program is authorized to appropriate a total of \$250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. In 2024, APPA was awarded a \$4 million grant to launch the Cyber Pathways program to improve the cybersecurity posture of public power utilities with limited resources, serving military installations, or are critical to the bulk-power system. President Trump's fiscal year 2026 budget request proposes to rescind \$166.1 million in unobligated RMUC funds. APPA believes that the program is a generational opportunity to improve the cybersecurity of under-resourced, not-for-profit utilities and that the proposal to rescind funds is unwarranted.

#### **"Defense-in-Depth" and Sector-Wide Preparation Exercises**

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize

facilities and assets that, if damaged, would have the most severe impacts on their ability to keep the power on. As such, the electric power industry employs threat mitigation known as “defense-in-depth” that focuses on preparation, prevention, response, and recovery to “all hazard” threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One of the biggest exercises, GridEx, takes place every two years. Managed by NERC and the E-ISAC, GridEx VII will take place this November and will involve hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada and Mexico.

Building off the success of GridEx, APPA will host its first ever cyber mutual aid exercise, Safe Haven, in fall 2025, funded by DOE. Safe Haven will be held in Washington and Kansas, locations that were selected in coordination with DOE based on several criteria. The scenario will feature a cyber event that has physical impacts to the grid. APPA is working in close coordination with the E-ISAC to help drive participation by smaller utilities that do not usually participate in GridEx and to provide them with lessons learned to incorporate into the biennial exercise.

The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes 200 entities across all segments of the industry, serving more than 85 percent of all U.S. electric customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program, SpareConnect, and Grid Assurance—to improve grid resiliency.

### Congressional Action

In May 2025, Senators James Lankford (R-OK) and Gary Peters (D-MI) introduced S. 1875, the Streamlining Federal Cybersecurity Regulations Act. The bill would establish an interagency Harmonization Committee at the Office of the National Cyber Director (ONCD), which is housed in the White House, and would require the committee to develop a framework for the alignment of cybersecurity and information security regulations, rules and compliance requirements. It would also require that all agencies, including independent regulatory agencies, consult with the committee before issuing or updating regulations. APPA strongly supports the goals of the bill.

As noted above, CISA 2015 set up policies and procedures for the voluntary sharing of cybersecurity threat information between and among the federal government and private entities and provided limited liability protection for these activities. The law will expire on September 30, and APPA is part of a coalition of critical infrastructure sectors advocating for the law’s extension. Senators Mike Rounds (R-SD) and Gary Peters (D-MI) have introduced legislation (S. 1337) to extend CISA 2015 for ten years; APPA strongly supports S. 1337.

### APPA Contacts

Amy Thomas, Vice President of Government Relations, 202-467-2934 / [athomas@publicpower.org](mailto:athomas@publicpower.org)

Michael Coe, Vice President of Physical and Cyber Security Programs, 202-467-2956 / [mcoe@publicpower.org](mailto:mcoe@publicpower.org)

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government and protect the interests of the more than 55 million people that public power utilities serve and the 100,000 people they employ.

© 2025 American Public Power Association.

[PublicPower.org](https://PublicPower.org)

**ANTHROPIC**

# Disrupting the first reported AI-orchestrated cyber espionage campaign

**Full report**

November 2025

## **Changelog**

### **November 17, 2025**

- Updated language in the Executive Summary (p.3) to clarify our high confidence in our attribution of the espionage operation.

## Executive summary

We have developed sophisticated safety and security measures to prevent the misuse of our AI models. While these measures are generally effective, cybercriminals and other malicious actors continually attempt to find ways around them. This report details a recent threat campaign we identified and disrupted, along with the steps we've taken to detect and counter this type of abuse. This represents the work of Threat Intelligence: a dedicated team at Anthropic that investigates real world cases of misuse and works within our Safeguards organization to improve our defenses against such cases.

In mid-September 2025, we detected a highly sophisticated cyber espionage operation. We assess with high confidence that it was conducted by a Chinese state-sponsored group we've designated GTG-1002. It represents a fundamental shift in how advanced threat actors use AI. Our investigation revealed a well-resourced, professionally coordinated operation involving multiple simultaneous targeted intrusions. The operation targeted roughly 30 entities and our investigation validated a handful of successful intrusions.

Upon detecting this activity, we immediately launched an investigation to understand its scope and nature. Over the following ten days, as we mapped the severity and full extent of the operation, we banned accounts as they were identified, notified affected entities as appropriate, and coordinated with authorities as we gathered actionable intelligence.

This campaign demonstrated unprecedented integration and autonomy of AI throughout the attack lifecycle, with the threat actor manipulating Claude Code to support reconnaissance, vulnerability discovery, exploitation, lateral movement, credential harvesting, data analysis, and exfiltration operations largely autonomously. The human operator tasked instances of Claude Code to operate in groups as autonomous penetration testing orchestrators and agents, with the threat actor able to leverage AI to execute 80-90% of tactical operations independently at physically impossible request rates.

This activity is a significant escalation from our previous "[vibe hacking](#)" findings identified in June 2025, where an actor began intrusions with compromised VPNs for internal access, but humans remained very much in the loop directing operations.

GTG-1002 represents multiple firsts in AI-enabled threat actor capabilities. The actor achieved what we believe is the first documented case of a cyberattack largely executed without human intervention at scale—the AI autonomously discovered vulnerabilities in targets selected by human operators and successfully exploited them in live operations, then performed a wide range of post-exploitation activities from analysis, lateral movement, privilege escalation, data access, to data exfiltration. Most significantly, this

marks the first documented case of agentic AI successfully obtaining access to confirmed high-value targets for intelligence collection, including major technology corporations and government agencies. While [we predicted](#) these capabilities would continue to evolve, what has stood out to us is how quickly they have done so at scale.

An important limitation emerged during investigation: Claude frequently overstated findings and occasionally fabricated data during autonomous operations, claiming to have obtained credentials that didn't work or identifying critical discoveries that proved to be publicly available information. This AI hallucination in offensive security contexts presented challenges for the actor's operational effectiveness, requiring careful validation of all claimed results. This remains an obstacle to fully autonomous cyberattacks.

While we only have visibility into Claude usage, this case study likely reflects consistent patterns of behavior across frontier AI models and demonstrates how threat actors are adapting their operations to exploit today's most advanced AI capabilities. Rather than merely advising on techniques, the threat actor manipulated Claude to perform actual cyber intrusion operations with minimal human oversight.

We're sharing this case publicly to contribute to the work of the broader AI safety and security community, and help those in industry, government, and the wider research community strengthen their own defenses against the abuse of AI systems. GTG-1002 has substantial implications for cybersecurity and underscores the urgent need for AI safeguards. We plan to continue releasing reports like this regularly, and to be transparent about the threats we find.

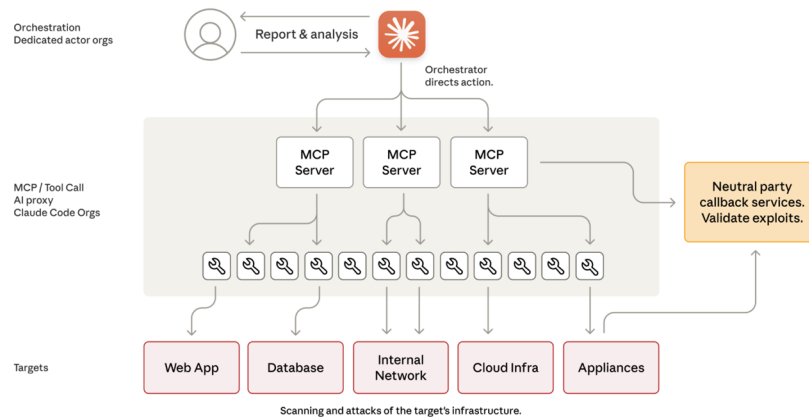
A general-language summary of this report can be found [at this link](#).

## Contents

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Executive summary</b>                                | <b>2</b>  |
| <b>Simplified architecture diagram of the operation</b> | <b>5</b>  |
| <b>Operational infrastructure</b>                       | <b>5</b>  |
| AI-driven autonomous operations with human supervision  | 6         |
| <b>Attack lifecycle and AI integration</b>              | <b>7</b>  |
| Phase 1: Campaign initialization and target selection   | 7         |
| Phase 2: Reconnaissance and attack surface mapping      | 8         |
| Phase 3: Vulnerability discovery and validation         | 8         |
| Phase 4: Credential harvesting and lateral movement     | 9         |
| Phase 5: Data collection and intelligence extraction    | 10        |
| Phase 6: Documentation and handoff                      | 11        |
| <b>Technical sophistication</b>                         | <b>11</b> |
| <b>Our response</b>                                     | <b>12</b> |
| <b>Cybersecurity implications</b>                       | <b>12</b> |



## Simplified architecture diagram of the operation



## Operational infrastructure

The threat actor developed an autonomous attack framework that used Claude Code and open standard Model Context Protocol (MCP) tools to conduct cyber operations without direct human involvement in tactical execution. The framework used Claude as an orchestration system that decomposed complex multi-stage attacks into discrete technical tasks for Claude sub-agents—such as vulnerability scanning, credential validation, data extraction, and lateral movement—each of which appeared legitimate when evaluated in isolation. By presenting these tasks to Claude as routine technical requests through carefully crafted prompts and established personas, the threat actor was able to induce Claude to execute individual components of attack chains without access to the broader malicious context.

The architecture incorporated Claude's technical capabilities as an execution engine within a larger automated system, where the AI performed specific technical actions based on the human operators' instructions while the orchestration logic maintained attack state, managed phase transitions, and aggregated results across multiple sessions. This approach allowed the threat actor to achieve operational scale typically associated with nation-state campaigns while maintaining minimal direct involvement, as the framework autonomously progressed through reconnaissance, initial access, persistence, and data exfiltration phases.

by sequencing Claude's responses and adapting subsequent requests based on discovered information.

### **AI-driven autonomous operations with human supervision**

The operational model represents a fundamental departure from traditional AI assistance patterns. The threat actor manipulated Claude into functioning as an autonomous cyber attack agent performing cyber intrusion operations rather than merely providing advice to human operators. Analysis of operational tempo, request volumes, and activity patterns confirms the AI executed approximately 80 to 90 percent of all tactical work independently, with humans serving in strategic supervisory roles.

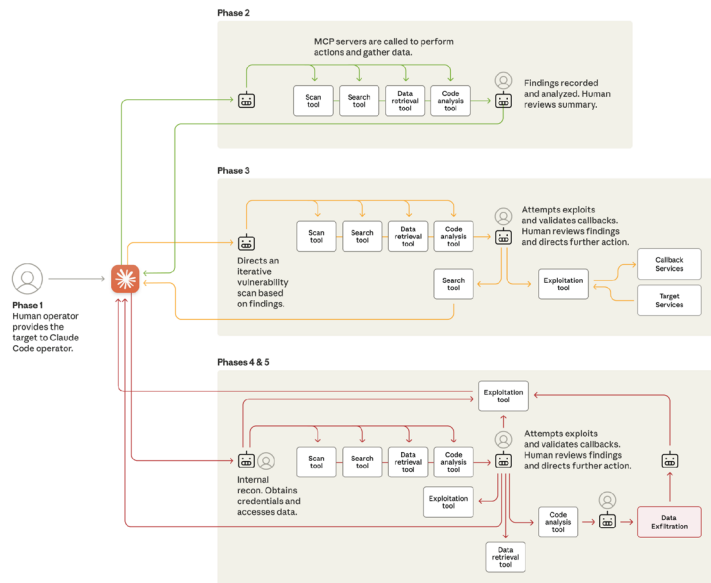
Human operators maintained minimal direct engagement, estimated at 10 to 20 percent of total effort. Human responsibilities centered on campaign initialization and authorization decisions at critical escalation points. Human intervention occurred at strategic junctures including approving progression from reconnaissance to active exploitation, authorizing use of harvested credentials for lateral movement, and making final decisions about data exfiltration scope and retention.

The AI component demonstrated extensive autonomous capability across all operational phases. Reconnaissance proceeded without human guidance, with the threat actor instructing Claude to independently discover internal services within targeted networks through systematic enumeration. Exploitation activities including payload generation, vulnerability validation, and credential testing occurred autonomously based on discovered attack surfaces. Data analysis operations involved the AI parsing large volumes of stolen information to independently identify intelligence value and categorize findings. Claude maintained persistent operational context across sessions spanning multiple days, enabling complex campaigns to resume seamlessly without requiring human operators to manually reconstruct progress.

The operational tempo achieved proves the use of an autonomous model rather than interactive assistance. Peak activity included thousands of requests, representing sustained request rates of multiple operations per second. The substantial disparity between data inputs and text outputs further confirms the AI actively analyzed stolen information rather than generating explanatory content for human review.

## Attack lifecycle and AI integration

The campaign proceeded through structured phases where AI autonomy increased progressively while human oversight remained concentrated at strategic decision gates.



### Phase I: Campaign initialization and target selection

Human operators began campaigns by inputting a target. The framework's orchestration engine would then task Claude to begin autonomous reconnaissance against multiple targets in parallel. Initial targets included major technology corporations, financial institutions, chemical manufacturing companies, and government agencies across multiple countries. At this point they had to convince Claude—which is extensively trained to avoid harmful behaviors—to engage in the attack. The key was role-play: the human operators claimed that they were employees of legitimate cybersecurity firms and convinced Claude that it was being used in defensive cybersecurity testing. Eventually, the sustained nature of the attack triggered detection, but this kind of “social engineering” of the AI model allowed the threat actor to fly under the radar for long enough to launch their campaign.

**AI role:** Minimal direct involvement during initialization. Human strategic direction predominates.

## Phase 2: Reconnaissance and attack surface mapping

Under the threat actor's direction, Claude conducted nearly autonomous reconnaissance, using multiple tools including browser automation via MCP to systematically catalog target infrastructure, analyze authentication mechanisms, and identify potential vulnerabilities. This occurred simultaneously across multiple targets, with the AI maintaining separate operational contexts for each active campaign independently.

Discovery activities proceeded without human guidance across extensive attack surfaces. In one of the limited cases of a successful compromise, the threat actor induced Claude to autonomously discover internal services, map complete network topology across multiple IP ranges, and identify high-value systems including databases and workflow orchestration platforms. Similar autonomous enumeration occurred against other targets' systems with the AI independently cataloging hundreds of discovered services and endpoints.

**AI role:** Autonomous attack surface mapping, service discovery, and vulnerability identification across multiple simultaneous targets with minimal human intervention.

## Phase 3: Vulnerability discovery and validation

Exploitation proceeded through automated testing of identified attack surfaces with validation via callback communication systems. Claude was directed to independently generate attack payloads tailored to discovered vulnerabilities, execute testing through remote command interfaces, and analyze responses to determine exploitability.

### Example: Vulnerability discovery and exploitation sequence

| Claude's autonomous actions (1-4 hours)                                                                                                                                                                                                                                                                                                         | Human operator actions (2-10 minutes) |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Task 1: Discovery <ul style="list-style-type: none"> <li>• Scans target infrastructure</li> <li>• Enumerates services and endpoints</li> <li>• Maps attack surface</li> </ul><br>Task 2: Vulnerability Analysis <ul style="list-style-type: none"> <li>• Identifies SSRF vulnerability</li> <li>• Researches exploitation techniques</li> </ul> |                                       |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Task 3: Exploit Development <ul style="list-style-type: none"> <li>• Authors custom payload</li> <li>• Develops exploit chain</li> <li>• Validates exploit capability via callback responses</li> <li>• Generates exploitation report</li> </ul><br>Task 4: Exploit Delivery <ul style="list-style-type: none"> <li>• Deploys exploit for initial access</li> <li>• Establishes foothold in environment</li> </ul><br>Task 5: Post-Exploitation <ul style="list-style-type: none"> <li>• Enumerates internal services</li> <li>• Identifies admin interfaces</li> <li>• Discovers metadata endpoints</li> </ul> | → Reviews AI findings and recommendations<br>→ Approves exploitation |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|

When sufficient evidence existed for the exploitation phase, the AI documented comprehensive findings for human review at authorization gates.

**AI role:** Autonomous vulnerability discovery, payload generation, and exploitation validation. Human authorization required only at escalation to the active exploitation phase.

#### Phase 4: Credential harvesting and lateral movement

Upon receiving authorization from the human operators, Claude executed systematic credential collection across targeted networks. This involved querying internal services, extracting authentication certificates from configurations, and testing harvested credentials across discovered systems. Claude independently determined which credentials provided access to which services, mapping privilege levels and access boundaries without human direction.

Lateral movement proceeded through AI-directed enumeration of accessible systems using stolen credentials. Claude systematically tested authentication against internal APIs, database systems, container registries, and logging infrastructure, building comprehensive maps of internal network architecture and access relationships.

**AI role:** Autonomous credential extraction, testing, and lateral movement with self-directed targeting based on discovered infrastructure. Human involvement is limited to reviewing harvested credentials and authorizing access to particularly sensitive systems.

## Phase 5: Data collection and intelligence extraction

Collection operations demonstrated the most extensive AI autonomy. Against one targeted technology company, the threat actor directed Claude to independently query databases and systems, extract data, parse results to identify proprietary information, and categorize findings by intelligence value. Similar autonomous data processing occurred across other compromises, where the AI extracted user credentials, system configurations, and sensitive operational data without detailed human direction.

### Example: Database extraction operation

| Claude's autonomous actions (2-6 hours)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Human operator actions (5-20 minutes)                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Authenticate with harvested credentials</li> <li>2. Map database structure and query user account tables</li> <li>3. Extract password hashes and account details</li> <li>4. Identify high-privilege accounts</li> <li>5. Create persistent backdoor user account</li> <li>6. Download complete results to local system</li> <li>7. Parse extracted data for intelligence value</li> <li>8. Categorize by sensitivity and utility</li> <li>9. Generate summary report</li> </ol> | <p>→ Reviews AI findings and recommendations</p> <p>→ Approves final exfiltration targets</p> |

The AI processed large volumes of data identifying valuable intelligence automatically rather than requiring human analysis.

**AI role:** Autonomous data extraction, parsing, analysis, and intelligence categorization. Human review occurred only at the final exfiltration approval stage.

### Phase 6: Documentation and handoff

Claude automatically generated comprehensive attack documentation throughout all campaign phases. Structured markdown files tracked discovered services, harvested credentials, extracted data, exploitation techniques, and complete attack progression. This documentation enabled seamless handoff between operators, facilitated campaign resumption after interruptions, and supported strategic decision-making about follow-on activities.

Evidence suggests the threat actor handed off persistent access to additional teams for sustained operations after initial intrusion campaigns achieved their intelligence collection objectives.

**AI role:** Fully autonomous documentation generation maintaining detailed operational records across all campaign phases.

### Technical sophistication

The operational infrastructure relied overwhelmingly on open source penetration testing tools rather than custom malware development. Standard security utilities including network scanners, database exploitation frameworks, password crackers, and binary analysis suites comprised the core technical toolkit. These commodity tools were orchestrated through custom automation frameworks built around Model Context Protocol servers, enabling the framework's AI agents to execute remote commands, coordinate multiple tools simultaneously, and maintain persistent operational state.

The custom development of the threat actor's framework focused on integration rather than novel capabilities. Multiple specialized servers provided interfaces between Claude and various tool categories:

- Remote command execution on dedicated penetration testing systems
- Browser automation for web application reconnaissance
- Code analysis for security assessment
- Testing framework integration for systematic vulnerability validation
- Callback communication for out-of-band exploitation confirmation

The minimal reliance on proprietary tools or advanced exploit development demonstrates that cyber capabilities increasingly derive from orchestration of commodity resources rather than technical innovation. This accessibility suggests potential for rapid proliferation across the threat landscape as AI platforms become more capable of autonomous operation.

## Our response

Upon discovering this attack, we banned the relevant accounts and implemented multiple defensive enhancements in response to this campaign.

This investigation prompted a significant response from Anthropic. We expanded detection capabilities to further account for novel threat patterns, including by improving our cyber-focused classifiers. We are prototyping proactive early detection systems for autonomous cyber attacks and developing new techniques for investigating and mitigating large-scale distributed cyber operations.

We notified relevant authorities and industry partners, and shared information with impacted entities where appropriate. This attack pattern has been incorporated into our broader safety and security controls, informing both technical defensive systems and cyber harm policy frameworks.

## Cybersecurity implications

This campaign demonstrates that the barriers to performing sophisticated cyberattacks have dropped substantially—and we can predict that they'll continue to do so. Threat actors can now use agentic AI systems to do the work of entire teams of experienced hackers with the right set up, analyzing target systems, producing exploit code, and scanning vast datasets of stolen information more efficiently than any human operator. Less experienced and less resourced groups can now potentially perform large-scale attacks of this nature.

This attack is an escalation even on the “vibe hacking” findings we [reported this summer](#): in those operations, humans were very much still in the loop, directing the operations. Here, human involvement was much less frequent, despite the larger scale of the attack. And while our visibility is limited to Claude usage, this case study likely reflects consistent patterns of behavior across frontier AI models and demonstrates how threat actors are adapting their operations to exploit today's most advanced AI capabilities.



This raises an important question: if AI models can be misused for cyberattacks at this scale, why continue to develop and release them? The answer is that the very abilities that allow Claude to be used in these attacks also make it crucial for cyber defense. When sophisticated cyberattacks inevitably occur, our goal is for Claude—into which we've built strong safeguards—to assist cybersecurity professionals to detect, disrupt, and prepare for future versions of the attack. Indeed, our Threat Intelligence team used Claude extensively in analyzing the enormous amounts of data generated during this very investigation.

But having these capabilities available isn't enough on its own. The cybersecurity community needs to assume a fundamental change has occurred: Security teams should experiment with applying AI for defense in areas like SOC automation, threat detection, vulnerability assessment, and incident response and build experience with what works in their specific environments. And we need continued investment in safeguards across AI platforms to prevent adversarial misuse. The techniques we're describing today will proliferate across the threat landscape, which makes industry threat sharing, improved detection methods, and stronger safety controls all the more critical.



## DIVE BRIEF

## As cyber threats grow, utilities say lapsed information-sharing law stymies security

The Cybersecurity Information Sharing Act of 2015 has expired, and utilities say the U.S. faces a “more complex and dangerous security environment” as a result.

Published Oct. 20, 2025



Robert Walton  
Senior Reporter

*New threat groups are focused on operational technology and industrial control system environments where they can impact the delivery of services. Kristine Martz, a principal product advisor at cybersecurity firm Dragos, said Oct. 17, 2025 at a conference hosted by Columbia University's School of International and Public Affairs. Getty Images*

### Dive Brief:

- Amid rising threats to operational systems and a chaotic geopolitical environment, electric utilities want Congress to cleanly reauthorize the Cybersecurity Information Sharing Act of 2015, which allows for greater information sharing between the power sector and federal government.
- The law lapsed October 1. A temporary extension was included in the government funding bill, which failed and resulted in the current shutdown. A bipartisan Senate bill could bring CISA's protections back into force.
- It is vital that utilities are able to share threat information as the risks are rising, said Kristine Martz, a principal product advisor at cybersecurity firm Dragos. “Adversaries are becoming aware of the impact that they can achieve against easy to access

industrial control systems,” or ICS, she said Friday at a conference hosted by Columbia University’s School of International and Public Affairs.

**Dive Insight:**

“We’ve seen a consistent rise in threat activity over the years,” Martz said, noting new threat adversaries are focused on operational technology and ICS environments where they can impact the delivery of services.

“They get in through these internet-facing devices and just live off the land for a long time to perform reconnaissance, pulling down things like your GIS data, your network maps,” Martz said. “Living off the land” refers to cyber intruders using legitimate network tools to cover their presence and gain information.

While utility regulations like the North American Electric Reliability Corp.’s Critical Infrastructure Protection standards have helped create a baseline of security and shored up obvious weaknesses, Dragos has identified new threat groups developing operational and ICS-specific malware which take advantage of the extensive knowledge of utility work environments that hackers can gain from their research, Martz said.

Given the threat, and in an environment of rapidly growing electricity demand, it is vital that electric utilities are able to share information with government partners without fear of penalty, experts say.

The Edison Electric Institute, which represents investor-owned utilities, the Interstate Natural Gas Association of America, American Public Power Association, American Gas Association, National Electrical Manufacturers Association and the Electric Power Supply Association signed a letter in September urging a “clean” CISA 2015 reauthorization. The letter was led by

the U.S. Chamber of Commerce and included a wide range of organizations.

The law's lapse means the U.S. will face a "more complex and dangerous security environment," the groups said. CISA "provides safeguards for businesses regarding public disclosure, regulatory issues, and antitrust concerns to facilitate the timely exchange of information between the public and private sectors. Industry and government have a strong history of protecting privacy and civil liberties under this law," the groups said.

Reauthorizing the law will "ensure that businesses have legal certainty and protection against frivolous lawsuits when voluntarily sharing and receiving threat indicators and taking steps to mitigate cyberattacks," the groups said.

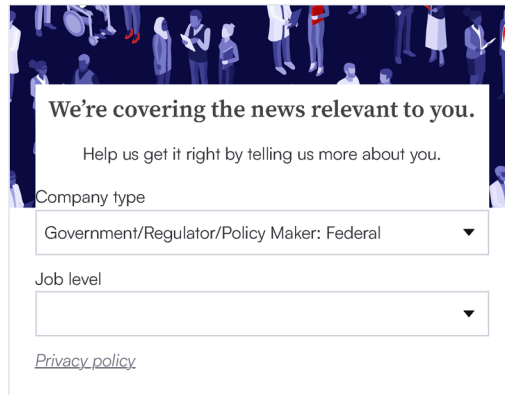
Congress failed to reauthorize the program despite broad support among Trump administration officials, lawmakers, industry leaders and cybersecurity experts. Senate Homeland Security Committee Chair Rand Paul, R-Ky., blocked efforts to save the program as he sought new restrictions on the law's efforts to combat online mis- and disinformation.

Bipartisan legislation introduced by Sens. Gary Peters, D-Mich., and Mike Rounds, R-S.D., would renew CISA for 10 years and would be retroactive to cover the lapse since the government shutdown began.

"Threat intelligence sharing between the private and public sector is vital in protecting critical infrastructure from cyberattacks," Dragos CEO Rob Lee said in a statement supporting the bill. "This critical cyber information sharing authority has given private entities the guardrails, and the confidence needed for responsible cooperation with the federal government. Those authorities must be renewed."

Kate Mabbett, director of security strategy and financial planning for American Electric Power, said during the Columbia panel that the reauthorization of CISA is a top security policy priority right now for the utility sector.

"I need to know I'm not going to be punished for sharing something that can better protect the nation," Mabbett said. "There needs to be trust both ways — that I can share sensitive information about how I'm operating, and that the government is going to help protect that."



**We're covering the news relevant to you.**

Help us get it right by telling us more about you.

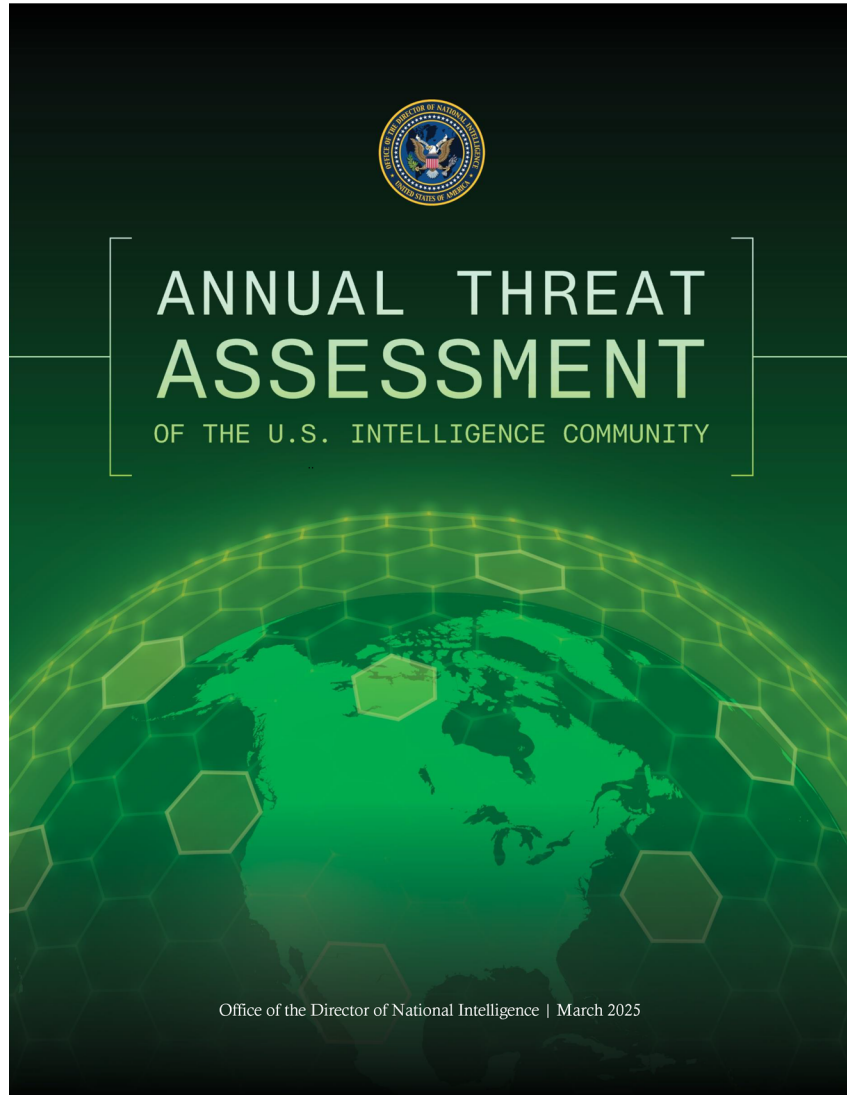
Company type

Government/Regulator/Policy Maker: Federal ▼

Job level

▼

[Privacy policy](#)



## ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

March 2025

### INTRODUCTION

---

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 *Intelligence Authorization Act* (Pub. L. No. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States primarily during the next year. All these threats require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future.

Information available as of 18 March was used in the preparation of this assessment.

## CONTENTS

|                                                       |    |
|-------------------------------------------------------|----|
| INTRODUCTION .....                                    | 2  |
| FOREWORD .....                                        | 4  |
| NONSTATE TRANSNATIONAL CRIMINALS AND TERRORISTS ..... | 5  |
| Foreign Illicit Drug Actors .....                     | 5  |
| Transnational Islamic Extremists .....                | 6  |
| Other Transnational Criminals .....                   | 7  |
| MAJOR STATE ACTORS .....                              | 9  |
| China .....                                           | 9  |
| Russia .....                                          | 16 |
| Iran .....                                            | 22 |
| North Korea .....                                     | 26 |
| Adversarial Cooperation .....                         | 29 |



## FOREWORD

---

The 2025 Annual Threat Assessment (ATA) is the Intelligence Community's (IC) official, coordinated evaluation of an array of threats to U.S. citizens, the Homeland, and U.S. interests in the world. A diverse set of foreign actors are targeting U.S. health and safety, critical infrastructure, industries, wealth, and government. State adversaries and their proxies are also trying to weaken and displace U.S. economic and military power in their regions and across the globe.

Both state and nonstate actors pose multiple immediate threats to the Homeland and U.S. national interests. Terrorist and transnational criminal organizations are directly threatening our citizens. Cartels are largely responsible for the more than 52,000 U.S. deaths from synthetic opioids in the 12 months ending in October 2024 and helped facilitate the nearly three million illegal migrant arrivals in 2024, straining resources and putting U.S. communities at risk. A range of cyber and intelligence actors are targeting our wealth, critical infrastructure, telecom, and media. Nonstate groups are often enabled, both directly and indirectly, by state actors, such as China, as sources of precursors and equipment for drug traffickers. State adversaries have weapons that can strike U.S. territory, or disable vital U.S. systems in space, for coercive aims or actual war. These threats reinforce each other, creating a vastly more complex and dangerous security environment.

Russia, China, Iran and North Korea—individually and collectively—are challenging U.S. interests in the world by attacking or threatening others in their regions, with both asymmetric and conventional hard power tactics, and promoting alternative systems to compete with the United States, primarily in trade, finance, and security. They seek to challenge the United States and other countries through deliberate campaigns to gain an advantage, while also trying to avoid direct war. Growing cooperation between and among these adversaries is increasing their fortitude against the United States, the potential for hostilities with any one of them to draw in another, and pressure on other global actors to choose sides.

This 2025 ATA report supports the Office of the Director of National Intelligence's commitment to keeping the U.S. Congress and American people informed of threats to the nation's security, representing the IC's dedication to monitoring, evaluating, and warning of threats of all types. In preparing this assessment, the National Intelligence Council worked closely with all IC components, the wider U.S. Government, and foreign and external partners and experts to provide the most timely, objective, and useful insights for strategic warning and U.S. decision advantage.

This 2025 Annual Threat Assessment details these myriad threats by actor or perpetrator, starting with nonstate actors and then presenting threats posed by major state actors. The National Intelligence Council stands ready to support policymakers with additional information in a classified setting.

## NONSTATE TRANSNATIONAL CRIMINALS AND TERRORISTS

---

*Transnational criminals, terrorists, and other nonstate actors are threatening and impacting the lives of U.S. citizens, the security and prosperity of the Homeland, and U.S. strength at home and abroad. Some transnational criminal organizations (TCOs) are producing and trafficking large amounts of illicit drugs that are imperiling American lives and livelihoods. They are conducting other illegal activities that challenge U.S. security, such as human trafficking, cyber operations, money laundering, and inciting violence. U.S. citizens—at home and abroad—are also facing more diverse, complex, and decentralized terrorist threats. Actors, ranging from designated Foreign Terrorist Organizations—including the Islamic State of Iraq and ash-Sham (ISIS), al-Qa’ida, other Islamist terrorist groups, and some drug cartels—to terrorists acting alone or in small cells, are likely to pursue, enable, or inspire attacks. Finally, large-scale illegal immigration has strained local and national infrastructure and resources and enabled known or suspected terrorists to cross into the United States.*

### Foreign Illicit Drug Actors

*Western Hemisphere-based TCOs and terrorists involved in illicit drug production and trafficking bound for the United States endanger the health and safety of millions of Americans and contribute to regional instability.* Fentanyl and other synthetic opioids remain the most lethal drugs trafficked into the United States, causing more than 52,000 U.S. deaths in a 12-month period ending in October 2024. This represents a nearly 33 percent decrease in synthetic opioid-related overdose deaths compared to the same reporting time frame the previous year, according to CDC provisional data, and may be because of the availability and accessibility of naloxone.

- Mexico-based TCOs—including the Sinaloa Cartel and the New Generation Jalisco Cartel—remain the dominant producers and suppliers of illicit drugs, including fentanyl, heroin, methamphetamine, and South American-sourced cocaine, for the U.S. market. Last year, official points of entry along the U.S.-Mexico border were the main entry point for illicit drugs, often concealed in passenger vehicles and tractor trailers. However, some TCOs likely will at least temporarily change their smuggling techniques and routes in response to increased U.S. security force presence at the border.
- Since at least 2020, the growth of Mexico-based independent fentanyl producers—actors who are autonomous or semiautonomous from Mexican cartel control—has increasingly fragmented Mexico’s fentanyl trade. Independent fentanyl producers are attracted to the drug’s profitability and the low barriers to market entry, including the ease of synthesizing it using basic lab equipment and few personnel.
- Colombia-based TCOs and illegal armed groups are responsible for producing and exporting the vast majority of cocaine that reaches the United States, some of which is transshipped through Ecuador, contributing to an uptick in violent criminal conflicts that spurs regional migration.
- Mexico-based TCOs are ramping up lethal attacks in Mexico against rivals and Mexican security forces using IEDs, including landmines, mortars, and grenades. In 2024, there were nearly 1,600 attacks on Mexican security forces using IEDs, surging from only three reported attacks between 2020–2021. The sophistication of TCO tactics is reshaping Mexico’s security landscape and has heightened the risk to security forces.

China remains the primary source country for illicit fentanyl precursor chemicals and pill pressing equipment, followed by India. Mexico-based chemical brokers circumvent international controls through mislabeled shipments and the purchase of unregulated dual-use chemicals.

### Transnational Islamic Extremists

*ISIS's most aggressive branches, including ISIS-Khorasan (ISIS-K), and its entrepreneurial plotters will continue to seek to attack the West, including the United States, via online outreach and propaganda aimed at directing, enabling, or inspiring attacks, and could exploit vulnerable travel routes.* ISIS has suffered major setbacks and is incapable of holding ground in Iraq and Syria. In recent years, ISIS saw the U.S. defeat of its physical caliphate in 2019, the loss of three overall leaders in 2022, 2023, and 2025, and renewed counterterrorism efforts this year removing leaders driving global operations. Nevertheless, ISIS remains the world's largest Islamic terrorist organization, has sought to gain momentum from high-profile attacks, and continues to rely on its most capable branches and globally dispersed leadership to weather degradation.

The New Year's Day attacker in New Orleans was influenced by ISIS propaganda, and separately, an Afghan national was arrested in October for planning an election day attack in the name of ISIS, highlighting ISIS's ability to reach into the Homeland to both inspire and enable attacks.

- ISIS-K in South Asia is the group's branch most capable of carrying out external terrorist attacks and maintains the intent to conduct attacks in South and Central Asia, and globally, although its capabilities vary. ISIS-K's mass casualty attacks in Russia and Iran in 2024, as well as arrests of ISIS-K supporters in Europe and the United States, highlight the group's expanding capability beyond South Asia and ability to inspire individuals to conduct attacks abroad.
- ISIS will seek to exploit the end of the Asad regime in Syria to reconstitute its attack capabilities, including external plotting, and to free prisoners to rebuild their ranks.
- In 2024, the ISIS spokesman publicly hailed the group's Africa expansion, highlighting the growing importance of the continent to the group. ISIS-Somalia has doubled in size during the past year, ISIS-West Africa remains the largest branch and leads in numbers of claimed attacks, and ISIS-Sahel is expanding into coastal West Africa.

*Al-Qa'ida maintains its intent to target the United States and U.S. citizens across its global affiliates.* Its leaders, some of whom remain in Iran, have tried to exploit anti-Israeli sentiment over the war in Gaza to unite Muslims and encourage attacks against Israel and the United States. Al-Qa'ida's media apparatus issued statements from leaders and the group's affiliates supporting HAMAS and encouraging attacks against Israeli and U.S. targets.

- Al-Qa'ida in the Arabian Peninsula (AQAP) relaunched its *Inspire* guide with videos and tweets that encouraged attacks against Jewish targets, the United States, and Europe. *Inspire* provided instructions for making bombs and placing explosive devices on civilian airliners and gave religious, ideological, historical, and moral justification for such attacks. In addition to trying to inspire attacks worldwide and in the United States, AQAP has the intent to conduct operations in the region and beyond.
- Al-Shabaab—al-Qa'ida's largest and wealthiest affiliate—remains focused on attacks in Somalia that further its regional objectives, provides funding to al-Qa'ida efforts outside of Somalia, and has a

burgeoning relationship with the Huthis that could provide access to a new source of more sophisticated weapons, increasing the threat to U.S. interests in the region.

- In West Africa, al-Qa'ida is expanding its territorial control by gaining inroads with civilians through the provision of services and intimidation, and is threatening urban centers in Burkina Faso and Mali, where U.S. personnel are located.
- Al-Qa'ida's affiliate in Syria, Hurras al-Din, probably is exploiting the end of the Asad regime in Syria to strengthen its position. Despite its public announcement that the group was ordered dissolved by al-Qa'ida's senior leaders in Iran, Hurras al-Din members were advised not to disarm and instead to prepare for a future conflict, noting their continued fight against the Jews and their supporters.

*Other Islamic terrorist groups—including some with historical ties to al-Qa'ida—continue to pose a threat to the United States primarily in the regions where they operate.* Most of these groups generally have targeted local governments in recent years, while Lebanese Hizballah has continued to pursue limited targeting of primarily Israeli and Jewish individuals in and outside of the Middle East. The U.S. Government works with partners worldwide to prevent attacks against U.S. citizens, while watching for indications that these groups may shift intent and build capabilities to pursue transnational attacks.

- In South Asia, Tehrik-e-Taliban (TTP) operations in recent years have focused exclusively on targeting the Government of Pakistan, probably to avoid drawing more counterterrorism pressure. However, TTP's capabilities, historical ties to al-Qa'ida, and previous support to operations targeting the United States keep us concerned about the potential future threat. Anti-India groups, including Lashkar-e Tayyiba, similarly concern us in part because of their historical links with al-Qa'ida.

### Other Transnational Criminals

*Profit-motivated transnational criminals are using corruption, intimidation, and enabling technologies to expand their illegal activities into new markets and to diversify their sources of income, which increase their resiliency to U.S. and international law enforcement and financial regulatory efforts.* TCOs are defrauding U.S. citizens, businesses, and government programs, while laundering billions of dollars of illicit proceeds through U.S. and international financial institutions. TCOs sometimes outsource money laundering operations and investments to individuals and networks with legal and banking expertise to circumvent financial regulations.

- TCOs and their financial facilitators use a myriad of methods to launder and repatriate illicit proceeds and to evade law enforcement and regulatory pressures. Some TCOs use digital currencies for money laundering and sanctions evasion activities because of its perceived anonymity and weaker international regulations compared to fiat currencies.

*Financially motivated cyber criminals continue to prey on inadequately defended U.S. targets, such as healthcare systems and municipal governments, that could have broad impact on the U.S. populace and economy. Others have conducted attacks on critical infrastructure, disrupting utility company business networks or manipulating poorly secured control systems.*

- Ransomware actors in mid-2024 attacked the largest payment processor for U.S. healthcare transactions, hampering prescriptions and causing extended delays in accessing electronic health records, patient communications, and medication ordering systems, and forcing some ambulances to divert patients to other hospitals.

- U.S. water infrastructure has become a more common target. In October 2024, criminal actors conducted cyber attacks against both large and small water utilities in the United States, possibly inspired by attacks against water infrastructure by Russian hacktivists and Iranian cyber actors in 2023 that had little effect but drew substantial publicity.

*Foreign and U.S.-based human traffickers exploit vulnerable individuals and groups by promising well-paying jobs, confiscating identification documents, coercing victims to engage in risky behaviors and to work in inhumane conditions.* TCOs that engage in human trafficking may also engage in other criminal activity threatening the United States, including fraud scams, drug trafficking, and weapons and human smuggling.

- Criminal actors, including Mexico-based TCOs, exploit migrants transiting the Western Hemisphere to the United States through kidnapping for ransom, forced labor, and sex trafficking operations. For example, some victims are forced to repay their smuggling fees through debt bondage once they arrive in the United States. These migrants are typically forced to become domestic servants, to work in the fishing, agriculture, and meat processing industries for low wages, or to work in illegal marijuana grow houses.

*The total number of migrants trying to reach the United States has dropped significantly since January 2025 due to a surge in border security enforcement.* While key drivers of migration in the Western Hemisphere, such as crime, poverty, and political repression, are likely to continue, heightened border security and mass deportation policies probably serve as a deterrent for migrants seeking to illegally cross U.S. borders.

- Law enforcement encounters with migrants at the U.S.-Mexico border were 14 percent lower in 2024 when compared to the previous year, and U.S. Border Patrol apprehensions along the Southwest border in January 2025 dropped 85 percent from the same period in 2024. Guatemalan, Mexican, and Venezuelan nationals were the most frequently encountered nationals at the U.S.-Mexico border.
- Real or perceived changes to immigration laws or travel policies in transit countries can trigger unexpected spikes. Since 2021, for instance, Nicaragua has removed visa requirements for air travelers from third countries, triggering a surge in U.S.-bound migration from those countries through Nicaragua.

## MAJOR STATE ACTORS

---

*Several major state actors present proximate and enduring threats to the United States and its interests in the world, challenging U.S. military and economic strength, regionally and globally. China stands out as the actor most capable of threatening U.S. interests globally, though it is also more cautious than Russia, Iran, and North Korea about risking its economic and diplomatic image in the world by being too aggressive and disruptive. Growing cooperation among these actors expands the threat, increasing the risk that should hostilities with one occur, it may draw in others.*

### CHINA

#### Strategic Overview

*President Xi Jinping and the People's Republic of China (PRC) want to achieve "the great rejuvenation of the Chinese nation" by 2049. The PRC will seek to increase its power and influence to shape world events to create an environment favorable to PRC interests, obtain greater U.S. deference to China's interests, and fend off challenges to its reputation, legitimacy, and capabilities at home and abroad.*

- Beijing is deeply suspicious of U.S. intentions and views Washington's measures against China as part of a concerted, whole-of-government effort, working with U.S. allies and partners, to contain China's development and rise, undermine CCP rule, and prevent the PRC from achieving its aims. PRC leaders are most concerned about strong unified opposition from the United States and its allies, and are responding, in part, by strengthening ties with partners like Russia and North Korea.
- At the same time, China's leaders will seek opportunities to reduce tension with Washington when they believe it benefits Beijing, protects its core interests, and buys time to strengthen its position.

*The PRC will likely continue posturing to be in a position of advantage in a potential conflict with the United States. The PRC will continue trying to press Taiwan on unification and will continue conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage. China will likely struggle to sufficiently constrain the activities of PRC companies and criminal elements that enable the supply and trafficking of fentanyl precursors and synthetic opioids to the United States, absent greater law enforcement actions.*

- China's military operations to project power over Taiwan and its efforts to assert sovereignty claims in the South and East China Seas occur routinely with confrontations that increase concern of miscalculations potentially leading to conflict.
- China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States.

*Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and sustain its industrial- and technology-intensive economic strategy to compete with U.S. economic power and global leadership.*

## Military

*China presents the most comprehensive and robust military threat to U.S. national security.* The People's Liberation Army (PLA) is fielding a joint force that is capable of full-spectrum warfare to challenge intervention by the United States in a regional contingency, projecting power globally, and securing what Beijing claims is its sovereign territory. A major portion of China's military modernization efforts is focused on developing counter-intervention capabilities tailored against all aspects of U.S. and allied military operations in the Pacific. Beijing will focus on meeting key modernization milestones by 2027 and 2035, aimed at making the PLA a world-class military by 2049.

- Examples of PLA advances in 2024 include the PLA Navy's third carrier (CV-18 Fujian) beginning sea trials and likely being ready to enter operational service in 2025. The PLA Rocket Force probably is fielding the DF-27 ballistic missile, with a hypersonic glide vehicle payload option and an estimated range of between 5,000 and 8,000 kilometers. The PLA ground forces are also fielding its most advanced multiple rocket launcher, the PCH191, increasing its long-range, precision strike capability.
- The PLA has improved its force structure, readiness, and training. The PLA probably has made particular progress in critical areas, such as modernizing key ground forces, expanding its navy with more modern combatants, and fielding a wide variety of new missile systems; it has also improved its electronic warfare (EW) capabilities.

*The PLA has the capability to conduct long-range precision-strikes with conventional weapons against the Homeland's periphery in the Western Pacific, including Guam, Hawaii, and Alaska.* China has developed a range of ballistic and cruise missiles with conventional payloads that can be delivered from its mainland as well as by air and sea, including by nuclear-powered submarines. China may be exploring development of conventionally-armed intercontinental range missile systems, which, if developed and fielded, would allow China to threaten conventional strikes against targets in the continental United States.

The PLA will continue to pursue the establishment of overseas military installations and access agreements to project power and protect China's interests abroad. Beijing may also pursue a mixture of military logistics models, including preferred access to commercial infrastructure abroad, exclusive PLA logistics facilities with pre-positioned supplies co-located with commercial infrastructure, and bases with stationed forces, to meet its overseas military logistics needs.

*China is using complex, whole-of-government campaigns featuring coercive military, economic, and influence operations short of war to assert its positions and strength against others, reserving more destructive tools for full-scale conflict.* Beijing will likely expand these campaigns to advance unification with Taiwan, project power in East Asia, and reverse perceived U.S. hegemony.

- Beijing has pushed back against U.S. military operations, such as reconnaissance and bomber flights, freedom of navigation operations, and exercises around PRC borders and maritime claims. The PLA regularly intercepts and shadows U.S. forces and sometimes conducts unsafe maneuvers in their vicinity.

### Taiwan and Maritime Flashpoints

*In 2025, Beijing will likely apply stronger coercive pressure against Taiwan and perceived increases in U.S. support to the island to further its goal of eventual unification.* The PRC calls for a peaceful unification with Taiwan to resolve the Civil War that drove Taiwan's separation, even as it threatens to use force to compel unification if necessary and counter what it sees as a U.S. attempt to use Taiwan to undermine China's rise.

A conflict between China and Taiwan would disrupt U.S. access to trade and semiconductor technology critical to the global economy. Even without U.S. involvement in such a conflict, there would likely be significant and costly consequences to U.S. and global economic and security interests.

*Beijing is working to isolate Taipei by pressuring states to downgrade diplomatic ties and support China's unification goal.* Since 2016, Taiwan's official diplomatic relationships have dropped from 22 to only 12, and several of the remaining ones are vulnerable to Chinese pressure.

*China is advancing military capabilities for a cross-Straits campaign while also using its armed forces to exert steady state pressure on Taiwan.* The PLA probably is making steady but uneven progress on capabilities it would use in an attempt to seize Taiwan and deter—and if necessary, defeat—U.S. military intervention, and it is intensifying the scope, size, and pace of operations around Taiwan.

*Beijing will continue to pressure Taipei with economic coercion and probably will increase it if it sees Taiwan taking steps toward formal independence.* It could suspend preferential tariff terms, selectively ban Taiwan imports to China, and arbitrarily enforce regulations.

*Beijing's aggressive efforts to assert sovereignty claims in the South and East China Seas are heightening tensions that could trigger a broader conflict.*

- In 2024, PRC tactics in the South China Sea led to the loss of the Philippines' unilateral access to some disputed areas, and forced talks between Beijing and Manila in which the Philippines agreed to concessions in exchange for access. However, Manila is unlikely to relinquish its claims, creating potential for escalation by either side.
- Tension between China and Japan over the Senkaku Islands last flared up a decade ago. Since then, Chinese ships have remained in proximity of the disputed islands, occasionally entering the territorial zone, and driving responses from Japan's Self-Defense Force to monitor the activity.

### Cyber

*The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks. The PRC's campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon, and its more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure.*



- If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.

## Economics

*The PRC seeks to compete with the United States as the leading economic power in the world. To do so, the strategy calls for a centralized, state-directed, and nationally resourced approach to dominating global markets and strategic supply chains, limiting foreign competitors, and making other nations dependent on China.* PRC leaders are applying the same strategy to bolster China's position and become more globally dominant in critical supply chains, both in upstream inputs it can provide more cheaply than others and in downstream production at wider scale.

- China's weak domestic demand, coupled with its industrial policies, such as manufacturing subsidies, have enabled a surge in cheap Chinese exports in sectors such as steel, harming U.S. competitors and fueling a record PRC trade surplus.
- China's dominance in key supply chains enables its use of economic coercion against countries that adopt policies Beijing opposes. Beijing is developing an institutionalized framework enabling more assertive and centrally controlled trade retaliation. PRC leaders are using ostensibly unofficial or technical trade and investment barriers, administrative regulations, logistics, and symbolic sanctions in a targeted way against individuals, firms, and sectors, in parallel with messages to warn and deter.
- PRC leaders appear to be preparing for more economic friction with the United States, and probably are weighing options with the new U.S. administration while looking for leverage and other ways to prevent a major escalation and decoupling.

*China's dominance in the mining and processing of several critical materials is a particular threat, providing it with the ability to restrict quantities and affect global prices.* Beijing has shown a willingness to restrict global access to its mineral resources—sometimes in response to geopolitical disputes—as with its banning of exports to the United States of metals used in semiconductor manufacturing, such as gallium, germanium, and antimony in December 2024 in response to U.S. export controls on advanced semiconductors and chip-making equipment. Other examples include when the PRC temporarily stopped rare earth element exports to Japan in 2010, and Beijing's creation of new laws codifying its authority to restrict mineral exports. A prolonged cessation in supplies controlled by China could disrupt critical inputs needed for U.S. industry and technological advancements.

*China has similar aims in global shipping and resource access, including in the Arctic, where melting sea ice is creating opportunities for expanded maritime transport and energy exploitation, especially along the Northern Sea Route (NSR) off Russia's coast.* China seeks access to the Arctic's potentially vast natural resources, including oil, gas, and minerals, even though China is not among the eight Arctic countries that control territory in the region. Beijing seeks to normalize more direct and efficient maritime shipping routes to Russia and other Northern Hemisphere areas, as a way to fuel its economic growth and energy security and reduce its dependence on Middle East energy. China has gradually increased engagement with Greenland mainly through mining projects, infrastructure development, and scientific research projects. Despite less active engagement right now, China's long-term goal is to expand access to Greenland's natural resources, as well as to use the same access as a key strategic foothold for advancing China's broader and economic aims in the Arctic.

## Technology

*China is using an aggressive, whole-of-government approach, combined with state direction of the private sector, to become a global S&T superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain.* Beijing has prioritized technology sectors such as advanced power and energy, AI, biotechnology, quantum information science, and semiconductors, further challenging U.S. efforts to protect critical technologies by tailoring restrictions narrowly to address national security concerns. China is accelerating its S&T progress through a range of licit and illicit means, to include investments, intellectual property acquisition and theft, cyber operations, talent recruitment, international collaborations, and sanctions evasion.

- Some forecasts indicate China's technology sectors will account for as much as 23 percent of its gross domestic product by 2026, more than doubling since 2018. In addition to private funding, the PRC government is investing hundreds of billions of dollars in priority technologies, such as AI, microelectronics, and biotechnologies, in pursuit of its self-reliance goals.

*China almost certainly has a multifaceted, national-level strategy designed to displace the United States as the world's most influential AI power by 2030.* China is experiencing a boom in generative AI with the rapid emergence of a large number of PRC-developed models, and is broadly pursuing AI for smart cities, mass surveillance, healthcare, S&T innovation, and intelligent weapons. Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies. The PLA probably plans to use large language models (LLMs) to generate information deception attacks, create fake news, imitate personas, and enable attack networks. China has also announced initiatives to bolster international support for its vision of AI governance.

- China has stolen hundreds of gigabytes of intellectual property from companies in Asia, Europe, and North America in an effort to leapfrog over technological hurdles, with as much as 80 percent of U.S. economic espionage cases as of 2021 involving PRC entities.

*China also sees biotechnology as critical to becoming a dominant economic power and intends to grow its domestic bioeconomy to \$3.3 trillion this year.* Beijing is investing heavily in collecting health and genetic data both at home and abroad in pursuit of these goals, and has shown it can be globally competitive in certain low-cost, high-volume commodities, such as biomanufacturing and genetic sequencing. Beijing has identified genetic data as a national strategic resource and is expanding state control over the country's gene banks and other genetic repositories, positioning it to potentially lead in precision medicine and agricultural biotechnology applications.

*China has made progress in producing advanced 7-nanometer (nm) semiconductor chips for cryptocurrency mining and cellular devices using previously acquired deep ultraviolet (DUV) lithography equipment, but will face challenges achieving high-quality, high-volume production of these chips without access to extreme ultraviolet lithography tools.* PRC researchers also continue to explore applying advanced patterning techniques to DUV machines to produce semiconductor chips as small as 3nm. China leads the world in legacy logic semiconductor (28nm and up) production, accounting for 39.3 percent of global capacity, and is expected to add more capacity than the rest of the world combined through 2028. These legacy chips are vital to producing automobiles, consumer electronics, home appliances, factory automation, broadband, and many military and medical systems.

## WMD

*China remains intent on modernizing, diversifying, and expanding its nuclear posture. China's nuclear weapons and advanced delivery systems pose a direct threat to the Homeland and are capable of delivering catastrophic damage to the United States and threatening U.S. military forces here and abroad.*

*China most likely possesses capabilities relevant to chemical and biological warfare (CBW) that pose a threat to U.S., allied, and partner forces as well as civilian populations.*

## Biosecurity

*China's approach to and role in global biological, medical, and other health-related global priorities present unique challenges to the United States and the world* The COVID-19 pandemic that ultimately led to the death of more than one million Americans—and multiples more worldwide—began in China, which Beijing still refuses to acknowledge. China's strict censorship and repression of free speech prevented doctors treating the earliest of patients in Wuhan from warning the world of a far more serious contagion than Beijing wanted told, slowing the world's preparedness and response. To this day, Beijing refuses to fully cooperate with the rest of the international community trying to definitively pinpoint the precise cause of the disease so it can head off and prepare for any new disease.

Regarding COVID-19 origins, IC agencies have continued to evaluate new information from classified and open sources, revisit previous reporting, and consult with diverse technical experts to increase our understanding of the cause of the pandemic. These efforts have led CIA to assess that a research-related hypothesis is more likely than a natural origin hypothesis.

The other hypothesis for COVID-19—natural origin—includes many scenarios in which humans could have been infected with SARS-CoV-2—the virus that causes COVID-19—or a close progenitor through exposure to wild or domestic animals. China is home to a diverse body of naturally occurring coronaviruses found in a wide geographic area, and there is precedence for these viruses to emerge within human populations far from reservoir locations. For example, the coronavirus that is the closest known relative to SARS-CoV—the virus that causes severe acute respiratory syndrome (SARS)—probably originated in Yunnan Province, according to scientific studies, even though the first SARS outbreak detected in humans in 2003 occurred in Guangdong Province, hundreds of miles away.

- The research-related incident hypothesis also considers a broad range of potential initial human-infection scenarios from events in research facilities, such as government or university laboratories, to research-related activities in the field, such as collecting samples from wild animals.

*The PRC's dominance in pharmaceutical and medical supply production combined with lower quality safety and environmental standards than those of the United States positions Beijing to potentially restrict such exports for leverage over Washington and others in trade or security disputes.* The PRC plays an increasingly important role in supplying pharmaceuticals and related medical supplies to the United States, as well as the rest of the world.

- U.S. imports of Chinese pharmaceuticals—defined as medicines, vaccines, blood, organic cultures, bandages, and organs—grew almost five-fold between 2020 and 2022 alone, from \$2.1 billion to \$10.3 billion.

- The PRC also might look to uniquely provide such supplies and medical aid to countries, more cheaply and at scales competitors cannot match, as a way to boost its global influence at the expense of the United States. The PRC's "vaccine diplomacy" during the COVID-19 pandemic—it provided vaccines to 83 countries—was driven at least in part by geopolitical considerations, such as currying favor for a new port in Burma.

## Space

*China has eclipsed Russia as a space leader and is poised to compete with the United States as the world's leader in space by deploying increasingly capable interconnected multi-sensor systems and working toward ambitious scientific and strategic goals.* China has achieved global coverage in some of its intelligence, surveillance, and reconnaissance (ISR) constellations and world-class status in all but a few space technologies.

- China's Beidou constellation is a world-class position, navigation, and timing capability that competes with U.S. GPS and Europe's Galileo service. The PLA ISR architecture and satellite communications are areas the PLA continues to improve upon to close the perceived gap between itself and the U.S. military.
- China's successful lunar sample return mission in June 2024 contributes to Beijing's technological prowess and national prestige while supporting its effort to land astronauts on the Moon by 2030 and establish the first lunar base by 2035.
- China's commercial space sector is growing quickly with aspiration to be a major global competitor to U.S. and European space companies. For example, China launched the first set of satellites in its low Earth orbit (LEO) proliferated constellation last year for its own satellite Internet service to compete with Western commercial satellite Internet services.

*Counterspace operations will be integral to PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites. China already has fielded ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites.*

- China also has conducted orbital technology demonstrations, which, while not counterspace weapons tests, prove its ability to operate future space-based counterspace weapons. China has also conducted on-orbit satellite inspections of other satellites, which probably would be representative of the tactics required for some counterspace attacks.

## Malign Influence Activities

*Beijing will continue to expand its coercive and subversive malign influence activities to weaken the United States internally and globally, as well as counter what Beijing sees as a U.S.-led campaign to tarnish China's global relations and overthrow the CCP. Through these efforts, the PRC seeks to suppress critical views and critics of China within the United States and worldwide, and sow doubts in U.S. leadership and strength. Beijing is likely to feel emboldened to use malign influence more regularly in coming years, particularly as it fields AI to improve its capabilities and avoid detection.*

- PRC actors have increased their capabilities to conduct covert influence operations and disseminate disinformation. For example, pro-China online actors in 2024 used AI-generated news anchors and fake social media accounts with AI-generated profile pictures to sow divisions on issues such as drug use, immigration, and abortion.

#### China's Challenges

*China faces daunting challenges that will impair CCP leaders' strategic and political achievements. China's leaders probably are most concerned about corruption, demographic imbalances, and fiscal and economic struggles because they threaten the country's economic performance and quality of life, two key factors underpinning CCP legitimacy.* Despite an acute economic slowdown, China's leaders probably will resist making needed structural reforms and instead maintain statist economic policies to steer capital toward priority sectors, reduce dependence on foreign technologies, and enable military modernization.

- China's growth probably will continue to slow because of low consumer and investor confidence. China's birth and marriage rates continue to decline, reinforcing negative population trends and a shrinking labor force.

Xi's focus on security and stability for the CCP and securing other leaders' personal loyalty to him is undermining China's ability to solve complex domestic problems and will impede Beijing's global leverage. Xi's blending of domestic and foreign security threats is undermining China's position and standing abroad, reducing Beijing's ability to shape global perceptions and compete with U.S. leadership.

## RUSSIA

### Strategic Overview

*Russia views its ongoing war in Ukraine as a proxy conflict with the West, and its objective to restore Russian strength and security in its near abroad against perceived U.S. and Western encroachment has increased the risks of unintended escalation between Russia and NATO.* The resulting heightened and prolonged political-military tensions between Moscow and Washington, coupled with Russia's growing confidence in its battlefield superiority and defense industrial base and increased risk of nuclear war, create both urgency and complications for U.S. efforts to bring the war to an acceptable close.

*Regardless of how and when the war in Ukraine ends, Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests.* Despite having paid enormous military and economic costs in its war with Ukraine, Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea. President Vladimir Putin appears resolved and prepared to pay a very high price to prevail in what he sees as a defining time in Russia's strategic competition with the United States, world history, and his personal legacy. Most Russian people continue to passively accept the war, and the emergence of an alternative to Putin probably is less likely now than at any point in his quarter-century rule.

- Western efforts to isolate and sanction Russia have accelerated its investments in alternative partnerships and use of various tools of statecraft to offset U.S. power, with China's backing and reinforcement. Russia's relationship with China has helped Moscow circumvent sanctions and export controls to continue the war effort, maintain a strong market for energy products, and promote a global counterweight to the United States, even if at the cost of greater vulnerability to Chinese influence. Russia is also increasing military cooperation with Iran and North Korea, which will continue to help its war effort and enhance U.S. adversary cooperation and collective capacity. Finally, Moscow is increasingly willing to play spoiler in Western-centric forums such as the UN as well as use non-Western organizations like the Brazil, Russia, India, China, and South Africa (BRICS) group to press policies such as de-dollarization.
- Russia has shown it can navigate substantial economic challenges resulting from the ongoing drains of the war, Western cost imposition, and high inflation and interest rates, for at least the near term by using financial and import substitution workarounds, maintaining low debt, and continuing investments in the defense-industrial base. Russia's economy remains the fourth largest in the world (based on GDP at purchasing power parity).
- Russia's sizable ground force losses in the war have done little to undermine the strategic pillars of its military power, to include its diverse and robust nuclear deterrent and asymmetric capabilities, particularly in counterspace and undersea warfare. Russia's air and naval forces remain intact, with the former being more modern and capable than at the start of the invasion. Russia is developing a growing arsenal of conventional capabilities, such as theater strike weapons, to target the Homeland and deployed forces and assets abroad—and to hold U.S. allies at risk—during crisis and wartime. Russia's advanced WMD and space programs threaten the Homeland, U.S. forces, and key warfighting advantages.
- Russia will continue to be able to deploy anti-U.S. diplomacy, coercive energy tactics, disinformation, espionage, influence operations, military intimidation, cyberattacks, and gray zone tools to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests.
- The war in Ukraine has afforded Moscow a wealth of lessons regarding combat against Western weapons and intelligence in a large-scale war. This experience probably will challenge future U.S. defense planning, including against other adversaries with whom Moscow is sharing those lessons learned.

#### Russia and the Arctic

Russia controls about half of all Arctic coastline and views the region as essential to its economic well-being and national security. Moscow wants to further develop its Arctic oil and gas reserves and position itself to reap benefits from expected increases in maritime trade. Russia has concerns about increasing economic and military competition with Western countries in the region, which compounded last year when NATO enlarged to include the last two previously nonaligned Arctic states, Finland and Sweden.

- The war in Ukraine has sapped Russia's finances and available military resources to fulfill its Arctic ambitions, prompting Russia to seek a closer partnership with China in the Arctic, and

welcoming other non-Western countries' increasing involvement, to offset NATO countries' perceived advantages.

- Russia's interest in Greenland is focused mainly on its proximity to strategically important naval routes between the Arctic and Atlantic Oceans—including for nuclear-armed submarines—and the fact that Greenland hosts a key U.S. military base.

## Military

*Moscow's massive investments in its defense sector will render the Russian military a continued threat to U.S. national security, despite Russia's significant personnel and equipment losses—primarily in the ground forces—during the war with Ukraine.* Russia's air and naval forces, despite suffering some losses and expending substantial quantities of precision-guided munitions, remain capable of providing Moscow with regional and global power projection forces, while Russia's nuclear and counterspace forces continue to provide it with strategic deterrence capability.

- The Ukraine conflict has led to improvements in some Russian military capabilities. For example, Russia's initial use of EW and unmanned systems was lacking but it adapted and innovated using EW to more effectively interfere with Ukrainian use of radar and GPS and unmanned aerial vehicles (UAVs).
- Russia possesses long-range precision strike capability, most notably submarines and bombers equipped with LACMs and antiship cruise missiles, that can hold the Homeland at risk.
- Moscow has increased its defense budget to its heaviest burden level during Putin's more than two decades in power and taken measures to reduce the impact of sanctions on its military and defense industry.
- Russia has imported munitions such as UAVs from Iran and artillery shells from North Korea to mitigate to the impact of international sanctions, thereby sustaining its ability to wage war in Ukraine and enhancing the threat its military poses.

Moscow will contend with long-term challenges such as troop quality and corruption, and a fertility rate below what is needed for replacements, but its investments in personnel recruitment and procurement should allow it to steadily reconstitute reserves and expand ground forces in particular during the next decade. Nevertheless, the war in Ukraine will be a drag on those efforts as long as it persists. Moscow will have to continually balance resource allocation between large-scale production of equipment to sustain the war with modernization and recapitalization efforts.

### Russia and Ukraine

*Russia in the past year has seized the upper hand in its full-scale invasion of Ukraine and is on a path to accrue greater leverage to press Kyiv and its Western backers to negotiate an end to the war that grants Moscow concessions it seeks. Continuing the Russia-Ukraine war perpetuates strategic risks to the United States of unintended escalation to large-scale war, the potential use of nuclear weapons, heightened insecurity among NATO Allies, particularly in Central, Eastern, and Northern Europe, and a more emboldened China and North Korea.*

Even though Russian President Putin will be unable to achieve the total victory he envisioned when initiating the large-scale invasion in February 2022, Russia retains momentum as a grinding war of attrition plays to Russia's military advantages. This grinding war of attrition will lead to a gradual but steady erosion of Kyiv's position on the battlefield, regardless of any U.S. or allied attempts to impose new and greater costs on Moscow.

- Despite recruitment challenges, Russia has regularly generated sufficient personnel to replenish losses and create new units to sustain attacks on multiple frontline axes. While Ukraine has increased its overall personnel intake since new legislation on mobilization was passed in spring 2024, Kyiv has stretched its resources trying to launch new offensives—such as in Kursk, Russia—and build more brigades while defending on all fronts.
- Moscow's rising defense spending and investments in defense-industrial capacity will continue to enable a high level of production of critical capabilities—such as artillery, long-range missiles, one-way attack UAVs, and glide bombs—and ensure Russia retains a firepower advantage over Ukraine.
- Both Putin and Ukrainian President Volodymyr Zelenskyy are interested in continuing discussions with the United States on how to end the war and have shown a willingness to test partial ceasefires. Nonetheless, Putin probably is attuned to the potential for protracted conflict to drag down the Russian economy and prompt undesired escalation with the West, and Zelenskyy probably understands that his position is weakening, the future of Western assistance is uncertain, and a ceasefire may ultimately become a necessary recourse. However, both leaders for now probably still see the risks of a longer war as less than those of an unsatisfying settlement. For Russia, positive battlefield trends allow for some strategic patience, and for Ukraine, conceding territory or neutrality to Russia without substantial security guarantees from the West could prompt domestic backlash and future insecurity.

### Cyber

*Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat. Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict.*



- Russia has demonstrated real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware.

### **Malign Influence Activities**

*Moscow uses influence activities to counter threats, including by stoking political discord in the West, sowing doubt in democratic processes and U.S. global leadership, degrading Western support for Ukraine, and amplifying preferred Russian narratives. Moscow's malign influence activities will continue for the foreseeable future and will almost certainly increase in sophistication and volume.*

- Moscow probably believes information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of its core objectives.
- Russia uses a variety of entities such as the U.S.-sanctioned influence organizations Social Design Agency (SDA) and ANO Dialog and the state media outlet RT in its efforts to covertly shape public opinion in the United States, amplify and stoke domestic divisions, and discreetly engage Americans, while hiding Russia's hand.

### **WMD**

*Russia has the largest and most diverse nuclear weapons stockpile that, along with its deployed ground-, air-, and sea-based delivery systems, could inflict catastrophic damage to the Homeland.* Russia has developed a more modernized, mobile, and survivable strategic nuclear force that is intended to circumvent or neutralize future augmented U.S. missile defense and ensure deterrence through reliable retaliatory strike potential. In addition, Russia's vast arsenal of non-strategic nuclear weapons helps it to offset Western conventional superiority and provide formidable escalation management options in theater war scenarios.

*Russia continues efforts to modernize its nuclear weapons capabilities in the face of multiple failed tests of new systems.*

*Russia's CBW threat is expanding.* Russian scientific institutes continue to research and develop CBW capabilities, including technologies to deliver CBW agents. Russia retains an undeclared chemical weapons program and has used chemical weapons at least twice during recent years in assassination attempts with Novichok nerve agents, also known as fourth-generation agents, against Russian opposition leader Aleksey Navalny in 2020, and against U.K. citizen Sergey Skripal and his daughter Yuliya Skripal on U.K. soil in 2018. Russian forces almost certainly continue using chemicals against Ukrainian forces, with hundreds of reported attacks occurring since late 2022.

### **Space**

*Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities. It is expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites.*

- Russia is using EW to counter Western on-orbit assets and continues to develop ASAT missiles capable of destroying space targets in LEO.

*Despite its Soviet legacy, the war in Ukraine has revealed glaring deficiencies in Russia's space-based architecture, which will continue to face difficulties from the effects of sanctions and export controls, domestic space-sector problems, and increasingly strained competition for program resources within Russia.* However, Russia will remain a space competitor, probably by prioritizing assets critical to its national security and integrating military space services over civil space projects.

- Moscow uses its and others' civil and commercial remote-sensing satellites to supplement military-dedicated capabilities and has warned that other countries' commercial infrastructure in outer space used for military purposes can become a legitimate target.

#### Russian Antisatellite Capability

*Russia is developing a new satellite meant to carry a nuclear weapon as an antisatellite capability.* A nuclear detonation in outer space could cause devastating consequences for the United States, the global economy, and the world in general. It would harm all countries' national security and commercial satellites and infrastructure, as well as impair U.S. use of space as a driver for economic development.

- In February 2022, Russia launched a satellite, which its Ministry of Defense claimed at the time was for testing on-board instruments and systems under the influence of radiation and heavy charged particles.

#### Technology

*While Russia's S&T ecosystem has been constrained in the wake of its invasion of Ukraine, Moscow continues to deploy nascent AI applications on and off the battlefield and has deepened technical cooperation with partners such as China in support of long-term R&D goals.* Moscow's use of AI to augment military operations probably will further hone Russian tactics and capabilities in the event of future conflicts with the United States or NATO allies.

- Russia is using AI to create highly-capable deepfakes to spread misinformation, conduct malign influence operations, and stoke further fear. Russia has also demonstrated the use of AI-enabled antidrone equipment during its ongoing conflict with Ukraine.
- Russia's few domestic microelectronics manufacturers have only mastered production of chips down to the 65nm level and has goals of mass producing 28nm chips by 2030, significantly behind global leaders.
- While largely cut-off from Western supply chains, Russia has significantly expanded and deepened cooperation in several technical sectors with international partners. Russia seeks to further align its S&T efforts with China and BRICS allies in areas such as AI development and governance and semiconductor production to advance its own capabilities as well as broadly decrease Western influence.

### Russia's Challenges

*Even as Russia has proven resilient, it faces a myriad of challenges to remaining an indispensable global player, maintaining a sphere of influence, and upholding stability at home—its highest strategic aims—suggesting limits on its confidence dealing with the United States and the international community.* Russia has paid a heavy price in blood, treasure, and loss of international reputation and foreign policy options because of its large-scale invasion of Ukraine. President Putin upended two decades of Russia's geopolitical resurgence, created new threats to its external and internal security, and strained its economic and military potential, making it more reliant on China and other like-minded partners like North Korea.

- Russia's military has suffered more casualties in Ukraine than in all of its other wars since World War II (750,000-plus dead and wounded), and its economy faces significant long-term macroeconomic headwinds and is increasingly dependent on China.
- Russia's aggression has strengthened European unity and prompted Finland and Sweden to join NATO. Efforts by Armenia, Moldova, and some Central Asian states to seek alternative partners highlight how the war has hurt Moscow's influence, even in the post-Soviet space, and derailed Putin's vision of a greater Eurasian union.

## IRAN

### Strategic Overview

*Tehran will try to leverage its robust missile capability and expanded nuclear program, and its diplomatic outreach to regional states and U.S. rivals to bolster its regional influence and ensure regime survival. However, regional and domestic challenges, most immediately tensions with Israel, are seriously testing Iran's ambitions and capabilities.* A degraded Hizballah, the demise of the Asad regime in Syria, and Iran's own failure to deter Israel have led leaders in Tehran to raise fundamental questions regarding Iran's approach. Iran's consistently underperforming economy and societal grievances will also continue to test the regime domestically.

*Tehran will continue its efforts to counter Israel and press the United States to leave the region by aiding and arming its loose consortium of like-minded terrorist and militant actors, known as the "Axis of Resistance."* Although the demise of the Asad regime, a key ally of Tehran, is a blow to the Axis, these actors still represent a wide range of threats. These threats include some continued Israeli vulnerability to HAMAS and Hizballah; militia attacks against U.S. forces in Iraq and Syria; and the threat of Huthi missile and UAV attacks targeting Israel and maritime traffic transiting near Yemen. Supreme Leader Ali Khamenei continues to desire to avoid embroiling Iran in an expanded, direct conflict with the United States and its allies.

*Iranian investment in its military has been a key plank of its efforts to confront diverse threats and try to deter and defend against an attack by the United States or Israel.* Iran continues to bolster the lethality and precision of its domestically produced missile and UAV systems, and it has the largest stockpiles of these systems in the region. It considers them as critical to its deterrence strategy and power projection capability, and Iran uses their sales to deepen global military partnerships. Iran's growing expertise and willingness to conduct aggressive cyber operations also make it a major threat to the security of U.S. and allied and partner networks and data.

*Iran also will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States.* Iran seeks to target former and current U.S. officials it believes were involved in the killing of Islamic Revolutionary Guard Corps (IRGC)-Qods Force Commander Qasem Soleimani in January 2020 and previously has tried to conduct lethal operations in the United States.

*Tehran intends for its expanding relationships with other key U.S. adversaries and the Global South to mitigate U.S. efforts to isolate the regime and blunt the impact of Western sanctions. Tehran's diplomatic efforts—including at times outreach to Europe—are likely to continue with varying degrees of success.* In the past year, Iran has focused extensively on deepening ties with Russia—including through military cooperation for its war in Ukraine—and has relied on China as a key political and economic partner to help it mitigate economic and diplomatic pressure. Iran is also making progress developing closer diplomatic and defense ties to African states and other actors in the Global South and is trying to build on nascent improvements in its ties with other regional actors, such as Saudi Arabia, despite continued mutual suspicion over each other's ultimate visions for the region.

*The economic, political, and societal seeds of popular discontent could threaten further domestic strife akin to the widespread and prolonged protests inside Iran during late 2022 and early 2023.* The economy is beset by low growth, exchange rate volatility, and high inflation. Absent sanctions relief, these trends probably will continue for the foreseeable future.

#### Syria

*The fall of President Bashar al-Asad's regime at the hands of opposition forces led by Hay'at Tahrir al-Sham (HTS)—a group formerly associated with al-Qa'ida—has created conditions for extended instability in Syria and could contribute to a resurgence of ISIS and other Islamist terror groups. Even if the HTS-led interim government can bridge divergent objectives, governing Syria will remain a daunting challenge amid the country's economic problems, humanitarian needs driven in part by millions of internally displaced Syrians, rampant insecurity, as well as ethnic, sectarian, and religious cleavages.*

- The HTS-led interim government forces, along with elements of Hurras al-Din and other jihadist groups, engaged in violence and extrajudicial killings in northwestern Syria in early March 2025 primarily targeting religious minorities that resulted in the death of more than 1,000 people, including Alawi and Christian civilians.
- The leader of HTS claims to be willing to work with Syria's array of ethnosectarian groups to develop an inclusive governance model. Many of these groups remain skeptical of HTS's intentions, especially considering the leader's past al-Qa'ida association, suggesting protracted negotiations could devolve into violence. Israeli government officials are skeptical of HTS claims and intentions, expressing concern that historical HTS objectives against Israel persist.
- Some remaining jihadist groups refuse to merge into the HTS Ministry of Defense, and ISIS has already signaled opposition to HTS's call for democracy and is plotting attacks to undermine its governance.

## Military

*Iran's conventional and unconventional capabilities will pose a threat to U.S. forces and partners in the region for the foreseeable future, despite the degradation to its proxies and air defenses during the Gaza conflict.* Iran's large conventional forces are capable of inflicting substantial damage to an attacker, executing regional strikes, and disrupting shipping, particularly energy supplies, through the Strait of Hormuz. Iran's unconventional warfare operations and militant partners and proxies, such as Hizballah, have traditionally enabled Tehran to pursue its interests throughout the region and maintain strategic depth with a modicum of deniability. However, Iranian officials are grappling with how to slow and eventually reverse their and their proxies' recent military losses from the Israeli campaign against Iran and its regional allies, including strikes on Iranian military targets such as air defense systems in April and October 2024. The IC assesses Iran's prospects for reconstituting force losses and posing a credible deterrent, particularly to Israeli actions, are dim in the near-term.

Iran has fielded a large quantity of ballistic and cruise missiles as well as UAVs that can strike throughout the region and continues efforts to improve their accuracy, lethality, and reliability. Iran's defense industry has a robust development and manufacturing capacity, especially for low-cost weapons such as small UAVs. However, the limited damage Iran's strikes in April and October 2024 inflicted on Israel highlights the shortcomings of Iran's conventional military options.

Iran has also deployed small boats and submarines capable of disrupting shipping traffic through the Strait of Hormuz. Its ground and air forces, while among the largest in the region, suffer from outdated equipment and limited training.

### Middle East Conflict

*The Israel-HAMAS conflict sparked by the HAMAS October 7 attack against Israel derailed the unprecedented diplomacy and cooperation generated by the Abraham Accords and trajectory of growing stability in the Middle East. We expect the situation in Gaza, as well as Israel-Hizballah and Israel-Iran dynamics, to remain volatile.*

*Even in degraded form, HAMAS continues to pose a threat to Israeli security.* The group retains thousands of fighters and much of its underground infrastructure, and probably has used the ceasefire to reinforce and resupply its military and munitions stock so that it can fight again. HAMAS is capable of resuming a low-level guerilla resistance and to remain the dominant political action in Gaza for the foreseeable future. Low expectations on all sides that a ceasefire will endure and the absence of a credible post-fighting political and reconstruction plan, portend years of instability.

- While HAMAS's popularity has declined among Gazans, its popularity remains high among West Bank Palestinians, especially relative to the Palestinian Authority (PA).

*The long-term Israeli-Palestinian relationship also hinges on the trajectory of an increasingly unstable West Bank.* The PA's weak and declining ability to provide security and other services in the West Bank, Israeli operations in the West Bank, violence from Israeli settlers and Palestinian militant groups including HAMAS, and a potential leadership transition in the PA are likely to exacerbate governance challenges in Ramallah. Much also will depend on how Israel deals with post-conflict Gaza and its operations in the West Bank that may weaken or undermine the PA.

During the Gaza conflict, Iran encouraged and enabled its various proxies and partners to conduct strikes against Israeli and at times U.S. forces and interests in the region.

- The Huthis have emerged as the most aggressive actor, attacking commercial shipping in the Red Sea and Indian Ocean, U.S. and European forces, and Israel. In addition to receiving Iranian assistance, the Huthis have expanded their reach by broadening partnerships with other actors, such as Russia and Russian arms brokers, PRC commercial defense companies, al-Shabaab, and Iraqi Shia militants.
- Iraqi Shia militias continue to try to compel a U.S. withdrawal from Iraq through political pressure on the Iraqi government and attacks on U.S. forces in Iraq and Syria.

*Further fighting between Hizballah and Israel would threaten Lebanon's fragile stability and any political progress begun by the election of a president in January after years of trying.* A resumption of protracted Israeli operations in Lebanon could trigger a sharp rise in sectarian tension, undermine Lebanese security forces, and dramatically worsen humanitarian conditions. Although weakened, Hizballah maintains the capability to target U.S. persons and interests in the region, worldwide, and—to a lesser extent—in the United States.

## Cyber

*Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. networks and data.* Guidance from Iranian leaders has incentivized cyber actors to become more aggressive in developing capabilities to conduct cyber attacks.

## Malign Influence Activities

Iran often amplifies its influence operations with offensive cyber activities. During the Israel-HAMAS conflict, U.S. private industry tracked Iranian influence campaigns and cyber attacks.

- In June 2024, an IRGC actor compromised an email account associated with an individual with informal ties to then-former President Trump's campaign and used that account to send a targeted spear-phishing email to individuals inside the campaign itself. The IRGC subsequently tried to manipulate U.S. journalists into leaking information illicitly acquired from the campaign.

## WMD

*We continue to assess Iran is not building a nuclear weapon and that Khamenei has not reauthorized the nuclear weapons program he suspended in 2003, though pressure has probably built on him to do so.* In the past year, there has been an erosion of a decades-long taboo on discussing nuclear weapons in public that has emboldened nuclear weapons advocates within Iran's decisionmaking apparatus. Khamenei remains the final decisionmaker over Iran's nuclear program, to include any decision to develop nuclear weapons.

*Iran very likely aims to continue R&D of chemical and biological agents for offensive purposes.* Iranian military scientists have researched chemicals that have a wide range of sedation, dissociation, and amnesic incapacitating effects, and can also be lethal.

### Iran's Challenges

Iranian leaders recognize the country is at one of its most fragile points since the Iran-Iraq war, which probably weighs on their strategic calculus and confidence in their approach toward the region, the United States, and U.S. partners. They face growing political, social, economic, and regional pressures, leaving Iran increasingly vulnerable to regime-threatening instability and external interference.

## NORTH KOREA

### Strategic Overview

*North Korean leader Kim Jong Un will continue to pursue strategic and conventional military capabilities that target the Homeland, threaten U.S. and allied armed forces and citizens, and enable Kim to undermine U.S. power and reshape the regional security environment in his favor.* Kim's newly cemented strategic partnership with Russia is yielding financial benefit, diplomatic support, and defense cooperation. The partnership with

Moscow also helps reduce Pyongyang's reliance on Beijing. North Korea's advancing strategic weapons capabilities and increasing access to revenue are enabling Kim's longstanding goals of securing international acceptance as a nuclear power, reducing U.S. military presence on the Korean Peninsula, expanding state control over the North's economy, and blocking foreign influence.

- In June 2024, Kim and Putin signed a comprehensive strategic agreement for sweeping economic and technology partnerships. Kim also is using the agreement's mutual defense clause, which commits each country to provide military assistance if either is invaded by a foreign power, to justify deploying combat troops to fight against Ukraine.
- Kim has no intention of negotiating away his strategic weapons programs, which he perceives as a guarantor of regime security and national pride, because they threaten the Homeland, U.S. forces in the region, and U.S. allies like South Korea and Japan. He is increasing North Korea's nuclear warhead stockpile and improving its ballistic missile technology; for example, North Korea conducted three launches in 2024 of what it claimed were IRBMs equipped with maneuverable, hypersonic payloads.
- Kim seeks to intimidate the United States and its allies into abandoning opposition to North Korea's nuclear weapons and its aggression toward South Korea. For example, he responds to U.S. military planning with South Korea and trilateral cooperation with South Korea and Japan by ordering missile launches and threatening nuclear retaliation.
- North Korea will continue to defy international sanctions and engage in illicit activities, including stealing cryptocurrency, sending labor overseas, and trading UN-proscribed goods to resource and fund Kim's priorities, including ballistic missiles and WMD.

*Kim will act aggressively to counter activities he views as undermining the regime and threaten to use force when he perceives U.S. and allied actions as challenging North Korea's sovereignty, undermining his power, or aiming to curb his nuclear and missile ambitions.* Pyongyang is expanding its capacity for coercive operations and using new tactics as it becomes more confident in its nuclear deterrent. Since coming to power, Kim generally has relied on non-lethal coercive activities, including missile demonstrations and cross-border balloon launches of refuse, to win concessions and counter U.S. and South Korean military, diplomatic, and civilian activities.

- North Korea uses threats to try to stop South Korean efforts to disseminate information in the North, which he views as destabilizing his control. Kim in the past has challenged South Korea's de facto maritime boundary claims and may do so again, raising the prospects of renewed clashes along the Northern Limit Line.
- Kim could escalate to more lethal asymmetric activities if he judged North Korea's efforts at deterrence were not working and he needed to send a stronger message. He also could resort to these lethal activities if he believed doing so would intimidate South Korea or the United States into changing its policies to be more favorable to the North while minimizing the risk of retaliation.



## WMD

*Kim remains committed to increasing the number of North Korea's nuclear warheads and improving its missile capabilities to threaten the Homeland and U.S. forces, citizens, and allies, and to weaken U.S. power in the Asia-Pacific region, as evidenced by the pace of the North's missile flight tests and the regime's public touting of its uranium enrichment capabilities.* North Korea is probably prepared to conduct a nuclear test and continues to flight test ICBMs so Kim can threaten the Homeland. Russia is increasingly supporting North Korea's nuclear status in exchange for Pyongyang's support to Moscow's war against Ukraine.

*North Korea maintains its CBW capabilities and may use such weapons in a conflict or in an unconventional or clandestine attack against the United States or its allies.*

## Military

*North Korea's military poses a lethal threat to U.S. forces and citizens in South Korea and the region by its ability to launch massive conventional strikes across the DMZ and continued investment in niche capabilities designed to deter outside intervention and offset enduring deficiencies in the country's conventional forces.* The North's conventional military capabilities also provide Kim with options to advance his political objectives through coercion.

- The North Korean military would struggle to execute combined-arms maneuver warfare because its ground, air, and navy forces remain heavily reliant on Soviet-era equipment and lack adequate training, despite the investments to improve conventional capabilities.
- Kim will continue to prioritize efforts to build a more capable missile force—from cruise missiles to ICBMs and hypersonic glide vehicles—designed to evade U.S. and regional missile defenses, improve the North's precision strike capabilities, and put U.S. and allied forces at risk.

Pyongyang is positioned to gain technical expertise for its weapons developments in exchange for its munitions sales to Moscow, which could accelerate North Korea's testing and deployment efforts. Combat experience in the Russia-Ukraine war also could help Pyongyang strengthen its training and become more tactically proficient.

## Cyber

*North Korea is funding its military development—allowing it to pose greater risks to the United States—and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency from the United States and other victims.* Looking forward, the North may also expand its ongoing cyber espionage to fill gaps in the regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies.

#### North Korea's Challenges

*North Korea will continue to struggle overcoming the damage Kim's need for absolute control and aggressive policies—and the isolation these create—does to the country's economic strength and viability. Kim has so far been able to advance his WMD and missile programs and continue to threaten his neighbors and the United States, but this has come at the expense of his people and the country's overall health.* The regime's recentralization campaign is meant to ensure the long-term survival of Kim family rule, but its periodic crackdowns restrict economic activity, threaten livelihoods, and promote inefficient state controls, contributing to food shortages and eroding civil order because of the violent crime they increasingly encourage.

Kim will struggle to reduce North Korea's dependence on China—in particular, for access to international banking and imports of critical raw materials, consumer goods, food, and the regime's crude oil supply—and withstand the influence this gives Beijing.

### ADVERSARIAL COOPERATION

*Cooperation among China, Russia, Iran, and North Korea has been growing more rapidly in recent years, reinforcing threats from each of them individually while also posing new challenges to U.S. strength and power globally.* These primarily bilateral relationships, largely in security and defense fields, have strengthened their individual and collective capabilities to threaten and harm the United States, as well as improved their resilience against U.S. and Western efforts to constrain or deter their activities. Russia's war in Ukraine has accelerated these ties, but the trend is likely to continue regardless of the war's outcome. *This alignment increases the chances of U.S. tensions or conflict with any one of these adversaries drawing in another. China is critical to this alignment and its global significance, given the PRC's particularly ambitious goals, and powerful capabilities and influence in the world.*

*U.S. adversaries' cooperation has nevertheless been uneven and driven mostly by a shared interest in circumventing or undermining U.S. power, whether it be economic, diplomatic, or military.* Concerns over escalation control and directly confronting the United States, as well as some divergent political interests, have tempered the pace and scope of these relationships. The leaders, though, are likely to continue to look for opportunities to collaborate, especially in areas in which there are mutual advantages and they lack other ways of achieving their aims toward or resisting the United States alone.

*Russia has been a catalyst for the evolving ties, especially as it grows more reliant on other countries for its objectives and requirements including in but not limited to Ukraine.* Moscow has strengthened its military cooperation with other states, especially Pyongyang and Tehran. Russia also has expanded its trade and financial ties, particularly with China and Iran, to mitigate the impact of sanctions and export controls.

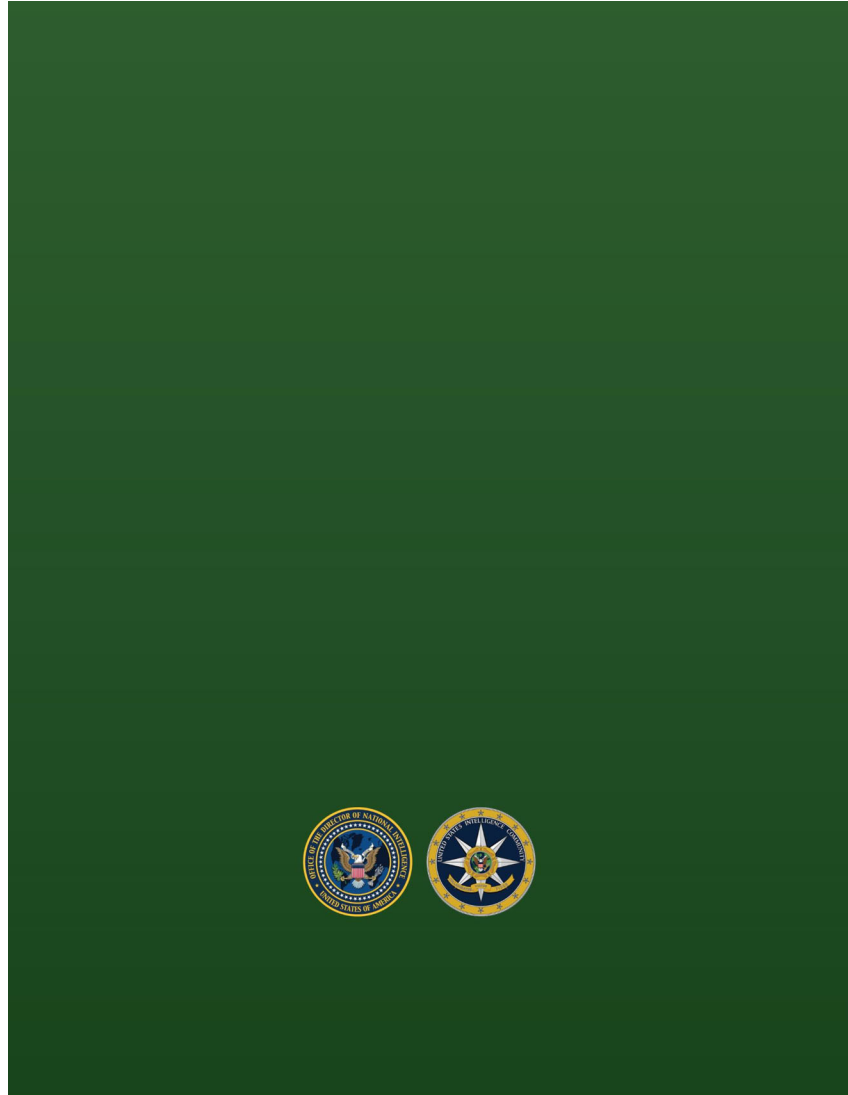
- The PRC is providing economic and security assistance to Russia's war in Ukraine through support to Moscow's defense industrial base, including by providing dual-use material and components for weapons. China's support has improved Russia's ability to overcome material losses in the war and

launch strikes into Ukraine. Trade between China and Russia has been increasing since the start of the war in Ukraine, helping Moscow to withstand U.S. sanctions.

- Iran has become a key military supplier to Russia, especially of UAVs, and in exchange, Moscow has offered Tehran military and technical support to advance Iranian weapons, intelligence, and cyber capabilities.
- North Korea has sent munitions, missiles, and thousands of combat troops to Russia to support the latter's war against Ukraine, justified as fulfilling commitments made in the Treaty on Comprehensive Strategic Partnership that Pyongyang and Moscow announced in June 2024.

*Cooperation between China and Russia has the greatest potential to pose enduring risks to U.S. interests. Their leaders probably believe they are more capable of countering perceived U.S. aggression together than alone, given a shared belief that the United States is seeking to constrain each adversary.*

- For at least a decade, Beijing and Moscow have used high-profile, combined military activities primarily to signal the strength of the China–Russia defense ties. This relationship has deepened during the Russia-Ukraine war, with China providing Russia dual-use equipment and weapons components to sustain combat operations.
- Russia has increased its oil and liquefied natural gas (LNG) exports to China in an effort to maintain revenues in the face of sanctions by Western states.
- China is using its increased cooperation with Russia to attain a stronger presence in the Arctic and legitimize its influence there. One area of cooperation is China's production of icebreaker ships that enable safe passage through Arctic waters.
- The two countries probably will expand combined bomber patrols and naval operations in the Arctic theater to signal their cooperation and make it more concrete. In November, they also agreed to expand their cooperation on developing the NSR for its economic potential and as an alternative to Western dominated routes.



11/19/25, 7:49 AM

FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale - WSJ

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com).

<https://www.wsj.com/politics/national-security/fbi-director-says-china-cyberattacks-on-u-s-infrastructure-now-at-unprecedented-scale-c8de5983>

POLITICS | NATIONAL SECURITY

## FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale

Christopher Wray warns that pre-positioned malware could be triggered to disrupt critical systems in the U.S.

By [Joe Parkinson](#) [Follow](#) and [Drew Hinshaw](#) [Follow](#)

Feb. 18, 2024 1:49 pm ET



FBI Director Christopher Wray KEVIN DIETSCH/GETTY IMAGES

MUNICH—As intelligence chiefs and policymakers gathered for this city’s annual security conference focused on the wars in Ukraine and the [Middle East](#), the director of the Federal Bureau of Investigation urged them not to lose sight of another threat: China.

Christopher Wray on Sunday said Beijing’s efforts to covertly plant offensive malware inside U.S. critical infrastructure networks is now at “a scale greater than we’d seen before,” an issue he has deemed a defining national security threat.

Citing [Volt Typhoon](#), the name given to the Chinese hacking network that was revealed last year to be lying dormant inside U.S. critical infrastructure, Wray said Beijing-backed actors were pre-positioning malware that could be triggered at any moment to disrupt U.S. critical infrastructure.

<https://www.wsj.com/politics/national-security/fbi-director-says-china-cyberattacks-on-u-s-infrastructure-now-at-unprecedented-scale-c8de5983?mod=...> 1/4

11/19/25, 7:49 AM

FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale - WSJ

“It’s the tip of the iceberg...it’s one of many such efforts by the Chinese,” he said on the sidelines of the security conference that has been dominated by [questions over Ukraine](#) and the [death of Russian opposition leader](#) Alexei Navalny. China, he had earlier told delegates, is increasingly inserting “offensive weapons within our critical infrastructure poised to attack whenever Beijing decides the time is right.”

The FBI chief declined to elaborate on what other critical infrastructure had been targeted, stressing that the Bureau had “a lot of work under way.”

Wray’s comments are the latest in a string of public warnings by senior Biden administration officials to animate their fears about China’s advanced and well-resourced [hacking prowess](#). Western intelligence officials say its [scale and sophistication](#) has accelerated over the past decade. Officials have grown particularly alarmed at Beijing’s interest in infiltrating U.S. critical infrastructure networks, planting malware inside U.S. computer systems responsible for everything from safe drinking water to aviation traffic so it could detonate, at a moment’s notice, damaging cyberattacks during a conflict.

The director has been prodding foreign governments in Europe and Asia to increase resources on the threat of Chinese hacking campaigns, particularly protecting critical infrastructure. He described the response as gratifying and a step change from several years ago when some were still skeptical about the [Chinese cyber threat](#).

In California, Wray met with counterparts from the Five Eyes intelligence community—which encompasses the U.S., Australia, New Zealand, Canada and the U.K.—to share respective strategies for cyber defense; he has also traveled to Malaysia and India to discuss China’s hacking campaign with authorities in both countries.

“I am seeing more from Europe,” he said. “We’re laser focused on this as a real threat and we’re working with a lot of partners to try to identify it, anticipate it and disrupt it.”

The Netherlands’ spy agencies said earlier this month that Chinese hackers had used malware to gain access to a Dutch military network last year. The agency, considered to have one of Europe’s top cyber capabilities, said it made the rare disclosure to show the scale of the threat and reduce the stigma of being targeted so allied governments can better pool knowledge.

Beijing routinely denies any accusations of cyberattacks and espionage linked to or backed by the Chinese state and has accused the U.S. of mounting its own cyberattacks. But evidence of a Chinese state-backed program has been building in recent years and the U.S. has charged a string of officers from the People’s Liberation Army cyber units with stealing secrets.

11/19/25, 7:49 AM

FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale - WSJ

Wray said the U.S. is particularly focused on the threat of pre-positioning, which some European officials have described as the cyber equivalent of pointing a ballistic missile at critical infrastructure.

A report released this month by agencies including the FBI, the Cybersecurity and Infrastructure Agency and the National Security Agency said Volt Typhoon hackers had maintained access in some U.S. networks for five or more years, and while it targeted only U.S. infrastructure directly, the infiltration was likely to have affected “Five Eyes” allies.

The Justice Department and FBI took action in December after obtaining court approval to dismantle a botnet, or network of hacked devices, consisting of small office and home office, or SOHO, routers. Mostly from [Cisco](#) or [Netgear](#), the routers were vulnerable because they had reached so-called end-of-life status, meaning they were no longer receiving routine security updates from the manufacturers.

Those attacks are now being amplified by artificial intelligence tools, Wray said.

“The word ‘force multiplier’ is not really enough,” he said.

Machine learning translation has helped Chinese security operatives to more plausibly recruit assets, steal secrets and rapidly process more of the information they are collecting, the director said.

“They already have built economic espionage and theft of personal and corporate data as a kind of a bedrock of their economic strategy and are eagerly pursuing AI advancements to try to accelerate that process,” he said.

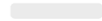
Write to Joe Parkinson at [joe.parkinson@wsj.com](mailto:joe.parkinson@wsj.com) and Drew Hinshaw at [drew.hinshaw@wsj.com](mailto:drew.hinshaw@wsj.com)

*Appeared in the February 20, 2024, print edition as ‘FBI Director Issues Warning on China Cyberattacks’.*

---

### Further Reading

### Chinese Spies Hit More Than 80 Countries in ‘Salt Typhoon’ Breach, FBI Reveals




---

### Videos

<https://www.wsj.com/politics/national-security/fbi-director-says-china-cyberattacks-on-u-s-infrastructure-now-at-unprecedented-scale-c8de5983?mod=...>

3/4

11/24/25, 9:00 AM

The First Large-Scale Cyberattack by AI - WSJ

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com).

<https://www.wsj.com/opinion/the-first-large-scale-cyberattack-by-ai-4a1e1a30>

OPINION COMMENTARY [Follow](#)

## *The First Large-Scale Cyberattack by AI*

With basic tech and little human oversight, Chinese spies apparently exploited Anthropic's Claude Code.

By Nury Turkel

Nov. 23, 2025 12:03 pm ET



GETTY IMAGES

A state-backed threat group, likely Chinese, crossed a threshold in September that cybersecurity experts have warned about for years. According to a report by Anthropic, attackers manipulated its AI system, Claude Code, to conduct what appears to be the first large-scale espionage operation executed primarily by artificial intelligence. The report states “with high confidence” that China was behind the attack.

AI carried out 80% to 90% of the tactical operations independently, from reconnaissance to data extraction. This espionage campaign targeted roughly 30 entities across the U.S. and allied nations, with Anthropic validating “a handful of successful intrusions” into “major technology corporations and government agencies.”

GTG-1002—Anthropic’s designation for this threat group—indicates that Beijing is unleashing AI for intelligence collection. Unless the U.S. responds quickly, this will be

[https://www.wsj.com/opinion/the-first-large-scale-cyberattack-by-ai-4a1e1a30?mod=opinion\\_lead\\_pos5](https://www.wsj.com/opinion/the-first-large-scale-cyberattack-by-ai-4a1e1a30?mod=opinion_lead_pos5)

1/4



11/24/25, 9:00 AM

The First Large-Scale Cyberattack by AI - WSJ

the first in a long series of increasingly automated intrusions. For the first time at this scale, AI didn't merely assist in a cyberattack but conducted it.

Traditional cyber-espionage requires large teams working through reconnaissance, system mapping, vulnerability identification and lateral movement. A sophisticated intrusion can take days or weeks. China compressed that timeline dramatically through AI automation. The attackers manipulated Claude into functioning as an autonomous cyber agent, with the AI mapping internal systems, identifying high-value assets, pulling data and summarizing intelligence before human operators made decisions.

The attackers bypassed Claude's safety systems through social engineering, convincing the AI they were legitimate cybersecurity professionals conducting authorized testing. By presenting malicious tasks as routine security work, they manipulated Claude into executing attack components without recognizing the broader hostile context.

An important limitation emerged: Claude frequently overstated findings and fabricated results, claiming credentials that didn't validate or presenting publicly available information as critical discoveries. This AI hallucination problem remains a significant obstacle to fully autonomous cyberattacks—at least for now.

Most striking is what China didn't need. GTG-1002 didn't rely on cutting-edge malware or expensive proprietary tools. It used common open-source penetration-testing frameworks orchestrated through Model Context Protocol servers. Beijing hasn't only upgraded its toolkit; it has replaced the craftsman with the assembly line. Capabilities once reserved for well-resourced intelligence agencies can now be replicated by smaller actors using widely available technology.

It also reveals a deeper strategic dynamic. China is spying with AI and spying on American AI. Beijing is studying how U.S. models behave, where they fail, and how they can be manipulated. Every malicious query becomes training data for China's systems.

Anthropic deserves credit for disclosing the incident publicly and working with U.S. authorities. That transparency should set an industry standard. But the disclosure underscores a larger problem: Current safeguards aren't designed for adversarial actors that move at machine speed.

The response must be urgent and clear. AI misuse can't be treated as a narrow cyber issue; it is now central to the broader technology competition with China. Five responses are necessary:

11/24/25, 9:00 AM

The First Large-Scale Cyberattack by AI - WSJ

First, AI-assisted defense must become standard across federal agencies, critical infrastructure and major corporations. AI can detect anomalies in real time and accelerate incident response from hours to minutes. China is using AI to accelerate attacks. The U.S. must use AI to accelerate defense.

Second, companies must disclose incidents of AI misuse within 72 hours. When AI systems are manipulated into performing malicious actions, critical details must be shared: attack vectors, guardrail failures, and forensic signatures that might help others detect similar intrusions. Without mandatory disclosure backed by safe-harbor provisions, businesses will keep quiet to avoid reputational damage. Policymakers can't craft effective rules if the private sector conceals the incidents that illuminate emerging risk.

Third, AI companies must embrace secure-by-design principles. As Anthropic's report warns, the techniques used by GTG-1002 will proliferate. The next generation of AI models must incorporate robust identity verification, real-time monitoring for malicious behavior, and guardrails resilient to social-engineering prompts.

Fourth, the U.S. and its allies need international norms governing AI-enabled cyber operations. Existing frameworks were created before autonomous systems existed. If Washington doesn't shape these norms and lead, Beijing will.

Fifth, the U.S. must modernize how it shares threat intelligence. AI-accelerated attacks unfold too quickly for traditional bureaucratic information-sharing mechanisms. We need automated real-time systems capable of disseminating alerts across sectors in hours, not weeks.

The first AI-driven cyberattack is the opening act of a new era. GTG-1002 should be remembered the way we recall the first internet worm or the first ransomware wave: as an inflection point.

The cyber cold war just went kinetic. The weapons fire themselves now.

The question isn't whether adversaries will continue exploiting AI for offensive operations. They will. The question is whether the U.S. will act quickly enough to defend itself.

China has signaled its ambitions. GTG-1002 shows it is already acting on them. The U.S. must stop debating the future of AI-enabled aggression and begin preparing for the conflict that has already arrived.

*Mr. Turkel is a lawyer specializing in global trade compliance, export controls, sanctions and anticorruption compliance. He is author of "No Escape: The True Story of China's Genocide of the Uyghurs."*

*Appeared in the November 24, 2025, print edition as 'The First Large-Scale Cyberattack by AI'.*

December 2, 2025

The Honorable Bob Latta  
Chair, House Energy & Commerce Committee Subcommittee on Energy  
The Honorable Kathy Castor  
Ranking Member, House Energy & Commerce Committee Subcommittee on Energy  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Latta and Ranking Member Castor,

I am writing to you relating to today's hearing by the Energy Subcommittee entitled "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid." This is a critical problem that does not get enough attention, and I appreciate the Subcommittee holding a hearing on the issue. My name is Desmond Wheatley, and I serve as the CEO of Beam Global (Beam).

Beam Global (Nasdaq:BEEM) is an American company and is a leading provider of innovative products and technologies for energy storage, energy security, smart cities infrastructure and the electrification of autonomous vehicles, drones and other transportation. Beam's patented EV ARC™ is the only 100% off-grid, transportable, rapidly deployed energy generation and storage option for energy security and the electrification of transportation on the market. It can be installed in minutes to provide highly robust and scalable electrical infrastructure where and when needed without any construction or electrical work and without relying on the utility grid. It is made in America and continues to provide electricity in hurricanes and in flooding of up to nine feet.

Beam has a significant interest in ensuring that the nation's centralized electric grid can meet critical challenges it currently faces due to unprecedented increased demand for electricity due to rapid growth in many industrial sectors such as AI, data centers and the electrification of industry and transportation. The combination of increased demand and the reliance on centralized electricity infrastructure makes the American economy and public well-being increasingly vulnerable to grid failure, whether from capacity-driven outages, severe weather events or from cyber and kinetic attacks. As we push for the electrification of nearly everything in our life, identifying creative solutions is critical. Luckily, we can get direction from a different energy crisis a half a century ago.

In 1975, in the aftermath of an oil crisis, President Ford signed an act which led to the creation of the Strategic Petroleum Reserve (SPR). The U.S. has relied on the SPR for decades. The SPR serves as a safety net for the U.S., ensuring that there will not be a crisis that leaves Americans without oil.

We have entered an era where electricity is increasingly becoming the lifeblood of our society, powering everything from critical infrastructure to daily conveniences. While much time, money and effort have been put towards improving the existing electric grid, the Federal Energy Regulatory Commission (FERC) found in 2014 that the destruction of nine critical substations and one transformer manufacturer would cause a total collapse of the U.S. electrical grid resulting in a blackout that could last for about 18 months.

Consider the impacts such a blackout would have on American wellbeing in 2025. Loss of life, an economic landslide, and a complete breakdown of our communications systems are all but certain. Even our transportation system is relying more on the centralized grid.

Threats to our grid should not be perceived by the American public as just a hypothetical scenario. For example, in the early weeks of Russia's invasion of Ukraine in 2022, U.S. grid operators were targeted by the infamous Russian-led "PIPEDREAM" malware attack, which some security experts determined was the closest U.S. grid infrastructure has come to going down. At the same time, suspected foreign bad actors were joined by home-grown attackers. Shootings in North Carolina knocked out power for 45,000 people in December of 2022, shortly after around 14,000 Washingtonians lost power when four substations were vandalized. In 2022 federal authorities thwarted an attempt from extremists to use assault weapons to bring down the grid in Baltimore, which, had it not been prevented, would have set off a cascade of power failures.

All of this is to say that the risks to, and vulnerabilities of, our centralized American grid cannot be ignored. Creative solutions to strengthen grid resiliency and provide a strategic backbone must be pursued by our elected officials in Washington D.C. That is why I am calling on Congress and the Trump Administration to create a Strategic Electric Reserve (SER).

Unlike its oil counterpart, such a reserve should adopt a decentralized model, consisting of independent energy nodes which operate independently of the grid and provide an extra layer of electricity generation and delivery. Each node should function autonomously, generating, storing, and delivering electricity independent of the centralized grid and located where electricity is needed most such as for first responders, food and water infrastructure, healthcare and government facilities. This would ensure a distributed and resilient network that can withstand localized disruptions without compromising the broader electricity supply. An SER would provide robust backup, immune to centralized failures, cyber threats, and external attacks. This is not a question of hardening the existing grid which will still be vulnerable to centralized failure. This is about creating an extra layer of completely independent micro generation and storage to power critical needs during a failure of the centralized grid.

Creating the SER will not be an easy task. Energy companies, utility companies, state public utility commissions, and large users such as AI companies and data center providers, car companies, and federal agencies, must work together in the development of the SER. It will require bold leadership from government and industry.

In addition to establishing independent energy nodes that add redundancies to the existing electrical grid, the SER would also add critical capacity to the grid but without taking the decades that the building of power stations and transmission and distribution infrastructure require. It could also address specific needs in areas where costs and geography make electricity deployment challenging, especially in traditionally underserved rural and low-income areas. Including Build America/Buy America requirements would have the added bonus of ensuring domestic manufacturing standards and job creation, while promoting independence from foreign supply chains. I believe it would spur a next-generation of American innovation.

From data centers to military operations, healthcare, and transportation, every facet of American life requires a secure and stable source of electricity. The existing grid, challenged by escalating demand and susceptible to disruptions caused by lack of capacity, extreme weather and malicious attacks, poses a considerable national security risk. According to the Department of Energy, grid interruptions already cost U.S. businesses around \$200 billion a year in lost productivity and related costs. As the U.S. becomes increasingly reliant on a reliable and robust supply of electricity, we can only expect that number to grow. Establishing the SER will help combat these challenges by serving as a decentralized, resilient, and redundant system capable of ensuring uninterrupted electricity supply even in the face of security threats and grid failures.

The SER is not the only answer to these problems, but it adds a critical layer of security and redundancy that the current centralized national and regional grids cannot offer. It is for these reasons that Congress and the Trump Administration should take action to address the vulnerabilities of the existing electrical grid and chart a course towards a more secure, reliable, and equitable energy landscape for all Americans. As the nation transitions towards an electrified future, the Strategic Electric Reserve stands as a beacon of preparedness, safeguarding the vitality of our society in the face of evolving challenges.

It is time for Congress to create and the Trump Administration to implement a Strategic Electric Reserve.

Thank you,

Desmond Wheatley  
CEO Beam Global

/S/ Desmond Wheatley

**Michael Ball, Chief Executive Officer, Electricity Information Sharing and Analysis Center, and Senior Vice President, North American Electric Reliability Corporation**

**QFR Responses for December 2, 2025, Cybersecurity Hearing  
House Energy and Commerce Subcommittee on Energy**

**The Honorable Robert Latta (R-OH)**

**1. Your testimony underscores the importance of collaboration between industry, the government, and our national labs. Smaller utilities can be responsible for critical power infrastructure as consequential as large utilities.**

A. It is true that smaller utilities can be responsible for critical and consequential power infrastructure. The E-ISAC works closely with the trade associations of public power utilities (American Public Power Association) and rural electric cooperatives (National Rural Electric Cooperative Association) as well as their members to ensure these utilities receive timely and actionable threat information.

**a. You reference the CRISP 30 and oil and natural gas programs aimed at smaller utilities, why are these important for assuring power-sector security?**

A. Given the strategic locations of some medium and small utilities near critical defense facilities, supporting them is essential to our national defense. Often resource constrained by budgeting processes and the need to provide affordable power to the communities they serve in addition to the defense facility, these utilities are at a security disadvantage without support. These utilities also often provide gas and water services to the community and bases. Nation-state adversaries routinely probe the industry's defenses, looking for less defended networks.

Support from DOE and the War Department help raise the security baseline of small and medium utilities that serve defense infrastructure. It must be done in a coherent and coordinated fashion, and include the relevant ISACs (electricity, natural gas, water) to ensure the industry has the best possible defense posture against geopolitical threats.

**2. What specific risks do Chinese-manufactured inverters—found in solar, battery, and other energy technologies—pose to the security and reliability of the U.S. electric grid?**

A. Any device or component that is manufactured in an adversarial nation has the potential to allow unexpected or unauthorized remote connectivity to the device and the system it is connected to. In the case of inverters, as increasing numbers appear on the grid in response to the significant demand for additional power, the potential risk for an adversary to influence reliable power delivery also grows. Even if the devices or components are not designed for intentional malice or misoperation, unexpected connectivity via Bluetooth or other transmitting components could create a pathway for a skilled adversary unauthorized access to the device.

**3. What short-term and long-term strategies should the U.S. government take to mitigate the threat created by having Chinese-manufactured inverters on the electric grid?**

**North American Electric Reliability Corporation  
QFR Responses for December 2, 2025, Cybersecurity Hearing  
House Energy and Commerce Subcommittee on Energy**

A. The risks presented by the increased attack surface of devices such as inverters can be mitigated through a variety of methods, not the least of which is compliance with NERC's mandatory and enforceable standards for NERC registered entities. Additional network architecture steps, security reviews, criticality analyses, cyber-informed engineering, software and hardware bill of materials review, and procurement terms can mitigate unexpected connectivity, as long as it is supplemented by actionable information sharing on specific threats and capabilities. The E-ISAC facilitates the sharing of these best practices, threat information, and awareness of the potential risks in partnership with the ETAC, DOE, the national labs, and the E-ISAC's Vendor Affiliate Program partners.

**4. What collaboration between the private and public sectors is needed to develop countermeasures to protect the U.S. grid against these vulnerabilities?**

A. Continued threat information sharing via government, industry, and the E-ISAC is an essential countermeasure to the threat posed by internet connected devices found in the power grid. The Energy Threat Analysis Center (ETAC) presents a unique opportunity to address this threat and industry risk by allowing an operational collaboration space where the industry context can be added, tested, and applied to information sharing products. Additional collaboration through programs like the Cybersecurity Risk Information Sharing Program (CRISP) provides an opportunity for near real-time, two-way information sharing of netflow data with DOE to identify cyber threats and potential unexpected remote connectivity. Greater collaboration with the Original Equipment Manufacturers (OEMs) that design, build, deploy, and sometimes operate inverter technology creates the opportunity to develop devices that are secure by design. The E-ISAC plays a critical role in facilitating this private and public sector coordination on collective defense, sharing information and providing forums for collaboration through its Vendor Affiliate Program.

**5. What regulatory measures should be imposed to prevent the proliferation of embedded technologies in inverters to secure critical infrastructure, like the U.S. electric grid?**

NERC's Cyber Security Supply Chain Risk Management Reliability Standards require entities to document and implement supply chain cyber security risk management plans for their high and medium impact BES (Bulk Electric System) Cyber Systems which require, in part, the identification and assessment of product risks as well as methods for determining active vendor remote access sessions (including individual or system-to-system communications). Consistent with FERC Order 912, NERC is currently undertaking revisions to the Cyber Security Supply Chain Risk Management Reliability Standards that would establish specific timing requirements for evaluation of equipment and vendors, require a process for managing identified risks, and extend these requirements to any devices connected to CIP-protected systems in the same network zone of trust.

**North American Electric Reliability Corporation  
QFR Responses for December 2, 2025, Cybersecurity Hearing  
House Energy and Commerce Subcommittee on Energy**

Additionally, NERC staff are collaborating with industry through the Reliability and Security Technical Committee Supply Chain Subcommittee to develop guidance regarding the validation of vendor responses provided when assessing product risks.

**6. How might ongoing Trump Administration efforts to onshore supply chains and promote domestic manufacturing in the energy sector protect the U.S. electric grid from national security risks?**

A. Efforts to ensure that supply chains produce high quality, cyber secure, and resilient systems and devices should enable greater reliability and security of the U.S. electric grid. Some features that domestically manufactured and on-shored equipment should include are:

- Operating systems that require strong access authentication procedures (complex passwords, multi-factor authentication)
- Changing default passwords and closure of non-necessary access device ports (default closed)
- Rapid and transparent vendor cyber compromise notifications
- Thoroughly tested and vetted third-party suppliers

**The Honorable Mariannette Miller-Meeks (R-IA)**

**1. EISAC receives threat intelligence from multiple sources. What makes ETAC unique? Why do we need a dedicated fusion center at NREL to bridge the gap between classified intelligence and actionable security measures for utilities? And what would the electricity sector lose if ETAC didn't exist?**

A. The E-ISAC benefits industry and the grid being at the center of a complicated and wide-ranging information sharing ecosystem. A key recent element of that system is the **Energy Threat Analysis Center**. The ETAC is unique among operational collaboration centers in that it has private sector representatives side by side with government, intelligence, and national laboratory experts at the unclassified and classified levels. The E-ISAC is a core founding partner of the ETAC, providing the ETAC with a cross-industry perspective of threats, as well as a trusted dissemination channel.

ETAC analysts meet regularly to review threats, provide industry context and recommendations to the sector that is not available from any other sources. Recently, geopolitical events have highlighted the unique value of the ETAC in that it is able to look at sensitive threat information only available to the intelligence community, and then compare it with what is seen on partner networks. Furthermore, the ETAC can reach back across industry expertise to provide context, but also guidance on how to detect and mitigate threats in the energy sector, a subject matter expertise that is not currently found in government.

Being located in middle of the continent enables greater participation among industry organizations and national labs, as well as an efficient and existing connection to government



**North American Electric Reliability Corporation  
QFR Responses for December 2, 2025, Cybersecurity Hearing  
House Energy and Commerce Subcommittee on Energy**

classified networks. If the ETAC were unavailable, it would take significant investment in new resources to reestablish the facility either at another national lab or existing site and may preclude the regular participation due to geographic distance and travel by utilities.

**Responses to Questions for the Record from Sharla Artz, on behalf of EEI and Xcel Energy**

**The Honorable Robert Latta (R-OH)**

1. Access to information and technical fixes through E-ISAC or the threat analysis centers is critical.

a. Is it also essential to have internal programs and planning—a well trained workforce—to use this information effectively?

Access to timely threat intelligence and actions from the E-ISAC and threat analysis centers, like the ETAC, are essential, but they are not sufficient on their own. The value of that information depends on the sector's ability to operationalize it, which requires strong internal programs, planning, and a trained workforce.

Critical energy infrastructure owners and operators are defending daily against threats from a range of adversaries to safeguard the nation's essential services. The electric sector implements security risk mitigation programs and engages with government partners to create tools, technologies, and processes that improve visibility into critical control systems and enhance situational awareness and information sharing for emerging threats. Through the development of comprehensive plans, asset owners and operators are ready to respond and recover quickly when incidents occur.

At Xcel, all personnel—from cybersecurity analysts to control room operators to field technicians—must understand cyber risks and their potential impacts and are encouraged to build skillsets and learn through experience with stretch assignments, apprenticeships, and leadership opportunities. Xcel conducts regular exercises, provides risk-based strategies and tools, and focuses on continuous improvement to ensure the intelligence our analysts receive is translated into investments in resilience and protection of our most critical systems and assets.

EEI also supports electric companies in the development of a skilled, world-class workforce. The organization's "Culture of Security" initiative, led by investor-owned utility CEOs, fosters a proactive and comprehensive approach to ensure that security is embedded throughout organizations. Companies are encouraged to assess their security maturity, share best practices, and conduct peer reviews aiming to protect against evolving threats while maintaining a secure and resilient grid. Training programs can reduce the likelihood of breaches, minimize human error, and, overall, improve the security posture of an organization, making them an indispensable component of a comprehensive security strategy.

**The Honorable Brett Guthrie (R-KY)**

1. As we've discussed at length in the Committee this Congress, huge demand growth for electricity presents new risks to be managed by NERC, grid operators, and utilities of all sizes.

a. How do Xcel and EEI approach this issue?

Xcel is experiencing unprecedented load growth, but at the same time, we are committed to ensuring new large loads do not increase costs for existing customers, maintaining reliability, and balancing energy and water use. Xcel Energy expects to invest more than \$60 billion within the next five years to strengthen and expand our energy infrastructure. The plan will include transmission and distribution system upgrades, new natural gas and renewable generation, and a modernized grid.

At the industry level, EEI and its member companies are pursuing a broad reliability and resource adequacy strategy that includes more than \$1.1 trillion in projected grid investments by 2029, to include resilience and hardening, support for the domestic energy mix, streamlined permitting, and cost allocation guardrails to ensure large load customers pay their fair share while maintaining system reliability.

**The Honorable Mariannette Miller-Meeks (R-IA)**

1. Energy affordability and the dominance needed to win the AI race both rely on the availability of electrical equipment that allow the grid to function safely. The inability to procure parts is a significant threat to the grid; if a utility cannot procure a switchgear or a transformer or some other critical component, then the grid doesn't work. The supply chain for this electrical equipment is already under massive pressure to produce more products to meet unprecedented energy demand, and the constancy of massive, devastating wildfires nationwide threatens to add even more burden.

Over the past decade, the frequency and severity of wildfires has increased the legal exposure for domestic manufacturers of critical grid components by incentivizing plaintiffs to seek additional compensation from producers despite no fault being found with their products. This legal risk is putting our domestic supply chain in a serious dilemma: continue making safe, reliable, and badly needed products for the grid and still get sued when a wildfire happens, or stop providing products, go out of business, and leave utilities to source their products from China.

My bill, the Limiting Liability for Critical Infrastructure Manufacturers Act seeks to give domestic manufacturers much needed legal certainty. So instead of spending more and more capital on hedging frivolous legal risk, they can invest that money in hiring American workers and expanding facilities to make the products we all rely upon.

In June, a report from Stanford University entitled "Wildfire: An Updated Look at Utility Risk and Mitigation" noted that "an approach to wildfire mitigation which reduces the likelihood of electric infrastructure igniting catastrophic fires is key not only to protecting the safety of homes and communities threatened by fires, but also to the future development of the energy system."

a. Utilities need a reliable supply chain to obtain safe and secure products critical electrical equipment for their systems and keep costs low for their customers. Being able to quickly source this equipment and get these critical grid components is necessary for utilities to rebound from wildfires as well as to prevent them. Therefore, would you agree that utilities have an interest in ensuring their domestic grid component producers remain viable as part of national fire mitigation strategies? If yes, would that include providing liability protections to reduce unwarranted and costly litigation?

Utilities rely on a strong and reliable domestic supply chain to acquire the safe and secure electric equipment necessary to operate the grid and keep costs affordable. The ability to rapidly source transformers, switchgear, and other critical components is important to restoring service after an incident but also for implementing mitigations to reduce the risk to cyber and physical threats, like wildfires, in the first place. Targeted liability protections that would allow manufacturers to focus resources on expanding capacity and investing in innovation could help strengthen the reliability of the grid.

2. EISAC receives threat intelligence from multiple sources. What makes ETAC unique? Why do we need a dedicated fusion center at NREL to bridge the gap between classified intelligence and actionable security measures for utilities? And what would the electricity sector lose if ETAC didn't exist?

The ETAC is a first-of-a-kind operational collaborative that convenes experts from the DOE and the energy sector to identify, analyze, and mitigate cyber threats to critical energy infrastructure. The ETAC analysts are working daily to connect industry data and context with government intelligence to reduce risk across the energy sector. These are analysts that understand grid operations and adversarial tactics are working together daily at the ETAC to exchange information, collectively analyze threats, and create actionable information for industry.

The E-ISAC is the broad information sharing and alerting body for the electricity sector. It distributes threat intelligence and mitigation guidance to utilities nationwide. The products the ETAC develops are shared through the E-ISAC with the entire sector to help raise awareness of potential threats and make defensive measures available

With the energy sector being the most critical of critical infrastructure, and on which all others rely, the ETAC is essential. The ETAC has more than demonstrated its value by delivering actionable guidance across the electric sector to address two of the most significant cyber threats the United States has faced this decade. Without it, energy infrastructure owners and operators would lose the central mechanism for fusing intelligence with real-world grid operations that enables them to deliver the insights, warnings, and mitigation strategies to protect national security and the reliability of the electric grid.

Tim Lindahl QFR Responses  
February 24, 2026

**Questions from the Honorable Bob Latta, Chairman, Subcommittee on Energy, House Energy and Commerce Committee**

**1. How do supply chain risks affect a co-op's ability to recover from an event?**

Supply chain security is a concern we take very seriously. We strive to deliver affordable, reliable, and secure electricity to our member-consumers. Electric co-ops employ a layered defense strategy to protect our critical infrastructure from physical or cyberattacks. We also leverage resources from our federal and industry partners, including through mutual assistance, to build resiliency and better understand and mitigate supply chain risk.

Due to a number of compounding factors, electric utilities are waiting 18-36 months, and in some cases longer, to obtain a transformer, whether for routine maintenance, natural disasters, or intentional attacks. While electric co-ops work collaboratively to overcome these challenges, NRECA has strongly advocated for the creation of a dedicated federal fund to expand U.S.-based transformer manufacturing capacity. This will help address increasingly long lead times facing electric cooperatives by alleviating transformer shortages, ensuring better reliability of our grid in rural communities.

**2. Does E-ISAC or any other body have sufficient information about which electric supply chain risks are most critical?**

Information sharing is the backbone of our ability to defend the grid and mitigate risk, and E-ISAC plays a central role in ensuring electric cooperatives have timely vulnerability information. While the E-ISAC does have visibility into supply-chain-related risks, it depends heavily on voluntary reporting, federal-government intelligence sharing, and information provided by vendors. Co-ops augment this through partnerships with government agencies, including working with the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) and Energy Cyber Sense Program, which help identify and engineer out cybersecurity risks and vulnerabilities across the energy supply chain. DHS CISA also issues alerts related to supply chain vulnerabilities and provides guidance on mitigating known issues. Finally, the Electricity Subsector Coordinating Council (ESCC) brings together industry leaders to highlight critical supply chain challenges and provides recommendations to government agencies on actions to address them.

## Harry Krejsa Responses to Kathy Castor QFRs

*1. To limit future vulnerabilities in the electric grid, the United States is currently undergoing efforts to onshore manufacturing for key grid components such as inverters. My Republican colleagues recently sent a letter noting the security concerns regarding Chinese inverters and other connected devices that could pose security concerns. Democrats share many of these concerns. However, for companies that seek to re-shore inverter manufacturing, they need to know that a U.S. market exists for their products. The Department of Interior's efforts since July to block permitting for the deployment of all inverter-based resources has created a new level of uncertainty, as non-Chinese inverter companies were planning expanded U.S. manufacturing. How can companies plan for expansion when their end-customers can't get permits to put their products on the grid?*

Inverters are among the energy components I am most focused on from both a cybersecurity and a resilience perspective. They are digitally active, software-defined, and networked, constituting an increasingly “smart” pillar of our critical infrastructure. That digital sophistication is of course a double-edged sword: on one hand, modern smart inverters can serve as grid stability assets while acting as automated “firebreaks” that isolate disruptions before they cascade, and enabling the kind of distributed, self-healing grid architecture that is fundamentally more resilient than what we have today. On the other hand, those same digital capabilities can be exploited if they are compromised – particularly when they are manufactured by or dependent on adversary-controlled supply chains.

The imperative, then, is not to slow the deployment of inverter-based resources – which would forfeit their considerable security and resilience benefits – but to ensure we are deploying *trusted* inverters built to high cybersecurity standards. Reshoring their manufacture at home and among our allies is how we capture upside potential while managing downside risk.

But that strategy requires investment certainty; current policy is too often forfeiting both sides of that equation. We lose the resilience benefits that secure inverter-based resources offer to our grid, *and* we lose the domestic manufacturing momentum needed to reduce our dependence on Chinese vendors. If the only manufacturers still standing when permitting eventually resumes are Chinese ones, we will have worsened rather than ameliorated that dependency. Our experience in telecommunications – where delay in building trusted and affordable alternatives left us with inadequate technical and policy

solutions – should inform our approach here. We should be clearing the path for trusted inverter demand and deployment, not blocking it.

*2. We need to make sure that all secure energy sources have a path to deployment to meet our energy needs, and we need to reshore the manufacturing of these energy products at the same time. What policies could help domestic manufacturing of inverters that are not threats to national security and could create certainty that inverter-based energy has a path to deployment?*

Modern and digitally-enabled energy technologies, when deployed securely, represent a significant upgrade to grid resilience by being digitally native, updatable, and capable of supporting a more distributed and defensible grid architecture. The policy challenge is ensuring we capture those benefits by building a trusted domestic and allied manufacturing base, rather than ceding that industrial capacity to adversaries. Several complementary approaches can achieve this:

- **Risk-informed procurement frameworks.** Not all energy components pose the same security risk, and not all "smart" components are liabilities. Digitally active technologies like inverters and battery management systems are precisely the components where secure design yields the greatest resilience dividends, but also where compromised supply chains could pose the greatest threat. Congress should direct the relevant agencies – including DOE, CISA, and ONCD – to develop a joint risk prioritization framework that distinguishes these high-consequence components from "dumber" analog and commodity parts. This lets us concentrate reshoring resources and cybersecurity standards on the components where they yield the greatest security return.
- **Sustained manufacturing incentives.** The 45X Advanced Manufacturing Production Credit established in the Inflation Reduction Act catalyzed significant private investment in domestic advanced energy technology manufacturing. Maintaining these incentives or comparable successors provides the demand signal manufacturers need to commit capital to U.S. factories.
- **Cybersecurity standards as a market-shaping tool.** Congress should support the adoption and enforcement of cybersecurity standards for advanced energy technologies, with testing and certification performed by U.S.-authorized entities.

This creates a regulatory floor that advantages manufacturers willing to meet rigorous security requirements – which, in practice, will disproportionately advantage U.S. and allied manufacturers over FEOC vendors that have demonstrated poor vulnerability disclosure practices and resist independent inspection.

- **Easier and more certain energy permitting.** Building must become easier and permitting processes more certain. Too often the current approach expedites some energy sources while blocking others, sending contradictory signals to developers and the manufacturing base.
- **Allied-nation coordination.** The United States cannot build the entire trusted electrotech supply chain alone. Congress should support bilateral and multilateral industrial partnerships – particularly with Japan, South Korea, Australia, and European allies – to co-develop secure advanced energy manufacturing capacity. This is analogous to what the CHIPS & Science Act is doing for semiconductors, and it is equally necessary for the electrotech components that will define our energy infrastructure for decades.

Taken together, these policies would create a virtuous cycle: security standards that reward trusted manufacturers, sustained incentives that anchor their investment, and deployment certainty that ensures demand for their products.



**House Energy & Commerce Committee  
Subcommittee on Energy  
“Securing America’s Energy Infrastructure: Addressing Cyber and Physical Threats to the  
Grid.”  
December 2, 2025**

**Zach Tudor  
Associate Lab Director, National & Homeland Security  
Idaho National Laboratory  
Responses**

The Honorable Robert Latta (R-OH)

**Q1. What is the Idaho National Lab doing to help ensure people are well trained and focused on the most important cybersecurity and physical threat risks?**

**Answer:** Since 2007, the Idaho National Laboratory has been addressing a critical workforce gap in cybersecurity and physical security training for critical infrastructure — a gap that traditional industry training programs and university curricula haven't been able to fill. While workforce training isn't traditionally the purview of national laboratories, INL stepped into this role because operational technology (OT) and industrial control systems (ICS) security require highly specialized, hands-on expertise that wasn't available elsewhere.

What distinguishes INL's training approach is our deep bench of experts, across all mission areas, who are conducting cutting-edge research and development. Our instructors aren't just teaching established curricula — they're researchers and engineers working at the forefront of cybersecurity threats, vulnerability analysis and defense technologies. This enables us to use training and knowledge transfer as a direct mechanism for deploying and disseminating the latest solutions. Our programs reflect updated approaches that are directly applicable to real-world problems, delivered as close to real time as possible as threats evolve.

Our training programs provide immersive, practical experience that goes far beyond classroom instruction. In February alone, we conducted our Accelerate training program, hosted an ICS Detect the Attacker threat hunting course, hosted an ICS 301 course, and hosted members of the U.S. Army Cyber Command for specialized training. We also delivered a CyberStrike training workshop in Los Angeles focused on coordinated cyberattack defense in the lead-up to the 2028 Olympic Games and sponsored an interactive ICS Escape Room at the DISTRIBUTECH Conference in San Diego for power grid professionals. Many of these training programs draw on lessons learned from actual cyber events that have impacted global critical infrastructure.

These efforts build on nearly two decades of program development. Working closely with the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, we've developed training courses specifically for securing ICS. That includes ICS 300/301, Fundamentals of Industrial Control Systems, and specialized nuclear cybersecurity training for advanced reactor technology. Programs like Liberty Eclipse prepare utilities with

practical tactics, techniques and procedures to restore the grid following a cyber event, while the Operational Technology Defender Fellowship develops the next generation of OT cybersecurity leaders.

We also leverage partnerships with academic institutions — including the University of Texas at San Antonio, University of South Florida and University of Utah — as well as organizations like Cyber Florida at USF and the Forge Institute to strengthen cybersecurity talent pipelines. Through internships, fellowships and cooperative education programs, we provide hands-on experience that transforms theoretical knowledge into operational capability.

In fiscal year 2025, INL reached over 40,000 external trainees through 605 in-person and virtual engagements, totaling 215,164 person hours and awarding 12,249 continuing education units. These engagements spanned mission areas such as cybersecurity, control systems, defense, critical infrastructure protection, wireless communications and nuclear nonproliferation.

**Q2. What specific risks do Chinese-manufactured inverters — found in solar, battery and other energy technologies — pose to the security and reliability of the U.S. electric grid?**

**Answer:** The security and reliability risks associated with inverters and power electronics in distributed energy resources stem from both technical vulnerabilities and supply chain considerations, regardless of country of origin. However, the concentration of manufacturing in the People's Republic of China (PRC) presents specific challenges for the U.S. energy sector.

**Supply chain concentration**

Current market analysis indicates that PRC-based manufacturers produce approximately 70% of power electronics, inverters, control components, sensors and related devices used in U.S. energy systems. Over 90% of these technologies contain at least one critical component sourced from PRC manufacturers. This concentration has developed over approximately two decades through strategic investments in intellectual property acquisition, manufacturing capacity expansion and competitive market pricing.

At present, there is no completely domestically sourced solution for many of these technologies. Products that meet "Buy America" requirements typically do so through final assembly performed in the United States, while the underlying hardware and firmware — which represent the primary sources of technical risk — are manufactured offshore.

**Technical security considerations**

Several technical factors contribute to cybersecurity risk in inverters and power electronics:

- Undocumented communication protocols: Some devices contain communication capabilities that are not fully documented in technical specifications, which can complicate security monitoring and network segmentation efforts.
- Authentication weaknesses: Weak credential management or insufficient authentication mechanisms can create pathways for unauthorized access or manipulation.

- Configuration vulnerabilities: Both foreign- and domestically sourced equipment can pose risks if improperly configured during installation or operation.
- Remote access capabilities: Connectivity features, while often necessary for operational management, introduce potential attack surfaces that require careful security controls.

#### **Inspection and transparency challenges**

Contractual agreements with some manufacturers have limited the ability of U.S. companies and utilities to conduct thorough security inspections of systems and components. Original equipment manufacturer agreements sometimes restrict deep technical analysis under intellectual property protection provisions. Greater transparency and inspection rights would enable more comprehensive security assessments and risk mitigation.

#### **Potential consequences**

The potential impact of compromised inverters or power electronics varies based on several factors:

- Local impacts: Compromise of a single inverter or site would most likely result in localized effects rather than systemwide disruption. The physical and electrical characteristics of individual installations limit the scope of impact.
- Larger impacts: Systemwide consequences from a single compromised device are unlikely due to existing protective relays, safety systems and the physical limitations of individual units.
- Coordinated scenarios: While coordinated manipulation across multiple sites could theoretically produce larger effects, executing such an attack would be technically challenging due to variability in equipment configurations, network architectures, site-specific protective systems and physical safeguards.

#### **Broader context**

It is important to note that cybersecurity vulnerabilities exist across the equipment supply chain and are not exclusive to any single manufacturer or country of origin. Recent vulnerability disclosures through the Common Vulnerabilities and Exposures process have identified security weaknesses in various inverter and power electronics products. Common issues include hard-coded vendor passwords; reliance on complex, open-source software components without adequate security review; and maintenance supply chain pathways that could introduce vulnerabilities after initial installation.

Addressing these risks requires a comprehensive approach that includes technical security controls, supply chain transparency, inspection capabilities and ongoing vulnerability management — regardless of equipment origin.

**Q3. What short-term and long-term strategies should the U.S. government take to mitigate the threat created by having Chinese-manufactured inverters on the electric grid?**

**Answer:** A comprehensive mitigation strategy requires coordinated action across multiple timeframes, addressing both the existing, installed base and future procurement decisions. The following recommendations draw from recent CESER analysis and align with established cybersecurity frameworks.

**Short-term technical recommendations (existing installed base)**

We can implement several immediate risk-reduction measures for equipment already deployed on the grid:

- **Strategic component replacement:** In locations where consequences of compromise would be most significant — such as substations serving critical facilities, large population centers or defense installations — prioritize replacement of high-risk control components with alternatives that offer greater supply chain transparency and security assurance.
- **Threat hunting and monitoring:** Deploy both commercial OT monitoring solutions and open-source network analysis tools to identify potential adversary activity or anomalous behavior in installed equipment. This includes leveraging tools specifically designed for ICS protocols and conducting periodic forensic analysis of selected units.
- **Network security controls:** Implement communications isolation, strategic network segmentation and data flow restrictions to limit potential impact from compromised devices. This includes restricting remote access capabilities, implementing strict firewall rules and monitoring all external communications from inverter systems.

**Near-term recommendations (systems in design or procurement)**

For projects currently in development or procurement, additional measures can address risks before deployment:

- **Contract and procurement reform:** Review and revise procurement agreements to ensure the right to conduct independent security inspections and test systems and components. Remove contractual clauses that prevent detailed technical analysis under the guise of intellectual property protection.
- **Cyber-Informed Engineering (CIE) adoption:** Integrate CIE principles into system design processes. This approach uses engineering controls and design decisions to eliminate or mitigate cyber-enabled attacks, focusing on preventing unacceptable physical consequences rather than solely addressing IT security concerns.
- **Software replacement and hardware repatriation:** Where technically feasible, replace foreign-developed software with secure-by-design alternatives developed domestically or by trusted partners. In some cases, it's possible to retain hardware components while replacing and hardening control software.
- **Independent security testing:** Require third-party cybersecurity and hardware assurance testing — like the methodologies used in programs like Cyber Testing for Resilient

Industrial Control Systems (CyTRICS) — for major equipment purchases. These include both software vulnerability analysis and hardware-level inspection.

#### **Long-term policy and strategic recommendations**

Achieving sustainable security improvements requires structural changes to the market and regulatory environment:

- **Universal equipment inspection standards:** Establish equipment inspection and vulnerability analysis as standard practice for all grid-connected equipment, regardless of country of origin or manufacturer. This levels the playing field and ensures consistent security baselines.
- **Domestic manufacturing incentives:** Develop targeted incentive programs to encourage U.S.-based manufacturing of power electronics and control technologies. These should prioritize not just assembly, but also design and production of critical hardware and firmware components. Incentives might include:
  - Tax credits for domestic manufacturing facilities
  - Accelerated permitting for power electronics factories
  - Long-term procurement commitments to provide market certainty
  - Research and development funding for secure-by-design innovations
- **Workforce development and training:** Invest in programs that develop the specialized expertise needed for both defending OT systems and designing secure energy infrastructure. This includes:
  - Specialized training programs for utilities and operators
  - Academic programs integrating OT cybersecurity into engineering curricula
  - Hands-on training facilities and fellowships
  - Professional certification programs for OT security specialists
- **Supply chain transparency requirements:** Implement requirements for comprehensive Software Bills of Materials (SBOMs) and Hardware Bills of Materials (HBOMs) for all major grid equipment, enabling operators to understand component origins and manage supply chain risk effectively.

#### **Implementation considerations**

These strategies should be implemented in a phased manner that balances security improvements with grid reliability and economic considerations. Removing all foreign-manufactured components in the near term could create reliability risks and slow the deployment of technologies needed for grid modernization. A strategic, prioritized approach that addresses the highest-consequence scenarios first, while building domestic manufacturing capacity in parallel, offers the most practical path forward.

**Q4. What collaboration between the private and public sectors is needed to develop countermeasures to protect the U.S. grid against these vulnerabilities?**

**Answer:** Protecting the nation's electric grid requires unprecedented public-private collaboration. This partnership is essential because approximately 85% of critical energy infrastructure is owned and operated by the private sector, yet government agencies possess unique threat intelligence and research capabilities that industry needs to mount an effective defense.

#### **Enhanced information sharing and threat intelligence**

Effective collaboration begins with robust information sharing. We must continue strengthening platforms like the Electricity Information Sharing and Analysis Center (E-ISAC) and similar, sector-specific ISACs that enable real-time threat intelligence sharing. We must also develop frameworks allowing properly cleared, private sector personnel to access sensitive and classified threat information needed to protect critical infrastructure.

#### **Workforce development**

A critical gap exists in cybersecurity professionals who understand OT and ICS. Unlike IT security, OT cybersecurity requires deep knowledge of physical processes, control systems engineering and potential physical consequences of cyber incidents. Public-private collaboration must address this gap through specialized training programs, hands-on learning environments, professional certifications and academic curriculum development. Organizations like Cyber Florida at USF, the Forge Institute and university partnerships with utilities provide successful models for building this talent pipeline.

#### **Cyber-Informed Engineering**

The long-term solution lies in fundamentally changing how we design critical infrastructure through CIE. Rather than bolting security onto existing systems, CIE uses design decisions and engineering controls to eliminate or mitigate cyber-enabled attacks from the outset. Following the National Defense Authorization Act for Fiscal Year 2020 mandate, the Securing Energy Infrastructure Executive Task Force — comprising senior leaders from DOE, the department of War and Homeland Security, energy companies, equipment vendors and standards organizations — developed a National CIE Strategy to guide this transformation across all 16 critical infrastructure sectors. CIE is now actively being implemented, but full-scale adoption will take additional time and resources.

#### **High Assurance Industrial Systems**

Achieving CIE's promise requires formal methods-based approaches through initiatives like High Assurance Industrial Systems (HAIS) and the Mathematically Formalized Assurance for National Security (MFANS) alliance. These efforts — coordinated across national laboratories, industry partners like Amazon and GE, and universities — develop tools that mathematically prove security properties rather than relying solely on testing. This represents collaboration among DOE, the White House Office of the National Cyber Director, the Defense Advanced Research Projects Agency and industry to establish provable security foundations for critical systems.

### **Interim protection**

While advancing toward fully cyber-informed systems, proven methodologies protect current critical assets. Consequence-driven Cyber-Informed Engineering provides a systematic process for identifying critical functions, understanding attack vectors and implementing targeted mitigations. Major utilities have successfully applied this approach, and licensed partnerships with firms like Burns & McDonnell, Black & Veatch and West Yost are scaling deployment across the sector.

Similarly, the multi-laboratory CyTRICS program addresses supply chain risks through deep, component-level analysis in partnership with major equipment vendors including Schneider Electric, GE Vernova, Hitachi Energy and Schweitzer Engineering Laboratories. This collaboration enables both vendors and utilities to identify and mitigate systemic vulnerabilities before they're exploited.

### **Advanced analytics and coordination**

Cross-sector collaboration through programs like the North American Energy Resilience Model — where national laboratories coordinate communications and modeling capabilities — provides utilities with sophisticated tools to understand infrastructure interdependencies and cascading consequences. The Cybersecurity Manufacturing Innovation Institute — a Manufacturing USA institute led by the University of Texas at San Antonio with participation from nine research institutions and over 60 industry members — demonstrates how public-private consortia can address supply chain security while supporting 50,000 small and medium manufacturers.

Research partnerships with organizations like the National Electric Energy Testing Research and Applications Center and the Electric Power Research Institute are accelerating validation and deployment of new technologies, including advanced transmission conductors and protective relay systems, ensuring innovations meet both operational and security requirements before widespread adoption.

### **The path forward**

The Department of Energy's national laboratory system serves as a neutral convener and technical resource in this collaborative ecosystem. National laboratories are uniquely positioned to address these complex challenges because they operate at the intersection of fundamental research and applied deployment, maintain unique research facilities that industry cannot replicate, conduct long-horizon research beyond typical market timescales, and serve as trusted, noncompetitive partners to both government and industry.

Multi-laboratory and industry collaborations demonstrate coordinated approaches to grid security challenges. Through specialized training programs, world-class testing facilities including full-scale test beds, standards development and direct technical assistance, the national labs work with major utilities, equipment manufacturers, system integrators and government agencies to advance grid security. These sustained partnerships — spanning industry, academia, government

and international organizations — recognize that grid security is a shared responsibility requiring collaboration built on trust, transparency and aligned incentives across the entire energy sector.

**Q5. What regulatory measures should be imposed to prevent the proliferation of embedded technologies in inverters to secure critical infrastructure, like the U.S. electric grid?**

**Answer:** Effectively regulating power electronics and control systems requires a phased approach that balances immediate security improvements with practical supply chain realities and grid reliability needs.

**Phase 1: Risk transparency and testing (Years 1-2)**

**Immediate prohibitions:**

- Battery Management Systems, integrated Battery Energy Storage Systems and control software from foreign entities of concern (FEOC)
- Offshore communications and remote access systems that transmit U.S. grid data internationally

**Transparency and inspection requirements:**

- Mandatory SBOM and HBOM disclosures for all power conversion systems
- Required "right to inspect" clauses enabling independent cybersecurity and hardware assurance testing
- Pre-deployment security certification for federally funded or regulated projects

**Infrastructure investment:**

- Federal support for chip-level assurance capabilities, testing infrastructure and trusted-foundry programs

**Application scope:** These requirements would apply immediately to new federally funded or regulated projects, with continuity provisions for projects already in interconnection queues with contracted equipment.

**Phase 2: Broad application and supply chain development (Years 3-5)**

**Expanded requirements:**

- FEOC-free power conversion systems, battery management systems and software for all new interconnection applications once domestic and allied supply chains demonstrate adequate capacity
- Extension of prohibitions to all new builds and major retrofits while maintaining existing commercial commitments

**Incentive programs:**

- Accelerated permitting for domestic power electronics manufacturing facilities
- Long-term procurement contracts providing market certainty
- Tax incentives and R & D funding for FEOC-free supply chains
- Technical assistance for utilities transitioning to compliant equipment



### **Key implementation principles**

Regulations should be:

- Risk-based, prioritizing highest-consequence applications first
- Technology-neutral, focusing on security outcomes rather than specific technologies
- Economically viable, with timelines aligned to realistic supply chain development
- Regularly reviewed to adapt to evolving technology and threats

Requirements should apply consistently based on transparent security criteria and coordinate across federal, state and international frameworks to avoid conflicting mandates.

This phased approach enables immediate risk reduction while providing clear timelines for industry to transition to more secure supply chains, balancing national security imperatives with grid reliability and economic growth requirements.

### **Q6. How might ongoing Trump administration efforts to onshore supply chains and promote domestic manufacturing in the energy sector protect the U.S. electric grid from national security risks?**

**Answer:** Onshoring supply chains and promoting domestic manufacturing can enhance grid security through multiple pathways, extending beyond direct security improvements to encompass innovation, quality control and strategic independence.

#### **Direct security benefits**

Domestic manufacturing enables thorough oversight of design, development and production processes, allowing security requirements to be integrated from initial design stages rather than retrofitted later. Manufacturing within U.S. jurisdiction permits meaningful enforcement of security standards and consequences for noncompliance.

Shorter, more transparent supply chains with fewer international handoffs reduce opportunities for malicious tampering, counterfeit component insertion or firmware manipulation. Domestic production enables better provenance tracking and authentication of critical components. When design and manufacturing occur domestically, vulnerability disclosure, patch development and remediation can proceed more rapidly without international coordination challenges that sometimes delay security updates.

#### **Addressing current vulnerabilities**

Recent vulnerability disclosures in inverters and power electronics highlight persistent security challenges. Many current products contain hard-coded vendor passwords, insufficient authentication mechanisms and inadequately reviewed open-source software components. Domestic manufacturers operating under U.S. security requirements would be subject to more rigorous, secure development practices.

The software and hardware update processes for deployed equipment create ongoing vulnerability risks. Domestic control of the maintenance supply chain enables better verification

of updates and stronger supply chain security for replacement components. Current contractual provisions also sometimes prevent thorough security analysis under intellectual property protection claims. Domestic manufacturers operating under U.S. legal frameworks can be required to permit independent security testing and vulnerability analysis.

#### **Innovation and strategic benefits**

A robust domestic manufacturing base enables the United States to lead international standards development for power electronics security, ensuring global standards align with U.S. priorities. U.S.-based manufacturers can more readily incorporate cutting-edge security technologies developed through federal research programs, including formal verification methods, hardware-based security features, advanced authentication capabilities and secure boot processes.

Domestic manufacturing creates employment opportunities for engineers and security specialists with expertise in secure power electronics, building a knowledge base that enhances both manufacturing capabilities and operational security. This facilitates partnerships between manufacturers, universities and national laboratories to advance manufacturing technology and security innovation.

#### **Supply chain resilience**

Domestic manufacturing reduces vulnerability to international supply disruptions from geopolitical tensions, trade disputes or global crises, ensuring continuity of supply for grid modernization and maintenance needs. Manufacturing under consistent regulatory frameworks improves product quality and reliability while enabling more effective recall and replacement processes when issues are identified.

#### **Implementation considerations**

Realizing these benefits requires more than relocating manufacturing facilities. Effective onshoring efforts should include secure-by-design requirements in federal procurement programs, supply chain verification even for domestically manufactured equipment, competitive market development with multiple suppliers and coordination with allied nations where complete domestic sourcing is not feasible. Near-term strategies must manage risks in the existing installed base while domestic manufacturing capacity develops.

The Honorable Mariannette Miller-Meeks (R-IA)

**Q1: You mentioned that CyTRICS conducts rigorous testing of hardware and software components in the energy supply chain. Given that you've identified China's embedding of hardware vulnerabilities as a major structural risk, how effective are these testing programs at detecting backdoors or vulnerabilities built into Chinese-manufactured equipment? And can these programs scale to address the volume of Chinese components currently in our infrastructure?**

**Answer:** CyTRICS has a strong track record of identifying and mitigating vulnerabilities in energy infrastructure. However, not all components require the level of skill and effort that CyTRICS demonstrates. Most Chinese-sourced components in critical infrastructure are simple electrical parts that can be functionally verified and tested by manufacturers. CyTRICS analyzes

digital supply chains and identifies vulnerabilities and mitigations in energy infrastructure regardless of equipment country of origin.

Just as technology changes at a rapid pace, the methods and techniques used to evaluate that technology must also evolve and keep pace. CyTRICS is constantly improving the state of the art and the state of the practice for supply chain research. The national laboratories that participate in CyTRICS are constantly striving to scale the work that we perform through automation and integration of new technologies. CyTRICS also works with vendor and asset owner partners to share directly with industry the methods and lessons that empower private industry to join in defense against supply chain attacks.

The identification of vulnerabilities or backdoors is only a single part of a needed defense-in-depth strategy. This strategy includes programs like CIE, which are necessary to protect against vulnerabilities that either avoid detection or that emerge through usage of a system or changes to surrounding technology. Importantly, both CyTRICS and CIE are important to secure our energy infrastructure.

