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 Engineering[1]. 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 energy[2], 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 States[4] 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 MW[6] 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 old[8] 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 capacity[9]. 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 years[10]. 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 added[11]. 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 cyberattack[13], illustrated in the 2013 attack on Bowman Dam in Rye, New York[14]. 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 Uría-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 Ave[15].

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 Ukraine[16]. 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 community[17].

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 equipment[18] 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 assets[20].

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 functions[21]. 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 functions[22] 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 Strategy[24] 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 Strategy[25], the National Cybersecurity Strategy Implementation Plan[26], 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 program[28], INL is implementing the recommendations in the national strategy by spreading awareness of CIE[29], working with universities to incorporate CIE into their engineering education[30], and developing tools for easier implementation of the methodology[31]. 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 Guide[32] 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, Puesh. 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." *McCrary Institute* , Auburn University, https://mccrary.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 Pittsburg. 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://inldigitallibrary.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 incidents[33]. 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 HydroSHIELD[35].

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:/ Cybersecurity & Infrastructure Security Agency. n. d. "Downloading and Installing CSET." Accessed April 4, 2024. https://www.cisa.gov/downloading-and-installing-cset.

[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 systems[36].

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 partners[37].

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 WPTO[38] performs research and development and creates tools to aid hydropower-asset owners in assessing where cybersecurity investments are needed[39] 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 federal[41] 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 Engineering[42] 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 Fellowship[43] 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 Service[44] 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 metrics[45] 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.