TESTIMONY OF MR. VERGLE GIPSON
SENIOR ADVISOR, IDAHO NATIONAL LABORATORY

before the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMLELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, & INNOVATION

concerning

"BUILDING ON OUR BASELINE: SECURING INDUSTRIAL CONTROL SYSTEMS AGAINS CYBERATTACKS"

SEPTEMBER 15, 2022

Introduction

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee, thank you for the invitation to testify on a topic critical to the security of our nation. My name is Vergle Gipson, and I'm a Senior Advisor at Idaho National Laboratory. Prior to joining the Laboratory five years ago, I retired from the Senior Executive Service after more than 30 years at the National Security Agency working a variety of cyber-related issues. I'm an expert in cyber threat and critical infrastructure cybersecurity.

Testimony

By nearly all measures, cyber risk to our nation's critical infrastructure continues to increase. Unfortunately, this trend is likely to continue because our adversaries view cyber vulnerabilities as a low-risk, often unattributable means by which to strike our nation. Foreign and domestic acts of cyber-enabled sabotage are possible because our nation's infrastructure is highly dependent on industrial control systems. Widely known as "operational technology," industrial control systems

govern and execute complex processes at substations, manufacturing facilities, water treatment facilities, military bases, transportation hubs, and much more. From regulating the flow of oil and natural gas in pipelines to purifying our drinking water supply, millions of digitally connected devices – such as protective relays, programmable logic controllers, and human-machine interfaces – keep our society running day-in and day-out. All of the nation's 16 critical infrastructure sectors rely on operational technology.

In contrast to Information Technology (IT) like personal computers, business networks, and databases, operational technology is not as widely protected. There are several reasons for this, and I will touch a on few of them:

- Refresh cycle: While most IT is upgraded or replaced every three to five years, operational technology is often built and designed to last for decades. Many of the industrial control systems in our critical infrastructure today were designed 20 or more years ago, before the need for robust cyber defenses was fully understood.
- Standardization: Most IT is designed, installed, and operated using industry best practices for cybersecurity that are widely adopted and accepted. By contrast, operational technology is often a custom engineering design, created to meet exact specifications for its end user.
- Management: IT is actively managed — software and firmware are updated, and patches are routinely installed. Operational technology is typically passively managed, only updated or replaced if a noticeable failure or fault occurs.
- Discovery tools: The IT industry has developed a wide range of products to detect and discover malicious code and vulnerabilities. For instance, think about the wide variety of anti-virus software available for purchase and use on home or business computers. By contrast, few discovery tools exist for operational technology.

- Intent: While threats against IT systems target information like financial data or proprietary business dealings, threats against operational technology target physical processes like the flow of electric power or the production of our food supply.

To help simplify this extraordinarily complex issue, I find it helpful to think of cyber risk as a function of threats, vulnerabilities, and consequences. As adversaries increase their capabilities and their intent to conduct malicious cyber activity, the threat to U.S. infrastructure rises. As the complexity and number of digital systems increases, the cyber vulnerabilities in U.S. infrastructure also rises. Not only are those vulnerabilities inherent in the systems themselves, but they're also introduced by adversaries through supply chain operations and other means. And as our society becomes more reliant on an increasing number of digitally connected systems, the consequences of cyberattacks also increase. In short, multiple factors affecting cyber threats, vulnerabilities, and consequences are driving the increase in cyber risk, and that trend is likely to continue.

In the last two decades, the risk of a cyberattack against our critical infrastructure has transitioned from being theoretically possible to documented and proven. As protection strategies, tools, and expertise have improved in the IT environment, adversaries have likewise improved their techniques and are expanding to other target-rich environments including critical infrastructure. However, this cyber risk can be greatly reduced and, in some cases, eliminated. We at Idaho National Laboratory, with our unique capabilities in cybersecurity for operational technology, are working with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), the Department of Defense (DoD), industry, and others to reduce cyber threats, vulnerabilities, and consequences.

Idaho National Laboratory (INL) is one of 17 U.S. Department of Energy (DOE) national laboratories and is managed by Battelle Energy Alliance. Located in Idaho Falls, Idaho, INL employs more than 5,400 researchers and support staff focused on innovations in nuclear research, renewable energy systems, and national security solutions. 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, engineering, and processes needed to secure systems and provide critical function assurance. With a large 890 square mile site, INL can not only create new industrial control system security solutions, but also test and demonstrate those security solutions at scale in full-size test environments.

For more than 18 years, CISA and its predecessor organizations have leveraged INL's unique capabilities and proven leadership in the discovery, development, testing, and demonstration of advanced technology solutions. Specifically, INL's experience providing solutions to address critical infrastructure security needs, and INL's relationships with both private and public stakeholders, has helped CISA address the needs of the entire critical infrastructure community against the ever-evolving set of natural and man-made hazards the nation faces. INL technical support to CISA includes:

- Vulnerabilities: Discovering and/or helping develop mitigations against hundreds of vulnerabilities affecting operational technology products including several high-profile vulnerabilities impacting U.S. Critical Infrastructure.

- Hunt and Incident Response Operations: Providing industrial control systems technical expertise during responses to operational technology-related incidents including identifying vulnerabilities and hunting for evidence of threat actors.
- Analysis: Developing analytic tools and platforms that enable both CISA and critical infrastructure partners to detect malicious and anomalous behavior, to identify and understand cross-sector dependencies, and to perform analysis of all potential hazards.
- Assessments: Developing and continuing to support methodologies and tools focused on the assessment and design review of critical infrastructure systems and environments.
- Training: Creating and delivering training focused on educating the industrial control systems and IT workforce on cybersecurity, and bridging the knowledge gap that exists within organizations, through unique hands-on experiences and virtual learning environments that require them to collaborate.

INL stands ready to do even more to reduce the cyber risks to our nation's critical infrastructure. INL's unique facilities are singularly positioned to support a wide variety of research, analysis, testing, and validation opportunities for federal and industrial collaborators. Comprising a cyber-physical infrastructure test range, co-located laboratories, several technology-specific test ranges, and available airspace, this premier research environment allows testing - from modeling and simulation to full-scale – to be conducted safely and securely. More than 100,000 square feet of specialized laboratory testing space staffed by experts in operational technology, cybersecurity, power systems engineering, vulnerability assessments, and dependency analysis enables the creation, testing, and demonstration of the next-generation control system cybersecurity solutions the nation needs now and well into the future.

To address some of the most critical research and capability gaps surrounding industrial control system cybersecurity, INL recommends the following:

1. Creation of an industrial control systems cybersecurity Center of Excellence: This Center of Excellence would serve as a focal point for increased information sharing among a community of practice that includes government, industry, academia, and other national laboratories; create a vehicle for further investments in cybersecurity research and development; and advance the science of securing operational technology to stay ahead of our cyber adversaries' rapidly evolving tactics.
2. Directed research to mature Cyber Informed Engineering (CIE): Cyber Informed Engineering encourages addressing cybersecurity issues early in the design lifecycle of engineered systems to reduce cyber risks. The Secretary of Energy recently released a National Cyber Informed Engineering Strategy focused on the energy sector that could be expanded to address all U.S. critical infrastructure.
3. Expansion of INL cyber-physical test environments to support development of cyber risk mitigations: This expansion would enable the research and development of mitigation strategies, the analysis of product and system vulnerabilities, the understanding of emerging adversary tactics, and other cybersecurity efforts reliant on representative test environments. This expansion should include the addition of full-scale, sector-specific, cyber-physical test environments for priority infrastructure systems, including water and wastewater, transportation, oil and natural gas, and critical manufacturing.

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