TESTIMONY OF

MR. RALPH F. LEY

DEPARTMENT MANAGER WORKFORCE DEVELOPMENT AND TRAINING

NATIONAL AND HOMELAND SECURITY DIRECTORATE

IDAHO NATIONAL LABORATORY

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

HOMELAND SECURITY SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, & INNOVATION

"THE CYBER TALENT PIPELINE: EDUCATING A WORKFORCE TO MATCH TODAY'S THREATS"

JULY 29, 2021

Chairwoman Clarke, Ranking Member Garbarino, and members of the committee, it is an honor and privilege to be with you today. My name is Ralph Ley, and I am the department manager for workforce development and training within the national and homeland security directorate at Idaho National Laboratory (INL). I'm grateful for the opportunity to testify on issues regarding the nation's cyber talent pipeline and ways to ensure our workforce is ready to meet future threats.

I want to thank this subcommittee for addressing what we believe is a foundational workforce development and education issue facing this nation from the standpoint of a continuously changing cyber threat landscape requiring professionals who have career-long access to updated curriculum containing new tactics, techniques, and procedures to sufficiently protect their networks and systems.

Our conversation today is an important step forward for establishing a unified team with a focused approach toward implementing solutions to cyber workforce issues and progress - our security will benefit from this unified effort, it is greatly needed and appreciated.

INL's nationally recognized expertise in industrial control systems (ICS) or operational technology (OT) cybersecurity stems from its long history and primary mission to conduct research, development and demonstration of solutions that assure the advancement of nuclear energy, clean energy, and critical infrastructure protection technologies. From the beginning related infrastructure were full of control systems to ensure their safe and efficient operations.

My department takes great pride in having the opportunities and responsibilities to lead, influence and execute a broad portfolio of educational programs and research which address cybersecurity issues and workforce development needs.

For over a decade Department of Energy (DOE) and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) sponsored ICS cybersecurity training courses have been conducted at INL in immersive classroom and hands-on learning environments. The target audience has been primarily private sector businesses and utilities who need their staff to understand the differences between protecting IT and OT networks and systems. Simply put, IT cybersecurity is based on keeping a business's information readily available, accurate, and dependable, whereas OT cybersecurity lives in a cyber-physical world manipulating businesses assets which can impact production and throughput/output of materials. These sponsored courses offered by INL are designed to bridge the knowledge gap by bringing together people who operate either their company's IT systems or OT systems and force them to work together in realistic work settings. The results of these courses accompanied by the significant increase in recent threats to OT systems has contributed heavily to industry's awareness, or better described – awakening - to the need for improved OT cybersecurity practices accompanied by established standards for workforce development and training.

Processes and procedures for securing IT systems are well documented in a wide variety of general overarching best practices and some industry specific standards. The same guidance has been late coming for securing OT systems, however this guidance is now much more readily available than even just a few years ago. Along with established cybersecurity procedures or standards has been guidance on what education and training is required by cyber-professionals to implement these new measures.

The National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) workforce framework, often referred to as the NICE Framework, is arguably the most well-known cybersecurity education and training standard. It addresses the education and training needs of the cybersecurity workforce by providing common vocabulary for the field and a detailed list of cybersecurity Knowledge, Skills, Abilities, and Tasks (KSATs) for each identified cyber work role. While the NICE Framework is intended to be applicable to a wide range of cybersecurity workers in an organization, IT roles and IT KSATs are ultimately the focus of the competency recommendations provided. As IT and OT systems become increasingly connected and vulnerabilities associated with both increases, the need to extend the framework to incorporate ICS systems has begun.

INL in collaboration with academic and industry partners has endeavored to assist in the efforts to address the lack of a similar framework and KSATs for OT work roles. A major first step was INL's collaboration with Idaho State University (ISU) and La Trobe University (LTU) in a two-phased project resulting in the, "*Building an Industrial Cybersecurity Workforce: A Manager's Guide"*. This non-prescriptive document is a first step towards identifying the unique knowledge and job roles required of ICS professionals and establishing a capable workforce.

NIST has recognized the value of this effort and has requested INL's participation in expanding the NICE Framework to incorporate OT roles and OT KSATs.

Lack of recognized OT job roles and associated KSATs has had a definite influence on the existing availability of OT-specific workforce training offerings. Years of research and development of education and training courses for CISA, DoD, and industry, collaboration with academic institutes, and interviewing students identified other potential influencers that appeared to be impeding the flow of the IT and OT cyber talent workforce pipeline. To validate INL's findings, we created a joint INL-ISU Industrial Cybersecurity Community of Practice (ICSCOP) recurring workshop and invited over 150 representatives from universities, government entities, and industry experts to participate. Participants were provided presentations on two known cyber workforce issues: 1) Curriculum Standards for ICS cyber-related degree programs, and 2) ICS workforce development factors. The resulting group discussion by participants validated previously identified influencers and established working groups to address solutions. Influencers span IT and OT topics and included:

- First, standardized curriculum. There needs to be standard curriculum requirements for cyber-related degree programs, IT and OT focused, offered by academic institutes. For example, the requirements to attain a degree in cybersecurity varies from university, to university making is hard for employers to know the level of competency of any individual possessing such a degree and seeking employment. Lack of standards also leave the individual unsure of their qualifications for jobs solely based on the degree.
- Second, employers do not understand the existing cybersecurity related tasks their employees are responsible for in their daily jobs. This makes it impossible to know what each employee's cyber education and training requirements are or to create a roadmap for improvement. It also makes it difficult to identify if there is a need to hire additional staff to address unfilled cyber job roles. Employers require a holistic process that can assist with identifying the existing cyber job roles of their employees, identify potential personnel gaps, suggest individual cyber education and training roadmaps, and link the level of education of employees to the cyber "health" of the organization.
- Third, Human Resource (HR) departments do not possess the necessary tools to identify and hire the best candidate for a cyber-related job position. They are forced to use the same hiring methods as other positions within their business: reviewing resumes and conducting interviews. Although academic institutes cannot create different degree programs tailored specifically for each individual business's needs, skills testing matched to standardized KSATs would assist employers with this issue and provide academic institutes a view of the most requested cyber skills by employers to adjust degree programs.
- Fourth, as mentioned previously, the pace of new cybersecurity emerging threats, new technology, vulnerabilities, etc., is faster than most of the existing board certification processes used by academic institutes to approve updated curriculum. This makes it harder for academic institutes to rapidly update materials and offer students programs with the most recent information. A central clearinghouse for approved new ICS cyber

related curriculum readily available for academic institutes to adopt if desired may be one solution.

- Fifth, closely aligned with the first influencer is the lack of availability of standardized hands-on or near hands-on training apparatus for ICS cybersecurity education programs, especially in rural geographical areas. A shared repository of curriculum and capabilities provided in a hub-and-spoke regional model where all academic institutes benefit from a national repository of resources is the needed.
- Sixth, the existing workforce needs continuing education options from local academic institutes other than the time consuming and expensive solution of employees obtaining another degree. The continuing education options must be trackable by individuals throughout their cyber careers and identify for employers the currency of the education the person has received. Academic institutes have begun establishing their own educational badge and/or credential systems. A recognized national standard for these systems is needed before employers will put stock in the validity of these necessary systems.

Outcomes from the ICSCOP workshops and working group meetings are not limited to validation of influencers impeding the flow of the cyber talent pipeline. INL is working with State and local government entities, academic institutes at all levels of education, and business around the State as collaborators and sounding boards of the workforce development solutions explored. The thought process to this approach is that if solutions can work in one State, they have a high probability of working in others.

An example of these activities is the Associate Lab Director for N&HS is a co-chairperson on a new task force led by the Idaho Department of Commerce. The purpose is to make Idaho the most secure state against cybersecurity attacks aimed at businesses, governmental entities, institutions, and citizens which will substantially improve and protect our growing economy. Activities include coordinating, informing, and training Idahoans across the state as to safeguards and resources from the perspective of many experts and interested groups. Recommendations from the taskforce will inform the Governor, Legislature and other stakeholders on major cybersecurity threats and opportunities for Idaho. This effort can easily be replicated by other States desiring a collaborative approach to addressing cybersecurity issues.

Other efforts include Idaho National Laboratory (INL) in collaboration with industry, academia, and the science and research communities kicked off a multi-year Idaho Cyber Research Project (ICRP). This project is designed to apply existing solutions to some of the major influencers. A small army of interns (20 to 30) from Idaho universities and 2-year colleges are assisting INL staff by visiting organizations desiring assistance with cyber “health” issues and providing potential solutions. Solutions include using tools that can provide a cyber workforce evaluation resulting in cyber training paths validated by job roles for employees, assistance implementing new approaches to hiring cyber candidates and current employee cyber skills testing, cyber job posting solutions, consideration of apprenticeship opportunities, creating a workforce cyber competency profile for a business, and collaboration opportunities with academic institutes desiring partnerships to improve cyber curriculum offerings to their sector-specific needs. Solutions that resonate with local entities and are validated will be briefed at future ICSCOP meetings to discuss options for adoption by a broader audience.

Finally, I would like to note that there are other issues facing the cyber workforce talent pipeline, but the ones listed are, in our opinion, the most problematic and biggest hinderances to a smoothly flowing talent pipeline. Many entities are working separately on solutions to the influencers I have outlined. This approach lends itself to creativity and flexibility with the multiple solutions offered to fit various entities needs; however, this approach can also lead to duplicative efforts and inefficient spending of scarce funds. We are seeing this issue arise with federal and DoD entities. The CISA office of Cybersecurity Defense Education and Training (CDET) is uniquely poised to implement and manage national cyber workforce R&D programs along with education and training courses. CDET should be looked to as the lead office for all CISA workforce development efforts. DoD should establish a similar, joint office and directly collaborate with CDET for efficiency.

INL stands ready to assist as needed in this nation's efforts to increase the cybersecurity posture of all citizens whether through workforce development and education or bringing to bear its ICS cybersecurity control systems experts, cyber researchers, engineers, and threat analysts.

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.