DEFENDING THE U.S. ELECTRIC GRID AGAINST CYBER THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 27, 2021

Serial No. 117–36

Printed for the use of the Committee on Oversight and Reform

Available at: *govinfo.gov, oversight.house.gov* or *docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
45–371 PDF WASHINGTON : 2021

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CORI BUSH, Missouri
DANNY K. DAVIS, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
PETER WELCH, Vermont
HENRY C. "HANK" JOHNSON, JR., Georgia
JOHN P. SARBANES, Maryland
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
MARK DESAULNIER, California
JIMMY GOMEZ, California
AYANNA PRESSLEY, Massachusetts
MIKE QUIGLEY, Illinois

JAMES COMER, Kentucky, *Ranking Minority Member*
JIM JORDAN, Ohio
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
PETE SESSIONS, Texas
FRED KELLER, Pennsylvania
ANDY BIGGS, Arizona
ANDREW CLYDE, Georgia
NANCY MACE, South Carolina
SCOTT FRANKLIN, Florida
JAKE LATURNER, Kansas
PAT FALLON, Texas
YVETTE HERRELL, New Mexico
BYRON DONALDS, Florida

RUSS ANELLO, *Staff Director*
DAN REBNORD, *Subcommittee Staff Director*
AMY STRATTON, *Deputy Chief Clerk*
CONTACT NUMBER: 202-225-5051
MARK MARIN, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

PETER WELCH, Vermont
HENRY C. "HANK" JOHNSON, JR., Georgia
MARK DESAULNIER, California
KWEISI MFUME, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida
JACKIE SPEIER, California

GLENN GROTHMAN, Wisconsin, *Ranking Minority Member*
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana

C O N T E N T S

INDEX OF DOCUMENTS

DEFENDING THE U.S. ELECTRIC GRID AGAINST CYBER THREATS

Tuesday, July 27, 2021

HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON NATIONAL SECURITY
COMMITTEE ON OVERSIGHT AND REFORM
Washington, D.C.

The subcommittee met, pursuant to notice, at 3:11 p.m., in room 2154, Rayburn House Office Building, Hon. Stephen F. Lynch (chairman of the subcommittee) presiding.

Present: Representatives Lynch, Welch, Johnson, DeSaulnier, Wasserman Schultz, Speier, Langevin, Grothman, Gosar, and Comer.

Also present: Representative Langevin.

Mr. LYNCH. This committee will now come to order. Without objection, the chair is authorized to declare a recess of the committee at any time. I now recognize myself for an opening statement.

Good afternoon, everyone. Before we begin, I would like to thank each of our witnesses for testifying before our subcommittee today. I would also like to thank my colleagues who are participating at today's hearing, both remotely and in person.

If you listened to the news over this past year, there's a good chance that you have heard about one of many cyber attacks that have targeted a high-profile technology company, research institution, energy pipeline, or even the Federal Government. Today, we will examine how this latest uptick in hacking attempts could affect the vital component of our critical infrastructure, and even U.S. national security, and that is the vulnerability of our electrical grid.

The electrical grid is the backbone of daily life here in America. It provides energy to heat our homes, power our hospitals, and charge our smartphones. It also is a priority target for state and non-state cyber adversaries. A successful attack on the electrical grid could have devastating consequences on U.S. national security and our economic interests.

Last month, Secretary of Energy, Jennifer Granholm, confirmed that cyber adversaries have the tools and capabilities necessary to shut down our electrical grid.

In a recent statement, the Department of Energy warned, and this is a quote, "The United States faces a well-documented and increasing cyber threat from malicious actors seeking to disrupt the electricity that Americans rely on to power our homes and businesses every day." In response, President Biden has taken decisive

meaningful action since assuming office to strengthen our national cyber defense and protect our critical infrastructure.

For example, in April, President Biden announced a 100-day plan led by the Department of Energy and the Cybersecurity and Infrastructure Security Agency, CISA, to strengthen the security and resilience of U.S.—of the U.S. electrical grid. And in May, President Biden issued an executive order that will modernize our national cybersecurity defenses and improve information-sharing between the U.S. Government and private sector, which is ultimately responsible for operating and securing the electrical grid.

I want to applaud and I am grateful to President Biden for recognizing the urgency of this threat; however, significant vulnerabilities continue to persist. And the Biden administration should consider whether additional regulations or policy initiatives are needed to strengthen the cyber defense and resiliency of our electrical grid. For example, as a growing number of network consumer devices connect to electrical distribution systems, these devices create additional gateways that hackers can exploit to gain access to the grid. These vulnerabilities are exacerbated by the fact that Federal cybersecurity standards do not currently apply to distribution systems, and are, instead, only mandatory for certain power generation and transmission systems.

Even those mandatory reliability standards that apply to electric generation and transmission systems do not fully incorporate leading cybersecurity guidance from the National Institute of Standards and Technology.

In addition, many key components of the electrical grid are produced, or rely upon parts produced by international suppliers. This equipment is vulnerable to tampering or espionage by foreign actors. Some of this equipment, especially large power transformers, can take over a year to produce, transport, and install. Even in an emergency, making the U.S. electrical grid heavily dependent on overseas manufacturing.

Last, but certainly not least, multiple Federal agencies and state and local entities, each with its own role, its own responsibilities, and its own authorities are all tasked with protecting the electrical grid. This creates ample opportunity for bureaucratic stovepiping and can undermine the incidence response to any events.

To that end, I look forward to hearing from our witnesses about how they are working together in sharing information to ensure malign cyber actors cannot slip through the cracks. With that, I would like to thank our witnesses for their service and for testifying before our subcommittee on this critically important issue. And I will now yield to my friend, the ranking member from Wisconsin, Mr. Grothman, for five minutes.

Mr. GROTHMAN. Thank you very much. And thank you for our witnesses for showing up today. There's an issue with far-reaching repercussions, something that scared me for a long time. An attack on the energy grid would be devastating for Americans and our national security. Hours, even hours without power would cause chaos. Extended disruptions could pose serious consequences to our national defense. Cyber attacks are growing in frequency. Particularly, scary ones from state-sponsored groups in Russia and China.

It would appear to the casual observer that these actors are testing us, testing our defenses, our response, our reaction.

Our defense must effectively and efficiently identify and disrupt potential attacks. Our response must harness the powers of government and the private sector to mitigate the fallout. Our reaction must be swift and strong to future attacks.

Each of you, each of our witnesses plays a vital role in the Nation's cyber defense. This hearing is a welcome opportunity to hear from all of you, and learn more about how our government operates in space, as well as what the fallback position is going to be if any of these attacks are effective. It's a balancing act between the government authority and the operation of private industry. The answer is not more unilateral costs of regulations—many more unilateral regulations. The answer lies within current authorities available to you and, frankly, your ability to work with each other. I hope we can hear more about the collaboration today.

In closing, I would like to say, hopefully, in the future, we can take up other security issues, the origin of the COVID, the Chinese biological weapons program, dangers of a nuclear Iran, a botched Iran deal, and President Biden's border crisis. I have been down there four times. I would love a hearing on that. It's a huge number of people crossing the border. We're, right now, at about 70,000 people a month. What is further disturbing is the vast number of illegal immigrants President Biden has been releasing in our country, well over 160,000 between Border Patrol and HHS.

The committee's held hearings after hearing during the Trump administration operating missions with the border. I have been down there four times. You would have a blast having a hearing on that. I hope, Mr. Chairman, we can work together to investigate these issues. I yield back and look forward to our witnesses to tell them.

Mr. LYNCH. The gentleman yields back. I have one important procedural matter. Without objection, the distinguished member from Rhode Island, Mr. Langevin, is recognized and waived on to the committee for the purpose of participating and questioning these witnesses. Mr. Langevin is a senior member of the House Armed Services Committee where he serves as chairman of the Subcommittee on Cyber Innovative Technologies and Information Systems. Mr. Langevin has led on a number of key pieces of legislation related to cybersecurity, including a bill to establish a position of National Cyber Director in the White House. He is also a commissioner on the Cyberspace Solarium Commission, and is a co-chair of the congressional Cybersecurity Caucus. So, welcome, Mr. Langevin.

Now, I would like to welcome our three witnesses. Today we are joined by Mr. Puesh Kumar, who is the Acting Principal Deputy Assistant Secretary in the Office of Cybersecurity, Energy Security, and Emergency Response at the Department of Energy. We are also joined by Mr. Eric Goldstein, who is the Executive Assistant Director for Cybersecurity at the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. And we are also joined by Mr. Joseph McClelland who is the Director of the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission.

So, to all of our witnesses, thank you for your willingness to appear and to help the committee with its work. We look forward to your testimony.

It is the custom of the committee to swear our witnesses. So, would the witnesses please stand and raise your right hand so that we can swear you in.

Do you swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Let the record show that the witnesses have each answered in the affirmative. You may be seated. And thank you. And without objection, your written statements will be made part of the record.

With that, Mr. Kumar, you are now recognized for five minutes of your summation of your written testimony.

STATEMENT OF PUESH M. KUMAR, ACTING PRINCIPAL DEPUTY ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, ON BEHALF OF DEPARTMENT OF ENERGY

Mr. KUMAR. Thank you, Chairman Lynch. Chairman Lynch, Ranking Member Grothman, and distinguished members of the subcommittee, thank you for the opportunity to testify on behalf of the Department of Energy to discuss the administration's continuing efforts to secure the Nation's energy infrastructure, helping to ensure that all Americans may rely on a resilient, secure, and clean energy system.

The energy sector provides critical resources, electricity and fuel that we all depend upon. As we recently witnessed with the Colonial Pipeline incident and impacts from extreme weather in Texas, disruptions to our energy system can have devastating impacts to the U.S. economy, and the livelihoods of millions of Americans. DOE's Office of Cybersecurity, Energy Security, and Energy Response, commonly referred to as CESER, plays a leading role in addressing the continuously evolving risks facing the energy sector, including the growing cyber threats that pose a strategic challenge to the United States.

Over the past few years, we have all witnessed an increase in the frequency and sophistication of attacks by a range of actors from cyber criminals to nation-states. As part of the Federal Government's coordinated efforts to proactively protect, defend, and assist the energy sector with the preparedness and response to all hazards, DOE is designated as the Sector Risk Management Agency, or the SRMA, for the energy sector, and is the coordinating agency for Emergency Support Function 12 under the national response framework.

Through these roles, DOE works across the Federal Government. CISA and FERC are certainly on speed dial, as well as our partners at the state, local, territorial, and Tribal levels.

Further, we have a strong relationship with the U.S. energy sector owners and operators. DOE and DHS serve as co-chairs of the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council. The Sector Coordinating Council structure allows the government, a growing state, to work closely with the industry to prepare for and respond to national

level disasters, or threats, to critical infrastructure. Collective preparedness and collective response are at the heart of our work.

With that in mind, there are five priorities that I have set for the CESER office to really ensure that we are targeting our resources on the critical issues that are facing the U.S. energy sector. The first priority is to increase the visibility of cyber threats, targeting industrial control systems of energy companies. This includes enhancing the government and industry's ability to detect and deter cyber threats.

As you mentioned, Chairman, we just launched the 100-day initiative for industrial control systems. And the goal there is to really start to get visibility into a part of the energy system that we haven't had as much visibility on before. Really starting to see the cyber threat actors in that environment and be able to quickly collaborate with them.

The second priority is to identify supply chain threats, and disclose vulnerabilities in the energy sector, both in their hardware, but also the software and the digital supply chain.

One of the efforts we have underway at CESER right now is a program called Cyber Testing for Resilient Industrial Control Systems. The idea behind the program as is commonly referred to as CyTRICS is to partner with manufacturers and suppliers for the most critical components in the energy sector, so that we can test for hardware and software vulnerabilities before those systems are ever deployed in the energy sector. And we're having tremendous success along those lines.

The third priority is to encourage the concept of security by design, and ensuring that cybersecurity is just built into the relevant research and development and demonstration across DOE and our national laboratories. It should be core component of everything we do.

To that end, we are focused on an effort we call cyber-informed engineering. The goal is to develop a framework so that when we have our engineers designing the next generation energy systems, cybersecurity is a core component of those early designs so that we're not trying to bolt on cybersecurity after the fact, but we're really building it in as a requirement to any design that we build in the energy sector in the United States.

The fourth priority is capacity building in the industry and the state, local, territorial, and Tribal communities. Working to strengthen things like threat information sharing, exercising with a sector so we're prepared to respond. And also, work force development is another key priority for us. And we just released an updated tool for the industry called Cybersecurity Capability Maturity Model, C2M2. We just released version two last week. The C2M2 model lets companies assess the maturity of their cybersecurity programs and make targeted investments in their programs going forward.

And, finally, the fifth priority is to ensure that when an incident does occur, regardless of hazard, CESER is ready to support the sector, and mitigate impacts and ensure the safe and sufficient restoration of the Nation's energy infrastructure. We do this through the deep subject matter expertise of energy systems across the DOE complex, including headquarters, national laboratories, power

marketing administrations, the Energy Information Administration, and the National Nuclear Security Administration. We're able to bring the different resources to the table in support of the response—in the case of a cyber response and work closely with our partners at CISA and FBI to ensure that we can have a coordinated response like we did with the Colonial Pipeline incident. Thank you for the opportunity to testify. I look forward to your questions.

Mr. LYNCH. Thank you. Mr. Goldstein, you are now recognized five minutes.

STATEMENT OF ERIC GOLDSTEIN, EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, ON BEHALF OF DEPARTMENT OF HOMELAND SECURITY

Mr. GOLDSTEIN. Thank you. Chairman Lynch, Ranking Member Grothman, members——

Mr. LYNCH. Can you turn your mic on?

Mr. GOLDSTEIN. It's on, but I will move it a bit closer.

Mr. LYNCH. OK.

Mr. GOLDSTEIN. It should be better.

Mr. LYNCH. Thank you.

Mr. GOLDSTEIN. Chairman Lynch, Ranking Member Grothman, members of the subcommittee, thank you for the chance to testify today on behalf of CISA. And thank you for your focus on this critical issue and bringing us here to discuss the work that we have done so far and the need to make further progress in addressing risk to the Nation's energy grid and broader critical infrastructure.

Cyber intrusions targeting organizations across all sectors of the economy reflect that is now an urgent threat to our national security, economic security, and public health and safety. As the lead agency for civilian cybersecurity, CISA seeks to actively reduce risks and reduce vulnerabilities across critical infrastructure in close partnership with sector risk management agencies, like the Department of Energy. In this role, we're particularly focused on reducing risk to national critical functions. Those services that are so essential to the American people that degradation of them would lead to debilitating effects on our economy, our security, or our ways of life.

Of course, the energy sector is essential to numerous national critical functions. Not only the power itself, but, of course, its dependencies: water, telecommunications, the ability to move around our communities.

Through a close partnership with DOE and our private sector partners, we seek to improve cybersecurity at a national level. And we do this in five principal ways: First, we seek to share timely and actionable information across the country with partners in the energy sector and across sectors to ensure that every organization has the information they need to secure their networks against current and emerging threats.

Second, we provide voluntary services, such as vulnerability assessments, red-teaming, penetration tests to help organizations understand vulnerabilities in their networks, and fix them before an adversary can intrude and cause a compromise.

Third, when an incident does occur, we provide incident response and threat-hunting assistance and coordinate the national asset response to cybersecurity incidents to mitigate the event and bring it to a swift resolution.

Fourth, we provide active detection tools to help companies on a voluntary basis, detect threats on their networks.

And fifth and finally, we conduct cross-sector analysis to understand how a cyber intrusion can cascade across sectors and impact national critical functions.

And as my colleague at DOE noted, we are doing a lot of this work today under the auspices of the White House's 100-day Control Systems Plan, in which we are focus on improving both security practices and the ability to detect threats across critical entities in the energy sector.

Going forward, it's clear that we have more to do. It is clear that we must act urgently to address this increasing threat to our national security. We are looking to drive this progress at CISA in a few ways.

First, we continue to work urgently on a voluntary basis with government and the private sector partners to gain visibility into cybersecurity threats and intrusions across the country. With this visibility, we are able to disseminate more actionable and timely information, we're able to provide more tailored response, and we're able to understand the breadth of risks affecting entities in this country. We look forward to working with Congress on enabling incident reporting legislation that will provide CISA with this needed visibility. And we're also looking to more broadly deploy our detection tool, such as the CyberSentry Program, which allows us to use commercial tools and government information to expand visibility into risks affecting the Nation's most critical infrastructure.

Additionally, we must continue to mature our voluntary partnerships with government in the private sector. We are shortly launching our newly renamed joint cyber defense collaborative as established in last year's NDAA to formalize our work between government and the private sector around mitigating and understanding emerging cyber campaigns affecting our country.

And, last, we must recognize that we are not going to, in the near term, prevent every cybersecurity intrusion. And we must focus on resilience and functional continuity. To this end, the Cyber Response and Recovery Fund, an initiative recommended by the Cyberspace Solarium Commission, and recently passed by the Senate, will significantly help CISA have the capacity to help entities respond and recover when damaging intrusions occur.

We know that the problem is severe, and trends are not pointing in the right direction. We are doing more, and we must act with urgency in managing this threat we are facing. CISA is prepared to lead this national effort in coordination with the SRMAs, with Federal law enforcement, our partners across this country. I will look forward to working with Congress in so doing. Thank you again for your time. I look forward to your questions.

Mr. LYNCH. Thank you. Mr. McClelland, you are now recognized for a five-minute summation for your testimony. Thank you.

STATEMENT OF JOSEPH H. MCCLELLAND, DIRECTOR, OFFICE OF ENERGY INFRASTRUCTURE SECURITY, ON BEHALF OF FEDERAL ENERGY REGULATORY COMMISSION

Mr. MCCLELLAND. Chairman Lynch, Ranking Member Grothman, and members of the subcommittee, thank you for the privilege to appear before you today to discuss defending the U.S. Electric Grid Against Cyber Threats. My name is Joe McClelland. I am the Director of the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission. I come before you as a commission staff witness, but I should note my remarks do not necessarily represent the views of the Commission or any other individual commissioner.

In the Energy Policy Act of 2005, specifically, through Section 15 of the Federal Power Act, Congress entrusted the Commission to approve and enforce mandatory reliability standards for the Nation's bulk power system. Section 215 requires the Commission to certify an electric reliability organization, or ERO, that is responsible for proposing for commission review and approval reliability standards, or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system.

The Commission certified the North American Electric Reliability Corporation, or NERC as the ERO. By statute, the bulk power system does not include electric distribution facilities. Section 215 of the Federal Power Act provides for stakeholder input into the ERO's development of reliability standards for the bulk power system. This process works relatively well to develop standards to address traditional operations and planning-related reliability events that may cause grid failures, or blackouts, such as from improper vegetation management, or failures associated with the operation of protection equipment. The nature of the national security threats from adversaries' intent on attacking our Nation's electric grid significantly differ from reliability vulnerabilities that have caused regional blackouts and reliability failures we have seen in the past. Widespread disruption of electric service can quickly undermine the U.S. Government, its military, and the economy as well as endanger the health and safety of millions of our citizens.

To help mitigate these advanced persistent and rapidly evolving threats, the Commission uses a two-pronged approach with regard to grid reliability, employing mandatory reliability standards to establish foundational practices, while also working collaboratively with industry the states and other Federal agencies to identify and promote best practices.

While the NERC Critical Infrastructure Protection, or CIP reliability standards are the foundation of the commission's work to address cybersecurity, there are additional measures that can and should be taken to further improve the industry's cybersecurity posture, considering these rapidly evolving threats. That is why the Commission established OEIS. OEIS partners with other Federal agencies, states, and industry to develop and promote best practices for critical infrastructure security. Working with these entities, OEIS helps identify new and emerging threats, informs the private sector of them, performs voluntary cybersecurity evaluations, and assists with mitigating actions.

For example, OEIS conducts voluntary architecture assessments of interested commission jurisdictional utilities' computer networks that can control the operations of their facilities. Conducted onsite, these assessments are specific to the organization, reviewing everything from the configuration of legacy equipment to the application of state-of-the-art protection systems.

Another example is that OEIS works with the Office of Director of National Intelligence, specifically, the National Counterintelligence and Security Center to conduct briefings and exchange information with state and industry officials about the current threats the industry is facing and what can be done to address them.

More broadly, OEIS works with the NERC Electricity Information Sharing and Analysis Center to rapidly issue bullets and alerts informing industry of specific vulnerabilities and threats, as well as best practices that can be used to defend against them.

As a final example, OEIS assists with the planning and execution of tabletop exercises, and participates in joint security programs with other government agencies.

Last month, OEIS assisted the National Guard units participating utilities in the New England states to conduct Cyber Yankee, a simulated cyber attack on system networks. This red-teaming exercise helped the New England utilities and National Guard units to prepare for these threats, including practicing government assistance to the utilities as part of the defense and recovery efforts. Exercises such as these are critical to maintaining readiness and ensuring our ability to respond to cybersecurity attacks.

In conclusion, cybersecurity threats pose a serious risk being to the bulk power system and its supporting infrastructures that serve our Nation. These are complex, persistent, and fast-evolving issues, and they won't be solved easily, and they will require a great deal of coordination and communication. Therefore, the Commission has adopted this two-pronged approach to best address the important security matters. Thank you for your attention and the opportunity to testify today. And I look forward to your questions.

Mr. LYNCH. Thank you. I will now recognize myself for five minutes for questions. Our adversaries are targeting all facets of the American life with frequent and increasingly sophisticated cyber attacks. In just the past few months, cyber attacks have frozen a major oil pipeline, shut down the world's biggest meat producer, and compromised one of the largest email servers in the world.

In a June 6 interview, Secretary of Energy Jennifer Granholm said, and I will quote her, "There are thousands of cyber attacks in all aspects of the energy sector." And she added, "It's happening all the time." Secretary Granholm also acknowledged that our adversaries, foreign nations, and criminal groups have the cyber capabilities to shut down the U.S. electric grid. We know that this threat exists because our adversaries have demonstrated it already.

In 2015, Russian intelligence agents used a sophisticated cyber attack to cripple industrial control systems of the Ukrainian electrical grid, shutting off power to hundreds of thousands of people in the dead of winter. In that case, thankfully, power was restored to most consumers in a matter of hours.

However, the message was clear, Russia is willing and able to target its adversary's electrical infrastructure. But it's not just Russia that we need to worry about—China, Iran, North Korea, and numerous sophisticated cyber criminal groups all view the U.S. electric grid as a priority target.

So, Mr. Goldstein, how would you describe the current risk of a major cyber incident on the electrical grid in the near future? Give me sort of a landscape assessment of where you think we are right now, to the best of your ability?

Mr. GOLDSTEIN. Certainly, Mr. Chairman. I think your description of the threat environment is apt. I think we have an environment today where there are many organizations throughout this country and across sectors of critical infrastructure that have not universally deployed these sort of strong security controls and managed no insecurity weaknesses that we know that our adversaries have the technical ability to exploit. This puts us in a position where the possibility of a highly damaging cybersecurity intrusion affecting a national critical function, such as the provision of power to the American people, is certainly a possibility.

Mr. LYNCH. Let me ask you, just on that point and this is for the entire panel. I doubt very much that we have a single point of failure, but as we saw with the Colonial Pipeline, you have got some infrastructure that—some pieces of infrastructure that are so critical to—in that case, it was the East Coast. But is this an assessment that there are several points of vulnerability, or geographically speaking?

And when you say certain entities are not using proper cyber hygiene, let's say, is that something that, as Mr. McClelland has pointed out, is that a standard that's recommended, or is it something that is actually required?

Mr. GOLDSTEIN. Certainly. So, I will defer to my colleagues at DOE and at FERC respectively for an assessment on points of failure in the grid, as well as on the mechanisms that could be utilized through FERC authorities. What I would note is that, you know, if all organizations do not urgently focus on understanding not only the vulnerabilities in their network that exists today, but also on the tactics, techniques, and procedures that we are seeing adversaries, whether nation-states or criminal gangs utilize, and don't urgently invest in putting in place controls that meet what we see our adversaries doing, then we are at urgent risk of a cybersecurity intrusion that could result in degradation of a national critical function, of which there are many, but certainly the energy sector is one.

This is why it is so urgent for all organizations to put cybersecurity investment at the top of their list recognizing that, you know, investments must be weighed against other considerations. But at CISA, we are urgently focused on making sure that all entities across critical infrastructure are focused on putting in place these strong controls and mitigating those known vulnerabilities that we know could be exploited to cause significant harm.

Mr. LYNCH. I am sorry. Mr. Kumar, Mr. McClelland, could you take a whack at that question well.

Mr. KUMAR. Absolutely, sir. Thank you for the question. I think that's a really important question, because I truly do believe that

the cyber challenge is a national security challenge that we are facing on a daily basis as you mentioned. It becomes even more complex when you think of the electricity sector that has over 3,000 electric utilities across the United States, and how it's all connected. This becomes even more complex and challenging. And, so, we need to be addressing this through three different ways. The Department is looking at it from three different tracks: One, what are those policies that we need to look at? Are those policies in coordination with our colleagues at FERC?

Two, what are tools and technologies that we can put on the grid that can detect these threats before they result in impacts? We need to continue investing in a lot of that R&D.

But then, the last one is when it does happen, just like with Colonial, how do we respond? Respond swiftly and have the backups necessary to immediately recover from a response. We are thinking about it from all three perspectives, and we need to continue to do more.

So, we at the Department are certainly working with FERC in terms of really understanding the bulk power system. So, how do we help the regulators at the Federal level understand the threat so that our standards are risk-based? So, as we see the threat evolve, so does the standard. We're doing the same thing with the states. So, the jurisdiction of regulatory standards through the distribution systems are in the hands of states.

And, so, our approach at the Department is to work with the public utility commissions and the public service commissions at the state level to ensure that they, No. 1, understand the threat. As my colleague, Joe, mentioned what we're trying to do is help them understand the threat at both the unclassified and classified level to inform how they work with their utilities at the state level.

The second thing is often the state, or the states, don't have the resources to actually make these informed decisions in terms of how much a cybersecurity investment is appropriate. So, what we have been doing is developing tools. So, the tool that I just mentioned, C2M2, Cybersecurity Capability Maturity Model. The utility is used to decide on investments in cybersecurity. We are providing a similar version of that tool to the states to use to gauge the cybersecurity of the utilities within their state. And, so, we need to do this three-pronged approach to continue pushing cybersecurity forward, sir.

Mr. LYNCH. Great. Mr. McClelland.

Mr. MCCLELLAND. I refer to a couple of quick quotes on the annual threat assessment. This was issued on April 9 of 2021. "We continue to assess that China can launch cyber attacks that, at a minimum, can cause localized temporary disruption to critical infrastructure within the United States."

Regarding Russia, Russia continues to target critical infrastructure, including underground, underwater cables, and industrial control systems in the United States, and in its allied countries. As compromising such infrastructure improves, and, in some cases, can demonstrate its ability to damage infrastructure during a crisis.

And then, last, I just refer you to the task force on cyber deterrence. This was in 2017. And this is just a precursor to your an-

swer. So first, major powers, Russia and China, have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack. This emerging situation threatens to place the United States in an untenable position. Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is at least for the next decade, the offense of cyber capabilities of the most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures.

So, back to my statement, my opening statement, FERC uses a dualfold approach. If you imagine two geometric shapes, a pyramid, foundationally, that's where we put the cybersecurity standards. These standards are developed in the open, and they're deliberative, and they're iterative. Our adversaries are capable of reading the standards and adapting those standards, even before they are put into place, which is spoken to by our intelligence community assessments.

However, at the apex of the pyramid, that's where the nation-state threats lie. It's a matter of information sharing between the agencies and between the industry to make certain that they can address these threats. And those threats really—sorry. I am sorry. I see the time.

Mr. LYNCH. Yes, thank you. The chair now recognizes the Ranking Member Mr. Grothman for five minutes for questions.

Mr. GROTHMAN. Thank you. Kind of what you said there, Mr. McClelland, is kind of a little bit scary. So, you feel today that our grid is vulnerable, and most people probably think it is, but you think it's significantly vulnerable to cyber attack?

Mr. MCCLELLAND. I would say that the worldwide threat assessment from DNI—the current threat assessment certain of our adversaries have the capability to target and disrupt these services.

Mr. GROTHMAN. OK. I think our cyber posture is three parts: it's defense, it's response, and reaction. If there were a successful attack on a significant part of the United States, do we have a fallback position? Or how we quickly do you think we could get back our grid?

Mr. MCCLELLAND. I think that depends on the attack. You know, was infrastructure simply interrupted? Were their services interrupted? For instance, was it a denial of service attack? Or were the adversaries able to gain access to the networks, and, particularly, the operational technology networks, and at that point, damage or destroy equipment that's necessary to operate the power grid?

Mr. GROTHMAN. That's kind of the question. If they damage equipment, do we have fallback position here? Would we have to build something new? I mean, what would happen if part of the grid you picked in that part of the United States is destroyed or disabled, how long would you be able to—before be able to get the grid up and going again?

Mr. MCCLELLAND. Well, the industry does operate to an N-minus–1 contingency, which means it can suffer the single largest contingency on the grid and continue operations. So, it can continue to provide power if it loses the single largest contingency. If there are multiple contingencies, those can result in prolonged out-

ages. And those outages depend on the extent of damage to the equipment and the availability of that equipment.

Mr. GROTHMAN. OK. So, you feel one attack, we always have a backup, and more than that, we could have big trouble?

Mr. MCCLELLAND. I am sorry. Would you repeat?

Mr. GROTHMAN. Do you feel we have enough to handle one attack without being a disaster, but if we have more than one, we have huge trouble? Is that accurate?

Mr. MCCLELLAND. If it's beyond the N-minus–1 contingency, then the power grid service can be interrupted. That is correct.

Mr. GROTHMAN. Mr. Goldstein, do you agree with that, or do you want to comment on the same question?

Mr. GOLDSTEIN. Sir, I will defer to my colleagues at the American DOE for their assessment. I will be resilient of the grid itself.

Mr. GROTHMAN. OK. Mr. Kumar.

Mr. KUMAR. Thank you for the question, sir. So, there's both the benefit and a concern when you have 3,000 electric utilities in the United States. The concern is certainly the complex nature of how it is all connected, and how we need to ensure that the cybersecurity posture across the board is raised up. But that complexity is also—it's a resiliency. Because of the different types of networks that are set up across the different utilities, what you can also have is some sort of resiliency built in because it's not going to be able to go—traverse from one utility to the next as easily.

With that said, to answer your question more specifically, you know, the concern that I have is more focused around supply chain threats. It is much like we saw with SolarWinds, where it took one supplier that was across 16,000 organizations. That's the threat that I am concerned about, and that's where I am focused on is what are those critical components, critical manufacturers and suppliers that are across the energy sector? And if they are impacted, then they can actually be the attack vector into these utilities. So, that's where a lot of my concern is right now in terms of addressing the supply chain threat, sir.

Mr. GROTHMAN. Do you feel we have enough defense right now to prevent that or no?

Mr. KUMAR. In terms of—the perspective we have is, currently the assessment that my colleague from FERC mentioned is we think that there is the capability to have a temporary and localized disruption to energy supply per the DNI's assessment. But in terms of the resiliency, I do think the sector does have resiliency built in, N minus one criteria that Joe mentioned is really important.

But in terms what we do right now is we practice the response. So, if this were to happen, how do we get either a spare transfer in, or another piece of equipment quickly in? So, that's something that we are constantly doing with the sector in terms of preparing for that type of incident.

Mr. GROTHMAN. I understand you might not be able to speak to this, but I want it on the record. It's important we don't let malign actors get away with these actions, especially if they are affiliated with nation-states like Russia or China. If something happened like you were describing, how quickly do you think we would be able to—say, one utility had huge problems, how quickly do you think

we would be able to get the grid in that area or that factory up and running again?

Mr. KUMAR. Sir, thank you for that question. It's a complex problem. It really depends on the type of attack vector. Is it a piece of software that's critically used? Is it a piece of hardware? And that's going to factor into how we respond as a government to really respond to this type of incident. Unfortunately, there isn't a great answer until you start to see it.

Now, with the SolarWinds type of incident, what we're focusing on is working with the GEs, the ABBs, the large industrial control system manufacturers, to ensure that there is backups and redundancy built into these systems so that we can go to a backup plan. And so, that is an area that we have been working with the sector on, and the concept is called spare tire. Can we go to a manual mode if we can't rely on our digital systems?

Mr. GROTHMAN. It seems to me that private companies, if there were not threat of attack, would not invest as much as they have to if there was an attack, right? If seems the question is for good of society as all, we need a fallback position. Do you think there's some role for government there or not?

Mr. KUMAR. Sir, I appreciate the question. I feel like government does have a role in terms of really working with the sector to bolster the defenses. This is why we launched the Industrial Control Systems Initiative because we really need to start looking at cyber adversaries in those critical systems, and then be able to correlate that information from our end. We want to correlate it with our colleagues at CISA from a cross-sector perspective, and then we want to correlate it with our intelligence community, so we can get a feedback loop back to the sector. And we need to continue pushing on this and incentivizing cybersecurity across the board.

Mr. GROTHMAN. I would like to thank the chair for his generosity.

Mr. LYNCH. Absolutely. The gentleman yields back. The chair recognizes the gentleman from Vermont, Mr. Welch, for five minutes.

Mr. WELCH. Thank you. Thank you, Mr. Chairman. I want to thank the witnesses, too. The National Institute of Standards and Technology cybersecurity framework includes guidance and best practices that are, of course, widely regarded as foundational elements.

Mr. McClelland, why do the North American Electric Reliability Corporation Standards not fully integrate the NIST cybersecurity framework?

Mr. MCCLELLAND. Thank you for the question. In August 2019, GAO submitted a report to Congress comparing the NERC CIP standards to the NIST framework. In that report, GAO concluded that the CIP standards did not cover some of the NIST framework requirements. In response to that report, FERC staff began an investigation to benchmark the NERC CIP standards against the GAO framework.

It's important to note right at the onset that the two bodies don't necessarily compare equally. And just a few examples, the NERC CIP standards focus, specifically, on operational technologies necessary to ensure operations to the bulk power system, where the

NIST framework focuses on both IT information technology and OT operational technology. The NERC CIP standards do not necessarily reflect best practices. They're foundational standards, and they're foundational practices, but——

Mr. WELCH. What do we have to do in order to get to a place where we have some confidence that we'll be able to resist these attacks?

Mr. MCCLELLAND. So FERC, after the analysis, FERC did issue notice of inquiry. It was in June 2020.

Mr. WELCH. Right.

Mr. MCCLELLAND. It, specifically, identified categories of function to the industry for open comment, asking whether or not the NERC CIP standards could improve in comparison to the NIST framework.

Mr. WELCH. So, what do you think? Do you believe the gaps in the current reliability standards do present a risk to the bulk electrical system?

Mr. MCCLELLAND. The comments were received. I just need to finish that quickly.

Mr. WELCH. I'm sorry.

Mr. MCCLELLAND. So, in September, we received comments. Now it's the subject of an ongoing proceeding. So, I can't speak any further about it. But I can tell you that the matter is under active consideration by the Commission, having received comments from any interested party and comparing the NERC CIP standards to the NIST framework.

Mr. WELCH. The bottom line, though, is that we really got to get some resolution on that in order to have a higher degree of confidence that we can resist the cyber attack, right?

Mr. MCCLELLAND. Again, I just cannot comment on an ongoing proceeding. I couldn't give any perspective on that proceeding. I am sorry, sir.

Mr. WELCH. All right. Let me ask this: On the NERC reliability standard, as I understand it, they're only mandatory for bulk power systems of over 1,500 megawatts of power. And there's some possibility that there could be a number of attacks that are on separate systems, but the aggregate can well be over 1,500 megawatts. And we don't have the information about how we would resist that attack. Does FERC now have any information? And has the agency assessed the impact of a cyber attack on geographically dispersed power systems?

Mr. MCCLELLAND. Yes, FERC is—that's another matter that is under active consideration at FERC. Again, it's the content of an internal deliberation, so I can't speak to it. But it is an important aspect, and FERC has identified that as such.

Mr. WELCH. So, where do we need to be to improve our confidence about our capacity to protect the grid? I mean, we got to get to the bottom of these questions, right?

Mr. MCCLELLAND. Right. And these are subjects of active proceedings at FERC.

Mr. WELCH. All right. Well, thank you very much, gentleman.

Mr. MCCLELLAND. Thank you.

Mr. WELCH. I yield back.

Mr. LYNCH. I'm just—I'm a little bit frustrated that we can't get at these answers because we have a proceeding elsewhere. What's the nature of your—the privilege that you're claiming here?

Mr. MCCLELLAND. As an active proceeding, one that's under deliberation, as a staff member, I cannot comment on the merits and the timing of that active proceeding. And this isn't——

Mr. LYNCH. I don't think he was asking you about a certain proceeding. He was asking you about how to protect the power grid for the country.

Mr. MCCLELLAND. It was in comparison, for instance, to the NERC—I am sorry, Mr. Chairman. Mr. Chairman, it was in comparing the NERC CIP standards to the NIST framework. And this is an active proceeding at the Commission. It's under deliberation.

Mr. LYNCH. So, if we went into classified session, would you be able to discuss it then?

Mr. MCCLELLAND. I could not, Mr. Chairman. Because the content and timing of a deliberation at FERC cannot be disclosed.

Mr. LYNCH. OK. We're going to have to have you back then. The chair recognizes the gentleman—I apologize to the gentleman that it was not fruitful.

Mr. WELCH. No, you better stated my puzzlement, and I appreciate that.

Mr. LYNCH. Oh. Absolutely. The chair now recognizes the gentleman from Arizona, Mr. Gosar, for five minutes.

Mr. GOSAR. Thank you, Mr. Chairman. As you are aware, the administration released 100-day plan in April to address cybersecurity shortcomings within our electric grid. The plan tapped the Department of Energy as the lead for its implementation rather than the Cybersecurity and Infrastructure Security Agency, or CISA. Some experts like Damon Small, technical director for security consulting at NCC Group North America, has pointed out that while the current plan takes a generation and transmission of bulk power into consideration, it fails to consider distribution. Original equipment manufacturers, or OEMs that supply industrial control systems, should be a part of that conversation as well.

Joe M. Weiss, a noted control systems cybersecurity expert, argues that the real danger to the grid does not lie in the networks, but rather in the industrial controllers and the hardware, like the transformers and turbines. And that the electric grid is vulnerable to electronic triggers buried in bulk, power equipment that is predominantly sourced from China.

Contributing to this danger, engineers who manage the industrial control systems used to be responsible for their cybersecurity, but now has surrendered that function to computer engineers, why it is argued that these systems are vulnerable for being disrupted by bad actors without the normal IT alerts being founded.

The Chinese Government is installing a back door and a large transformer destined for our substation in Colorado. And a SolarWind attack is proof of the supply chain attacks that were not detected by IT network monitoring our threat intelligence. This needs to be our focus.

Mr. Kumar, what percentage of the U.S. energy grid includes components manufactured overseas?

Mr. KUMAR. Sir, thank you for the question. And understanding the supply chain of our critical energy systems is very important to us. To that end, the President issued an executive order really focused on America supply chains. And one of the key components of that is looking at those critical components, like transformers, as you rightfully noted, that are so critical to the reliability of our electric grid, and where are we manufacturing a lot of those components? And one of the key things that we have seen with large power transformers, as—sir, you certainly recognize, as we don't manufacture the large power transformers in the United States anymore. And that is a huge gap that we have as a country.

And so that is something that we're certainly going to be looking at in terms of where we are producing a lot of these critical, critical components on the U.S.—in the U.S. energy sector as part of some of that report.

Mr. GOSAR. So, to answer my question, zero are made here in the United States? They're in foreign countries, right?

Mr. KUMAR. So, when you talk about large power transformers, today, large power transformers are built abroad. You are absolutely right.

Mr. GOSAR. Thank you. So, was it necessary for the Biden administration to suspend President Trump's EO restricting the procurement of foreign electric equipment? Couldn't Secretary Granholm have been reviewed the executive order without suspending it? Mr. Kumar?

Mr. KUMAR. Thank you for that question, sir. Again, the supply chain security is of the most is a critical component of our energy sector, as I mentioned during my——

Mr. GOSAR. I understand, but isn't it—well, it wouldn't be plausible, much better off that the Secretary didn't suspend President Trump's initiative, because it would have helped us along this pathway?

Mr. KUMAR. Sir, what we found was we got feedback from the private sector that they were looking for additional clarification. So, one of the things that we have done is we want to take a more holistic approach.

One of the other things that we took into account was we had SolarWinds happen last year. SolarWinds really changed how we're thinking about supply chain threats across the board. And, so, what we wanted to do was have consistent policy that actually helped move the ball forward. And, so, this pause in that policy allowed us to seek input from the private sector, interagency, and others to really develop a stronger policy related to supply chain security. So, that's where we're focused. And we just received input through our RFI process. And we're in the process of reviewing all of the RFIs so that we can come back with a stronger approach. And I would be happy to followup with you on that, sir.

Mr. GOSAR. Yes, so, I guess my point in time here is, is that no we're suspending a lot of the necessary supply chains here in this country that can be manufactured, whether it be electronic pieces, whether it be the rare earths and copper manufacturing process pieces for these transformers and in these big aspects.

So, I mean, it seems like we're in a negative transfer abyss. That is, we're chasing our tail around and around and around. We don't

have the supply chains. We don't have the critical elements to build them. We don't have the manufacturing to build them. This is a complex issue. And time is of the essence. And it doesn't seem like we're going to be getting anywhere quick unless we fast-track this. Is that your understanding?

Mr. KUMAR. Sir, so in the interim, where we have been focusing all of our efforts is working with manufacturers directly. So, we just signed partnerships with ABB, Hitachi, Schneider, and Schweitzer. And they have come on board with DOE to test pieces of their equipment. Because reality is, a lot of this equipment, whether it's hardware or software is sourced globally. And so what we really need to get to is really working with the manufacturers and suppliers to actually engineer out a lot of the cybersecurity concerns.

So, we actually have had a lot of positive success with those manufacturers to ensure that we can actually test their equipment down to the chip level, and down to the firmer level. So, we have had a lot of success on that. And we're going to continue to do that, and we look forward to participation by some of those other manufacturers to come to the table, whether they're manufacturers of large power transformers, or SCADA equipment, or relays. Those critical components, we want to partner with them. We want to help them really ensure that they know the pedigree of their software and hardware before this equipment ever gets deployed on our electric grid.

Mr. GOSAR. And one more last question, Mr. Chairman. So, what other agencies are we working with, or are we siloing this? It seems like this is a very complex issue that transcends in different agencies. So, isn't there a great process here to work functionally with all the agencies to have a cohesive, well-planned, thoughtful process?

Mr. KUMAR. Thank you for raising that. I think it's one of the reasons that the sector risk management agency structure works so well in this country. Because what happens is, if we're focused on something from an energy perspective, we want to ensure that our partners at CISA are aware of those vulnerabilities and threats, because we want them to be looking at them across the board. We want them to be looking at chemical industrial control systems and industrial control systems in other sectors. So, we partner very closely with our colleagues at CISA.

In fact, last year, actually earlier this year, we released a really critical vulnerability in relays that was being used in a specific manufacturer. And how we released it was in close coordination with our partners at CISA to get the word out there, once we had worked with the manufacturer to find a patch.

So, you are absolutely right that we need to be working collaboratively, and that's how we do it with CISA. But we're also working with our colleagues at FERC to help inform their process. And then, of course, we work with the intelligence community because we want them to know where are the threats, where are risks in these groups of proponents so they can help us through their own missions to really help us address these risks.

Mr. GOSAR. Thank you, Mr. Kumar. And I yield back, Mr. Chairman. Thanks for your indulgence.

Mr. LYNCH. The gentleman yields back. Just a clarification on the gentleman's question and your answer. The large transformer manufacturers who are no longer operating within the United States, are they U.S. companies, or are they foreign companies?

Mr. KUMAR. Sir, it's a mixed bag in terms of——

Mr. LYNCH. So, we do have U.S. manufacturers that are manufacturing large transformers overseas?

Mr. KUMAR. So we have, for example, ABB, Hitachi.

Mr. LYNCH. Yes.

Mr. KUMAR. They're producing more of the medium voltage transformers in the United States right now. And so there are some manufacturers that are making transformers in the United States, they are just not the large power transformers. And so one of the things we would like to do is partner with them to really encourage a lot of this domestic manufacturing of those transformers. But there are other transformers that are being built by other countries out there as well, and I would be happy to followup with you with the list of those companies.

Mr. LYNCH. All right. Thank you. Thank you very much.

The chair now recognizes the gentlelady from California, Ms. Speier, for five minutes. Welcome.

Ms. SPEIER. Thank you, Mr. Chairman.

Let me ask Mr. Kumar to begin. Since 85 percent of our U.S. electrical grid relies on parts and equipment from overseas, I mean, it's prime to be somehow manipulated or compromised as a result. And I know FERC has approved a new supply chain risk management reliability, but I don't know if it goes far enough.

So, first of all, let me ask you, Mr. Kumar, are you also working with the NSA and their interface with their corporate entities outside of the intelligence community?

Mr. KUMAR. Congresswoman, absolutely. We want to take a whole-of-government approach. These challenges, particularly when it comes to supply chain challenges, are too great. We have to be leveraging the authorities, the capabilities, and the expertise across the government. And so we're absolutely working on the intelligence side with our colleagues. In the broader intelligence community, NSA is certainly included. But also in terms of protecting critical infrastructure, this is where we need to be partnering with other agencies, such as CISA, who helps us all be connected in these efforts as we look at our supply chain.

I do want to raise up an issue you mentioned, I think it's an important one, and that's looking at a lot of our components and particularly just new components that we're putting onto the grid. This is where we think it's of the utmost important to employ a philosophy in the United States of security by design, and the concept is we really need to be looking at the next generation systems.

So, to that end, what we have done is we've collaborated with DOE's Office of Energy Efficiency and Renewable Energy as we start to look at wind turbines, solar panels, nuclear generation, and, of course, fossil energy. How do we ensure that the R&D being done on those systems has cybersecurity embedded into it? So, this is a mandate that the Secretary, Secretary Granholm, has asked CESER to lead across the board, that cyber is a core component of

everything that the Department does, through the R&D at headquarters but through our national laboratories as well.

Ms. SPEIER. Thank you.

Mr. Goldstein, can you tell us about the programs that CISA has undertaken to warn critical infrastructure owners and operators about risks specific to foreign-produced equipment and software?

Mr. GOLDSTEIN. Certainly. Thank you for that question. As my colleague at DOE noted, CISA really focuses on understanding broad cross-sector risks to the Nation's critical infrastructure in close collaboration with the SRMAs that bring unique sectoral expertise for entities within their purview.

At CISA, we manage the Information and Communications Technology Supply Chain Risk Management Task Force, which is a public-private body intended to bring together the producers and developers of much of the platform technologies that we see ubiquitously utilized across sectors in order to understand the risks posed by certain technologies and also, most critically, to drive best practices to reduce supply chain risk throughout the life cycle.

Ms. SPEIER. So here—excuse me. Here's my question, though. You can have the wherewithal to provide this support and information to these many operators around the country, but if they either don't know about it or don't avail themselves of it, they become that much more vulnerable to foreign attacks. So, what are you doing to somehow lure them into a discussion and a training that will provide them that kind of information?

And then, second, have you created a list of banned foreign-produced equipment and software that is known to pose a threat to the U.S. critical infrastructure cybersecurity?

Mr. GOLDSTEIN. Certainly. As to the first question, our hope is that luring is not required. Our hope is that by communicating effectively with critical infrastructure across this country through the multiple information sharing groups that CISA administers in coordination with the SRMAs and our other partners in government, we are able to share timely and actionable information about vulnerable hardware and software that may need to either be mitigated or replaced.

And our focus here really is on the vulnerabilities as opposed to the foreign providence in the first instance. And by sharing information about vulnerable technology assets, that then enables an infrastructure owner-operator to take concrete steps to address a particular risk in their environment.

To your second question, ma'am, there is not currently a list maintained by CISA of banned technology assets for critical infrastructure. It does bear noting that Congress recently created the FASC, which is an interagency body intended to assess the risk of foreign-produced vulnerable devices in Federal networks and has the authority to issue exclusion orders for those assets. That body is active now, and presumably an exclusion order issued by the FASC could be taken up by sectors across critical infrastructure or by sectoral regulators.

Ms. SPEIER. All right. Thank you.

Let me just conclude by urging all of you to recognize that we are the last to respond more often than not. Huawei was operational in this country for over 10 years before we finally got the

message that they shouldn't be allowed to do so. ZTE is yet another example. We are very late in doing what we should do early on, and I just hope that you recognize your responsibility to act swiftly when there is either known or suspected foreign intrusions and/or equipment that poses a problem to us.

With that, Mr. Chairman, I yield back.

Mr. LYNCH. The gentlelady yields back.

The chair now recognizes the gentleman from Georgia, Mr. Johnson, for five minutes.

Mr. JOHNSON. Thank you, Mr. Chairman, and thank you for holding this very important hearing.

And if I can pull my questions up here.

OK. It was not long ago that a cyber attack on Colonial Pipeline, a company located not far from my district, disrupted the lives of millions and threatened our economy. This was just one of the many recent attacks which have raised serious concerns about America's ability to defend its critical infrastructure and economy from cyber threats. But these attacks have also presented opportunities to learn and to harden our defenses.

One lesson is crystal clear: Information sharing between the government and the private sector is absolutely essential to defending our Nation against cyber attacks. This is absolutely true for electric utilities, and for this process to work, private utility companies must quickly and fully disclose any cyber intrusions on their systems to the Federal Government.

Mr. McClelland, I understand that under current NERC reliability standards, electric utilities are required to report certain cyber incidents to the Federal Government. Is that correct?

Mr. MCCLELLAND. That is correct, Representative.

Mr. JOHNSON. And can you describe for me the types of incidents that must be reported and why utilities are not required to report all incidents?

Mr. MCCLELLAND. The attacks—as I understand the requirements, the standard, the attacks require the utilities, the applicable utilities to report either successful cyber intrusions or cyber incidents that may not have constituted a cyber intrusion but they were threats to the utility system.

Mr. JOHNSON. How effective has this requirement proved to be in practice?

Mr. MCCLELLAND. The requirement is relatively new. I'm not familiar with the results, but I'd be happy to take that as a question for the record and provide a followup answer for you.

Mr. JOHNSON. Well, thank you. I appreciate that.

And to all of the witnesses, does the government have data on incidents that go unreported?

Mr. GOLDSTEIN. Thank you, Congressman. It's a great and important question, and the answer is we don't have enough data. We know that there are still across sectors a number of intrusions today that are not reported to the U.S. Government, either to CISA, to an SRMA, or to Federal law enforcement, and this presents a few problems.

First, it precludes the government, including CISA, from offering assistance to the victim. It limits our ability to develop actionable information that could be used to protect other victims before simi-

lar events occur, and it limits our ability to understand the extent of national risk, for example, adversary campaigns that are emerging across sectors of the economy.

As you may be aware, CISA recently worked with TSA to establish a security directive requiring reporting of incidents affecting certain pipelines to CISA, but even so, this sector-by-sector approach may in itself not reach the breadth of reporting that the U.S. Government needs to understand national risks.

And for that reason, we very much look forward to working with Congress to ensure that there's incident reporting legislation passed into law that would provide the breadth of reporting needed to understand and manage these significant threats.

Mr. JOHNSON. Well, Mr. Goldstein what mechanisms does the government have to enforce these reporting requirements? How often are they used and how effective are they?

Mr. GOLDSTEIN. I'm very sorry.

Mr. JOHNSON. Do I need to repeat that question?

Mr. GOLDSTEIN. Yes, sir. If you wouldn't mind, that would be great. I appreciate it.

Mr. JOHNSON. OK. What mechanism does the government have to enforce these reporting requirements? And how often are they used and how effective are these enforcement requirements, enforcement mechanisms?

Mr. GOLDSTEIN. Got it. Thank you, sir. It's a great question.

So, one challenge today is there is no blanket reporting requirement for businesses or critical infrastructure in this country. Instead, these reporting requirements are generally sectoral and enforced by the unique authorities of a given regulator. And so, for example, the enforcement authorities that FERC may be able to levy would be dramatically different than the TSA or the Federal Reserve Board. And so absent a common reporting regime and a common mechanism of enforcement, it is difficult to assess the efficacy and to ensure that the breadth of reporting is coming in to CISA and thereby to our partner agencies.

Mr. JOHNSON. Thank you, Mr. Goldstein.

From CISA's perspective, are the current NERC reporting standards comprehensive enough or do we need additional mandatory reporting requirements for electrical utilities?

Mr. GOLDSTEIN. So over—as a broad question, there are two challenges with reporting requirements today. The first is, because they have developed sector by sector, they have divergent requirements, for example, the definition of an incident, as well as the timeframe for reporting and the content of a report. And then, as we've discussed, the fact that they are currently sectoral means that they are incomplete and do not cover the breadth of organizations that should be reporting to the Federal Government when they have an intrusion that could impact the sort of national critical function that we care so much about.

Certainly, the existing NERC standards, as my colleague noted, are fairly new. Our understanding is that they do provide the necessary degree of data and that reporting does come to CISA as defined in the regulation, but, of course, you know, there may be other aspects of the energy grid for which additional reporting

would be beneficial to help the U.S. Government understand the breadth of risks, which is a commonality that we see across sectors.

Mr. JOHNSON. Mr. Goldstein, should electrical utilities be obligated to give CISA access to systems to conduct forensic analysis in the wake of an attack?

Mr. GOLDSTEIN. Thank you, Congressman. Our perspective is that it is critically important for the U.S. Government to have access to information about cybersecurity intrusion subsequent to a security incident. This allows us to glean information that we can use to protect others. It also allows us to understand if the intrusion is correlated to, for example, a nation-state campaign that's affecting multiple sectors.

One way of enabling that information is by providing CISA with the ability to conduct incident response or threat hunting services for a victim. That is a service that we are ready, willing, and frequently provide. But it is also the case that if a victim organization chooses to bring in one of the many highly qualified commercial incident response firms, that is perfectly reasonable as well. The key part is that CISA then gets information from that incident response that we can use to do our job and protect others.

Mr. JOHNSON. Thank you.

Any additional authorities necessary to respond to and deter any cyber attacks?

Mr. GOLDSTEIN. Thank you, Congressman. So, I think we've discussed here the main one, which is broader requirements for incident reporting for significant cybersecurity incidents across this country. That will go a long way toward helping, not only CISA, but our partners at the SRMAs and Federal law enforcement understand the breadth of cybersecurity risks we are seeing and take urgent action response.

Mr. JOHNSON. Thank you.

Mr. Chairman, I believe my time has expired, and I appreciate the additional time.

Mr. LYNCH. OK. The gentleman yields back.

Let me just ask, to followup on the gentleman's question. In my district, we had a couple of incidents where a gas line inadvertently released gas into the general community. We had the FBI come in. I didn't have them come in, but they came in pursuant to the pipeline operator's request.

Would the FBI be a—would they have a data base, or would they be a repository of some of these incident reports if they are called in to investigate?

Mr. GOLDSTEIN. So, we work extraordinarily closely with the FBI every day. We conduct joint incident response together. We notify victims together. You know, our general rule as a government is a call to one is a call to all, and I think that actually now works very well in practice. But even the FBI, even given their breadth of personnel in the field offices across the country, still has certainly insufficient visibility into cybersecurity intrusions. And so some entities today call CISA, some call the FBI, some may call an SRMA.

You know, we need a cohesive approach to this problem as a country that is going to ensure that we actually understand the nature of the threat we are seeing, we understand how our adversaries are breaking into networks across critical infrastructure, we

are helping to prevent similar attacks before they occur, and we are understanding the potential impacts of critical functions before they manifest and result in service disruptions that could harm the American people.

Mr. LYNCH. OK. Thank you.

The chair now recognizes the distinguished gentleman from Rhode Island, Mr. Langevin, for five minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

First, I want to thank you for the accommodation allowing me to waive on to the committee for the purpose of asking questions at the hearing, and I want to thank you for your leadership on cybersecurity. I know how serious you take this issue, and we appreciate the leadership of these gentlemen and the work that we have been able to collaborate on together.

Likewise, I would like to thank the panel for their testimony this afternoon, the work that you're doing to try to protect the Nation against cyber threats, especially those of significant consequence.

That said, Mr. Kumar, I just wanted to followup on a line of questioning. You talked about the different power generation piece of equipment, some that are produced here, others, the larger ones, that are produced overseas, if I understood all of that correctly. And given the fact that these are not like batteries that sit on a shelf and you just, you know, pop one in and out easily if something becomes disabled, and understanding the Aurora threat, where for the first time back in 2007 saw how a cyber attack through a data intrusion could cause physical damage to a turbine, would not it be wise to have a, say, industry strategic national stockpile of additional power generation equipment of a certain number that, were a turbine or series of turbines be destroyed, that we would have the ability to reconstitute quickly as opposed to these things take months to build, ship, and install, and not having some on hand? Have we done any of that? Are we thinking about it in those terms?

Mr. KUMAR. Thank you for the question, sir. So, the Department did do research in this case. We looked at whether a strategic transformer reserve made sense in the country. So, we actually did a series of reports, and we worked very closely with our industry partners to really look at what are the challenges when it comes to bringing in these critical pieces of equipment, as you rightfully identified. And so what we found through a lot of that reporting was we should be thinking about strategic transformers and the sharing of transformers.

And so to that end, since writing some of these reports, the industry itself has set up three different programs in the electricity industry to really share transformers during an emergency. It's Grid Assurance, SpareConnect, and the STEP program. These programs allow one utility to share a transformer with another utility. Grid Assurance goes a step further. It actually goes beyond just transformers. It's looking at relays and other critical equipment.

So, our hope is, as we start to identify these critical pieces of equipment, particularly ones perhaps that are long lead kind of equipment, how do we inform that back to the private sector so they can continue developing these mechanisms to have these types of reserves.

The government's role, another portion that we feel like we need to address and help with is these large power transformers are 200 to 300 tons, and what we often find is the logistics of moving a transformer at 20 miles an hour, maybe less, across from one part of the country to the other is a huge challenge of moving such a large piece of equipment. So, the focus we've had is working with our colleagues at the Department of Transportation, of course the states, to really understand the logistics of moving these large power transformers from point A to point B.

The other piece that I referenced earlier, sir, is that we need to really look at domestic manufacturing. How do we incentivize some of that domestic manufacturing of these critical components in the United States? I know that is a key focus of Secretary Granholm as we start to develop this report regarding America's supply chains, and so there's going to be more to come on that.

Mr. LANGEVIN. Thank you. I think it's an important issue to address.

Director Goldstein, thank you for being here. As you know, I'm a big proponent of the Joint Cyber Planning Office currently being stood up at CISA, and I think the JCPO will be critical for bringing the interagency, including the Department of Energy and the private sector, together to coordinate planning and exercises to protect critical infrastructure like the grid.

So, Director Goldstein, can you give us a status update on JCPO? In addition, how do you view the planning and exercise function of the office fitting in with other operations and analytics functions carried out by CISA?

Mr. GOLDSTEIN. Thank you for the question, sir. And as always, thank you for your work on behalf of our national cybersecurity mission. We are deeply grateful every day for it.

We continue to make progress in implementing critical function which, as you note, is going to be foundational to our ability to prioritize, plan for, exercise, and then execute coordinated cyber defense operations with government and the private sector. We are preparing now for our initial launch of the organization, which will involve multiple private sector companies as well as our partners across the interagency, and we intend for that work to be really a pilot for what this effort will be able to do when it scales forward.

The way that I would think about this for broader integration is this will be our effort to, in the first instance, understand what are the most significant risks that we care about managing as a national cybersecurity community, with CISA, of course, at the helm for civilian cyber defense; how do we develop plans jointly with the interagency and with industry to understand how we mitigate the plans——

[Audio interruption.]

Mr. LYNCH. Someone's got a live mic. We ask all members to mute.

Mr. GOLDSTEIN. Thank you, sir. My apologies.

Mr. LYNCH. Thank you. You may proceed.

Mr. GOLDSTEIN. Thank you.

Once we have our list of prioritized risks, develop joint plans with government and the private sector, exercise those plans in the same joint manner between industry and the private sector, and

then when a risk manifests, execute those plans to ensure that we are taking collective action to mitigate risks to entities that could be harmed.

So, if we think about layering this in with our existing model for cyber defense operations, you know, we could envision a planning sprint focused on certain risks through the energy sector, where we would ensure that CISA's asset response capabilities, DOE's expertise as the SRMA, and then our partners in industry, but not just industry in the energy sector, but cross-sector entities in the private sector, are all coming together saying, when the bad day that we've discussed today occurs, how do we take joint action to ensure not only that we're minimizing the impacts to the energy sector but we are understanding and proactively addressing cross-sector impacts; bringing together team members from government and the private sector to do this work, both in person and via our analytics platform that we are developing for joint collaboration, in coordination with the interagency and our partners across industry.

So, this really will be the formalization of CISA's critical role in leading civilian cyber defense for the country, but it's a role that we can't do alone and requires the robust collaboration from day one with the SMRAs, with our other partners, including Federal law enforcement and the intelligence community, and perhaps most critically, the private sector who, of course, are going to be the executors of so much critical work to mitigating the risk.

Mr. LANGEVIN. Thank you very much.

Mr. Chairman, I had two additional questions, but I could submit those for the record.

Mr. LYNCH. You can fire away, Jim, if you want.

Mr. LANGEVIN. OK. Thanks, Mr. Chairman.

So, Director Goldstein, last year's NDAA also required us to develop a Continuity of the Economy plan. So, this plan will govern how we respond to and recover from a significant disruption to our economy, thinking of in terms of what to prioritize first if the bad day happens and what do we need to get up and running first to keep our economy on track, you know, one perhaps epitomized by a cyber attack on the power system.

So, our intent in drafting this provision was that CISA, including the cybersecurity division and the National Risk Management Center, would play a key role in drafting the report. Can you give me an update on where things stand with the Continuity of the Economy plan?

Mr. GOLDSTEIN. Excellent. So, certainly, we share your focus about the need to robustly consider and plan for Continuity of the Economy under all conditions. I think it is symbatic underlining much of what we discussed today. I understand that the administration is still considering the appropriate way to implement that provision in the NDAA, but certainly I recognize the urgency and importance of this kind of work and would be glad to get you an update for the record on progress in making that decision.

Mr. LANGEVIN. Thank you.

I really do hope to see movement from the White House study on this. Maybe even the actual cyber director can take the reigns. And I hope this subcommittee, Mr. Chairman, will keep on this issue as well.

The last question I had, Director Goldstein, we've also discussed the report required by section 9002 of last year's NDAA in Sector Risk Management Agencies, or SRMAs. As you know, the report was due July 1. Though I appreciate Director Easterly was only recently confirmed and might need some time to review it, our goal, with the clarification of the roles and responsibilities of SRMAs, was to empower them to fulfill their jobs, while also ensuring CISA gets the support it needs, whether in terms of risk data or incident response coordination.

How do you see, Director, the relationship between DOE and CISA evolving in light of section 9002 and the forthcoming report?

Mr. GOLDSTEIN. Absolutely. So, we are urgently working on the report, and we appreciate the patience, as we make sure that we get it right, because, as you know, this is critically important work that really is foundational for delineation of not just roles but also resources, capabilities across agencies in managing this, a significant risk.

CISA and DOE have an extraordinarily close relationship. You know, in general, CISA sees ourself—and I should speak to the mission element of CISA, because CISA, of course, is also an SRMA for multiple sectors. But the mission delivery portion of CISA in cybersecurity that I'm privileged to lead, we see ourselves as a service provider to sectors to give them actionable information, cybersecurity services, incident response assistance upon request, and understanding cross-sector dependencies that could affect the provision of sectoral functions and, thereby, cause impacts to the American people.

DOE, of course, has extraordinary expertise, as we've offered today, on understanding both nuance dependencies and relationships within the sector, the nature in which a cybersecurity intrusion could impact sector entities, and the ability uniquely to actually understand productivity that is manifesting in the sector.

And so our goal working with our partners in DOE is first and foremost to make sure that we are robustly sharing information so that the cross-sector information that CISA has, including information, of course, from Federal civilian networks, we are sharing with our partners at DOE, we are sharing with our partners in the energy sector, so that when we are seeing a threat manifesting in the Federal Government or a different sector, it can be used to protect partners across the energy grid.

Additionally, as my colleague, Mr. Kumar, has discussed today, DOE is engaged in a variety of activities focused on understanding supply chain risks, resilience issues within the energy sector. That is all work that CISA is executing at a cross-sector model to understand risks across the board. And so the more that CISA and DOE can work together on ensuring that lessons we are learning from the energy sector can be generalized broadly and ensuring that we are providing cybersecurity services to the energy sector in deep coordination with DOE, the sector will be stronger but, more importantly, we will be stronger as a Nation.

Mr. LANGEVIN. Thank you.

Mr. Chairman, thank you very much for the generosity and the time, and I yield back.

Mr. LYNCH. The gentleman yields back.

Mr. Kumar, just to clarify on your answer to Mr. Langevin, Chairman Langevin, he asked you about these very large transformers. As a former ironworker, I've had the opportunity to try to move some of those transformers. It is a traffic-stopping operation. I appreciate the difficulty. But I think the wider question is about redundancy. And so, we don't have to move transformers around in order to get them online.

Is there—so rather than looking at it from an inventory situation where we have transformers that can be brought in, what about redundancy where we have capabilities or the capacity that can be brought online for very, very important national security purposes, especially here in the D.C. area? I mean, where do we stand on that in terms of redundancy that might be brought online in the event that one of these large generating facilities gets taken down?

Mr. KUMAR. Sir, thank you for that question. It's—really the concept of resiliency and redundancy are really core to how we're thinking about these problems. We first must understand the risk to the sector and then start to build some of that resiliency and redundancy into it, so that if you do have a situation, as you mentioned, with a transformer going down, how do we ensure we still have those critical functions, those critical facilities, like military installations that continue to serve power to those installations.

So, what we're looking at is we're really looking at an all-of-the-above strategy. One of the options that we're thinking about is what's the role of solar, wind, energy storage, nuclear generation that can be brought in to actually create a microgrid and actually develop resilience into cities and states and, in particular, serve the critical facilities, like military installations.

So, we really need to build in that resilience into the grid so that if we do—if we are impacted by an incident, we can have another source of generation to continue having us going forward. So, that's how we're really thinking about this problem broadly.

Mr. LYNCH. Thank you.

The chair now recognizes the very patient gentlelady from Florida, Ms. Wasserman Schultz, for five minutes.

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman.

Mr. Chairman, according to a March 2021 GAO report, electrical distribution systems, the systems responsible for delivering our electricity from transmission lines to consumers and businesses across America, quote, faced significant cybersecurity risks. And as more and more homes, businesses, and smart devices are connected to electrical distribution systems, the exposure and complexity of these systems grows, rendering them, quote, increasingly vulnerable to cyber attacks.

The electricity in many large cities across the United States is provided by a single distribution utility. If a distribution utility servicing a major city like New York or Miami were to be the victim of a cyber attack, the consequences could be devastating. In fact, GAO found that—and I quote—even if a cyber attack on the grid's distribution system did not impact the bulk power system, such an attack could still have significant national consequences.

Yet, despite this, distribution utilities are not subject to any Federal cybersecurity regulations. The NERC reliability standards

apply only to electrical generation and transmission systems, while distribution systems are regulated at the state and local level.

Mr. Kumar, given the growing cyber threats to distribution systems, do you think there should be mandatory Federal cybersecurity standards for electrical distribution systems?

Mr. KUMAR. Thank you for the question, Congresswoman. This is certainly an increasing and complex threat. As you rightfully talked about, we are integrating more and more, whether it's distributed energy resources, we're connected more, and it's all happening at the distribution level. And so what we are focused on, we, as DOE, do not have the regulatory authority in terms of the distribution system. I would certainly defer to my colleague at FERC regarding regulatory authorities. But where we're focused is the states do have regulatory authority over the utilities at the distribution level.

And so where we've been focusing our efforts on really educating the state public utility commissions about the threat, No. 1; then, No. 2, providing them with the tools that they can use to then look at the cybersecurity investments of the utilities at the distribution level within their cities, states, and communities.

And so that's where we're focusing a lot of our efforts is to really help those states who have the ultimate regulatory authority to do more in that space.

We also offer a tool called C2M2 that is applied to distribution, transmission, and generation facilities. Any utility of any size can use this tool to gauge its cybersecurity posture today, and they can actually see where they land in terms of their cybersecurity posture and then make the necessary investments to their cybersecurity using these tools that we provide to the states.

Ms. WASSERMAN SCHULTZ. OK. And I would like to hear what Mr. Goldstein thinks.

Mr. GOLDSTEIN. So, as a general point—and thank you for that question, ma'am. I do appreciate it.

As a general point, efforts that we can take as a country to drive adoption of better security controls would lead to improvements to our national security, economic security, public health and safety. There are a number of roads that we can take to that outcome, and I would defer to the sectoral expertise of my colleagues at DOE and FERC to consider which incentives are most appropriate for distribution entities. But, in general, we know that we need to take steps to catalyze urgent investment in better security. Certainly, regulation and standards is one path to that end. There may be other incentives that could also enable the same investment.

And I would just note one example. You know, there are certainly bills proposed in Congress that would enable broader cybersecurity grants that is also an additional method to catalyze more cybersecurity investment and certainly one that CISA supports. And so the end state that we seek is better security. I think given the nuances of a given sector and even given entities within a sector, the particular package of incentives to reach that goal may differ.

Ms. WASSERMAN SCHULTZ. OK. And continuing in the same risk category, despite growing cyber risks to electrical distribution systems, GAO also found in its March 2021 report that DOE's current

cybersecurity strategy for the electric grid does not fully address risks to distribution systems. DOE officials have argued that the Department is prioritizing the security of the bulk power system, asserting that a cyber attack on a distribution system would likely be, quote, less significant than an attack on the bulk power system.

However, GAO also found that DOE has not conducted any up-to-date assessment of the impacts of a cyber attack on distribution systems or whether such an attack could affect the wider bulk power system.

Mr. Kumar, how can DOE be sure that an attack on one or more electrical distribution systems would be relatively insignificant if it has not studied the likelihood and potential impacts of such an attack? And will you commit to conducting an updated assessment of the potential scale and impacts of an attack on electrical distribution systems and report your findings back to Congress?

Mr. KUMAR. Congresswoman, I appreciate the question. We are absolutely focused on the distribution system. I've read the GAO report, and we are taking actions today to really look at the distribution system.

One of the key things that we're doing today is we've partnered with our Energy Efficiency and Renewable Office and our Office of Electricity to really think about the distribution systems and how do we embed security by design into those next generation systems at the distribution level.

We're also working with our state PUCs, as I mentioned, and the goal here is really understand the threats. And what we find is there may be a mismatch in understanding what the threat is so that we can then inform requirements.

At a very basic level, you know, we are encouraging things like the NIST cybersecurity framework that Congressman Welch had mentioned. We think that's a great tool to actually look at your cybersecurity posture as a utility, whether you're a distribution utility or a transmission utility.

Ms. WASSERMAN SCHULTZ. Well, I mean, I appreciate your commitment to looking at the GAO report, and once you do that, will you commit to conducting an updated assessment of the potential scale and impacts of an attack on electrical distribution systems and report your findings back to Congress?

Mr. KUMAR. We can do that, ma'am.

Ms. WASSERMAN SCHULTZ. Thank you.

And, Mr. Chairman, I guess, if you don't mind, 30 more seconds.

Mr. LYNCH. Of course.

Ms. WASSERMAN SCHULTZ. Thank you.

Distribution systems are the systems on which Americans rely to bring electricity to their homes and businesses, because I know that's not terminology I'm familiar with, so providing a definition is pretty important. You know, those are the systems that light our streets and run our trains.

In Florida, we actually experienced a close call earlier this year when hackers breached the computer system operating a water treatment plant and boosted chemicals to dangerous levels. And now, luckily, a human operator was able to intervene before any damage was done. But this frightening attack demonstrates the

damage that can be done if a malignant actor wants to impact public safety.

So, it's critically important for DOE to conduct a cybersecurity assessment of our electrical distribution systems so we can address any persistent vulnerabilities before they can be exploited and people can be harmed. So, I appreciate the opportunity to talk about that at this hearing.

I yield back.

Mr. LYNCH. The gentlelady yields back. Her points are well taken. Thank you.

As we close, I would like to recognize the gentleman from Wisconsin for any concluding remarks.

Mr. GROTHMAN. Yes. I'd like to thank you for having this hearing. You know, we didn't have a huge turnout here, and it's the type of hearing that I guess is kind of boring, except for all of a sudden it was the most important hearing we ever had if something disastrous would happen sometime in the next year.

Is it OK if I ask Mr. Kumar just one more question?

What you said kind of concerned me. It concerns me in a wide variety of places the things we don't make in this country, but I wondered if you'd share with us where the large transformers are made. And if we were subject to a cyber attack, is there anything we would need to repair the damage that is not made in this country?

Mr. KUMAR. Sure. Thank you for that question. I can take that back in terms of where the large power transformers are made and provide that back to you in terms of a QFR, if that works for you, sir.

Mr. GROTHMAN. That's fine and wonderful.

OK. Again, I'd like to thank you for being here. And I've often felt that this sort of thing is such a very important issue, and it's never going to be in the paper until some disaster happens and then people say, where was Congress. So, thanks for having it and maybe——

Mr. GOSAR. Glenn? Glenn, would you yield? This is Congressman Gosar.

Mr. GROTHMAN. Sure.

Mr. GOSAR. Mr. Chair, one of the things—I know it says cybersecurity is the issue today, but what about when a foreign actor owns the utility that accesses the grid? I mean, I'm thinking about a lot of these solar fields that are operated by foreign actors. And what oversight do we have for them? Because you could actually have a systemic shutdown from within the owned grid system because of that access. Have we ever considered any of that, Mr. Chairman?

Mr. LYNCH. I'd refer that question to our witnesses.

Mr. GOLDSTEIN. Certainly. Thank you for the question, sir.

So, there are certainly processes in place. I would call out the Committee on Foreign Investment in the United States, or CFIUS, that is intended just for this purpose, to assess the national security risk of foreign investment in critical infrastructure or other assets that could be critical to national security, economic security, et cetera. I certainly cannot speak to foreign investment in any particular energy entity or utility, but the U.S. Government does have structures in place to evaluate this sort of foreign investment

and bar acquisitions or put conditions thereupon if national security risks are identified.

Mr. GOSAR. That's if they're identified, right?

Mr. GOLDSTEIN. I'm sorry, would you remind repeating that?

Mr. GOSAR. Yes. That's if they're identified. If they run under the radar, I mean—I mean, it depends a lot on the state oversight, if I'm not mistaken, right?

Mr. GOLDSTEIN. So, in general, it is certainly the case that risks would need to be identified as a part of the assessment process. There are processes in place to assess, to identify foreign acquisitions. There are reporting requirements thereof, and there are processes that are administered on an ongoing basis to assess the risks posed by such acquisitions, and, again, preclude acquisitions or put conditions thereupon if such risks are deemed dilatory to national security.

Mr. GOSAR. I will followup with some questions to find out that systematic oversight. Thank you.

Thank you, Mr. Chairman. And thanks, Glenn.

Mr. LYNCH. The gentleman yields back.

Mr. GROTHMAN. That said, maybe sometime we can do something in the future on this, maybe in a more secure location, but thanks again for having the hearing.

Mr. LYNCH. I thank the gentleman.

Before we close, I have a quick housekeeping matter. I'd like to ask unanimous consent to enter into the record a written statement submitted by the American Public Power Association and the National Rural Electric Cooperative Association.

So, without objection, so ordered.

Mr. LYNCH. I think at this point our witnesses have suffered enough. So, in closing, I want to thank our panelists for their remarks. I want to commend my colleagues for their participation in the important conversation that we have had about the vulnerability of our electrical grid.

With that, without objection, all members will have five legislative days within which to submit additional written questions. And I know there are some questions outstanding that we've had commitments during the hearing. But in any event, all members will have five legislative days within which to submit additional written questions for the witnesses through the chair which will be then forwarded again to the witnesses for their response, and I ask our witnesses to please respond as promptly as you are able.

And, with that, this hearing is now adjourned.

[Whereupon, at 4:53 p.m., the subcommittee was adjourned.]