

**THE FEDERAL AND NON-FEDERAL ROLE
OF ASSESSING CYBER THREATS TO AND
VULNERABILITIES OF CRITICAL WATER
INFRASTRUCTURE IN OUR ENERGY SECTOR**

HEARING
BEFORE THE
SUBCOMMITTEE ON
WATER AND POWER
OF THE
COMMITTEE ON
ENERGY AND NATURAL RESOURCES
UNITED STATES SENATE
ONE HUNDRED EIGHTEENTH CONGRESS
SECOND SESSION
APRIL 10, 2024



Printed for the use of the
Committee on Energy and Natural Resources

Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON ENERGY AND NATURAL RESOURCES

JOE MANCHIN III, West Virginia, *Chairman*

RON WYDEN, Oregon	JOHN BARRASSO, Wyoming
MARIA CANTWELL, Washington	JAMES E. RISCH, Idaho
BERNARD SANDERS, Vermont	MIKE LEE, Utah
MARTIN HEINRICH, New Mexico	STEVE DAINES, Montana
MAZIE K. HIRONO, Hawaii	LISA MURKOWSKI, Alaska
ANGUS S. KING, JR., Maine	JOHN HOEVEN, North Dakota
CATHERINE CORTEZ MASTO, Nevada	BILL CASSIDY, Louisiana
JOHN W. HICKENLOOPER, Colorado	CINDY HYDE-SMITH, Mississippi
ALEX PADILLA, California	JOSH HAWLEY, Missouri

SUBCOMMITTEE ON WATER AND POWER

RON WYDEN, *Chair*

BERNARD SANDERS	JAMES E. RISCH
CATHERINE CORTEZ MASTO	MIKE LEE
JOHN W. HICKENLOOPER	JOHN HOEVEN
ALEX PADILLA	BILL CASSIDY

RENAE BLACK, *Staff Director*
SAM E. FOWLER, *Chief Counsel*
SARAH KESSEL, *Professional Staff Member*
JUSTIN J. MEMMOTT, *Republican Staff Director*
PATRICK J. MCCORMICK III, *Republican Chief Counsel*
JACK HOLT, *Republican Junior Counsel*

CONTENTS

OPENING STATEMENTS

	Page
Wyden, Hon. Ron, Subcommittee Chair and a U.S. Senator from Oregon	1
Risch, Hon. James E., Subcommittee Ranking Member and a U.S. Senator from Idaho	2

WITNESSES

Turpin, Terry, Director, Office of Energy Projects, Federal Energy Regulatory Commission	4
Wright, Virginia, Cyber-Informed Engineering Program Manager, Idaho National Laboratory	14
Aaronson, Scott, Senior Vice President, Security and Preparedness, Edison Electric Institute	27

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Aaronson, Scott:	
Opening Statement	27
Written Testimony	30
Responses to Questions for the Record	52
Risch, Hon. James E.:	
Opening Statement	2
Turpin, Terry:	
Opening Statement	4
Written Testimony	7
Responses to Questions for the Record	46
Western Governors' Association:	
Letter for the Record	54
Policy Resolution 2022-05	55
Wright, Virginia:	
Opening Statement	14
Written Testimony	16
Responses to Questions for the Record	48
Wyden, Hon. Ron:	
Opening Statement	1

**THE FEDERAL AND NON-FEDERAL ROLE
OF ASSESSING CYBER THREATS TO AND
VULNERABILITIES OF CRITICAL WATER
INFRASTRUCTURE IN OUR ENERGY SECTOR**

WEDNESDAY, APRIL 10, 2024

U.S. SENATE,
SUBCOMMITTEE ON WATER AND POWER,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m. in Room SD-366, Dirksen Senate Office Building, Hon. Ron Wyden, Chair of the Subcommittee, presiding.

**OPENING STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON**

Senator WYDEN. The Subcommittee will come to order, and today we are going to be looking at critical infrastructure sector issues, particularly threats and cybersecurity. I also want to thank the Ranking Minority Member. We have had really good cooperation with the staff on this and that's how it should be.

The dams that generate our hydropower are no exception to the serious set of threats that we are facing in cybersecurity, generally. Countries like China and Russia present a significant national security concern, as they have the ability to shut down core functions of our society, and even cause death, by hacking critical infrastructure.

Today, the Subcommittee is being told by the Federal Energy Regulatory Commission, which licenses 2,500 dams, that the dams responsible for well over half of the non-federal power generation have not received a cybersecurity audit. And currently, there is no plan to complete these missing audits any time soon. FERC has told my staff—we want to thank them for their cooperation and the forthcoming way in which they have handled this—they have told my staff that they simply don't have the ability to review the remaining dams within the next decade. A big part of the challenge is that FERC has just four cybersecurity experts to oversee 2,500 dams. Today, there are no minimum standards, no audits of a majority of dams, and bad cybersecurity. That is inviting cybersecurity trouble in the Pacific Northwest.

As the Chairman of the Subcommittee responsible for dams, I don't want to sit around and wake up to a news report about a small town in the Pacific Northwest getting wiped out because of a cybersecurity attack against a private dam upriver. FERC cyber-

security rules only apply to dams that are remotely managed over the internet. This practice enables companies to save money by not requiring an operator on-site. Those cost savings for the dam operator lead to significantly greater cyber risks. In addition, there are no mandatory cybersecurity requirements for dams only administered by on-site operators. To make matters worse, FERC cybersecurity rules have not been updated since 2016, they aren't specific enough, and are mostly about paperwork and checking boxes. FERC doesn't have the resources it needs to be an effective regulator of the cybersecurity of private-sector-run dams. This is a problem for the Congress to address.

Now it's time for Congress to step up. The seriousness of cyber threats to critical infrastructure has been clear for years. Companies and agencies across the Federal Government have been slow to respond to the cyber threats, which are the result of a combination of factors, including weak regulation, no audits, and no accountability. For example, last year I asked the Department of Homeland Security Cyber Safety Review Board to look into the theft of senior government officials' emails from Microsoft servers. DHS published the board's report last week, which documented numerous cybersecurity problems that seriously undermine U.S. national security. Microsoft software is used widely across the U.S. Government and industry. And if you look at these practices, which we have seen for years now, they are undermining America's cyber defenses and creating a serious threat to national security.

One of the central issues is that the United States does not have a more coordinated approach to cybersecurity. The cybersecurity of each part of our society is regulated in a different way, and some end up not being regulated at all. Some have rules. Some have the honor system. My own view is, this is not good enough. So there is no wonder that there are broad parts of our government and society with awful cybersecurity, no effective rules, and no cyber safety regulatory efforts. The Congress needs to address cybersecurity broadly rather than playing whack-a-mole one industry or agency at a time. Unfortunately, we can't solve the biggest problem in this Subcommittee. We can accelerate updating FERC's cybersecurity standards, making sure those standards are effective and apply to all dams. That will help protect the United States from a serious national security threat.

I look forward to working with our witnesses and all members of the Committee to deal with this scope and scale of an enormous challenge in our hydroelectric systems and others so the Congress is equipped to develop targeted responses. Before I yield to Senator Risch, I want the record to note, and I guess I talked for about seven minutes, and I didn't hear anybody talk about is this a Democratic approach or a Republican approach. This is an American approach. And I intend to work very closely with the Ranking Minority Member, my friend from the Pacific Northwest, Senator Risch.

**OPENING STATEMENT OF HON. JAMES E. RISCH,
U.S. SENATOR FROM IDAHO**

Senator RISCH. Well, thank you, Mr. Chairman. You and I have served together for many years, not just on this Committee, but

also both of us are senior members of the Intelligence Committee, and cybersecurity has certainly been in our wheelhouse. With that in mind, it is only fitting that we meet to discuss the two topics as pertinent as hydropower and energy security and resiliency in this Committee meeting.

I have here, as a witness, Ms. Virginia Wright, who is the Cyber-Informed Engineering Program Manager at the Idaho National Laboratory. Glad to have her with us. But also, Mr. Chairman, you should know that Mr. John Wagner is here, who is the Director of the Idaho National Laboratory. The INL, as most people know, is the flagship laboratory, not only in the United States, but the world and the universe for nuclear energy. Interestingly, what most people don't know is that the INL is quickly becoming also the flagship laboratory for cybersecurity matters, and as big as the nuclear issue is there and has been since shortly after World War II, the budget for cybersecurity is increasing. And within a few years, or maybe even less, the budget for cybersecurity at that lab is going to overtake the budget for nuclear. So the Idaho National Laboratory is a big deal for Idaho, it's a big deal for America, and certainly, it's a big deal in the field of cybersecurity.

You know, it's really impossible to overstate the importance of dam infrastructure in Idaho. Dams have allowed us in Idaho to transform desert into fertile farmland, account for flood control, and transport commodities far beyond Idaho, and are critical to meeting our growing energy demands. Hydropower accounts for over half of our in-state electricity generation and contributes significantly to affordability. Idaho boasts the fourth lowest electric rates in the country, thanks in large part to hydropower, which, of course, dams are critical to. We've got an array of federal, local, and private dams ranging from a couple of kilowatts to the Brownlee Dam, operated by Idaho Power, on the Idaho-Oregon border, which is the largest generation capacity of any privately owned dam in America. Besides being a clean, renewable, and affordable resource, hydropower is also integral to our security and resiliency. Hydro facilities provide dispatchable, always-on power with the ability to ramp up in the case of extreme weather events and stabilize the grid. Additionally, many hydropower facilities are black-start capable, meaning they can quickly come back online after an incident without the need for external power from the grid. Hydropower fulfills a backstopping role in so much of our energy security. It is vital. We best ensure that hydroelectric infrastructure itself is secure.

In Idaho, we are proud to be home to experts working diligently to that end at the Idaho National Lab. My Committee colleagues have heard me discuss at length INL's role as our flagship nuclear energy research institution. But what a lot of people don't realize is, as I have said, is that cybersecurity is increasing dramatically. INL performs cutting-edge energy system research and development, ensuring cyber and physical threat information in conducting cyber and physical security assessments. I am pleased to have with us today, as I said, an important person that is involved in that from the lab. She and her team at the INL, in partnership with DOE, pioneered the CIE, the cyber-informed engineering concept to build cyber and safeguard practices into infrastructure from the be-

ginning. CIE and other related practices are now being implemented across critical infrastructure development and improvements. I look forward to learning more about this important work—work that is, as we have underscored already, critically important to our infrastructure and how we can improve its application to the resiliency of our hydropower infrastructure.

Thank you, Mr. Chairman.

Senator WYDEN. Thank you very much, Senator Risch, and it's good to have Idaho in the house today.

Senator RISCH. It is.

Senator WYDEN. It is very welcome, and I can just tell you, Ms. Wright, the staff has already been very complementary of a number of things going on there at the Idaho National Laboratory. So we look forward to working closely with you.

We've got three really good witnesses today.

Terry Turpin, Director of the Office of Energy Projects at FERC. He started his career at the Commission in 1998 as a staff engineer, where he was responsible for the review of natural gas pipeline applications. If I read in detail all of his accomplishments, I would have you here until breakfast tomorrow, but we are glad you are here Mr. Turpin. Welcome.

As I say, Virginia Wright, Program Manager for Cyber-Informed Engineering at the Idaho National Laboratory. She leads implementation of the National Strategy for Cyber-Informed Engineering at the Department of Energy. So, she's already been recognized by her colleagues nationally and we wanted to note that.

Then we have Scott Aaronson, Senior Vice President of Security and Preparedness, Edison Electric Institute. Scott leads the EEI Security and Preparedness team, where he focuses on industry security and resilience initiatives and partnerships between government and electric companies. And I think it's well known that we work very closely with you and a cross section of environmental and labor leaders to get the clean energy tax credits, and we very much appreciate your contributions there at EEI.

So let's go right to our witnesses. We will start with you, Mr. Turpin, and I think we have a general agreement, everybody is going to try and stick to five minutes, and it's going to be a little crazy after a while because we have some votes and whatnot, but let's just get all our witnesses in before anything happens in the way of votes, and we will go with Mr. Turpin, Ms. Wright, and Mr. Aaronson.

Mr. Turpin, welcome.

STATEMENT OF TERRY TURPIN, DIRECTOR, OFFICE OF ENERGY PROJECTS, FEDERAL ENERGY REGULATORY COMMISSION

Mr. TURPIN. Thank you very much, sir.

Chairman Wyden, Ranking Member Risch, and members of the Subcommittee, good afternoon. My name is Terry Turpin, and I am Director of the Office of Energy Projects at the Federal Energy Regulatory Commission. The Office is responsible for taking a lead role in carrying out the Commission's activities in reviewing infrastructure projects. This includes the licensing, administration, and safety of non-federal hydropower projects, the authorization of

interstate natural gas pipelines and storage facilities, and the authorization of liquefied natural gas terminals. I appreciate the opportunity to appear before you today to discuss the Commission's program regarding cybersecurity for dam structures associated with hydropower. As a member of the Commission staff, the views I express in my testimony are my own and not necessarily those of the Commission or of any individual Commissioner.

There are hydropower projects in nearly every U.S. state and on most major river systems of the U.S., with more than 100 gigawatts of electric generation capacity installed. Approximately 57 gigawatts of this generation are owned and operated by non-federal parties, such as private companies, private utilities, municipalities, electric cooperatives, private citizens, Indian tribes, and state agencies. Under the Federal Power Act, non-federal hydro-power projects must be licensed by the Commission if they are located on a navigable waterway, occupy federal land, use surplus water from a federal dam, or are located on non-navigable waters over which Congress has jurisdiction under the Commerce Clause. In accordance with the Federal Power Act, the Commission currently regulates over 1,600 non-federal projects, which includes about 2,500 dams.

The Commission's dam safety and security program includes a focus on ensuring that the wide range of dam owners and operators both understand the cybersecurity measures needed to protect their control systems and are also aware of potential threats and vulnerabilities. In recognition of this, the Commission has developed cybersecurity measures drawn from a risk-based, descriptive model approach, which allows for flexibility in regulating such a diverse set of entities. These measures were built on guidelines issued by the National Institute of Standards and Technology, approaches developed through the North American Reliability Corporation's standards development process, and informed through outreach to the regulated industry. These measures allow dam operators and owners the ability to implement a defense-in-depth strategy based upon unique risks and constraints that they face, and enable them to adapt to changes in the cybersecurity vulnerability and threat landscape. Dam owner/operators were required to implement these measures by the end of calendar year 2018.

Commission cybersecurity specialists audit dam operators' efforts regarding vulnerability and security assessments, documentation of cyber assets and associated criticality designations, implementation of cybersecurity controls, and the posture of on-site security. The audit process helps focus owner/operators' efforts on what cybersecurity measures will be most effective for their critical features to prevent a failure path that could lead to downstream consequences. Commission security specialists also monitor classified intelligence, open-sourced information, and unclassified government issuances from the FBI, the Cybersecurity and Infrastructure Security Agency, Homeland Security Information Network, and the Electricity Information Sharing and Analysis Center. This allows staff to discern pertinent security-related events, incidents, and trends, as well as to ensure that FERC licensees are made aware of potential threats and vulnerabilities. By the end of Fiscal Year 2024, staff of the security branch will have performed 271 physical security inspections

and completed cybersecurity audits covering the owner/operators responsible for 37 percent of the installed non-federal hydropower capacity. By the end of Fiscal Year 2025, we will have completed audits covering 70 percent of that installed generation capacity.

That concludes my remarks, and I would be very happy to answer any questions you might have.

[The prepared statement of Mr. Turpin follows:]

**Written Testimony of Terry Turpin
Director, Office of Energy Projects
Federal Energy Regulatory Commission
before the
Energy and Natural Resources Committee
Subcommittee on Water and Power
United States Senate
April 10, 2024**

Chairman Wyden, Ranking Member Risch, and members of the Subcommittee, good afternoon, and thank you for the opportunity to appear before you today.

My name is Terry Turpin and I am the Director of the Office of Energy Projects at the Federal Energy Regulatory Commission. The Office is responsible for taking a lead role in carrying out the Commission's responsibilities in reviewing infrastructure projects, including: (1) the licensing, administration, and safety of non-federal hydropower projects; (2) the authorization of interstate natural gas pipelines and storage facilities; and (3) the authorization of liquefied natural gas terminals. I appreciate the opportunity to appear before you to discuss the Commission's program regarding cybersecurity for dam structures associated with hydropower. As a member of the Commission's staff, the views I express in this testimony are my own, and not necessarily those of the Commission or of any individual Commissioner.

I. Federal and Non-Federal Roles in Hydropower Oversight

There are hydropower projects in nearly every state and on most major river systems of the U.S. with more than 100 (gigawatts) GW of electric generation capacity installed. Of this capacity, approximately 43 GW is supplied by facilities owned and operated by federal entities, principally the Army Corps of Engineers (COE), the Bureau of Reclamation (BOR), and the Tennessee Valley Authority (TVA).¹ Approximately 57 GW of hydropower generation capacity is owned and operated by non-federal parties such as private, non-utility companies; private utility companies; municipalities; electric cooperatives; private citizens; Indian Tribes; and state agencies. Under the Federal Power Act, non-federal hydropower projects must be licensed by the Commission if they: (1) are located on a navigable waterway; (2) occupy federal land; (3) use surplus water or water power from a federal dam; or (4) are located on non-navigable waters over which Congress has jurisdiction under the Commerce Clause, involve post-1935 construction, and affect interstate or foreign commerce. In accordance with the Federal Power Act, the Commission currently regulates over 1,600 non-federal hydropower projects comprised of over 2,500 dams. These projects represent most, but not all, non-federal hydropower.

¹ Megan M. Johnson, Shih-Chieh Kao, and Rocio Uria-Martinez. 2023. *Existing Hydropower Assets (EHA) Plant Database, 2023*. HydroSource. Oak Ridge National Laboratory, Oak Ridge, Tennessee, USA. https://doi.org/10.21951/EHA_FY2023/1972057

Multiple entities hold cybersecurity oversight responsibly for different components within a hydropower facility. For example, the North American Electric Reliability Corporation is responsible for setting and enforcing cybersecurity standards related to generating equipment and controls that support the Bulk Electric System. Alternatively, cybersecurity standards for the control systems related to the safe storage and conveyance of water at hydropower facilities typically falls under the purview of government agencies. For federal hydropower facilities (*i.e.* outside of the Commission's jurisdiction), the COE, BOR, and TVA establish and implement cybersecurity standards for the facilities they own and operate and the Commission has no authority regarding them. For non-federal hydropower facilities, the Commission oversees a comprehensive safety and security program, discussed below.

II. History of the Commission's Dam Safety Program

The Commission is responsible for ensuring that the water-retaining and conveyance features of licensed hydropower projects are designed, constructed, operated, and maintained using current engineering standards and meet federal guidelines for dam safety. During the nearly 60 years the Commission's dam safety program has been in existence, the principal focus has been on dam safety problems associated with: increased risk from natural hazards (*e.g.*, floods, earthquakes), the effectiveness of maintenance activities for ensuring structural integrity; the development/implementation of emergency response plans; and the efficacy of Owner's Dam Safety Programs. Dams are inspected and evaluated by Commission staff and/or independent consultants hired by the licensee on a frequency correlated to the scope of potential downstream impacts. The results of evaluations of both Commission staff and independent consultants include detailed engineering studies, recommendations for dam safety improvements, and a determination whether a dam can safely continue to operate. Each year, Commission dam safety engineers conduct approximately 2,000 inspections related to incident response, construction, and operation of dams.

Beginning in 2001, the Commission incorporated physical security review into the dam safety program. In addition to the consideration of potential downstream impacts, the agency added an assessment of a facility's vulnerability to attack (*i.e.* facility configuration, structural condition, accessibility, and attractiveness as a target). Dams with higher potential downstream consequences and higher vulnerability were required to have more stringent physical security measures than those with a lower combination of potential consequences and vulnerabilities. Security measures were developed by the licensee through conducting vulnerability assessments; developing security plans; undertaking security upgrades and modifications; and maintaining communications with law enforcement entities. FERC engineering staff reviewed the thoroughness of the vulnerability assessments and security assessments conducted by the licensees and evaluated installed physical security measures during dam safety inspections.

In 2016, the Commission's dam safety program was further expanded to address cybersecurity of the control systems used to manage operation of the water control features of a project (e.g., flow bypass systems, reservoir level monitors, flow meters, piezometers, embankment movement indicators). The cybersecurity review program focused on ensuring owner/operators implemented appropriate measures around remotely operable physical features, such as spillway gates, as well as any instrumentation and digital controls needed for dam safety and/or operational decisions regarding the safe flow and storage of water.² Identification of remotely operated equipment and/or remotely accessible instrumentation was paired with a dam's potential downstream impacts and vulnerability to assess whether adequate levels of cyber protection were in place.

Dams with either no remote connectivity, or remote connectivity which posed no risk if compromised, were assigned a "Non-Critical" designation. Dams with remote connectivity and potential impacts to: population (less than 60 within 3 miles; less than 800 within 60 miles, or less than a total population of 12,500); economic losses (\$300 million or less); disruption of essential services such as water supply for water treatment plants and irrigation (impacts affecting less than a municipal-wide area); or potential generation loss (1,500 MW or less) were designated as "Operational" assets. Dams with remote connectivity and potential impacts higher than those thresholds were designated as "Critical" assets.

Dam owners/operators subject to FERC oversight vary widely in capabilities, resources, organizational structure, and size. In recognition of this, the Commission developed cybersecurity measures drawn from a risk-based, descriptive model approach which allowed for flexibility in regulating such a diverse set of entities. As opposed to prescriptive methods, these cybersecurity measures allowed dam operators/owners the ability to implement a defense-in-depth strategy based on the unique risks and constraints they faced. This approach also allows the Commission's required measures to adapt to changes in the cybersecurity vulnerability and threat landscape. These cybersecurity measures were built on standards issued by the National Institute of Standards and Technology, approaches developed through the North American Electric Reliability Corporation standards development process, and were informed by outreach to the regulated industry.³

Cybersecurity measures were divided into two levels: Baseline Measures and Enhanced Measures. Baseline measures were intended to address the most common threat scenarios that might be used to compromise an operational control system. Baseline measures included providing physical security and access restrictions to control system

² Generation and connected transmission digital equipment controls associated with the Bulk Electric System are required to comply with the North American Electric Reliability Corporation's Critical Infrastructure Protection Reliability Standards. Accordingly, such generation and associated transmission digital equipment are not covered by FERC's dam safety requirements, but rather have oversight provided by FERC's Office Electric Reliability.

³ Federal Energy Regulatory Commission. *Security Program for Hydropower Projects Revision 3*. <https://www.ferc.gov/dam-safety-and-inspections/security-program-hydropower-projects-revision-3>.

assets. Owners were directed to monitor and periodically review network connections, including remote and third-party connections. All cybersecurity procedures were to be reviewed annually and updated as necessary.

Baseline measures also included information security and coordination responsibilities such as developing a cross-functional cybersecurity team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks. Owners needed to define information and cybersecurity roles, responsibilities, and lines of communication among the operations, information technology, and business groups, as well as with outsourcers, partners, and third-party contractors. They also needed to establish and document standards for cybersecurity controls for use in evaluating systems and services for acquisition.

Additionally, baseline measures that address the system lifecycle included incorporating security into control system design and operation, whether designing a new system or modifying an existing system, to ensure creation of a sustainable and reliable system. Owner/operators were required to establish and document policies, standards, and procedures for assessing and maintaining system status and configuration information, for tracking changes made to control systems network, and for patching and upgrading operating systems and applications. Owners were also encouraged to implement a supply chain risk management program to ensure vendors followed practices such as software development standards to ensure trustworthy software throughout the development lifecycle. Network traffic access control and functional segregation were required to ensure segmentation of control system networks from less secure networks such as business networks and the Internet through the use of firewalls and similar network traffic access control protections.

Training was specified as an important component of a good cybersecurity program and owners were required to provide training in information security awareness, on an annual basis or as necessitated by changes in the control system, for all users before permitting access. Individuals with significant control systems security roles were to have advanced training specific to their roles.

Enhanced user access control security measures included restricting physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, robust identity verification, secured communication gateways, access control lists, separation of duties practices, least privilege practices, and/or other secure access mechanisms and practices. Owner/operators were required to conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Owners were also directed to evaluate the need for enhanced networking control technologies for wireless networks prior to implementation. Enhanced vulnerability assessment security measures included conducting periodic vulnerability assessments of the control system security, including as appropriate in a non-production environment, not to exceed 12 months.

Owner/operators with dams considered “Non-Critical” were not required to implement these practices given their lack of remotely operable assets or lack of potential downstream impacts, but such licensees were required to re-evaluate this designation annually to monitor for changes. Dams designated as “Operational” required licensees to implement Baseline Cyber Security Measures. Operators with dams considered “Critical” were required to implement both Baseline Cyber Security Measures and Enhanced Cyber Security Measures.

Dam owner/operators needed to implement measures appropriate to the dam designation by the end of calendar year 2018. Licensees were required to submit a letter to the Commission by December 31, 2018, and each year thereafter, certifying compliance with both physical and cybersecurity requirements. Owner/operators needed to maintain documentation regarding vulnerability assessments, security practices, and network architecture at the facility site for review by FERC engineers during any dam safety inspection. During the dam safety inspection, FERC engineers would review measures taken by the licensee regarding remotely operable water conveyance and monitoring equipment.

III. Current Security Program

Following a spillway failure at the Oroville dam in February 2017, the Commission convened an independent panel to review the performance of the Commission’s dam safety program.⁴ The panel’s conclusions, issued December 2018, included a recommendation to remove security inspections from the duties of traditional dam safety engineers and hire technical staff to assess security aspects of the Commission’s jurisdictional facilities. Separating these functions would position the Commission to improve the breadth and scope of all dam inspections. Existing civil engineers would remain focused on evaluating dam structure integrity and performance and conducting review of auxiliary/ancillary structures, while security issues would be addressed by cyber-and physical- security specialists. By 2020, the Commission had created and staffed a security branch composed of four cybersecurity specialists and five physical security specialists.

Security specialists monitor open-source information, unclassified government issuances and classified intelligence to discern pertinent security related events, incidents and trends. Staff also reviews alerts from the E-ISAC (NERC), FBI Cyber Outreach, FEMA (DHS), HSIN (DHS), ICS-CERT, US-CERT, and Shields Up & Shields Ready (CISA) to ensure that FERC licensees are made aware of potential threats or vulnerabilities.

Dam owner/operator’s implementation of physical and cybersecurity measures are reported to the Commission in an Annual Security Compliance Certification (ASCC). Staff review each ASCC to assess the status of an operator’s efforts regarding: vulnerability/security assessments; documentation of cyber assets and associated criticality designations; implementation of cybersecurity controls; the posture of on-site security; and

⁴ Federal Energy Regulatory Commission. *Oroville Dam Service Spillway (P-2100)*. <https://www.ferc.gov/dam-safety-and-inspections/oroville-dam-service-spillway-p-2100>.

identification of contacts for security alerts. The accuracy and completeness of these submittals, along with an entity's size and criticality of remotely controlled assets, factor into which owners/operators and dams are identified for either a physical security inspection or a cybersecurity audit.

During the scheduled audit, FERC security branch auditors facilitate a discussion with the owner/operator's staff on the project's critical features and potential impact to population, economy, and disruption of essential services. The overview helps focus efforts on what cybersecurity measures would be most effective for those features and assets to mitigate a failure path that could lead to downstream consequences. After auditors have established an understanding of the physical project operations and potential impacts, they review network architecture diagrams with the dam owner/operator staff. This allows the entire team to understand project digital communication paths, logical interconnections, and system designs. The network architecture review enables identification of the types of network protection and monitoring the organization has in place, how critical systems are segmented from less critical systems, and how communications and data flow are secured. Review of the network diagrams permits auditing of the cybersecurity policies, management practices, and other administrative controls that are employed to ensure protections are implemented and remain in place. Written cybersecurity policies and procedures are reviewed and referenced as needed during the audit to support evidence of mitigation implementation and to identify any areas for improvement. In addition, a select set of assets are physically inspected to verify security posture based on the documentation provided and the information gathered during owner/operator staff interviews. These assets generally include the organization's main operations, dispatch and/or control center that monitors or operates multiple hydropower facilities.

Following each audit, formal recommendations are issued for follow-up by the dam owner/operator and security branch staff tracks resolution of those recommendations. When instances arise where needed measures require multi-year capital improvement projects (such as upgrading all physical and digital networking devices for improved reliability), dam owners/operators propose a risk-based plan and schedule of milestones along with temporary mitigation measures. Identified milestones are tracked with letters of confirmed completion throughout the project's duration. At any point during the implementation process, a progress audit can be conducted to validate completed milestones and progress.

IV. Conclusion

Since 2016, the Commission has incorporated review of licensee's cybersecurity measures into its program for ensuring the safety of non-federal hydropower projects. The Commission's focus has been on ensuring that the wide range of dam owners/operators understand the measures needed to protect the control systems used to manage operation of the water control features at jurisdictional projects and that these licensees are aware of potential threats or vulnerabilities. Beginning in FY 2022, the Commission undertook audits

of owner/operators with remotely operable assets designated as “Critical” to assess compliance with the Commission’s physical and cybersecurity standards. By the end of FY 2024, staff of the security branch will have performed 271 physical security inspections and completed cybersecurity audits covering the owner/operators responsible for 37% of the installed non-federal hydropower generation capacity.

Senator WYDEN. You almost set the land speed record for getting your testimony in, and I thank you.

Senator RISCH. Very much appreciated.

Senator WYDEN. Yes, indeed.

Ms. Wright, welcome.

STATEMENT OF VIRGINIA WRIGHT, CYBER-INFORMED ENGINEERING PROGRAM MANAGER, IDAHO NATIONAL LABORATORY

Ms. WRIGHT. Chairman Wyden, Ranking Member Risch, and members of the Subcommittee, thank you for the opportunity to testify on a topic critical to our nation's national security. My name is Virginia Wright, and I am a program manager at the Idaho National Laboratory, one of the 17 U.S. Department of Energy National Laboratories. From our decades-long work in building and testing more than 50 nuclear reactors in the high desert west of Idaho Falls, INL has developed a deep understanding of the cybersecurity and engineering needed to secure systems and provide critical function assurance.

INL, sponsored by the Department of Energy, has developed an approach to cybersecurity which starts at the critical functions of the system and the technology that performs those functions. This methodology, called cyber-informed engineering (CIE), asks the engineers who design and operate infrastructure systems to develop engineered controls which can mitigate the worst consequences that could be caused, even if adversaries penetrate digital defenses and gain control of operational technology. CIE is a method readily applicable to ensure that the modernization of the hydropower fleet incorporates designed-in cyber protections which complement the analog nature of the engineering inherent in today's facilities. The U.S. hydroelectric fleet generates 240 billion kilowatt-hours per year, and is very diverse in size, operational configuration, automation level, and importance as baseload. Hydroelectric facilities range in generating capacity from less than one megawatt to the U.S.'s largest, Grand Coulee Dam, which generates more than 6,800 megawatts. Fewer than 400 facilities supply more than 90 percent of U.S. hydropower. Additionally, 87 percent of the U.S. fleet is over 30 years old, with rotating machinery and physical components that have lasted far beyond the expected service life.

The largest facilities are operated by the U.S. Army Corps of Engineers, Bureau of Reclamation, Tennessee Valley Authority, and large commercial utilities—organizations with well-resourced cybersecurity programs. Many of the remaining small and medium-sized facilities are operated by entities with few resources to invest in vulnerability analysis and threat detection, but they all face the same threat landscape. Significant investments by Congress have allocated more than \$753 million to programs to maintain and advance the existing hydropower fleet. These improvements will result in increased generation and grid services and they will also add digital technology used for automation and interconnection of systems within hydropower facilities, increasing the fleet's exposure to cyber threats and vulnerabilities.

In testimony before the House Select Committee on January 31, U.S. officials provided stark warnings about the capabilities and in-

tent of hackers linked to the People's Republic of China. In her testimony, CISA Director Jen Easterly stated, "This is truly an 'everything, everywhere, all at once' scenario." Given the rising awareness that U.S. critical infrastructure is being actively targeted by nation-state actors with the ability to gain covert access and the intent to cause catastrophic harm, a broadly capable cybersecurity program is necessary, but not sufficient. The Federal Government must provide aid and incentives for critical infrastructure operators to proactively find and eliminate avenues for cyber adversaries to cause harm. This is especially true for small organizations who operate infrastructure with the potential for damaging impacts. Cyber-informed engineering can be used to engineer-out adversary opportunities and engineer-in protections from sabotage in both existing and newly upgraded infrastructure.

While the Federal Government can provide financial resources and the expertise of the national laboratories with their ready stockpile of capabilities, defending against "everything, everywhere, all at once" will require everyone, both federal and non-federal, to join forces. To address some of the most critical needs for assessing cyber threats and vulnerabilities of critical water infrastructure in our energy sector, INL has developed a series of urgent recommendations. Further recommendations and details about each are in my written testimony. Number one, use Cyber-informed engineering to add "secure by engineering design" protections from the impact of cyberattacks on the existing fleet and in designs for the future. Number two, support vulnerability assessments on commonly used technology within the hydroelectric fleet. Number three, develop hardening guidance to address well-known weaknesses in digital systems used in hydropower. And number four, increase the pace and the financial support for threat hunting across the hydropower fleet.

I appreciate the opportunity to testify today, and I want to thank you for your attention to this very important issue for our nation. I look forward to your questions.

Senator WYDEN. You will have them momentarily.
[The prepared statement of Ms. Wright follows.]

**Testimony of Virginia Wright,
Program Manager for Cyber-Informed Engineering,
Idaho National Laboratory Before the U.S. Senate Committee on Energy and Natural
Resources,
Subcommittee on Water and Power
Oversight hearing to examine the federal and non-federal role of assessing cyber threats and
vulnerabilities of critical water infrastructure in our energy sector.**

April 10, 2024

Chair Wyden, Ranking Member Risch, and members of the Subcommittee, thank you for the opportunity to testify on a topic critical to our nation's national security. My name is Virginia Wright, and I'm a program manager at the Idaho National Laboratory (INL), focused on Cyber-Informed Engineering¹. Idaho National Laboratory, managed by Battelle Energy Alliance, is one of 17 U.S. Department of Energy (DOE) national laboratories. Located in Idaho Falls, Idaho, INL employs more than 6,000 researchers and support staff with a common vision, to change the world's energy future and secure our nation's critical infrastructure. INL's national security mission focuses on protecting the nation's critical infrastructure, preventing the proliferation of weapons of mass destruction, and providing direct support to America's warfighters. From our decades-long work in building and testing more than 50 nuclear reactors in the high desert west of Idaho Falls, INL has developed a deep understanding of operational technology and the cybersecurity and engineering needed to secure systems and provide critical-function assurance. Over my seventeen years at INL, I have led programs focused on infrastructure cybersecurity research and development supporting the Department of Energy, Department of Defense, and private industry. Most recently, my work has addressed improving the security of the digital supply chain for the nation's critical infrastructure and developing methodologies to incorporate engineering-based protections to augment the cybersecurity protections present on the grid.

Background

Hydropower is one of our nation's largest sources of renewable energy. In 2023, US hydropower generated almost 240 billion kilowatt hours of energy², providing 6.2% of US utility-scale generation and 28.7% of the utility-scale renewable electricity generated in the US.³

¹ INL. n.d. "Cyber-Informed Engineering." Idaho National Laboratory, Idaho Falls, ID. Accessed April 4, 2024. <https://inl.gov/national-security/cie/>.

² EIA. n.d. "Total Energy." U.S. Energy Information Administration. Accessed April 4, 2024. Accessed April 4, 2024. <https://www.eia.gov/totalenergy/data/browser/?tbl=T07.02A#?f=A>

³ EERE. n.d. "Hydropower Basics." Energy Efficiency & Renewable Energy Water Power Technologies Office. Accessed April 4, 2024. <https://www.energy.gov/eere/water/hydropower-basics>.

There are more than 2,000 hydropower facilities operating in the United States⁴ and most US states have conventional hydroelectric generation facilities.⁵

Another energy-sector hydropower technology, pumped-storage hydropower, is a technology which provides grid resilience akin to batteries. It works by pumping water into elevated reservoirs using excess generated energy from the grid, then releasing that water back into a lower reservoir when additional generation is needed. Pumped storage hydropower is the largest form of US energy storage. As of 2022, the US had just over 23,000 MW⁶ of pumped storage hydroelectric generating capacity in service at 40 operating facilities.⁷

In my testimony today, I will address both conventional hydropower and pumped-storage hydropower as critical water infrastructure in the energy sector.

The United States hydroelectric fleet has operated reliably since Wisconsin's Whiting plant opened in 1891. Most of the fleet, especially the larger plants, were designed to provide stable baseload for the grid. But 87% of the US fleet is over 30-years old⁸ and most of its rotating machinery and physical components have lasted far beyond their expected service life. Many plants have been automated to allow partially attended or unattended operations, which require remote connectivity.

The fleet is very diverse, in size, operational configuration, automation level, and importance as baseload. Hydroelectric facilities range in generating capacity from less than 1 MW to the US's largest, Grand Coulee Dam, which generates more than 6,800 MW. Fewer than 400 facilities supply more than 90% of the US conventional hydropower capacity⁹. Most of the large facilities are operated by the US Army Corps of Engineers, Bureau of Reclamation, the Tennessee Valley Authority and large commercial utilities, organizations with well-resourced cybersecurity programs. Many of the remaining small and medium-sized facilities are operated by entities

⁴ Whyatt, M. V. et al. 2023. "Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021." PNNL-32053, Pacific Northwest National Laboratory, Richland, WA. <https://doi.org/10.2172/1899145>.

⁵ EIA. n.d. "Hydropower explained." U.S. Energy Information Administration. Accessed April 4, 2024. <https://www.eia.gov/energyexplained/hydropower/>.

⁶ EIA. n.d. "Hydropower explained Where hydropower is generated." U.S. Energy Information Administration. Accessed April 4, 2024. <https://www.eia.gov/energyexplained/hydropower/where-hydropower-is-generated.php>.

⁷ EERE. 2024. "U.S. Department of Energy Opens Technical Assistance Opportunity to Support Hydropower Project Development." Energy Efficiency & Renewable Energy Water Power Technologies Office. <https://www.energy.gov/eere/water/articles/us-department-energy-opens-technical-assistance-opportunity-support-hydropower>.

⁸ IRENA. 2023. "The Changing Role of Hydro Power: Challenges and Opportunities." International Renewable Energy Agency. https://mc-cd8320d4-36a1-40ac-83cc-3389-cdn-endpoint.azureedge.net/-/media/Files/IRENA/Agency/Publication/2023/Feb/IRENA_Changing_role_of_hydropower_2023.pdf?rev=85b54f8dd8794f8fbc6270b5a1e0b92a.

⁹ Whyatt, M. V. et al. 2023. "Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021." PNNL-32053, Pacific Northwest National Laboratory, Richland, WA. <https://doi.org/10.2172/1899145>.

with few resources to invest in vulnerability analysis and threat detection. But they all face the same threat landscape.

More than \$753 million dollars have been allocated to programs to create incremental new hydropower generation, incentivize efficiency, and maintain and advance the existing hydropower fleet in recent years¹⁰. These improvements will result in increased generation and grid services across the fleet. They will also increase the amount of digital technology used for automation and further interconnect operational components within hydropower facilities, and this could increase the fleets' exposure to cyber threats and vulnerabilities.

As of the end of 2022, 117 conventional hydropower projects were in the pipeline to add 1,200 MW of hydropower capacity. Ninety-five percent of these projects retrofit formerly non-powered dams with generation capability, and as a part of the upgrade, digitized controls and communication will be added¹¹. In the same timeframe, 96 pumped-storage hydropower projects were under development with a combined power storage capacity of 91,000 MW. Some of the planned upgrades integrate hydropower facilities with intermittent renewable energy resources, furthering the role that hydropower plays to balance energy systems.

Threat Landscape

According to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity threats to critical infrastructure are one of the most significant strategic risks for the United States."¹² They note that nation states are targeting US critical infrastructure and seek to gain access to industrial control systems in the energy sector and maintain persistent access to energy networks to lay foundations for future operations. The recent Annual Threat Assessment issued by the Director of National Intelligence discusses the People's Republic of China's willingness to use cyber operations against critical infrastructure to cause public panic and delay US action. It highlights Russia's ability to target critical infrastructure, including industrial control systems. It also notes Iran's opportunistic approach to cyberattack¹³, illustrated in the 2013 attack on Bowman Dam in Rye, New York¹⁴. The attacker leveraged a cellular modem to gain a remote connection to the dam and obtained significant operational data about the facility. Because the sluice gate, which was his target, had been taken offline for maintenance prior to the attack, he did not cause damage. Speculation after the incident concluded that the attacker's purpose was to target a significantly larger dam,

¹⁰ DOE. n.d. "Hydroelectric Incentives Funding in the Bipartisan Infrastructure Law." Department of Energy, Grid Deployment Office. Accessed April 4, 2024. <https://www.energy.gov/gdo/hydro>.

¹¹ Uriá-Martínez, R. M., and M. Johnson. 2023. "U.S. Hydropower Market Report." Oak Ridge National Laboratory, Oak Ridge, TN. <https://www.energy.gov/sites/default/files/2023-09/U.S.%20Hydropower%20Market%20Report%202023%20Edition.pdf>.

¹² DHS. n.d. "Secure Cyberspace and Critical Infrastructure." Department of Homeland Security. Accessed April 4, 2024. <https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure>.

¹³ Office of the Director of National Intelligence. 2024. "Annual Threat Assessment of the U.S. Intelligence Community." <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.

¹⁴ Seals, Tara. 2016. "Iran Behind NY Dam Attack, Financial DDoS Onslaught." Infosecurity Magazine, March 24, 2016. <https://www.infosecurity-magazine.com/news/iran-behind-ny-dam-attack/>.

the Arthur R. Bowman Dam, in Prineville, Oregon, rather than the very small dam on Bowman Ave¹⁵.

Though that attacker was not successful, other international attacks affecting hydropower companies have succeeded. In April of 2023, Hydro Quebec's website and customer app were made temporarily unavailable in a distributed denial of service attack attributed to a Russian actor group unhappy with Canadian policies supporting Ukraine¹⁶. Though not yet detected in hydropower, the Volt Typhoon campaign advisory, published by DHS CISA, provides chilling insight about how threat actors might target information-technology systems and remote-communication technology as the initial stage of a cyberattack which could be used to target the energy sector. A fictional scenario, developed by Aon, a risk management company, describes impacts which could occur from a successful attack on hydropower, including financial loss, loss of power, damage to equipment, flooding, and further impacts to the downstream community¹⁷.

Within the energy sector, key cyberthreats include ransomware, exploitation of remote access, supply-chain attacks, phishing, and malware. Impacts to energy entities from these adversarial techniques can range from loss of information, productivity, and revenue to sabotage of operational processes and damage to equipment¹⁸ or the environment. The dam sector faces cybersecurity threats similar to those affecting the overall energy sector; however, adversaries targeting dams seek impacts beyond just power outages including flood, loss of navigation and water supply and safety and economic impact to the facility and downstream communities.¹⁹ The use of outdated equipment—often with hard-coded and default passwords, rural facility locations, smaller operators with few resources for cybersecurity, and the variability of hydropower facilities—cause unique challenges to cyber defense. In recent work in the hydropower sector, INL found that the operational technology networks at smaller facilities lacked critical security protections and that many facilities allow remote access for maintenance and operational support. Most operators did not have basic visibility into operational network traffic or the expertise and manpower to monitor networks for emerging threats and vulnerabilities. When surveyed, asset owners and operators have described a need for threat

¹⁵ Cohen, Gary. "Throwback Attack: How the Modest Bowman Avenue Dam Became the Target of Iranian Hackers." *Industrial Cybersecurity Pulse*, 12 Aug. 2021, www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/.

¹⁶ Tomesco, F. 2023. "Pro-Russian group takes responsibility for cyberattack on Hydro-Quebec." *The Gazette*, April 13, 2023. <https://montrealgazette.com/news/local-news/hydro-quebec-website-and-app-blacked-out-in-cyberattack>.

¹⁷ Laus, J. and M. Honea. n.d. "Silent Cyber Scenario: Opening the Flood Gates." AON. Accessed April 4, 2024. <https://www.aon.com/reinsurance/gimo/20181025-gimo-cyber>.

¹⁸ MITRE. n.d. "ICS Matrix." MITRE Corporation. Accessed April 4, 2024. <https://attack.mitre.org/matrices/ics/>.

¹⁹ Dechant, Jason, and James Morgeson. *Assessing Cyber Security Risk for the Dams Sector*. 2018. <https://apps.dtic.mil/sti/trecms/pdf/AD1122504.pdf>

and vulnerability information linked to their specific operational contexts and, where possible, to their assets²⁰.

As an applied-energy laboratory, INL performs research, but also have unique experience in systems design, development, demonstration, and deployment. This applied engineering focus has also permeated our approach to cybersecurity. At the INL, we specialize in the cybersecurity of operational technology (OT). These are the systems and software that control physical systems and devices and the processes that perform the physical work of an organization. In hydropower, operational technology includes generators, turbines, and systems for water conveyance, automation, control, protection, substation operation, and auxiliary functions²¹. Each of these systems has networked interconnections through which the system is controlled and exchanges data.

OT is different from Information Technology, which includes the systems and software which exchange data about the work of an organization. IT systems typically support the business functions of an organization and rather than performing or controlling physical work; IT systems operate on data. Most cybersecurity approaches focus on data. They begin with the assumption that if access and control of data and the networks through which the data is exchanged can be controlled, adversary action can be prevented.

INL, because of our focus on engineering, has developed a different approach to cybersecurity—which starts in a different place—at critical functions²² of the system and the operational technology which performs those functions. This methodology, called Cyber-Informed Engineering (CIE)²³, asks the engineers who design and operate infrastructure systems to identify the worst consequences which could occur if an adversary was able to penetrate through digital defenses and sabotage operational technology. For each high-consequence event, engineers consider whether there is the possibility to add an engineered control which might eliminate the opportunity for a digital sabotage or which would mitigate the impact an adversary could have, even with control over the digital system. Engineered controls could be analog and, thus, impervious to cyberattack, or they might be digital, but with different networking from the operational technology that performs critical functions. After developing and designing-in engineering controls, engineers then collaborate with the cybersecurity team to ensure that system defenses protecting data robustly address the identified consequences. They also devise alternate operating modes to be used if a critical system is rendered

²⁰ Whyatt, M. V. et al. 2023. "Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021." PNNL-32053, Pacific Northwest National Laboratory, Richland, WA. <https://doi.org/10.2172/1899145>.

²¹ Sanghvi, A. D. and R. Cryar. 2023. "Cybersecurity Value-at-Risk Framework." In proceedings of the 2023 IEEE Power and Energy Society General Meeting, Orlando, FL, July 16–20, 2023. <https://www.nrel.gov/docs/fy23osti/84412.pdf>.

²² Dechant, Jason, and James Morgeson. Assessing Cyber Security Risk for the Dams Sector. 2018. <https://apps.dtic.mil/sti/trecms/pdf/AD1122504.pdf>

²³ "Cyber-Informed Engineering (CIE)." Idaho National Laboratory - Cyber-Informed Engineering, Idaho National Laboratory, <http://www.inl.gov/cie>. Accessed 7 Apr. 2024.

inoperable or untrustworthy and create and practice operational plans for system defense with the cyber defense team. CIE is a methodology readily applicable to ensure that the modernization of the hydropower fleet incorporates designed-in cyber protections which benefit from the analog nature of the engineering inherent in today's facilities.

In 2020, Congress directed the DOE to create a Cyber-Informed Engineering Strategy²⁴ and DOE's Cybersecurity, Energy Security and Emergency Response (CESER) organization turned this research concept into a methodology which could be implemented to protect the nation's energy infrastructure. CIE has been highlighted in the National Cybersecurity Strategy²⁵, the National Cybersecurity Strategy Implementation Plan²⁶, and the recent report on Strategy for Cyber-Physical Resilience authored by the President's Council of Advisors on Science and Technology (PCAST)²⁷. Partnered with the National Renewable Energy Laboratory (NREL) and sponsored by DOE CESER as part of their Energy Cyber Sense program²⁸, INL is implementing the recommendations in the national strategy by spreading awareness of CIE²⁹, working with universities to incorporate CIE into their engineering education³⁰, and developing tools for easier implementation of the methodology³¹. With asset owners, we apply CIE to existing infrastructure, and with researchers, we apply CIE into the research concepts which will become the energy infrastructure of the future. CIE is advancing the practice of engineering to become cyber-informed, incorporating engineering to prevent the impact of cyberattack as part of the overall standard of care. INL's Cyber-Informed Engineering Implementation Guide³² is a first step to provide a set of questions engineers can consider for cyber-informed system design. For hydroelectric facilities performing upgrades or retrofits to add digital capabilities,

- ²⁴ DOE. 2022. "National Cyber-Informed Engineering Strategy." U.S. Department of Energy. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20%20June%202022_0.pdf.
- ²⁵ White House. 2023. "National Cybersecurity Strategy." <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.
- ²⁶ White House. 2023. "National Cybersecurity Strategy Implementation Plan." https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.
- ²⁷ Executive Office of the President. 2024. "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World." Report to the President. https://www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.
- ²⁸ Kumar, P. 2023. "The National Cybersecurity Strategy: A Path Towards a More Secure and Resilient Energy Sector." Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response. <https://www.energy.gov/ceser/articles/national-cybersecurity-strategy-path-toward-more-secure-and-resilient-energy-sector>.
- ²⁹ "Cyber-Informed Engineering (CIE) Practitioners' Workshop." *McCrory Institute*, Auburn University, <https://mccrory.auburn.edu/events/cie-practitioners-workshop/>. Accessed 7 Apr. 2024.
- ³⁰ Pittwire. 2023. "In this program, Pitt students are working to protect the electric power grid." University of Pittsburgh. Accessed April 4, 2024. <https://www.pitt.edu/pittwire/features-articles/undergraduates-protect-electrical-power-grid-shure>.
- ³¹ Wright, V. L. et al. 2023. "Cyber-Informed Engineering Implementation Guide." INL/RPT-23-74072, Idaho National Laboratory. <https://www.osti.gov/biblio/1995796>.
- ³² Wright, V. L., B. R. Lampe, and S. D. Chanoski. 2024. "Cyber-Informed Engineering: Cybersecurity for Microgrids Workshop Workbook." INL/MIS-24-76646, Idaho National Laboratory, Idaho Falls, ID. https://indigitalibrary.inl.gov/sites/STI/STI/Sort_90569.pdf.

CIE could provide cyber protection engineered into the design of the facility rather than added after the fact.

For the most-consequential hydropower facilities, for example, the 400 which supply 90% of hydropower, a complementary methodology to CIE, called Consequence-Driven Cyber-Informed Engineering (CCE), can be used to identify additional needed defenses. CCE is a rigorous four-phase process for applying CIE's core principles to a specific organization, facility, or mission by identifying its most critical functions, discovering the methods and means an adversary would likely use to manipulate or compromise it, and determining the most-effective means of removing or mitigating those risks. INL's CCE methodology is licensed to a number of industry partners allowing non-federally driven application of this methodology.

Another INL tool, Malcolm, was designed to provide hydropower operators visibility into the networks interconnecting their operational technology. Malcolm supplies dozens of prebuilt dashboards, providing an at-a-glance overview of network traffic for both IT and OT and identifying the network sessions comprising suspected security incidents³³. Malcolm was developed by INL at the request of the Bureau of Reclamation, under the sponsorship of DHS CISA. This tool is available as open-source software and has been deployed to the major Bureau of Reclamation dams in the west, locally to Idaho Falls Power, and to a Bureau of Indian Affairs hydroelectric dam. As part of this effort, INL also conducted tabletop assessments, performed hunt and incident-response activities, and provided recommendations to improve dams' cybersecurity postures. Malcolm and another tool, called the Cyber Security Evaluation Tool (CSET)³⁴, and used to evaluate an organization's security posture, have been bundled together and tailored to the needs of hydropower operators through a DOE Water Power Technology Office (WPTO) effort called HydroSHIELD³⁵.

Many hydropower facilities are only one facet of critical infrastructure operated by their asset owner, and understanding the interdependencies within these systems of systems is crucial to resilient operations and incident response. INL's All Hazards Analysis (AHA) is a dynamic dependency-analysis framework that enables critical-infrastructure knowledge discovery and decision support. AHA identifies dependencies and associated risks, giving decision-makers and emergency managers a comprehensive view of interconnected infrastructure systems. AHA uses an optimized framework for the collection, storage, analysis, and visualization of critical-infrastructure information. Using a function-based approach, it presents information in the form of nodes (infrastructure) and links (dependency relationships). Because AHA continually learns, it can blend general and facility dependency profiles with new information and changing

³³ INL. n.d. "Malcolm: A Network Traffic Analysis Tool Suite." Accessed April 4, 2024. <https://inl.gov/national-security/ics-malcolm/>.

³⁴ <https://www.cisa.gov/downloading-and-installing-cset>. n.d. "Downloading and Installing CSET." Accessed April 4, 2024.

³⁵ INL. n.d. "INL Cyber SHIELD for Renewables." Idaho National Laboratory. Accessed April 4, 2024. <https://resilience.inl.gov/inlcybershield>.

network structure. This allows for more-detailed sector and consequence analysis than would be possible with other infrastructure modeling systems³⁶.

The Cyber Testing for Resilient Industrial Control System (CyTRICS™) program, sponsored by DOE CESER, may be an important model to inform vulnerability analysis for hydropower technology. CyTRICS works with vendors to identify high-priority OT components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing. CyTRICS leverages best-in-class test facilities and analytic capabilities at six DOE national laboratories and strategic partnerships with key stakeholders, including technology developers, manufacturers, asset owners and operators, and interagency partners³⁷.

The water sector may provide an instructive analog to guide consideration of the testing, training, and exercise facilities needed to allow scaled testing of the impacts of cyberattack on hydropower facilities. Like the hydropower subsector, the water sector is rapidly adopting OT and other digital tools while it also attempts to maintain aging and obsolete software and controls. INL's Water Security Test Bed may serve to model the kinds of testing facilities needed for hydropower cybersecurity. Established in 2013 through a partnership between the US Environmental Protection Agency (EPA) and INL, this facility, located in the INL Critical Infrastructure Test Range, part of INL's 890 square mile site, is a center for research, development, and testing of national water security and other drinking-water distribution issues. It can not only test, at or near full-scale, the impacts of cyberattack on water systems, but it also addresses biological and chemical vulnerabilities due to natural or accidental causes or malicious acts.

The hydropower fleet has multiple agencies guiding the maturity of their operational cybersecurity programs. The DHS Dam Sector Program Office acts as the sector-specific risk agency and offers guidance and assessments available to all operators. The Federal Energy Regulatory Commission (FERC) inspects dams for safety and both physical and cybersecurity. DOE's WPTO³⁸ performs research and development and creates tools to aid hydropower-asset owners in assessing where cybersecurity investments are needed³⁹ and how to respond to cybersecurity incidents. Some generating facilities are also subject to the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) standards and must develop a program to guide cybersecurity performance attuned to the criticality of equipment. In addition, large operating entities and the states may have additional guidelines

³⁶ INL. n.d. "All Hazards Analysis – AHA." Idaho National Laboratory. Accessed April 4, 2024. <https://inl.gov/national-security/ics-aha/>.

³⁷ DOE. n.d. "CyTRICS Cyber Testing for Resilient Industrial Control Systems." Department of Energy: Office of Cybersecurity, Energy Security, and Emergency Response." Accessed April 4, 2024. <https://cytrics.inl.gov/>.

³⁸ EERE. n.d. "About the Water power Technologies Office (WPTO)." Office of Energy Efficiency & Renewable Energy. Accessed April 4, 2024. <https://www.energy.gov/eere/water/about-water-power-technologies-office-wpto>.

³⁹ NREL. n.d. "Cybersecurity value-at-Risk Framework." The National Renewable Energy Laboratory, Golden, CO. Accessed April 4, 2024. <https://cvf.nrel.gov/>.

for cybersecurity performance. These programs seek to form capable cybersecurity programs which are resilient to a broad set of vulnerabilities and threats.

In testimony before the House Select Committee on January 31, US officials provided stark warnings about the capabilities and intent of hackers linked to the People’s Republic of China. In her testimony, CISA Director Jen Easterly stated, “This is truly an Everything Everywhere, All at Once scenario. And it’s one where the Chinese government believes that it will likely crush American will for the U.S. to defend Taiwan in the event of a major conflict there.”⁴⁰ Given the rising awareness that US critical infrastructure is being actively targeted by nation-state actors with the ability to gain covert access and the intent to cause catastrophic harm, a broadly capable cybersecurity program is necessary, but not sufficient. The federal⁴¹ government must provide aid and incentives for critical-infrastructure operators to find and eliminate avenues for adversaries to cause harm through digital sabotage of critical infrastructure. This is especially true for small organizations who operate infrastructure with the potential for damaging impacts.

Cyber-Informed Engineering can be used to engineer-out adversary opportunities and engineer-in protections from sabotage in both existing and newly upgraded infrastructure. Where commonly used equipment may provide the opportunity for a vulnerability to be targeted across infrastructure, the government can help to prioritize vulnerability assessment, development of mitigations, and patching. Further, this research can be used to develop hardened-configuration guidance and guides to extracting forensic data from the equipment during and after a cyberattack. While the federal government can provide financial resources and the expertise of the national laboratories with their ready stockpile of capabilities and other cybersecurity experts in federal service; defending against “everything everywhere all at once” will require everyone, both federal and non-federal, to join forces.

Recommendations

To address some of the most-critical needs for assessing cyberthreats and vulnerabilities of critical water infrastructure in our energy sector, INL recommends the following, expressed in terms of “Now,” “Soon,” and “Someday”:

Now:

- Use capabilities like the Department of Energy’s Cyber-Informed Engineering⁴² to add engineering protections from the impact of cyberattacks on existing the existing

⁴⁰ Jones, D. 2024. “CISA, FBI confirm critical infrastructure intrusions by China-linked hackers.” Cybersecurity Dive, February 7, 2024. <https://www.cybersecuritydive.com/news/cisa-fbi-critical-infrastructure-china-hacker/706935/>.

⁴¹ Thorsen, D. E. et al. 2020. “Hydroelectric Cybersecurity Response and Recovery Overview.” PNNL-30593, Pacific Northwest National Laboratory, Richland, WA. <https://doi.org/10.2172/1879890>.

⁴² DOE. n.d. “Cyber-Informed Engineering.” Office of Cybersecurity, Energy Security, and Emergency Response. Accessed April 4, 2024. <https://www.energy.gov/ceser/cyber-informed-engineering>.

infrastructure within the hydropower fleet and in the designs for future hydropower infrastructure. For federally funded upgrade initiatives, support technical assistance focused on designing operational-technology cybersecurity into new capabilities.

- Support vulnerability assessments on commonly used technology within the hydroelectric fleet, sharing results with vendors. For owners and operators, suggest vulnerability mitigations and secure configurations that integrate with existing maintenance and sustainability operations. Work with vendors to develop forensic quick start guides to speed the acquisition of attack indicators when adversary activity is suspected.
- Develop hardening guidance to address well-known weaknesses in remote-communication infrastructure and default passwords in OT systems, working with vendors where possible.
- Increase the pace and the financial support for threat hunting across the hydropower fleet and across all critical infrastructure. Ensure that all industry operators have a cybersecurity incident-response plan that addresses both IT and OT and that they exercise that plan at least annually, informed by threat scenarios provided by the Sector Risk Management Agencies (SRMAs).

Soon:

- Increase support for hydropower operators to gain visibility into traffic on their OT networks and the expertise to differentiate expected operations from adversary action. Where technical assistance is needed, support grants for commercial or federal assistance to smaller-asset owners. Work with states to explore the ability to leverage National Guard resources when concerns about imminent threat activity are heightened.
- Instantiate a hydropower-focused Operational Technology Fellowship⁴³ program through DOE's WPTO. Participants would learn cybersecurity strategies and tactics that adversarial state and nonstate actors use in targeting U.S. hydroelectric infrastructure and how the U.S. government is countering these activities.
- Develop small-scale hydropower cybersecurity testbeds like INL's Control Environment Laboratory Resource capability (CELR) to allow exploration and demonstration of how threat actors might target hydropower. Deploy them regionally for use for federal, academic, and commercial research.
- Explore federally funded apprenticeships, focused on operational-technology threat-hunting and incident response to support smaller hydroelectric entities. An organization like the Cybersecurity and Industrial Infrastructure Security Apprenticeship Program (CIISAp) may provide a foundation to build the future workforce of cybersecurity defenders for hydropower.

Someday:

⁴³ DOE. n.d. "Operational Technology Defender Fellowship [Fact Sheet]." Accessed April 4, 2024. <https://otdefender.inl.gov/>.

- Explore a program like CyberCorps® Scholarship for Service⁴⁴ to incentivize cybersecurity practitioners to consider careers defending rural dam locations.
- Explore the overlapping cybersecurity responsibilities between the Dam SRMAs, FERC, NERC, and DOE to eliminate redundancy and ensure that guidance is effectively targeted to the needs of the hydropower industry.

My sister laboratory, Pacific Northwest National Laboratory, developed a set of metrics⁴⁵ which I recommend to evaluate the effectiveness of any initiative undertaken in response to this threat:

1. Are a significant number of hydropower facilities helped? (community propagation)
2. Are cybersecurity risks [and threats] substantially reduced (impact)
3. Is there a clear path and short time to put in place? (speed to adoption)
4. Is the maintenance burden minimal? (ease of ownership)

Conclusion

Addressing cybersecurity threats to US critical water infrastructure within our energy sector requires an approach focused on preventing the potential for catastrophic harm which could result if an adversary effort was successful. This necessitates, first, looking at the engineering and operational technology that ensures the reliable operation of the facility to add protections that prevent an adversary—even if it obtains control—from doing harm and, second, removing vulnerabilities and adding protections which prevent that access in the first place. Our rapidly modernizing hydropower fleet is an attractive target for adversaries and needs support to defend against the currently assessed nation-state threat. Cyber-informed engineering and other cyber-physical capabilities enable INL to play a significant role in identifying threats and mitigating vulnerabilities to hydroelectric infrastructure. Your commitment to increase support, both federal and non-federal, for threat and vulnerability assessment will ensure our critical infrastructure’s resilience against disruption from nation-state offensive cybersecurity operations. We must ensure that all of our critical-infrastructure operators have the tools and expertise needed to prevent catastrophic impacts from cyberattack.

I appreciate the opportunity to testify today, and I want to thank you for your attention to this very important issue for our nation. I look forward to your questions.

⁴⁴ U.S. Office of Personnel Management. n.d. “CyberCorps: Scholarship for Service.” Accessed April 4, 2024. <https://sfs.opm.gov/>.

⁴⁵ Whyatt, M. V. et al. 2023. “Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021.” PNNL-32053, Pacific Northwest National Laboratory, Richland, WA. <https://doi.org/10.2172/1899145>.

Senator WYDEN. Mr. Aaronson.

**STATEMENT OF SCOTT AARONSON, SENIOR VICE PRESIDENT,
SECURITY AND PREPAREDNESS, EDISON ELECTRIC INSTI-
TUTE**

Mr. AARONSON. Thank you, Chairman Wyden.

Chairman Wyden, Ranking Member Risch, members of the Subcommittee, I appreciate the opportunity to testify before you today on this important topic on critical infrastructure security, and specifically, those interdependencies among the electricity, water, and dam sector. You are going to hear some very consistent themes across the three witnesses. My name is Scott Aaronson. I am Senior Vice President for Security and Preparedness at the Edison Electric Institute, or EEI. EEI is the trade association representing all of the nation's investor-owned electric companies. These companies serve more than 250 million Americans and represent five percent of the United States' gross domestic product. We are fond of saying it's the first five percent of GDP since all other sectors rely on our product. And that number is only growing. With the proliferation of data centers for artificial intelligence and fueling our digital economy, more manufacturing and industrial processes relying on electricity, adoption of electric vehicles across the transportation sector, and electricity increasingly used for home heating, America's electric companies are more important than ever to our nation's security, economic competitiveness, and the lives and safety of our customers and your constituents. This is a responsibility EEI's members take very seriously.

In addition to the extraordinary growth, the grid is also changing. With more distributed resources, two-way flows, grid-scale battery storage, clean energy sources, and broad digitization enabling customer control and better visibility into this increasingly complex system, this is an exciting time to be a part of the electric power sector. But these changes also can bring new risks and an evolving attack surface. As the Director of National Intelligence Worldwide Threat Assessment has said publicly since 2019, "Near-peer nation-states are targeting critical infrastructure to hold the United States at risk at a time of their choosing." To address these risks, the electric power sector uses a defense-in-depth approach that seeks to protect our most critical assets from compromise while also understanding that defenses are never infallible. So resilience, redundancy, and the ability to recover are integral to our defenses too.

This resilience comes from a diversity of resources and systems that limit single points of failure. It also comes from the development and exercising of plans to operate degraded or to restart systems, known as black-start capabilities, and perhaps most importantly, a culture of mutual assistance that supports response and recovery against all hazards. This is most apparent when storms and natural hazards hit, but has grown to include cyber mutual assistance capabilities and spare equipment sharing programs. The energy grid is one big machine with thousands of owners and operators. This community has found common cause to work together to address the risks posed by both Mother Nature and man-made threats.

In addition to these resilience efforts, the electric power sector also has a regulatory regime that includes mandatory and enforceable cyber and physical security standards. It may surprise the Subcommittee, but the electric power sector strongly supports these regulatory requirements. They provide a foundational level of security, and we appreciate Congress codifying the concept of an electric reliability organization in the Federal Power Act as part of the Energy Policy Act of 2005. This construct allows experts from grid operators and other stakeholders to develop standards that are enforced by the Federal Energy Regulatory Commission. That said, regulations alone cannot guarantee security because security is not a check-the-box exercise. In fact, in order to keep up with adversaries, asset owners and operators must be more nimble and creative than just abiding by baseline regulations. This is where the value of partnerships is key.

In addition to my role at EEI, I also am privileged to be a member of the secretariat that supports the Electricity Subsector Coordinating Council (ESCC). Along with the cooperative and public power segments of the industry, the ESCC brings more than two dozen CEOs and leaders from across the sector to work with senior government officials to prepare for and respond to serious threats to grid operations. The ESCC has been held up as a model for how critical infrastructure sectors can partner with each other and leverage both the industry's visibility into its systems and our operational excellence, along with the government's intelligence gathering capabilities and national security responsibilities. In addition to responding to major incidents, other ESCC priorities include securing the grid of the future and enhancing operation and collaboration between government and industry security experts.

Fortunately, a recent example of the value of this partnership was the Chinese state-sponsored cyber threat known as Volt Typhoon that became public earlier this year. Fortunately, the electric power sector had been aware of the risk long before it made news. In fact, a small group of pilot companies participating in the Energy Threat Analysis Center (ETAC) had been working side-by-side with government to understand this threat and to develop and socialize mitigation strategies. These lessons were shared with the broader sector through the Electricity Information Sharing and Analysis Center (E-ISAC), showing a commitment to collective defense and information sharing that will serve us well as the electric power sector adapts to the new threats and challenges facing critical infrastructure operators.

In addition to working with the government, the ESCC also values cross-sector partnerships. While we are that first five percent of GDP, we also rely on other sectors to support our sector's operations and resilience. We need telecommunications to communicate with field personnel and to ensure systems remain in balance; transportation and pipelines to move fuel; and water to generate steam, cool systems, and for hydropower through dams. As you know, these resources play a critical role in both the black-start capabilities that I mentioned earlier and in producing energy that provides important support to grid operations, particularly in the West. Again, EEI and its members are deeply committed to these partnerships, regulatory constructs, and resilient strategies, and to

working together as both the energy grid and geopolitical risks continue to evolve.

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

[The prepared statement of Mr. Aaronson follows:]

30

**STATEMENT OF SCOTT L. AARONSON
SENIOR VICE PRESIDENT, SECURITY AND PREPAREDNESS
EDISON ELECTRIC INSTITUTE**

**BEFORE THE U.S. SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SUBCOMMITTEE ON WATER AND POWER**

**HEARING TO “EXAMINE THE FEDERAL AND NON-FEDERAL ROLE OF
ASSESSING CYBER THREATS TO AND VULNERABILITIES OF CRITICAL WATER
INFRASTRUCTURE IN OUR ENERGY SECTOR”**

APRIL 10, 2024

Introduction

Chairman Wyden, Ranking Member Risch, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Senior Vice President for Security and Preparedness at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for nearly 250 million Americans and operate in all 50 states and the District of Columbia. For EEI's member companies, securing the energy grid from all hazards, including cyber threats, is a top priority. I appreciate your invitation to discuss this important topic on their behalf.

The energy grid powers our way of life and is critical to America's security and economic competitiveness. Today, demand for electricity is growing dramatically across the economy to support evolving customer needs, as well as critical technologies like artificial intelligence and the proliferation of data centers that fuel our digital lives. Ensuring a secure, reliable, resilient energy grid is a responsibility that EEI's member companies and the electric power sector take extremely seriously.

Threat Landscape

As the grid continues to evolve, so, too, do the threat actors who seek to undermine U.S. critical infrastructure. For years, the U.S. intelligence community has warned of the potential for malicious nation-state exploitation of U.S. critical infrastructure. Today, we know from our federal partners that People's Republic of China state-sponsored cyber actors known as Volt Typhoon have compromised multiple U.S. critical infrastructure providers with the intent of disrupting operational controls.

With the increasingly complex geopolitical threat landscape and the sophistication of ransomware operations by transnational organized criminals, we have seen an uptick in threats to critical infrastructure organizations across all sectors. The infiltration of the controls of a New York dam in 2013, and the exploitation of programmable logic controllers in Pennsylvania and across the Water and Wastewater Systems Sector by Iranian government-affiliated cyber actors in late 2023, are clear examples of the opportunistic approach that nation-state adversaries like Iran will continue to leverage and are a stark reminder of the need to continue to monitor and to harden U.S. critical infrastructure.

Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, government at all levels can and must play a role in protecting it, especially when it comes to defending against nation-state actors.

To address this, EEI's member companies and the electric power sector take a "defense-in-depth" approach with several layers of security strategies designed to eliminate single points of failure. There are three main components to our defense-in-depth approach:

1. Mandatory and enforceable reliability, physical security, and cybersecurity regulations;
2. Partnerships among industry and government; and
3. Efforts to enhance our resilience to all hazards.

All Hazards Security: Defense-in-Depth

Cyber and physical security threats will continue to evolve, which is why the electric power sector focuses on enhancing visibility into critical control systems, improving situational awareness and information sharing for emerging threats, and ensuring we have comprehensive plans in place to respond and recover quickly when incidents occur.

Standards. Under the Federal Power Act and Federal Energy Regulatory Commission (FERC) oversight, the electric power sector is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed \$1 million per violation per day. These mandatory standards continue to evolve using the process created by Congress to allow for input from subject matter experts across the industry and government.

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

In addition to complying with standards, the sector strongly believes in advancing a culture of security. Thanks to leadership from the chief executives of all U.S. investor-owned electric companies, EEI developed a "Culture of Security" initiative that has provided tools to improve security culture for individual electric companies and a venue for sharing practices across the industry.¹

Self-assessments are now conducted by companies annually. In addition to demonstrating that security is a priority for the "C-suite," these yearly exercises provide a venue for security teams and leaders across business units to address corporate security culture and to better align efforts.

When it comes to securing specific systems like operational technology for power delivery, much of the expertise is in the sector. To leverage this expertise, electric companies are now piloting a peer review program to have security professionals from electric companies review their peers, identify opportunities for improvement, and socialize best practices.

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

Through these standards and voluntary regimes, the bulk power system and other critical grid components benefit from a baseline level of security. While these standards are important,

¹Scott Aaronson, Edison Electric Institute, Protecting the energy grid is a team sport (October 2021), <https://www.securitymagazine.com/articles/96231-protecting-the-energy-grid-is-a-team-sport>.

regulations alone are insufficient given the dynamic threat environment, and they must be supplemented by industry-government partnerships and coordinated response and recovery efforts.

Partnerships. As threats evolve, the value of industry-government partnership and the need to remain vigilant cannot be overstated. The electric power sector has worked with government partners to develop and deploy sophisticated threat monitoring tools and to create an environment where threat intelligence is shared in near real-time and where operational collaboration among asset owners and government operators is the norm. This gets information into the hands of system operators quickly to better protect and defend their critical systems against rapidly evolving threats. While the sector values current coordination efforts, there is opportunity to continue to enhance timely and actionable information sharing through partnerships like the Electricity Subsector Coordinating Council (ESCC), the Cybersecurity Risk Information Sharing Program (CRISP), and the Energy Threat Analysis Center (ETAC).

Through partnerships like the ESCC, government and industry leverage one another's strengths. The ESCC consists of electric company CEOs and trade association leaders who represent all segments of the electric sector and who actively partner with government executives to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort, unity of guidance, and unity of message among participating organizations.

This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-sector coordination. The ESCC has been seen as a model across critical infrastructure sectors due to its CEO-level engagement and prioritization of security and preparedness for all hazards. This unity of effort driven by industry working with government has produced significant, tangible results. The sector continues to deploy CRISP, an industry-government partnership that includes industry, DOE, Pacific Northwest and Argonne National Laboratories, and the Electricity Information Sharing & Analysis Center (E-ISAC), which manages the program. More than 75 percent of U.S. electric customers are served by a company that has deployed CRISP, and this program will continue to grow as the information gleaned from its sensors and the associated analysis have proven extremely valuable to identifying and addressing cybersecurity risks.²

The sector also leverages DOE's ETAC, another public-private partnership that benefits from the tools and insights energy infrastructure owners and operators have deployed on their systems, coupled with DOE's National Laboratories and the intelligence community that come together to exchange data, identify risks, and develop mitigation strategies to protect energy systems from adversaries like Volt Typhoon, among others. I would like to thank Chairman Manchin and Ranking Member Risch for their leadership on the *ETAC Establishment Act* and encourage the

² Sonal Patel, POWER, DOE Lays Out How Power Sector Could Win the Cybersecurity Battle (May 2018), <https://www.powermag.com/doi-lays-out-how-power-sector-could-win-the-cybersecurity-battle/>.

Committee to consider this legislation as a way to build on the progress of the ETAC pilot program.

Response and Recovery. The electric power sector is proud of its record on reliability, but outages and incidents do occur. When these happen, many key investments help companies restore power safely and as quickly as possible. EEI's member companies invest more than \$150 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure. The industry's culture of mutual assistance deploys a world-class workforce amidst the toughest conditions to restore power for customers safely and efficiently.

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

Industry-government exercises, such as the biennial GridEx, sharpen the industry's skill set, ensuring that, when incidents happen, our playbook has been tested before it is put into action. Most recently, GridEx VII included more than 15,000 participants from approximately 250 North American organizations, including the electric industry, cross-sector partners from natural gas and telecommunications, and U.S. and Canadian government partners.³ The two-day exercise tested operational and policy measures that would be needed to restore the energy grid following a severe cyber and physical security attack. These drills sharpen not just the unity of effort between electric companies and government agencies, but also practice unity of message to ensure that we speak with one voice to our customers and your constituents during incidents.

Critical Infrastructure Interdependencies

The electric power sector is proud of the work we do to build "defense-in-depth" across our industry, but we understand that alone is not enough. We also must work with government and cross-sector industry partners to build that same "defense-in-depth" across the nation to reduce systemic risk and to ensure all are prepared for, and can respond to, national-level incidents. The federal government can support industry in reducing systemic risk associated with critical infrastructure interdependencies by:

1. Coordinating with industry on the revision of Presidential Policy Directive 21 (PPD-21);
2. Considering interdependencies in the revision of the National Cyber Incident Response Plan (NCIRP);
3. Evaluating critical infrastructure supply chain interdependencies; and

³ North American Electric Reliability Corporation, GridEx VII Report Highlights Further Action to Enhance Grid Resilience (April 2024), <https://www.nerc.com/news/Headlines%20DL/GridEx%20VII%20Lessons%20Learned%20Report.pdf>.

4. Prioritizing and resourcing the most critical of U.S. critical infrastructure, including such regimes as Defense Critical Electric Infrastructure (DCEI) and Systemically Important Entities (SIE) as established by the Cyberspace Solarium Commission.

PPD-21 on Critical Infrastructure Security and Resilience. This policy directive identifies the energy sector as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors. PPD-21 also delineates roles and responsibilities to specific federal agencies known as Sector Risk Management Agencies (SRMAs). SRMAs are meant to serve as a day-to-day federal interface for prioritizing, collaborating, and coordinating sector-specific activities including cyber incident response.

The productive relationship between the power sector and DOE as its SRMA often serves as an example for other sectors, especially through its ESCC leadership model. As the Administration pursues plans to revise this decade-old policy document, we welcome the opportunity for industry engagement to elaborate on the best practices learned through collaboration with our SRMA.

In the context of today’s hearing, there are three SRMAs to consider—DOE as the SRMA for the Energy Sector, the Environmental Protection Agency (EPA) as the SRMA for the Water Sector, and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) as the SRMA for the Dams Sector. Clarifying federal roles and responsibilities through the PPD-21 revision will help coordination across sectors like the energy, water, and dams sectors.

NCIRP. Both water and dams are integral to the operation of the electric system, and government and industry across each sector should be in lock step to ensure timely and effective cyber incident response. Hydropower provides about 40 percent of the “black start” resources necessary to restore power in the event of grid failure.⁴ In addition, dams are a key piece of the operations and deployment of renewables across the U.S. grid, particularly in the West.⁵ Accordingly, we also encourage CISA to consider these interdependencies as it revises the NCIRP this year.

Supply Chain Interdependencies. The integrity of the information and communications technology (ICT) supply chain is important to the operation and reliability of critical infrastructure. A compromise of this integrity can result in the delivery of a product with malicious functionality. Similar to other risks, the ICT supply chain risk cannot be fully mitigated, but it can be managed.

This risk cuts across all sectors, but also across functional and organizational boundaries within a given entity, touching multiple activities throughout the procurement cycle. While much of the responsibility for ICT supply chain integrity falls on the cyber asset manufacturers, the end-users bear much of the risk.

⁴ Jose R. Garcia, et al., Oak Ridge National Laboratory, Hydropower Plants as Blackstart Resources (May 2019), <https://www.energy.gov/eere/water/articles/hydropower-plants-black-start-resources>.

⁵ Abhishek Somani, et al., Pacific Northwest National Laboratory, Hydropower’s Contributions to Grid Resilience (Oct. 2021), https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-30554.pdf.

Support from government to help protect the supply chain, testing of components, and better collaboration across the critical sectors in concert with manufacturers are all important opportunities for managing the ICT supply chain risk.

CISA's National Risk Management Center conducts critical infrastructure risk interdependence analyses, including dam failure simulation modeling and cross-sector risks for the electric power sector. Through this effort, CISA may consider analyzing supply chain interdependencies that could lead to cascading risk across multiple sectors. As critical infrastructure owners and operators work to root out potential risk associated with reliance on foreign components, we look to SRMAs like CISA, DOE, EPA, and other federal partners to help address this shared national security responsibility. We must prioritize investments in key supply chains *now* to build out the infrastructure necessary to support the increased demand for electricity needed to leverage technologies key to U.S. competitiveness and national security.

Risk Management. Finally, we encourage our federal partners to continue to work with cross-sector owners and operators to prioritize critical infrastructure risk mitigation—because if everything is critical then nothing is. Instead of trying to achieve the impossible task of protecting every asset from every threat, the electric sector sets priorities to protect the most critical energy grid components against likely threats; to build redundancy into the system to make it more resilient; to coordinate preparation and response efforts with the government; and to develop contingency plans for response and recovery if grid operations are impacted.

DOE has included \$2.5 million for DCEI in its Fiscal Year 2025 Congressional Justification, and CISA has similarly prioritized efforts to designate and support SIEs. As each of these efforts, and others, may progress, we urge our federal partners to harmonize efforts and to streamline initiatives to ensure practical application across interdependent critical infrastructure sectors.

Opportunities and Challenges with Artificial Intelligence (AI)

The energy grid is becoming increasingly dynamic and complex. As EEP's member companies work to build and secure the grid of the future, technological applications like AI offer great potential for American economic competitiveness and innovation, while also creating new challenges.

AI systems have the potential to bring many benefits to society, including enabling electric companies to better analyze and use vast amounts of data and to operate an increasingly complex grid that includes more distributed resources. In the years ahead, the need to significantly expand the capacity of the transmission system will necessitate greater coordination across a wide range of stakeholders.⁶ The increased usage of AI will rely on an expanded network of data centers and data centers rely on large amounts of electricity. As mentioned, we must prioritize investments in

⁶ See DOE, National Transmission Needs Study (Oct. 2023) (finding that significant intra-regional and interregional transmission capacity expansion will be needed to address a range of issues, including increased electricity demand, the need to interconnection new clean resources, alleviate system congestion, and improving reliability and resilience), https://www.energy.gov/sites/default/files/2023-12/National%20Transmission%20Needs%20Study%20-%20Final_2023.12.1.pdf.

critical electric infrastructure supply chains *now* to build out the infrastructure needed to support the increased use of AI across the U.S.

In addition, for the opportunities of AI to be fully realized, it must be developed, deployed, and operated in a secure and responsible way. Security must be a core requirement, not just in the development phase, but throughout the life cycle of the AI systems in the energy sector and across all infrastructure sectors that will support these technological advancements.

Conclusion

Thank you again for holding this hearing. I am hopeful that my testimony underscores the industry's commitment to security and our willingness to work with both public and private partners across all sectors to address all hazards. We appreciate the bipartisan support that grid security legislation historically has enjoyed in Congress and the work you have done to enhance the energy sector's security posture. We look forward to working together to continue to build critical infrastructure security and resilience for the safety, security, and well-being of all Americans.

Senator WYDEN. Thank you, Mr. Aaronson.

And we have five Senators here, so there's a considerable amount of interest. We may be expecting some more, so we will just proceed to get into questions.

Let me start with you, Mr. Turpin, and again, I thank FERC for the cooperation that we have had. Now, you all haven't updated your cybersecurity requirements for commercial dam operators since 2016. And obviously, a lot has changed in cybersecurity over the past eight years. I am of the view that there is a need to update these requirements and incorporate the cybersecurity best practices that generally are part of what other federal regulators abide by. Your thoughts?

Mr. TURPIN. Well, I quite agree. We issued them in 2016 as a way to get the program started. We have been auditing facilities, and from those lessons learned, the full intention is to update those and incorporate the views of other agencies and things that are always being learned in this rather dynamic landscape.

Senator WYDEN. How long will it take to do that? Could you have that ready to go, say, in six months?

Mr. TURPIN. Well, I don't think six months. We will be at 70 percent of the facilities by the end of next year, and I think we will definitely move to update it then. In the interim, we, of course, will be applying anything we have learned as we move forward with all of the entities.

Senator WYDEN. So how long would it take to update the requirements? I appreciate the fact that you all want to make progress. I just think it's important to have a clearly understood kind of loadstar, a real focus that everybody can abide by. I see Senator Cantwell, my partner on the Finance Committee. We are going to have a hearing on cybersecurity and healthcare in the Finance Committee. There may be some broad principles, and here is the Senator from Nevada as well. We will see some principles that will come out of that healthcare hearing, but what goes on with dams isn't necessarily what goes on with cybersecurity for health care. Dams and health care are different.

So your thoughts about getting an actual target date—would nine months work better? I don't want to go month by month, but I do want to get—

Mr. TURPIN. Sure.

Senator WYDEN. I do want to get a target date for an update.

Mr. TURPIN. Yes, absolutely. And I mean, nine months would be achievable, I think.

Senator WYDEN. Good.

Mr. TURPIN. We will see, over the next five months, we will have completed 37 percent of those audits and that will be very informative for updating and getting—

Senator WYDEN. I will quit while I am ahead, nine months.

With respect to oversight, you all have really no mandatory cybersecurity requirements for dams that aren't connected to the internet. I am concerned about foreign spies being able to jump the air gap and hack systems in our network, such as by distributing spyware on thumb drives. Do you agree that U.S. dams need robust cybersecurity defenses, even if their systems are not connected to the internet?

Mr. TURPIN. I do. We started focusing on those that were remotely operable as a way to get the program up and running, but I don't think it comprises the entire universe of what needs to be protected.

Senator WYDEN. All right. One last question: The Department of Homeland Security Cyber Safety Review Board looked into the theft of senior government officials' emails from Microsoft servers and Secretary Raimondo and others, and my understanding is Microsoft products were used widely in the dam sector. Is that right?

Mr. TURPIN. That is correct.

Senator WYDEN. Okay. So how do we take that Cyber Safety Review Board set of conclusions and obviously, Secretary Raimondo and others are concerned about what the rules are going to be, and what do we say about Microsoft and others meeting tough cybersecurity standards coming on?

Mr. TURPIN. Yes, and so, obviously, the report is of great concern, and as it was issued last week, we are going through it and we will be using that to inform any changes we might make, especially as we move forward over the next nine months.

Senator WYDEN. Well, consult with all of us, and we would appreciate that.

Senator Risch.

Senator RISCH. Thank you, Mr. Chairman.

Ms. Wright, I have a series of questions for you. On this issue on dams, do you deal only with dams that generate electricity—and I assume the vast majority of dams do some type of hydroelectric generation—but if you have just a flood control dam or something like that, do you still—are they in your sphere?

Ms. WRIGHT. So Senator, for the dams that provide agricultural or water holdback services, there still can be digital equipment that operate some components with those dams. There can be communication and status indicators that are installed on those dams. For that equipment, certainly, methodologies like cyber-informed engineering and other cybersecurity defenses would be appropriate. Also, as we begin to modernize these agricultural dams to become power-producing dams, as many of the more recent investments allow, that will introduce a significant amount of digital technology, which will change the risk for those agricultural dams. It is compounded by the fact that many of these agricultural dams are located in very rural communities who may not have access to excellent cybersecurity services. So we will have to work on trying to ensure that cybersecurity protections are designed-in as opposed to reactively applied afterwards.

Senator RISCH. So what percent of the dams are—ballpark, if you can give me one—what percent are the ag type dams that don't generate electricity? Are you able to give an estimate there?

Ms. WRIGHT. Senator, I am not today, but I would be delighted to get that answer and bring it back to you.

Senator RISCH. Well then, to get right down to it, how does this work? Do the dam operators come to you? Do you come to them? Are they subject to a regulatory mandate? Where are we on that? Just give me a general idea of how this works.

Ms. WRIGHT. For cyber-informed engineering, our approach is very broad, and we would be very open to working with hydroelectric owners and operators to apply the methodology at their facilities. As of yet, we have not done so, but we are eager for that opportunity. Right now, the owners and operators have voluntary access to a number of services offered by the Department of Energy's CESER organization, offered by DHS's Department of Dams, and other federal entities. Those tools include ones that allow network visibility that helps to rank consequences of cyber threats and that inform how one might perform an incident response activity at a hydroelectric facility.

Senator RISCH. And are there private-sector companies that are involved in this effort also?

Ms. WRIGHT. Yes, sir. With cyber-informed engineering we are attempting to make every one of our developments very public, and we have communities of practice where the private sector learns about cyber-informed engineering and can apply it.

Senator RISCH. So can you give me any kind of an idea of the hydroelectric dams, how many of them are now subject to the CIE methodology? How many of them are in practice? What percent?

Ms. WRIGHT. Right now, not very many. However, the benefit for the hydroelectric sector is that these dams are marvels of U.S. engineering, and because of their age, they have older equipment that is not subject to cyber vulnerabilities. So there is an excellent opportunity to leverage what already exists and build in protections as modernization brings digital equipment into the dam sector.

Senator RISCH. So Mr. Aaronson, your constituency, they are dialed in on this, I assume? Tell me what the thought process is.

Mr. AARONSON. Yes, they are, and we really appreciated the Idaho National Lab's leadership on this. I think cyber-informed engineering is a concept that absolutely reflects our vision of resilient operations. The idea here is, digital equipment is terrific, but we operated the grid for the better part of the 20th century without digital overlay. How can we operate degraded? How can we operate through a cyber incident? How can we rely on non-digital equipment to make it harder for the adversary. You know, one of the things I talk about a lot, just to maybe dig in a little bit, there are two ways to deter an adversary. The first is that the attack doesn't have the intended impact. So an adversary attacks using cyber means and we still maintain operations. The other way that you deter is that an attack has a consequence, which is the purview of our Armed Forces and intelligence community, and increasingly, the electric power sector has a responsibility to support military installations who are supporting forward operations. So this relationship between the electric power sector, defense installations, the intelligence community, and using things like cyber-informed engineering gives us a holistic approach to deterrents where the attack doesn't have the intended impact and our military can do its job.

Senator RISCH. So back to you, Ms. Wright. How rapidly are these dams being restructured to modernize their operations? What's the velocity of that or non-velocity of it that's going on, or are you able to speak to that?

Ms. WRIGHT. I would like to bring some exact numbers back to you—

Senator RISCH. For the record, why don't you do that?

Ms. WRIGHT. But what we were able to observe is that federal entities have granted a number of modernization efforts that are being carried out, both by asset owners and vendors who supply services to the grid, many to refit these agricultural dams to be power-producing and others to add advanced instrumentation to dams to make them more responsive to changing grid conditions.

Senator RISCH. I am assuming—my time is up, but let me close with this—I am assuming, well, we all know that the Idaho National Lab is world-class in control systems, developing operations, understanding them, and of course, that has been going on for decades there because of their work with nuclear. And I believe that the cyber growth there is a result of our expertise in control systems. I am assuming your operations bring the two of those together—the control systems and the cyber operations.

Ms. WRIGHT. Senator, that's right. And thank you for the opportunity to address that. The cyber-informed engineering methodology takes advantage of a practitioner who has been left out of a great many of the cybersecurity conversations, and that is the engineer who designs a system to perform in the first place and operates the critical practices. By leveraging the knowledge of that engineer, you can identify the consequences that would be most impactful in the event of a cyberattack and remediations that may be non-digital and out-of-phase with the adversary to accomplish what my colleague has talked about, deterring the adversary because of the lack of an impact resulting from their activity.

Senator RISCH. That is all quite helpful.

Thank you, Mr. Chairman.

Senator WYDEN. I thank my colleague.

Senator Hickenlooper.

Senator HICKENLOOPER. Yes, thank you, Mr. Chair, and thanks to all three of you for taking time out of your busy lives and being here with us, appreciate that.

Mr. Aaronson, some of the emerging technologies like AI are, obviously, offering exciting opportunities to make our grid more efficient and more reliable—all types of electricity. And making use of these large datasets, I think, can help us predict demand more accurately, and also to manage supply more effectively. To make progress on this potential, President Biden has given an executive order on AI, including a call for a report on how AI can improve our grid infrastructure. So how can we test the impacts of new modernizing technologies on the grid and ensure that those improvements are safe, effective, and defensible? And then, the other question, and this gets back a little bit to what Ms. Wright was talking about—does increased reliance on AI and other technologies introduce new security threats that we should address on the front end?

Mr. AARONSON. I see we only have a little under four minutes to answer this question.

[Laughter.]

Mr. AARONSON. So I will say, at a very high level, first of all, I agree completely that artificial intelligence has a lot of promise for grid operations. Electric companies already are using versions of artificial intelligence. I think the inflection point recently has been

generative AI, but artificial intelligence and machine learning has been a part of this sector for quite some time. At the end of the day, it helps with grid operations, it helps with efficiencies, just as most digitization technologies do. I would say one of the ways, as I said a second ago, and as Ms. Wright was mentioning, part of what we need to do to negate the risk is to make sure that we are not putting all of our eggs in the digital basket, whether it's AI, whether it's just digital controls broadly, or what have you. The ability to operate degraded remains important, so let's not rely exclusively on AI, but for blue sky operations, AI is extraordinary. This risk that comes from artificial intelligence certainly comes from adversaries leveraging it, and it comes from poisoning the datasets that ultimately we would be relying on.

And so, one of the things, I think, you need to think about when we think about artificial intelligence is, at the end of the day, it is hardware, it is software, it is data, it is algorithms. We know how to protect those. Now, do we completely understand the nuances of how AI will change that threat landscape? We do not. And so, I think we need to do this in a thoughtful, deliberative way, but that's not to say that AI is good or bad. AI is here and it is happening and it is valuable to grid operations. Let's just do it in a safe, responsible way.

Senator HICKENLOOPER. I agree completely. And I think touching on that, certainly with hydroelectric generation, oftentimes that generation is somewhat isolated, and generally, it's not cost effective to have redundancy built into those systems at the sufficient level.

Ms. Wright, I have to ask, do you think the NERC standards are sufficient to protect our grid, not just from cyberattacks but from the consequences that prey upon this vulnerability that's unavoidable, I think, to a certain extent when you have remote generation, which in many, not just hydroelectric, but other types of generation can be somewhat isolated. Are the NERC standards sufficient, or do we need additional state and local measures as well?

Ms. WRIGHT. Thank you, Senator.

The NERC standards are sufficient to guide the development of a broadly based cybersecurity program that enables an asset owner to respond to a very broad category of cyber events. Where the Federal Government has advanced knowledge of very specific threats, there are opportunities for the Federal Government to offer aids that are specifically targeted to those threat conditions where a broadly based cybersecurity strategy may not offer sufficient protection. So in that measure, they are both sufficient, but there are additional capabilities that can be offered by the Federal Government.

Senator HICKENLOOPER. So what more should be done? What should we be thinking? What should we be doing?

Ms. WRIGHT. So first, identifying what is the most important, and identifying means to protect it. We cannot, as several of my colleagues have said, we cannot spread our cybersecurity investment across all of the assets. Second—and cyber-informed engineering takes advantage of this—use what is there. Take the basic engineering that is already present at several of the hydroelectric facilities and use it to create defenses. And third, help focus and

optimize investments that asset owners are making by responding with very fast targeted threat information. The ETAC program that was already mentioned and the bulletins by E-ISAC do a great job of providing a broad set of information to the electric sector community. Where those can be further refined for the hydroelectric sector, there will be amazing benefits.

Senator HICKENLOOPER. That's great.

I guess I am out of time. So I will yield back to the Chair.

Senator WYDEN. I thank you, Senator Hickenlooper. We are waiting for our colleagues to return. It's a hectic day here and I am just going to ask a couple of others and see if my friend Senator Risch would like to as well.

Ms. Wright, you gave us a number of concrete recommendations to improve cybersecurity, and I like the breakdown of "do it now", "you might have a little bit of time", and then a longer timeline. What do you think is most important for Congress to help the small dam operators? You know, we tried to say from the beginning, big guys are out in front and are looking at the internet issue and the like, but what do you think would be most helpful for the small dam operators that are not currently subject to cyber requirements and basically are short of resources to protect themselves?

Ms. WRIGHT. I am going to give some very similar answers, Senator, and thank you for that opportunity. First, the small dam operators need targeted information. It is interesting to talk about "everything, everywhere, all at once," but in a small cooperative or small operation where the person doing the cybersecurity may also be in charge of the billing, developing the resources to respond to everything is outside of their means. So targeted threat intelligence, tools that reduce the burden on an asset owner by being very appropriate for application in the hydropower environment, not just something general that applies across the wide expanse of critical infrastructure, and finally, access to technical providers who can aid in the installation of these solutions and potentially for their maintenance over time.

Senator WYDEN. Okay.

I think we are just trying to get everybody's location and see. We have a vote on as well, so we will see if we can wrap up fairly quickly.

Mr. Turpin, apropos of what Ms. Wright is doing with her categories of recommendations: "immediate", "you have a little bit of time", and "maybe a bit more time", are you guys working on anything resembling that? I have tried to open the debate up in terms of when you all thought you could get us an update on the rules.

Mr. TURPIN. Right.

Senator WYDEN. What else are you trying to put on a calendar here, I guess would be the way I would ask it?

Mr. TURPIN. Right. So I mean, right now, the focus is on moving through those audits and trying to understand, you know, how to improve that. I think, as we learn things over this next year, we will definitely be using that on the day-to-day and not waiting for anything to, you know, to have to be done in an update in nine months. I would echo Ms. Wright's thoughts that it's difficult with the smaller operators, given, as you said, the big folks are already out there running full charge. It is when you get down to the bulk

of the operators that are very small organizations that are going to need the help. And so I think we will be trying to look at some of the research that Idaho has done and try to figure out how we could apply that to help the small operators as well.

Senator WYDEN. Well, let's do this. We are going to liberate you all and I want to again thank the Ranking Minority Member. We have worked together on so many things in this Committee and elsewhere, and I think this is really important work to do. I think the pace of change in the cyber area is so extraordinary. We are going to have to have good people like you three working with us as we examine these issues, and we thank you.

We are going to hold the record open for colleagues to submit written questions.

And with that, we will adjourn and thank our witnesses.

[Whereupon, at 3:23 p.m., the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

**U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024 Hearing: Cyber Threats to and Vulnerabilities of
Critical Water Infrastructure in the Energy Sector
Questions for the Record Submitted to Mr. Terry Turpin**

Questions from Senator Ron Wyden

Question 1: During the hearing you said that FERC is able to update the 2016 cybersecurity requirements in a 9 month timeframe. What does the process of updating these requirements entail for FERC?

Response: Under the Administrative Procedures Act and the Paperwork Reduction Act, the Commission is required to seek public comment on the establishment of any compliance requirements and on any proposed collection of information. In addition, after receiving and addressing any comments, the Commission is required to submit the collection of information to the Office of Management and Budget for review.

Are you able to continually perform your regularly-scheduled cybersecurity audits for our country's hydropower dams and update the regulations concurrently?

Response: The Cyber Security Audits for FY24 have all been coordinated and scheduled with the hydropower licensees to be examined. Meeting the 9 month timeframe for the process described above would require some Audits to be rescheduled to a future date. However, a 12-15 month timeframe for issuing revised cybersecurity guidance would be achievable with the existing resources available to the Commission without affecting the audit schedule and other dam safety efforts.

Questions from Senator Maria Cantwell

Question 1: To help make vital cybersecurity upgrades, as well as environmental and safety upgrades, Sen. Murkowski and I have introduced the Maintaining and Enhancing Hydroelectricity and River Restoration Act. The bill would provide a 30 percent federal cost-share to help dam owners make security and other upgrades to keep our baseload hydropower system online for decades to come.

If you are able, can you describe the level of resources that non-federal hydropower facilities must devote to staying ahead of cyber threats? I realize there is a lot of variation across facilities but just give us a sense of what dam owners are facing.

Response: Based on our experience, we have found that owners/operators and others in the industry are facing resource challenges in hiring and retaining qualified cybersecurity staff. It is often difficult to find cybersecurity experts with both the technical knowledge of the legacy specialized devices used at facilities and an understanding of potential impacts to hydropower operations. This pairing is crucial in order to implement and maintain a robust cybersecurity program.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024 Hearing: Cyber Threats to and Vulnerabilities of
Critical Water Infrastructure in the Energy Sector
Questions for the Record Submitted to Mr. Terry Turpin

Do you agree that providing a 30 percent federal cost share for cybersecurity upgrades at non-federal dams would help industry deploy the latest standards and monitoring technology in this evolving space?

Response: Yes, any type of cost sharing program would assist the dam sector in addressing cybersecurity. This may be particularly true for small hydropower operators who have limited financial resources.

Question 2: Hydropower facilities are not the only bulk power system facilities that are under cyberattack threat. There is a vital linkage between grid reliability and resiliency and our nation's natural gas pipelines. I would like your views on how FERC can help protect both from cyberattacks and the potential need for mandatory reliability and cybersecurity standards for pipelines.

Do you believe that the reliability of America's natural gas pipeline system is also at risk due to a growing number of cybersecurity threats?

Response: Yes. As Chairman Phillips has indicated, cybersecurity should be a priority in the energy industry, including for natural gas pipelines.

Do you believe that the mandatory cybersecurity standards that FERC has been setting for the bulk power sector have increased the grid's resilience to cyberattack?

Response: My expertise at the Commission involves the review of hydropower facilities and natural gas projects but does not extend to the Bulk Power System. However, I note that Chairman Phillips has previously indicated that he believes the standards set by FERC have increased the grid's resilience to cyberattacks.

Will future hydrogen pipelines also be vulnerable to cyberattack without mandatory reliability and cybersecurity standards?

Response: My expertise at the Commission involves the review of hydropower facilities and natural gas projects but does not extend to hydrogen pipelines. However, as stated above, cybersecurity should be a priority for any hydrogen pipeline infrastructure.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024, Hearing: *Cyber Threats to and Vulnerabilities of
Critical Water Infrastructure in the Energy Sector*
Questions for the Record Submitted to Ms. Virginia Wright

Questions from Senator Maria Cantwell

Question 1: To help make vital cybersecurity upgrades, as well as environmental and safety upgrades, Sen. Murkowski and I have introduced the Maintaining and Enhancing Hydroelectricity and River Restoration Act. The bill would provide a 30 percent federal cost-share to help dam owners make security and other upgrades to keep our baseload hydropower system online for decades to come.

If you are able, can you describe the level of resources that non-federal hydropower facilities must devote to staying ahead of cyber threats? I realize there is a lot of variation across facilities but just give us a sense of what dam owners are facing.

Dam owners are facing cybersecurity threats ranging from criminal actors who are seeking to monetize denial of critical infrastructure computer systems and services, usually through ransomware, “hacktivists” using digital sabotage to spur a social or political objective, and at least three¹ significant nation-state cyber programs performing persistent offensive actions against United States (U.S.) critical infrastructure to preposition capabilities, demonstrate political and offensive might, and weaken the U.S. resolve to provide support and resources overseas.

To defend against these threat actors, facility operators must, at an absolute minimum²:

- 1) Design cybersecurity capabilities into critical systems³,
- 2) Eliminate or tightly secure external digital connections to vendors, maintenance providers, and other entities,
- 3) Monitor systems and networks for indication of unauthorized access or misuse,
- 4) Be prepared to execute a well-practiced plan for responding to cybersecurity events whether on business systems or operational technology,
- 5) Identify and mitigate vulnerabilities with the highest potential to impact the organization,

Even in the smallest facilities, these activities require skilled practitioners and significant time.

Do you agree that providing a 30 percent federal cost share for cybersecurity upgrades at non-federal dams would help industry deploy the latest standards and monitoring technology in this evolving space?

¹ Office of the Director of National Intelligence. (2024). Annual Threat Assessment of the U.S. Intelligence Community. Retrieved from <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>

² Conway, T., & Lee, R. (2022). The Five ICS Cybersecurity Critical Controls. SANS. Retrieved from <https://sansorg.egnyte.com/dl/R0r9qGEhEe>. Critical Controls.”. <https://sansorg.egnyte.com/dl/R0r9qGEhEe>.

³ National Institute of Standards and Technology (NIST). (2022). NIST Special Publication 800-82 Revision 3: Guide to Industrial Control Systems (ICS) Security. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>

**U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024, Hearing: *Cyber Threats to and Vulnerabilities of
Critical Water Infrastructure in the Energy Sector*
Questions for the Record Submitted to Ms. Virginia Wright**

The “Maintaining and Enhancing Hydroelectricity and River Restoration Act of 2023” provides a 30% federal investment in hydropower upgrades, repairs or reconstructions for multiple objectives, including “to meet federal dam safety and security standards.” As the Federal Energy Regulatory Commission (FERC) updates its hydropower cybersecurity standards first enacted in 2016, operators will likely need to invest in additional technology to meet those requirements. A 30% investment will speed up necessary security upgrades and will be an excellent tool for aiding compliance with more stringent security standards.

To make best use of new technologies, operators will need access to knowledgeable technical practitioners, often not available in rural areas, to install, configure, use, and maintain these technical solutions. The benefits provided by this tax credit would be greatly extended in a pairing with a program to attract early career cybersecurity professionals to support new technology and enhance existing security for hydropower. The National Science Foundation’s Scholarship for Service program⁴ and the Cybersecurity and Industrial Infrastructure Security Apprenticeship Program (CIISAP)⁵ may provide templates for success.

Question 2: Hydropower facilities are not the only bulk power system facilities that are under cyberattack threat. There is a vital linkage between grid reliability and resiliency and our nation’s natural gas pipelines. I would like your views on how FERC can help protect both from cyberattacks and the potential need for mandatory reliability and cybersecurity standards for pipelines.

The tight coupling between natural gas supply and electric power generation, especially during extreme cold or hot weather, has been demonstrated time and again. The Transportation Security Administration (TSA), as the sector risk management agency for pipelines, has taken initial steps toward improving pipeline cybersecurity through a series of mandatory security directives,⁶ but unofficial feedback suggests that there is room to improve both the efficacy and the process around this effort. FERC should work with TSA to assess whether the gas pipeline infrastructure most consequential to electric reliability has requirements commensurate with the associated electric infrastructure and come to consensus on a “high water mark” level of protection for the combined gas-electric energy system from mandatory standards. It is outside my expertise to comment on the authorities and jurisdictional changes that would be necessary to apply North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards to certain natural gas pipelines, or to create a new “Gas Resiliency Organization” similar to the FERC – designated Electric Reliability Organization (currently NERC). However,

⁴ National Science Foundation. (2023). CyberCorps® Scholarship for Service (SFS) Program. Retrieved from <https://new.nsf.gov/funding/opportunities/cybercorps-scholarship-service-sfs/nsf23-574/solicitation#:~:text=The%20SFS%20Program%20provides%20funds,%2C%20quantum%20computing%2C%20and%20aerospace.>

⁵ Siemens Energy. (2024). Industrial Cybersecurity Apprenticeship Program (CIISAP). Retrieved from <https://www.siemens-energy.com/us/en/home/careers/industrial-cybersecurity-apprenticeship-program-ciisap.html>.

⁶ Transportation Security Administration. (2021). Security Directive (SD) Pipeline Security Enhancements for Certain Pipelines Transporting Liquid and Natural Gas, SD 2021-01C. Retrieved from <https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01c.pdf>.

**U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024, Hearing: *Cyber Threats to and Vulnerabilities of
Critical Water Infrastructure in the Energy Sector*
Questions for the Record Submitted to Ms. Virginia Wright**

I note from a technical perspective that there are useful lessons and insight in both to be applied whatever the legal arrangement may be.

Do you believe that the reliability of America’s natural gas pipeline system is also at risk due to a growing number of cybersecurity threats?

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and other agencies have issued repeated warnings describing nation-state actors with the intent and capability to perform attacks on US critical infrastructure^{7, 8}. Our natural gas pipeline system, like all our critical infrastructure, is at risk of being targeted by these persistent, resourced adversaries who need only one variance from secure practice to gain entry. We have seen pipelines fall victim to ransomware⁹ and now understand the impact that can result even from an attack on business systems. Programs like CISA’s hygiene scans,¹⁰ and CyberSentry,¹¹ as well as the Department of Energy’s Cyber-Informed Engineering (CIE),¹² Consequence-Driven Cyber-Informed Engineering (CCE),¹³ the Operational Technology Defender Fellowship,¹⁴ and the Liberty Eclipse program¹⁵ can support standards and regulation by providing U.S. pipeline owners and operators with more robust capabilities for detection and defense.

⁷ Federal Bureau of Investigation. (2024). Chinese government poses broad and unrelenting threat to U.S. critical infrastructure, FBI director says. Retrieved from <https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says#:~:text=FBI%20Director%20Christopher%20Wray%20on%20infrastructure%20is%20a%20prime%20target>

⁸ Jones, D. (2024, February 7). CISA, FBI confirm critical infrastructure intrusions by China-linked hackers. Cybersecurity Dive. Retrieved from <https://www.cybersecuritydive.com/news/cisa-fbi-critical-infrastructure-china-hacker/706935/>

⁹ Cybersecurity and Infrastructure Security Agency. (2023). The Attack on Colonial Pipeline: What We’ve Learned, What We’ve Done Over the Past Two Years. Retrieved from <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

¹⁰ Cybersecurity and Infrastructure Security Agency. (n.d.). Cyber Hygiene Services. Retrieved from <https://www.cisa.gov/cyber-hygiene-services>

¹¹ Cybersecurity and Infrastructure Security Agency. (n.d.). CyberSentry Program. Retrieved from <https://www.cisa.gov/resources-tools/programs/cybersentry-program>

¹² U.S. Department of Energy. (n.d.). Cyber Informed Engineering. Retrieved from <https://www.energy.gov/ceser/cyber-informed-engineering>

¹³ U.S. Department of Energy. (2023). Thinking Like an Adversary Helps Secure Our Critical Infrastructure. Retrieved from <https://www.energy.gov/ceser/articles/thinking-adversary-helps-secure-our-critical-infrastructure>

¹⁴ Idaho National Laboratory. (n.d.). OT Defender. Retrieved from <https://otdefender.inl.gov/>

¹⁵ U.S. Department of Energy. (n.d.). Liberty Eclipse. Retrieved from <https://www.energy.gov/ceser/liberty-eclipse>

**U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024, Hearing: *Cyber Threats to and Vulnerabilities of
Critical Water Infrastructure in the Energy Sector*
Questions for the Record Submitted to Ms. Virginia Wright**

Do you believe that the mandatory cybersecurity standards that FERC has been setting for the bulk power sector have increased the grid's resilience to cyberattack?

NERC's 2023 *State of Reliability Technical Assessment*¹⁶ stated that in 2022, no customer outages resulted from cyber-attack, even with seven reported incidents and attempts. This was attained in an environment with increasing severity of vulnerabilities, threats, and a larger digital footprint which could be targeted by cyber adversaries. Other sectors, including the water sector, transportation, and critical manufacturing did experience impacts.

NERC Reliability Standards, specifically the CIP Standards provide a common framework to formulate and describe the staff, processes, and technology needed for cybersecurity performance. In their compliance with the standards, asset owners achieve auditable results that drive organizational accountability for security performance. The establishment of the standards and the review process create a necessary and desirable exchange between asset owners and regulators.

Will future hydrogen pipelines also be vulnerable to cyberattack without mandatory reliability and cybersecurity standards?

Any infrastructure leveraging digital technology and interconnected architectures will be vulnerable to cyber-attacks, and this includes future hydrogen pipelines. The hydrogen industry already has robust standards for safety¹⁷ because of hydrogen's flammability and propensity to affect materials. The application of Cyber-Informed Engineering can leverage these safety controls to limit the impacts that a cyber-attack on hydrogen pipelines could have, and INL researchers have described how CIE could be applied in a hydrogen generation project¹⁸. In the National Cybersecurity Strategy¹⁹, the White House cites the need for performance-based regulations, built on existing frameworks, standards, and guidance and encourages adoption of secure-by-design. As hydrogen emerges as a key aspect of our critical energy infrastructure, establishing such regulations early in the subsector's maturity will allow those standards to be designed into the technologies leveraged in the sector.

¹⁶North American Electric Reliability Corporation. (2023). Technical Assessment. Retrieved from https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Technical_Assessment.pdf

¹⁷ U.S. Department of Energy. (n.d.). Safe Use of Hydrogen. Energy.gov. Retrieved from <https://www.energy.gov/eere/fuelcells/safe-use-hydrogen#:~:text=A%20number%20of%20hydrogen's%20properties,in%20case%20of%20a%20leak.>

¹⁸ U.S. Department of Energy. (2013). Small Modular Reactors: Nuclear Fission to Markets. Idaho National Laboratory. Retrieved from https://inldigitalibrary.inl.gov/sites/sti/sti/Sort_46017.pdf

¹⁹ White House. (2023). National Cybersecurity Strategy 2023. Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024 Hearing: *Cyber Threats to and Vulnerabilities of*
Critical Water Infrastructure in the Energy Sector
Questions for the Record Submitted to Mr. Scott Aaronson

Questions from Senator Maria Cantwell

Question 1: To help make vital cybersecurity upgrades, as well as environmental and safety upgrades, Sen. Murkowski and I have introduced the Maintaining and Enhancing Hydroelectricity and River Restoration Act. The bill would provide a 30 percent federal cost-share to help dam owners make security and other upgrades to keep our baseload hydropower system online for decades to come.

Can you describe the level of resources that non-federal hydropower facilities must devote to staying ahead of cyber threats? I realize there is a lot of variation across facilities but just give us a sense of what dam owners are facing.

Do you agree that providing a 30 percent federal cost share for cybersecurity upgrades at non-federal dams would help industry deploy the latest standards and monitoring technology in this evolving space?

Answer 1:

Edison Electric Institute (EEI) members provide electricity for nearly 250 million Americans and operate in all 50 states and the District of Columbia. For EEI's member companies, securing the energy grid from all hazards, including cyber threats, is a top priority.

While most critical infrastructure is owned by the private sector, the federal government can play a role in providing the threat intelligence needed to stay ahead of cyber threats and in delivering the resources necessary to do so, especially when it comes to defending against nation-state actors. Access to intelligence helps EEI's member companies build security into our planning, which is a more cost-effective way to reduce risk.

EEI's member companies and the electric power sector take a "defense-in-depth" approach with several layers of security strategies designed to eliminate single points of failure. As part of that approach, many EEI member companies deploy North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) controls at their hydropower facilities to enhance their security posture even though these standards are not required for non-bulk electric system facilities. EEI member companies also actively engage with the Cybersecurity and Infrastructure Security Agency's (CISA) Dam Sector Coordinating Council to help shape security policy for hydropower facilities.

EEI's member companies welcome the opportunity to work with Congress, NERC, CISA, and other federal partners to discuss the resources necessary to maintain a strong cybersecurity posture at hydropower facilities.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Water and Power
April 10, 2024 Hearing: *Cyber Threats to and Vulnerabilities of*
Critical Water Infrastructure in the Energy Sector
Questions for the Record Submitted to Mr. Scott Aaronson

Question 2: Hydropower facilities are not the only bulk power system facilities that are under cyberattack threat. There is a vital linkage between grid reliability and resiliency and our nation’s natural gas pipelines. I would like your views on how FERC can help protect both from cyberattacks and the potential need for mandatory reliability and cybersecurity standards for pipelines.

Do you believe that the reliability of America’s natural gas pipeline system is also at risk due to a growing number of cybersecurity threats?

Do you believe that the mandatory cybersecurity standards that FERC has been setting for the bulk power sector have increased the grid’s resilience to cyberattack?

Will future hydrogen pipelines also be vulnerable to cyberattack without mandatory reliability and cybersecurity standards?

Answer 2:

The 2023 Annual Threat Assessment of the U.S. Intelligence Community said, “China almost certainly is capable of launching cyberattacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines.”¹ As technology continues to evolve, so, too, do the threat actors who seek to undermine U.S. critical infrastructure. This is why the electric power sector focuses on enhancing visibility into critical control systems, improving situational awareness and information sharing for emerging threats, and ensuring we have comprehensive plans in place to respond and recover quickly when incidents occur.

Following a May 2021 ransomware attack that disrupted a key pipeline, the Transportation Security Administration (TSA) issued security directives mandating minimum cybersecurity standards for the nation’s critical pipelines.² Since then, TSA has collaborated with owners and operators to make the standards more outcomes-based rather than compliance-based.

EEI’s member companies strongly support efforts to address risk through an outcomes-based approach that is harmonized with existing federal efforts. At a time when the national cyber workforce is already stretched thin, we welcome the opportunity to work with Congress, TSA, FERC, and any other federal partners necessary to discuss maintaining critical infrastructure security and resilience while also avoiding duplication of effort.

¹ <https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>

² <https://www.tsa.gov/news/press/releases/2023/07/26/tsa-updates-renews-cybersecurity-requirements-pipeline-owners>



MARK GORDON
GOVERNOR OF WYOMING
CHAIR

MICHELLE LUJAN GRISHAM
GOVERNOR OF NEW MEXICO
VICE CHAIR

JACK WALDORF
EXECUTIVE DIRECTOR

April 10, 2024

The Honorable Ron Wyden
Chair
Subcommittee on Water and Power
Committee on Energy and Natural Resources
United States Senate
304 Dirksen Senate Building
Washington, DC 20510

The Honorable James E. Risch
Ranking Member
Subcommittee on Water and Power
Committee on Energy and Natural Resources
United States Senate
304 Dirksen Senate Building
Washington, DC 20510

Dear Chair Wyden and Ranking Member Risch:

In light of the Subcommittee's April 10, 2024, hearing, Cyber Threats to and Vulnerabilities of Critical Water Infrastructure in our Energy Sector, attached please find Western Governors' Association (WGA) Policy Resolution 2022-05, Cybersecurity. The resolution provides recommendations to address threats to critical infrastructure and calls for improved agency coordination.

I request that you include this document in the permanent record of the hearing, as it articulates Western Governors' policy positions and recommendations related to this urgent issue.

Thank you for your attention to this matter and your consideration of this request. Please contact me if you have any questions or require further information.

Sincerely,

A handwritten signature in black ink that reads 'Jack Waldorf'. Below the signature, the name 'Jack Waldorf' and title 'Executive Director' are printed in a standard font.

Jack Waldorf
Executive Director

Attachment



Policy Resolution 2022-05

Cybersecurity

A. **BACKGROUND**

1. In the age of automation, digitization, big data, artificial intelligence, and machine-to-machine learning, the United States' capabilities to prevent, detect and respond to cyberattacks are of ever-growing importance to our society. The cybersecurity of our nation is an all-of-government and industry-wide endeavor.
2. Aging information technology (IT) infrastructure and systems pose serious cybersecurity risks and increase vulnerabilities for government and organizations. Due to the longstanding financial and national security implications of prior cybersecurity breaches resulting in data theft and other adverse outcomes, modernizing these systems to help prevent successful cyberattacks and better safeguard our data is imperative.
3. The COVID-19 pandemic has transformed society and accelerated the shift to a virtual environment, further increasing vulnerabilities across systems as threat actors become more complex and widespread. Ransomware attacks, a type of malicious software attack that threatens to publish sensitive information or impedes access to data or computer systems until the victim pays a ransom to the attacker, have grown by 148 percent due to the rise in remote activities. These attacks can shut down public and private sector operations, posing particular challenges to critical infrastructure functions.
4. Cybersecurity is especially imperative for critical infrastructure, which includes the nation's electric grid, energy resource supply and delivery chains, finance, communications, election systems, the chemical industry, commercial facilities, critical manufacturing, defense industrial base, emergency services, food and agriculture, government facilities, health care and public health, information technology, transportation, and water and wastewater systems. Large-scale cyber incidents, including the SolarWinds and Colonial Pipeline attacks, demonstrate the risk cybercrime now presents to national security.
5. Addressing cybersecurity needs across critical infrastructure sectors is further complicated by the increasing interdependency and interconnectedness of our nation's data systems to a myriad of non-critical infrastructure systems and a dynamic threat environment. Effective cybersecurity programs require strategic and functional relationships and information sharing between federal, state and local levels of government, and the public and private sectors.
6. The cybersecurity of their states and the nation is a high priority of Western Governors. State governments are responsible for securing public networks, the state's digital assets, and citizen data, as well as coordinating their cybersecurity efforts with federal agencies and potentially-affected private entities (e.g., utilities, financial institutions, transportation, and health). Governors lead efforts to plan and implement state cybersecurity programs, respond to cyberattacks, and investigate intrusions.

7. National Guard cyber protection teams, serving in 59 cyber units, provide invaluable assistance to states across the country with threat assessment and cyber incident response and remediation. Currently, states can mobilize Guard members through State Active Duty (SAD) and Title 32 of the U.S. Code. Supported by state funds, Governors can activate SAD for disasters or homeland defense, although state constitutions or statutes often constrain deployment of the Guard to state emergencies. Title 32 gives Governors the authority to order the Guard to duty, using federal funds, with the approval of the President or the Secretary of Defense. However, this process can create barriers to rapid and nimble action in the face of cyberattacks. While both of these functions are vital resources, potential exists to further leverage the capabilities of the National Guard for the cybersecurity posture of states.
8. Although state and local governments remain significant targets for cyberattacks, they often lack adequate funding to address these issues and modernize their systems. According to a study by Deloitte and the National Association of State Chief Information Officers, state cybersecurity budgets comprise less than 3 percent of their overall IT budgets.
9. Prior to the passage of Public Law 117-58, the Infrastructure Investment and Jobs Act, the Homeland Security Grant Program was the primary federal mechanism to provide cybersecurity funding to state, local, territorial, and Tribal governments. Over the years, less than 4 percent of that funding was allocated to cybersecurity. Such low levels of funding have been insufficient for states to meet their pressing, and rapidly growing, cybersecurity needs. The Infrastructure Investment and Jobs Act sought to address this issue by establishing a much-needed standalone cybersecurity grant program for state and local governments, marking a huge increase in federal support for state and local cybersecurity efforts.
10. The \$1 billion program will be administered by the Federal Emergency Management Agency (FEMA) for four years, with the Cybersecurity and Infrastructure Security Agency (CISA) serving in an advisory role. Funding will be distributed to states, tribes, and territories, who must allocate about 80 percent to their localities. States must also meet varying match requirements to share the financial burden and account for cybersecurity costs in their budgets.
11. State election systems remain targets of foreign interference. As Governors, we remain committed to protecting our states' election systems. There is nothing more fundamental to the enduring success of our American democracy, and we take seriously our responsibility to protect the integrity and security of our elections. This is an imminent national security threat that transcends party lines. This is a matter of protecting and preserving fair elections – the underpinning of our democracy.
12. The Office of Management and Budget and Department of Homeland Security May 2018 Federal Cybersecurity Risk Determination Report and Action Plan concluded that 71 of 96 federal agencies are at risk or high risk of cyber intrusions. It also determined that federal agencies are not equipped to determine how threat actors seek to gain access to their information. This deficiency results in ineffective allocations of the agencies' limited cyber resources.

13. Currently, there is a severe deficit of cyber workers, especially in government. Our nation cannot defend itself without a well-trained, experienced cyber workforce. The public sector must dedicate resources to “K through gray” cybersecurity education, training, work-based learning and apprenticeships, and recruitment programs and encourage the private sector to do the same through effective policy.
14. While investments in workforce development and human capital are a key component in addressing workforce shortages, states can leverage other tools to meet the scale of these challenges. Technology and innovation will be needed to alleviate workforce strains and keep pace with a wide range of attacks while also reducing burdens associated with operational functions.

B. GOVERNORS’ POLICY STATEMENT

1. Western Governors urge Congress to improve coordination of congressional oversight and legislative activity on cybersecurity, including by reducing the number of committees in Congress that have jurisdiction over this issue.
2. Western Governors support modernizing our systems to be more resilient to minimize vulnerabilities and protect against unauthorized access to information and data theft. We request that FEMA and CISA work collaboratively with Governors in executing the newly created state and local cybersecurity grant program to ensure the funds are administered in a flexible and measurable manner to all states, Tribes, and territories. Designated, flexible, and measurable cybersecurity funding would help ensure that states, Tribes, and territories have resources to build resilient systems and meet growing cybersecurity challenges.
3. The federal government has a responsibility to provide adequate funding for states to meet election security needs. Western Governors encourage Congress and the Administration to work cooperatively with states in developing election security legislation and mandates, and to fully fund implementation.
4. Federal agencies must engage in early, meaningful, substantive, and ongoing consultation with Governors or their designees on all aspects of cybersecurity. Western Governors advise the federal government to clearly define the roles for state representatives in CISA’s recently established Joint Cyber Defense Collaborative.
5. Western Governors recommend that the federal government continue the DHS State, Local, Tribal, and Territorial Engagement Program, which provides cybersecurity risk briefings and resources to Governors and other officials. The Governors also support CISA Central, with which state chief information officers regularly interact.
6. The federal government must continue to clarify the roles and responsibilities of federal agencies in preventing, preparing for, and responding to cyberattacks. Centralized authority, points of contact, and formalized communication pathways are necessary to address increasingly complex threats. In addition, these pathways must occur at each level within government and other organizations.
7. The federal government must also improve agency coordination to use often-constrained security resources more efficiently and harmonize disparate regulations that put an

unnecessary burden on state governments. Western Governors urge Congress to provide appropriations for the Office of the National Cyber Director commensurate with the importance of the office's position in leading federal coordination efforts.

8. The National Institute for Standards and Technology (NIST) Cybersecurity Framework and other standards can facilitate effective, consistent, and risk-based decision making in government and industry. Real-world simulations of attacks on critical infrastructure are essential to prepare our nation for potential threats.
9. The federal government should build a stronger international framework for cybercrime and use the full range of economic tools, including travel and financial sanctions, to deter cyberattacks organized, supported, or harbored by nation-states.
10. Western Governors recognize the need for states, Tribes, and territories to work together to address gaps or vulnerabilities in these systems to reduce disruptions. The public sector, particularly the federal government, must take steps to mitigate global supply chain and national critical infrastructure risks (e.g. ransomware) in collaboration with the private sector.
11. Western Governors implore Congress and the Administration to reduce bureaucratic burdens and change restrictive guidance related to deploying the National Guard under USC Title 32 for cybersecurity prevention, detection, and response activities. Clarifying the use of the National Guard for these purposes and streamlining the approval process would improve state capacity to confront cyberattacks, contain threats, and help protect neighboring jurisdictions. Western Governors also support efforts to develop civilian cybersecurity reserves, which help alleviate workforce shortages and augment National Guard forces.
12. The Administration should propose, and Congress should provide, long-term authorization and sufficient appropriations for high-quality cybersecurity education and workforce development programs to grow and sustain the cybersecurity workforce, including those that target underrepresented populations, those that include rotational components to retain personnel, and work-based learning opportunities such as apprenticeships. The federal government should also expand the CyberCorps: Scholarship for Service program and continue to support educational initiatives, such as NIST's Initiative for Cybersecurity Education and National Centers of Academic Excellence in Cyber Defense.
13. Government and industry should increase the cybersecurity awareness of government and private employees through training and education. Western Governors encourage the federal government to develop a national cybersecurity literacy and awareness campaign to educate citizens about how to stay safe online and prevent effective cyberattacks.
14. Western Governors support incentives for the creation of and participation in programs that encourage information sharing across all levels government, industry verticals, and regions. We also support other policies that incentivize the private sector to improve cybersecurity and share information regarding cyber threats as early as possible, including policies to improve access to information or create common standards for information-sharing. The federal government should emphasize the benefits of information sharing, while alleviating private sector concerns with this essential communication. The federal

government and states should continue to investigate liability protections, such as safe harbor provisions, for entities that report cyber intrusions.

15. Our nation requires innovation in detecting, preventing, and responding to continually evolving cyber threats. More research is required to understand the use of blockchain and encryption by perpetrators and its utility for defense against cyber threats, and address vulnerabilities of other emerging technologies, including connected vehicles and Internet of Things devices. The federal government should provide funding and technical assistance for these and other types of cybersecurity research and development.

C. GOVERNORS' MANAGEMENT DIRECTIVE

1. The Governors direct WGA staff to work with congressional committees of jurisdiction, the Executive Branch, and other entities, where appropriate, to achieve the objectives of this resolution.
2. Furthermore, the Governors direct WGA staff to consult with the Staff Advisory Council regarding its efforts to realize the objectives of this resolution and to keep the Governors apprised of its progress in this regard.

This resolution will expire in December 2024. Western Governors enact new policy resolutions and amend existing resolutions on a semiannual basis. Please consult <http://www.westgov.org/resolutions> for the most current copy of a resolution and a list of all current WGA policy resolutions.

