BUILDING ON OUR BASELINE: SECURING INDUSTRIAL CONTROL SYSTEMS AGAINST CYBER ATTACKS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 15, 2022

Serial No. 117–69

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

50–027 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MAYRA FLORES, Texas

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ELISSA SLOTKIN, Michigan
KATHLEEN M. RICE, New York
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
ANDREW R. GARBARINO, New York, *Ranking Member*
MICHAEL GUEST, Mississippi
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
JAKE LATURNER, Kansas
JOHN KATKO, New York *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
AUSTIN AGRELLA, *Minority Subcommittee Staff Director*
AARON GREENE, *Subcommittee Clerk*

CONTENTS

BUILDING ON OUR BASELINE: SECURING INDUSTRIAL CONTROL SYSTEMS AGAINST CYBER ATTACKS

Thursday, September 15, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. Yvette D. Clarke [Chairwoman of the subcommittee] presiding.

Present: Representatives Clarke, Jackson Lee, Langevin, Slotkin, Rice, Torres, Garbarino, Guest, Clyde, and LaTurner.

Chairwoman CLARKE. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will be in order.

The subcommittee is meeting today to receive testimony on "Building Our Baseline: Securing Industrial Control Systems Against Cyber Attacks".

Without objection, the Chair is authorized to declare the committee in recess at any point.

Good morning. I would like to thank the witnesses for participating in today's hearing on securing the industrial control systems at the heart of our Nation's critical infrastructure. This is a topic that we, as lawmakers and Federal officials, don't spend nearly enough time talking about, working on, or funding. We rely on industrial control systems and other operational technology, or OT, to make sure we have power in our houses, clean water to drink, and the countless other functions and services essential to our health, safety, and livelihoods. Still, questions about how we secure these critical OT systems tend to take a backseat to traditional IT security. That is simply not an option in today's threat landscape, as OT becomes more interconnected, integrated with IT systems, and attractive target to our adversaries.

In our industrial environment, the risks are not to stolen customer data or reputational harm to a company. The consequences can be deadly. An OT disruption could hurt our communities, our economy, and even our National security. Yet, in a recent report, the National Telecommunications Security Advisory Committee, or NSTAC, found that our "biggest gap" in OT security is our "lack of urgency." The NSTAC diagnosis was simple: "The U.S. has the technology and the knowledge to secure the systems but has not

prioritized the resources" to do so. In a hearing earlier this year, I said that the United States desperately needs to revamp its playbook for critical infrastructure cybersecurity. It is particularly true for OT security.

Fortunately, I believe we are starting to see a shift in attitudes and the Biden administration is helping to lead that charge. In his first few months in office, President Biden launched a new ICS Cybersecurity Initiative, envisioned as a series of cybersecurity sprints, starting with the electricity subsector and then expanding to other sectors like pipelines and water. Last July, President Biden formalized this initiative in a National Security Memorandum on Improving Control System Security. The Memorandum also directed CISA to work with NIST on a set of cybersecurity performance goals to serve as clear guidance to operators about the level of security the American people can trust and should expect for such essential services. This statement reflects a commitment to three principles that should underpin the Federal approach to OT security.

First, the American people are entitled to trust that the services they have grown to rely on meet a reasonable, baseline standard of security and resilience. Second, critical infrastructure operators have a responsibility to earn and maintain the trust of the American people. Finally, the Federal Government has a responsibility to bring its expertise, convening power, and resources to bear in support of this effort.

I am pleased to have the Federal Government's lead convener for critical infrastructure, and the principal architect of those baseline standards, CISA, on our panel today. I know CISA has been working to complete the Common Baseline performance goals and I understand they will soon be finalized. I see these baseline goals as having real promise to reshape the OT security landscape, but they will only be as effective as CISA's ability to engage and incorporate the feedback they are hearing from stakeholders.

I am also pleased to have another leader in Federal OT cybersecurity here today, the Idaho National Laboratory, to talk about how they are working to secure OT systems and support some of CISA's most critical OT programs, like CyberSentry, which I worked to codify last year. I would like to see this program grow and expand to new stakeholders, and I look forward to hearing how Congress can support that growth.

I would also like to hear from CISA how it is targeting its efforts toward OT operators with the greatest need, and the fewest resources, for instance, small utilities or State and local governments.

In this subcommittee, we often talk about the need to meet sectors where they are, recognizing their different security postures, resources, and expertise. That applies here as well. We need to do everything we can to make sure that efforts like the ICS sprints and the performance goals are designed to benefit all stakeholders, not just the most sophisticated. That will require the administration to identify lessons learned, and apply them, for instance, to the upcoming chemical sector sprint.

Finally, as we are shoring up these programs and ICS investments, I also want to hear how we are investing in our ICS security work force and doing so in a way that fosters diversity.

I thank our witnesses for joining us today and I look forward to our discussion.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

SEPTEMBER 15, 2022

I would like to thank the witnesses for participating in today's hearing on securing the industrial control systems at the heart of our Nation's critical infrastructure. This is a topic that we, as lawmakers and Federal officials, don't spend nearly enough time talking about, working on, or funding. We rely on industrial control systems and other operational technology, or OT, to make sure we have power in our houses, clean water to drink, and countless other functions and services essential to our health, safety, and livelihoods. Still, questions about how we secure these critical OT systems tend to take a backseat to traditional IT security.

That is simply not an option in today's threat landscape—as OT grows increasingly connected to the internet, is more integrated with IT systems, and becomes a far more attractive target for cyber criminals and our adversaries. In an industrial environment, the risk of a cyber compromise is not limited to stolen customer data or reputational harm to a company. The consequences can be deadly. An OT disruption could hurt our communities, our economy, and even our National security. And yet, in a recent report, the National Telecommunications Security Advisory Committee, or NSTAC, found that our "biggest gap" in industrial cybersecurity is our "lack of urgency." The NSTAC's diagnosis was simple: "the U.S. has the technology and the knowledge to secure these systems but has not prioritized the resources" to do so.

In a hearing earlier this year, I said that the United States desperately needs to revamp its playbook for critical infrastructure cybersecurity. That is particularly true for OT security. Fortunately, I believe we are starting to see a shift in attitudes—and the Biden administration is helping to lead that charge. In his first few months in office, President Biden launched a new ICS Cybersecurity Initiative—envisioned as a series of cybersecurity sprints—starting with the electricity subsector and then expanding to other sectors like pipelines and water. Last July, President Biden formalized this Initiative in a National Security Memorandum on Improving Control System Security.

The Memorandum also directed CISA to work with NIST on a set of cybersecurity performance goals to serve as clear guidance to operators about the level of security "the American people can trust and should expect for such essential services." This statement reflects a commitment to three principles that should underpin the Federal approach to OT security. First, the American people are entitled to trust that the services they have grown to rely on meet a reasonable, baseline standard of security and resilience. Second, critical infrastructure operators have a responsibility to earn and maintain the trust of the American people. And finally, the Federal Government has a responsibility to bring its expertise, convening power, and resources to bear in support of this effort.

I am pleased to have the Federal Government's lead "convener" for critical infrastructure, and the principal architect of those baseline standards, CISA, on our panel today. I know CISA has been working to complete the Common Baseline performance goals required by NSM–5, and I understand they will soon be finalized. I see these baseline standards as having real promise to reshape the OT security landscape—but they will only be as effective as CISA's ability to engage and incorporate the feedback they are hearing from stakeholders.

I am also pleased to have another leader in Federal OT cybersecurity here today—Idaho National Laboratory—to talk about how they're working to secure OT systems and support some of CISA's most critical OT programs, like CyberSentry, which I worked to codify last year. I would like to see this program grow and expand to new stakeholders, and I look forward to hearing how Congress can support that growth. I would also like to hear how CISA is targeting its efforts toward OT operators with the greatest need, and the fewest resources—for instance, small utilities or State and local governments.

In this subcommittee, we often talk about the need to meet sectors where they are—recognizing their different security postures, resources, and expertise. That applies here as well. We need to do everything we can to make sure that efforts like the ICS sprints and the performance goals are designed to benefit all stakeholders—not just the most sophisticated. That will require the administration to identify lessons learned, and apply them—for instance, to the upcoming chemical sector sprint.

Finally, as we're shoring up these programs and ICS investments, I also want to hear how we're investing in our ICS security workforce—and doing so in a way that fosters diversity.

Chairwoman CLARKE. The Chair now recognizing the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman Clarke, what is sure to be an informative hearing today. I thank you to our witnesses for being here to discuss the threats posed by industrial control systems, also known as operational technology.

The magnitude of these threats is often difficult for people to grasp, including Members of Congress. Securing the foundational technology that underpins our Nation's most critical functions is a National imperative. Industrial control systems are responsible for safely and securing operating informational technology throughout many critical infrastructure sectors, such as energy, water, and transportation systems.

Most Americans are accustomed to the reliable delivery of National critical functions, like electricity and clean water, but many are not aware of the serious cyber risks these sectors face.

In 2017 the world's biggest shipping company, Maersk, was one of the high-profile victims of the NotPetya attack. During this attack, NotPetya malware was able to infiltrate the company's industrial control systems, ultimately causing container ships and ports to grind to a halt for almost 9 days. Unfortunately, this incident was not solely isolated to the maritime and transportation sector as the pharmaceutical, food, and other industries were impacted as well.

What is more, in 2021 alone 80 percent of industrial control system organizations reportedly experienced ransomware attacks. As more industrial control systems across critical infrastructure sectors become connected to the internet, the attack surface will continue to grow exponentially. These legacy industrial control systems were not originally designed to be internet-facing unless they do not have the appropriate level of cyber resilience baked into their foundations.

To mitigate threats we must consider a thoughtful approach complementing—but sometimes unique from—our approach to traditional informational technology cybersecurity. While we must continue to innovate and evolve as a Nation to deliver better-, faster-, and greater-performing services, we must also incorporate baseline cybersecurity protocols to these industrial control system environments to protect U.S. National and economic security.

The Cybersecurity Infrastructure Security Agency works closely with Federal and private-sector partners to secure industrial control systems across the Federal enterprise and throughout each of the 16 critical infrastructure sectors. I am eager to hear CISA's perspective for the industrial control systems security from Eric Goldstein and I am looking forward to diving into the sector-specific industrial control system concerns of Mr. Gipson from the Idaho National Laboratory.

Again, I would like to thank you all for being here. As I mentioned earlier, we look to experts like you to help us comprehend the magnitude of the threats facing industrial control systems and

the potential solutions Congress could employ to bolster industrial control system cyber resilience.

I look forward to learning something new today from each of our expert witnesses.

Thank you again, Madam Chair, for holding today's hearing and I yield back.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW R. GARBARINO

Thank you, Chairwoman Clarke, for holding what is sure to be an informative hearing. And thank you to our witnesses for being here today to discuss the threats posed to industrial control systems (ICS), also known as Operational Technology (OT). The magnitude of these threats is often difficult for many people, including Members of Congress, to grasp.

Securing the foundational technology that underpins our Nation's most critical functions is a National imperative. ICS systems are responsible for safely and securely operating informational technology (IT) and operational technology (OT) throughout many critical infrastructure sectors such as energy, water, and transportation systems, among others. Most Americans are accustomed to the reliable delivery of National critical functions, like electricity and clean water, but many are not aware of the serious cyber risks these sectors face.

In 2017, the world's biggest shipping company, Maersk, was one of the high-profile victims of the NotPetya attack. During this attack, the NotPetya malware was able to infiltrate the company's ICS systems, ultimately, causing container ships and ports to grind to a halt for almost 9 days. Unfortunately, this incident was not solely isolated to the maritime and transportation sector, as the pharmaceutical, food, and other industries were impacted, as well. What's more, in 2021 alone, 80 percent of ICS organizations reportedly experienced ransomware attacks.

As more ICS systems across critical infrastructure sectors become connected to the internet, the attack surface will continue to grow exponentially. These legacy ICS systems were not originally designed to be internet-facing, and thus they do not have the appropriate level of cyber resilience baked into their foundations. To mitigate threats, we must consider a thoughtful approach, complementing—but sometimes unique from—our approach to traditional IT cybersecurity. While we must continue to innovate and evolve as a Nation to deliver better, faster, and greater performing services, we must also incorporate baseline cybersecurity protocols into these ICS environments to protect U.S. National and economic security.

The Cybersecurity and Infrastructure Security Agency (CISA) works closely with Federal and private-sector partners to secure industrial control systems across the Federal enterprise and throughout each of the 16 critical infrastructure sectors. I'm eager to hear CISA's perspective on ICS security from Eric Goldstein, and I'm looking forward to diving into the sector-specific ICS concerns of Mr. Gipson from the Idaho National Laboratory.

Again, I would like to thank you all for being here. As I mentioned earlier, we look to experts like you to help us comprehend the magnitude of the threats facing industrial control systems, and the potential solutions Congress could employ to bolster ICS cyber resilience. I look forward to learning something new today from each of our expert witnesses. Thank you again Madam Chair for holding today's hearing.

Chairwoman CLARKE. I would like thank the Ranking Member.

Members are also reminded that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3, 2021 colloquy regarding remote procedures. Members may also submit statements for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

SEPTEMBER 15, 2022

Operational technology underpins almost every aspect of how we live and work. From generating and distributing the electricity lighting this room, to ensuring that the water coming from the faucets is clean enough to drink, operational technology is the backbone of the National critical functions essential to public health, public

safety, and National security. In the late summer, two "National critical functions" in Mississippi failed.

Jackson, Mississippi is in the midst of a water crisis, leaving over 100,000 of my constituents without a clean water supply or appropriately-managed wastewater. They cannot use the water coming out of the faucets in their homes to brush their teeth, bathe, or wash the dishes. Tens of millions of gallons of untreated wastewater has flowed into Jackson-area waterways. Jackson schools had to revert to remote learning earlier this month because the toilets would not flush. Although the water crisis was not caused by a cyber attack, its horrific impacts and cascading consequences underscore the urgency of ensuring the safety, reliability, and functionality of the industrial control systems that support National critical functions. For me, the Jackson water crisis frames the way I think about today's hearing.

Since I became Chairman of the committee again in 2019, I have expressed my concerns about the cybersecurity posture of the water sector, and I am pleased that we now have a President who has made improving it a priority. Earlier this year, the full committee received testimony from the American Water Works Association about the challenges facing municipal water authorities as they work to improve their cybersecurity and about the ICS Cybersecurity Initiative water "sprint." We learned that water authorities struggle to stretch their budgets to invest in cybersecurity, and that Federal support needs to be tailored to the existing maturity and resources of the sector.

A draft report on the convergence of operational and information technology by the National Security Telecommunications Advisory Committee released in August confirmed these findings. As the committee continues its oversight of the Federal Government's ICS security efforts, we are learning that stakeholders are eager to partner—provided that the Government is collaborative and transparent. Toward that end, I have three goals for this hearing.

First, I am interested in knowing what support CISA has provided to the city of Jackson during the water crisis—including in helping the city understand the cascading effects of being without water. Second, I want to understand what CISA learned about the cybersecurity posture of the water sector through the ICS cybersecurity sprint, and what resources CISA brought to bear as it collaborated with the Environmental Protection Agency. Finally, I am interested in learning how CISA is encouraging ICS owners and operators to prioritize cybersecurity and resilience and invest in it accordingly.

I support the development of voluntary security guidelines, but they will only make us more secure if the private sector agrees to implement them. There are certain things the public should be able to rely on. Being able to drink the water coming out of the faucet is one of those things. If we are going to rely on voluntary security goals to protect ICS from cyber attacks, we must ensure that stakeholders are incentivized and able to implement them.

Chairwoman CLARKE. I now welcome our panel of witnesses.

First, I would like to welcome Mr. Eric Goldstein, the executive assistant director for cybersecurity at the Cybersecurity Infrastructure Security Agency, CISA. Mr. Goldstein runs CISA's cybersecurity division. Previously, Mr. Goldstein was the head of cybersecurity policy, strategy, and regulation at Goldman Sachs. Mr. Goldstein also served at CISA's predecessor agency, the National Protection and Programs Directorate.

Next we will hear from Mr. Virgil Gipson, a senior advisor at Idaho National Laboratories Cyber Integration Center. Before joining INL, Mr. Gipson spent over 3 decades at the National Security Agency, NSA, where he served in senior leadership in technical roles.

Without objection, the witness' full statements will be inserted in the record.

I now ask both witnesses to summarize their statements for 5 minutes, beginning with Mr. Goldstein.

STATEMENT OF ERIC GOLDSTEIN, EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. GOLDSTEIN. Thank you.

Madam Chair, Ranking Member, Members of the subcommittee, it is a privilege to rejoin the group today and talk about this critically important topic. I applaud your focus on this issue, as well as the depth of understanding and insight reflected in both of your opening statements.

Madam Chair, as you noted, the security of control systems in operational technology is of paramount importance for this country. Americans rely every day on services enabled by control systems, from health care to mass transit to water to energy. This priority is of the utmost importance for CISA and the broader Biden-Harris administration. This priority is exemplified, Madam Chair, as you noted, by President Biden's National Security Memorandum on securing critical infrastructure control systems issues just last year, which called for a series of cybersecurity sprints and the development of cybersecurity performance goals.

At CISA, our work to enable and support security and control systems is predicated on three core principles.

First, a focus on partnership, understanding the diverse ecosystem of organizations across the control systems community that must come together to enable important change.

Second, the important differences between operational technology and more traditional IT, which requires thoughtful consideration when adopting appropriate cybersecurity solutions.

Third, the fact that many organizations using control systems face uniquely high demands for availability and face unique operational risks, which further requires deep consideration and collaboration when recommending or supporting particular security measures.

Now, with these principles in mind, at CISA we are focused on deepening our operational collaboration across the ICS community, on providing trusted and authoritative guidance to help organizations adopt the right security measures at the right time across the ecosystem, and developing cybersecurity performance goals that will help organizations make the right investments with their next security dollar to drive progress toward the most important security outcomes.

Now, of course, we start first in everything we do with partnership and operational collaboration. We were delighted this past April to stand up our Joint Cyber Defense Collaborative ICS Group, which brings together device manufacturers, integrators, security providers, and owner/operators to take on shared challenges in the control systems and OT space. This group right now is working on a cyber defense plan focused on enhancing the efficiency, effectiveness, and speed of sharing the threat vulnerability information across this broad ecosystem.

Now, Madam Chair, you raised a wonderful point, which is the importance when thinking about collaboration of not just focusing on the most mature organization, but those that are, as we call them, target-rich and cyber-poor. Making sure that those organiza-

tions that are less resourced are still able to raise their own bar for cybersecurity. In that regard, we are looking forward to launching our State and Local Tribal and Territorial Cyber Grant Program. We are expanding our regional forces to meet organizations where they are and proving easy-to-use guidance and assessment tools.

Now, on this last point, we are also really focused on serving as a trusted and authoritative source of guidance. I mean the cybersecurity performance goals play an important role here. These goals, which again were derived from the President's National Security Memorandum, call on CISA and NIST to work collaboratively in developing a set of goals that organizations can use to inform resource prioritizations. Now, really importantly, these goals are voluntary by design, were developed as part of a richly collaborative process. We received over 2,000 comments on the draft goals over 2 rounds of feedback and countless workshops and listening session. Excitingly, these goals are designed to be used in conjunction with the NIST cybersecurity framework that is already adopted by many organizations across the country. The goals, when they are launched, will provide more specificity and measurability to help organizations prioritize their security investments. Even when the goals are launched, our dialog and our work will continue as we will keep receiving feedback on the baseline cross-sector goals and begin our work in developing center-specific goals that are tailored to the unique considerations of each individual sector.

You know, the risk we face as a country in securing our control systems and OT is extraordinary. CISA, with our partners, is taking on this challenge head-on by providing performance goals, making work easier for organizations that are less mature, serving as a trusted and authoritative source of guidance, including by enabling the coordinated disclosure of vulnerabilities in control systems, and enabling increased visibility across the control systems and OT landscape by encouraging adoption of commercial solutions and by providing our cyber protection ability to organizations that need it most.

Thank you again for the privilege of joining today. It is always an honor and I look forward to your questions.

[The prepared statement of Mr. Goldstein follows:]

PREPARED STATEMENT OF ERIC GOLDSTEIN

SEPTEMBER 15, 2022

Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee, thank you for your invitation to testify today on behalf of the Cybersecurity and Infrastructure Security Agency. I appreciate the opportunity to highlight how CISA supports our Nation's industrial control systems (ICS) and operational technology (OT) communities against cyber threats that have the potential of impacting National Critical Functions and the provision of essential services to the American people.

As reflected in President Biden's National Security Memorandum (NSM)—5, "Improving Cybersecurity for Critical Infrastructure Control Systems," securing ICS and OT assets is a top priority of the Biden-Harris administration, and CISA is privileged to serve in a central role in implementing this directive, alongside our Federal and industry partners. NSM–5 directed an unprecedented focus on ICS cybersecurity across the U.S. Government through a series of "sprints" focused on the electricity, pipeline, and water sectors and through the development of baseline cybersecurity performance goals.

Our Nation's ICS and OT community is a complex ecosystem comprised of device manufacturers, integrators, owners and operators of critical infrastructure, and security providers. CISA serves as a trusted partner within the ICS and OT ecosystem to provide information, guidance, and capabilities that enable faster and more scalable reduction of risks facing ICS and OT assets. Our goal is to meet the unique requirements of the ICS and OT community by continuously evaluating and improving our capabilities to support the areas of greatest need, recognizing that many ICS and OT environments require approaches and solutions that differ from traditional Information Technology environments.

OPERATIONAL COLLABORATION

Over the past decade, we learned that traditional methods of public-private partnership characterized by intermittent, unidirectional information sharing did not scale to meet the pace of the adversary or the velocity of technological change. With the support of Congress, we shifted the paradigm toward continuous collaboration to empower synchronized cybersecurity planning, cyber defense, and response. The Joint Cyber Defense Collaborative (JCDC) brings together critical partners in Government and the private sector to engage in persistent collaboration and joint cyber defense planning.

In April 2022, we expanded the JCDC to focus on ICS security and brought in new partners to help lead this important work. Through the creation of focused collaboration channels, the JCDC–ICS is positioned to quickly share, analyze, and enrich information about threats and vulnerabilities affecting ICS assets. Additionally, the JCDC–ICS initiative catalyzed a new planning effort intended to expedite collaboration across the ICS ecosystem, bringing together Government, critical infrastructure operators, ICS vendors, and ICS security providers with unprecedented cohesion and scale. As we continue to bring on new partners, CISA will mature the JCDC's structure and operational approaches to maximize value for the ICS community.

SERVING AS AN AUTHORITATIVE SOURCE OF TRUSTED INFORMATION

As a core part of our mission to advance security of the ICS and OT communities, CISA collaboratively develops trusted information to help organizations more effectively mitigate vulnerabilities. This information generally takes two forms.

First, we develop Cybersecurity Advisories with inter-agency and international partners on urgent threats and risks, such as the joint product with the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) from April 13, 2022, on APT cyber tools targeting ICS/SCADA devices; our joint product with the Department of Energy (DOE) on March 29, 2022, regarding targeting uninterruptable power supplies; and our March 24, 2022, joint product with FBI and DOE on threats from Russian state-sponsored cyber actors targeting the energy sector. These products, many of which benefited from input from private-sector partners, are intended to turn raw intelligence into actionable guidance information with increased speed for organizations across the country.

Second, CISA's ICS Vulnerability Response and Disclosure program regularly publishes ICS Advisories to share information about impactful vulnerabilities. The program serves as a trusted partner with cybersecurity researchers and product vendors to effectively identify, enable mitigation, and publicly disclose vulnerabilities impacting control systems and operational technology. CISA coordinated the timely disclosure of thousands of vulnerabilities and their associated mitigations, which otherwise would affect systems and hardware supporting critical functions such as the electric grid, hospitals, building automation systems, defense systems, data centers, and other crucial systems. In 2022, CISA already has published over 300 such Advisories representing thousands of vulnerabilities in a variety of ICS/OT products. These vulnerabilities impact products used across a wide variety of sectors, including Energy, Critical Manufacturing, Water and Wastewater Systems, Food and Agriculture, and Chemical. We work closely with stakeholders across Government and industry to identify the most impactful ways to disseminate vulnerability information, including through machine-readable data that can be ingested and actioned through automation and by providing guidance that enables prioritization of the most significant risks. CISA will soon begin producing machine-readable ICS Advisories in the Common Security Advisory Framework (CSAF) format, which will enable automated and timely exchange of vulnerability advisory information in an interoperable manner, and we urge all vendors of ICS and OT products to adopt this approach.

ENABLING OPERATIONAL VISIBILITY

A prerequisite for optimized operational collaboration and provision of timely, actionable guidance is visibility into the targeting of ICS and OT systems. We must know how malicious actors are attempting to compromise systems, where they are succeeding, and which security measures are most effective in stopping them. To gain visibility into the breadth of malicious activity targeting American networks, we work with our JCDC partners to build an ecosystem of continuous collaboration where traffic or an incident seen by one partner can be rapidly shared across both private and public-sector entities for analysis, enrichment, and correlation. To gain deeper visibility into particular sectors, we are partnering with a small number of ICS security companies to give our analysts the ability to determine whether a given threat has been seen before, while preserving anonymity of the security companies' customers.

Finally, for select critical infrastructure entities, we provide access to our CyberSentry program. CyberSentry is a CISA-managed threat detection and monitoring program that allows our analysts to directly detect attempts to compromise critical ICS networks. Through a strategic and narrow deployment, CyberSentry leverages sensitive data to provide enhanced visibility that can be used by CISA and our partners to better defend critical infrastructure networks. CyberSentry is not a replacement for a company's own ICS cybersecurity program or security providers; rather, this program provides an additive layer of visibility where the Nation needs it most. We continue to encourage all organizations to adopt commercial ICS monitoring solutions by publishing guidance that provides a list of criteria organizations should consider when evaluating a commercial ICS monitoring solution. We are grateful to Congress for authorizing the CyberSentry program, and we look forward to expanding it to additional partners in the months to come.

ENABLING PRIORITIZED INVESTMENT

A key pillar of President Biden's NSM–5 directed CISA and NIST to develop cybersecurity performance goals for critical infrastructure, which "should serve as clear guidance to owners and operators about cybersecurity practices and postures that the American people can trust and should expect for such essential services." Referred to as the Common Baseline, it aims to identify a set of practices that critical infrastructure owners and operators should employ to protect systems supporting National Critical Functions and reduce risks to National security, economic security, and public health and safety. This Common Baseline represents a combination of best practices for IT and OT owners and sets forth a prioritized list of security controls. These practices are also intended to be a benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.

Unlike other control frameworks, the Common Baseline considers not only the practices that address risk to individual entities, but also the aggregate risk to the Nation. Rather than a comprehensive catalog, the Common Baseline captures a core set of high-impact controls and practices with known risk-reduction value that are broadly applicable across sectors. Organizations can use the Common Baseline to prioritize the security controls which work most effectively to reduce risk in their environments. This prioritization can help determine how to most prudently allocate investments toward specific security practices.

The Common Baseline is voluntary by design, and the draft goals were developed through a highly collaborative process. CISA received over 2,000 comments across two separate rounds of review, which included multiple workshops with critical infrastructure partners, ICS and OT experts, and the general public. Importantly, the Common Baseline is designed to be utilized in conjunction with and in support of the NIST Cybersecurity Framework (CSF), which is the de facto standard for all organizations to build and evaluate their cybersecurity programs. The Common Baseline extends the CSF by identifying the most impactful controls across both IT and OT systems and describes both the scope and measurements for those controls so that it is easier for asset owners to implement and attest to their security posture. Organizations that are already using the NIST CSF or other frameworks can easily determine where they are already making progress toward achieving particular goals in the Common Baseline and where more investment may be required. We look forward to releasing the next iteration of the Common Baseline this fall, with continued collaboration across the cybersecurity community on further maturation of the baseline goals and sector-specific goals.

CONCLUSION

Advancing the security and resilience of industrial control systems (ICS) will continue to be a top priority for CISA and the Biden-Harris Administration. As the lead agency for civilian cybersecurity and the National coordinator for critical infrastructure security and resilience, we will continue to partner with organizations across the ICS and OT ecosystem to identify and reduce risk facing our Nation's most critical systems. With the continued support of Congress, we will make measurable progress toward these essential goals.

Chairwoman CLARKE. Thank you, Mr. Goldstein, for your testimony here today.

I will now recognize Mr. Gipson to summarize his statement for 5 minutes.

STATEMENT OF VERGLE GIPSON, SENIOR ADVISOR, CYBERCORE INTEGRATION CENTER, IDAHO NATIONAL LABORATORY, U.S. DEPARTMENT OF ENERGY

Mr. GIPSON. Chairwoman Clarke, Ranking Member Garbarino, Members of the subcommittee, thank you for the invitation to testify on a topic critical to the security of our Nation.

I am Vergle Gipson and I am a senior advisor at Idaho National Laboratory. I am an expert in cyber threat and critical infrastructure cybersecurity.

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 to strike our Nation. Acts of cyber-enabled sabotage are possible because our Nation's infrastructure is highly dependent on industrial control systems.

These industrial control systems, also known as operational technology, govern and execute complex processes at substations, manufacturing facilities, water treatment facilities, military bases, transportation hubs, and much more.

In contrast to information technology—IT, like personal computers and business networks—operational technology is not as widely protected. There are several reasons for this including, first, systems management. Most IT is upgraded or replaced every 3 to 5 years, software and firmware is frequently updated and patches are routinely installed. On the other hand, operational technology is often designed to last for decades and is typically only updated if a noticeable failure occurs.

Second is standardization. Most IT is designed and operated using industry best practices for cybersecurity that are widely adopted. By contrast, operational technology is often custom-engineered for specific systems.

Third, is discovery tools. The IT industry has developed a wide range of products to discover malicious activities and vulnerabilities. However, a few discovery tools exist for operational technology.

To help simplify this complex issue, I find it helpful to think of cyber risk as a function of threats, vulnerabilities, and consequences. As adversaries increas their capabilities and their intent to conduct malicious cyber activity, the threat to U.S. infrastructure rises. As the complexity and number of digital system increases, the cyber vulnerabilities in U.S. infrastructure rises. As our society becomes more reliant on an increasing number of

digitally-connected systems, the consequences of cyber attacks also increase.

However, this cyber risk can be greatly reduced, and in some cases eliminated. We at Idaho National Laboratory are working with CISA, the Department of Energy, the Department of Defense, industry, and others to reduce cyber threats, vulnerabilities, and consequences.

Idaho National Laboratory is managed by Battelle Energy Alliance for the Department of Energy and is focused on innovations in nuclear research, renewable energy systems, and National security systems. From our decades of work building and testing more than 50 nuclear reactors, the Lab has developed a deep understanding of operational technology and the cybersecurity, engineering, and processes needed to provide critical function assurance.

For more than 18 years, CISA and its predecessor organizations, have leveraged the Lab's capabilities and proven leadership. Current Laboratory technical support to CISA includes discovering cyber vulnerabilities and partnering to develop mitigations, providing technical expertise in response to cyber incidents, developing analytic tools to detect malicious behavior and to identify cross-sector dependencies, developing methods and tools to assess the security of critical infrastructure systems, and creating cybersecurity and infrastructure protection training for the industrial control systems work force.

Looking forward, to address some of the most critical gaps surrounding industrial control system cybersecurity, the Lab recommends, first, creating an industrial control system cybersecurity center of excellence to drive research and development among the community of practice. Second, maturing cyber-informed engineering to address cybersecurity issues early in the life cycle of engineered systems by leveraging the Department of Energy's National cyber-informed engineering strategy. Third, expanding cyber physical test environments to support development of sector-specific cyber risk mitigations.

I appreciate the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Gipson follows:]

PREPARED STATEMENT OF VERGLE GIPSON

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 5 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 3 to 5 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. As our society becomes more reliant on an increasing number of digitally-connected systems, the consequences of cyber attacks 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 cyber attack 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 cannot 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, test-

ing, 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 air space, 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 life cycle 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.

Chairwoman CLARKE. Thank you, Mr. Gipson, for your testimony here today.

I will remind the subcommittee that we will each have 5 minutes to question the panel.

I will now recognize myself for questions.

The Biden administration has taken proactive steps to secure critical infrastructure control systems, but there is much more to do. So my question is to both of you gentlemen.

What more could the administration be doing toward industrial cybersecurity? What milestones should we be looking at to see over the next 5 to 10 years?

Mr. GOLDSTEIN. Thank you, ma'am, that is a wonderful question.

As you know, the administration has made this issue an absolute top priority and we have now set forth a strategy and a series of efforts that we believe will make measurable impact, working with our partners, in the months and years to come.

A few of these lines of effort include the cybersecurity performance goals. We look forward to releasing the baseline cross-sector goals here soon and then immediately turning to work on the sector-specific performance goals. Where sectors uniquely utilize control systems and OT, we look forward to exploring how these performance goals can help organizations prioritize the right investments in securing their ICS and OT environments on a voluntary basis in accordance with the performance goals.

Of equal importance is our collaborative work, particularly with the vendor security provider and integrator community, as the Ranking Member noted, to ensure that we are providing needed support and assistance in adopting, for example, more security protocols and security by design measure in many control systems and OT technologies that were designed historically for availability and reliability and now need to be improved to ensure that security is also top in mind. We will be doing a lot of that work through our Joint Cyber Defense Collaborative, but again working closely with our partners across sectors.

Beyond that, we are also really focused on ensuring that we are enabling prompt identification of vulnerabilities in the control systems and OT environment to ensure that when a risk is identified, it is rapidly remediated across sectors to reduce, as my co-witness noted, the opening that our adversaries have to cause an intrusion and cause harm.

Mr. GIPSON. So we at Idaho National Lab provide technical support to CISA and others in the administration, other organizations. As I laid out in my testimony a moment ago, big things on our mind include that center of excellence to do more to encourage cyber informed engineering, changing the culture among engineers to recognize cybersecurity as a fundamental tenet just as engineers currently recognize functionality, reliability, and safety.

Then, finally, having more representative test environments that are close to real life to experiment and develop mitigations that will work in the real world environment for specific sectors.

So there is so much that needs to be done here.

So in addition to all of the great cyber hygiene things that need to be done to establish a baseline across our critical infrastructure, we also need to identify what are those high-consequence events that we simply can't allow to occur as a Nation and then working together between Government and industry to find ways to mitigate the risks to eliminate those high-consequence events that could be catastrophic.

Chairwoman CLARKE. As the Federal Government funnels resources into new infrastructure projects today, how can we make sure the OT investments we are making now have security built in for the threats of tomorrow?

Mr. GOLDSTEIN. Thank you, ma'am.

Certainly we are at a unique time in this country's infrastructure where resources, including through the Infrastructure, Investment and Jobs Act, will cause an extraordinary maturation and modernization of this country's infrastructure across sectors. At CISA we are working with our partners across the Federal Government to provide guidance and support to enable adoption of security by design and security by default principles in as many of those projects as possible. Certainly our colleagues, for example, at the Department of Energy are taking a similar approach. So with the extraordinary work of Congress here in enabling funding through the IIJA, we will hope that this funding will lead not only to dramatic modernization and access for all Americans, but also increases its security as well.

Mr. GIPSON. This is a big opportunity for us in the United States that a lot of the existing infrastructure simply isn't securable from a cyber viewpoint. So as we are upgrading and replacing infrastructure, it is the perfect time to make that infrastructure cyber secure and defendable. The design stage is the right place to start. So we have to find a way to educate those who are engineering and building new systems and those who are engineering and building the components in those systems, that that work is done with cybersecurity in mind, so when those new systems are installed and become operational they can be defended.

Chairwoman CLARKE. Very well.

I now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for his questions.

Mr. GARBARINO. Thank you, Chairwoman.

Mr. Goldstein, you mentioned in your opening statement that you are looking forward to the State and local grant program. Where are we with that right now?

Mr. GOLDSTEIN. Thank you, sir.

As you know, we are really excited for this program. It is really a new opportunity to drive some extraordinary maturation across our partners, many which lack resources to adopt needed security practices in the face of modern threats. We are preparing in the near future to announce the notice of funding opportunity, which is going to provide the window for SLTT organizations to apply for cybersecurity grants. We see these grants as being foundational, not only in providing the ability to deploy needed technologies, but also for organizations to really increase their level of cybersecurity governance, to develop cybersecurity plans, programs, and procedures that are necessary to manage effectively the risk that we are all seeing everyday.

Mr. GARBARINO. So but in the near future you are expecting——

Mr. GOLDSTEIN. Yes, sir.

Mr. GARBARINO [continuing]. To open up for application? Great. It is good to hear.

I wanted to ask you, because this is something that came out yesterday, the Office of Management and Budget released new

guidance on secure software procurement requirements and, you know, directive under the President's Improving National Security Executive Order, and the common concern we have heard from industry is that requirements like this are often inconsistent across the Federal agencies. Is CISA planning on working with or have they worked with OMB to ensure that there is consistency of these new requirements across the Federal Civilian Executive Branch?

Mr. GOLDSTEIN. Absolutely. At the outset we are really excited to see OMB's software security memo be released. This memo is going to significantly increase accountability and transparency for the security of software used by the Federal Executive branch. But we feel that the implications are likely broader. So as we think through putting forth voluntary guidance for organizations, how to think about software security, how to make the right requests for suppliers of software for the organizations, including critical infrastructure, the work being done by CISA and OMB for the Federal Government we feel like is ostensible to be adopted on a voluntary basis by entities across the country. So as one example of that, as we think through what performance goals might look like for the IT sector, we are going to work really collaboratively with IT organizations across the country to think through how do we adopt performance goals that are harmonized with software security guidance elsewhere so we ideally have one set of expectations or voluntary guidance for organizations, regardless if they are working with a Federal entity or the private sector.

Mr. GARBARINO. I appreciate the work that you are doing with industry here. So thank you.

Mr. Gipson, in your opening statement you talked about the ability to identify high-consequence events and also eliminate their ability to happen. Where are we on that? I mean have we identified these high-consequence events? Or I know they probably change daily, but I mean do we have a baseline yet?

Mr. GIPSON. So I will speak to where we are with—and Idaho National Lab activity in partnership with the Department of Energy, the Department of Homeland Security, and the Department of Defense, we have been initially piloting and now operationalizing an effort we call—it is a mouthful—consequence-driven cyber-informed engineering. So this is a process we go through with oftentimes asset owner and operators to train them on how to bring together those who work IT cybersecurity with those who work OT cybersecurity with the engineers and with the operators, all with a focus on securing the systems and the critical infrastructure from those high-consequence events.

So the first pilot occurred in 2017 and things have matured greatly since then and the program has been commercialized somewhat. So now it is spreading. So there is a path forward here, it just needs to grow.

Mr. GARBARINO. I imagine these high-consequence events are sector-specific. So what might be high-consequence event for one sector is not for another. So how do we get it to mature? What is the next step? Because it seems like we should be moving quickly on this to develop the list and then have that grow.

Mr. GIPSON. I could not agree with you more. Yes, this needs to move out more quickly.

So this is where time back to the Department of Energy's National cyber-informed strategy comes in. DOE has a plan for how to reach the work force and the practitioners so that they start adopting the CIE activities. We have from the Lab worked with the National Risk Management Center to prioritize those critical infrastructure entities and various sectors. So there is a lot that Government has done, but this is a big change across the sector and needs to be funded either privately or through the Government.

Mr. GARBARINO. I appreciate that.

Madam Chairman, I yield back.

Thank you.

Chairwoman CLARKE. The Chair will recognize other Members for questions they may wish to ask the witnesses. In accordance with the guidelines laid out by the Chairman and the Ranking Member in their February 3 colloquy, I will recognize Members in order of seniority, alternating between Majority and Minority.

Members are also reminded to unmute themselves when recognized for questioning.

The Chair now recognizes the gentlewoman from New York, Ms. Rice, for 5 minutes.

Ms. RICE. Thank you, Madam Chair.

Mr. Goldstein, thank you so much for joining us. As has been said, it is great to hear from you again.

Can you tell us what factors CISA takes into account when deciding whether a critical infrastructure operator should be allowed access to CISA's CyberSentry program?

Mr. GOLDSTEIN. Of course. Thank you so much, ma'am. It is a wonderful question.

So at the outset, our approach for gaining visibility into cyber threats targeting critical infrastructure is that every organization should adopt leading commercial solutions so that they themselves have visibility and can act quickly to detect and remediate possible intrusions into their network. That is something that we work closely with all of the leading security vendors to ensure that we are supporting them in providing access to the right companies in this country.

Now, for a small number of critical entities across sectors, the U.S. Government has an operational need to get a more granular and near-real-time understanding into threats targeting control systems and operational technology. So the CyberSentry program is a set of commercial solutions that CISA provides to a constrained number of organizations across sectors where CISA's own analysts are able to gain visibility into cyber threats attempting to access and impact control systems and OT networks. Actually of course note that CyberSentry is a great partnership at Idaho National Labs.

We really focus CyberSentry on those organizations that are most consequential to our National security, economic security, and public and health and safety, and where we reasonable expect targeting by advanced adversaries and where CISA's ability to operationalize sensitive information gives the company an added layer of security and allows CISA to quickly detect and assess if an advanced adversary is attempting an intrusion.

So with the great support of Congress we look forward to expanding this program over the next fiscal year and beyond. But this program really is intended for those most consequential and most targeted entities in our country.

Ms. RICE. How does CISA envision expanding the CyberSentry program to additional partners, as you mentioned in your technology? Is CyberSentry scalable to the extent that it can serve a larger number of systems, or does it need to remain focused only on those facing the greatest resource challenges?

Mr. GOLDSTEIN. Our view is that CyberSentry really should remain focused on the most consequential and the most targeted entities in this country. Certainly we do intend to expand the program, both next fiscal year and beyond, and bring in more partners across sectors, but at the same time we are working very closely with commercial cybersecurity companies and with our partners in the Joint Cyber Defense Collaborative, such that we have layered ways to gain visibility into threats targeting critical infrastructure. So for those organizations that are part of CyberSentry, CISA will be able to gain our own visibility into threats targeting ICS and OT networks, but also at partnering with commercial cybersecurity companies and partnering directly with critical infrastructure. Through the Joint Cyber Defense Collaborative we are able to get similar visibility as well.

So our goal is every organization should adopt cybersecurity detection and prevention capabilities, every organization should work with CISA to ensure that we are collaborating and sharing information for that top tranche of organizations most consequential, most at risk. That is where our CyberSentry tool is really useful even as it expands beyond the number of entities today.

Ms. RICE. Great. Thank you so much.

Programs like CyberSentry and the Joint Cyber Defense Collaborative play an important role in protecting our critical industrial control systems, but infrastructure operators must have access to a skilled and well-trained cyber work force of their own that understand the particular needs of OT security and how it differs from IT security.

CISA's recent draft of IT-OT conversions report noted that only 68 qualified workers are available for every 100 cybersecurity jobs and over 600,000 jobs open up for cybersecurity workers every year here in the United States. It is even more difficult to find cyber professionals that understand the OT environment.

Mr. Gipson, how does the Idaho National Lab support Federal efforts to train a work force tailored specifically to OT environments and how quickly can a cyber professional trained to secure IT be trained to protect critical OT systems as well? How can this committee support Federal efforts to develop our OT security work force?

Mr. GIPSON. Thank you very much for that question.

So Idaho National Lab has been involved in training the cybersecurity work force for decades at this point and specializing in the training of those who can do the operational technology cybersecurity.

So to take someone who is already trained in information technology cybersecurity and train them to do operational technology,

the principles are exactly the same. So it is not a state change for those individuals. What is different is the technical details of it, the data protocols, the vulnerabilities, the specific threats. So to take an IT person and turn them into an OT cybersecurity person, that is doable and Idaho National Lab does that routinely with CISA funding for many in the commercial work space.

Now, to take those OT professionals and make them truly capable of securing critical infrastructure, it takes a lot more than simply the OT cybersecurity professional. We need to be able to train those engineers who are designing the systems, the operators who are running the systems, and encourage the collaboration of multiple parties to ensure cybersecurity. I know training does that, it forces collaboration and that collaboration is in many cases a culture change in companies and so that is the longer pole in the tent.

Ms. RICE. Thank you to both of you witnesses for appearing here today.

I yield back the balance of my time, Madam Chair.

Thank you very much.

Chairwoman CLARKE. I thank the gentlelady from New York.

The Chair now recognizes for 5 minutes the gentleman from Georgia, Mr. Clyde, for 5 minutes.

Mr. CLYDE. Thank you Chairwoman Clarke and Ranking Member Garbarino for holding this important hearing dedicated to improving the cybersecurity of our Nation's industrial control systems.

Over the past few years we have witnessed numerous cyber attacks, both in the United States and abroad. Every day we see new technology on the market and new devices connecting to the internet. Unfortunately, it seems that at times our technological advances have outpaced our ability to maintain secure IT and OT systems. Cyber attacks can have devastating consequences, both for the consumer and for the system operators. However, many private industrial control system operators may not even be aware of the inherent risks involved when connecting their system to the internet.

So, Mr. Goldstein, it is good to have you back for another hearing, sir. I know in the past we have asked you about the resources CISA has provided to help small businesses establish and improve cybersecurity measure with respect to information technology. Could you explain what services CISA provides to small businesses to maintain the security of operations technology? There are a lot of small businesses and a lot of them don't really have any idea what CISA does for OT.

Mr. GOLDSTEIN. Yes, sir, absolutely. Thank you for that question. Of course, a pleasure to rejoin the group here.

I really can't overstate the importance of CISA's regional work force here. For many small and medium organizations, even as we push out guidance on our website, on social media, via virtual meetings and webinars, we know that is not going to reach many organizations in this country. So with the support of Congress we are dramatically increasing our regional footprint across the country so that our regional cybersecurity experts can meet with local chambers of commerce, can knock on the door of the local water

utility and have, as you note, sir, a really focused conversation about risks facing operational technology and control systems.

This is really one important aspect of the cybersecurity performance goals, because the goal of the performance goals—and other frameworks like it—is to provide a really succinct and simple place to start. So organizations that may not be resourced to develop a fully mature cybersecurity program, may not have resources to deploy best-in-class cybersecurity technologies, there are still steps that they can take that will dramatically improve their security today.

So a combination of easy-to-use succinct guidance in our regional work force that is able to get out there, knock on doors, sit down for a cup of coffee and have a conversation, that is really our key to make sure that we are getting the word out the right ways.

Mr. CLYDE. OK. Thank you.

So on a scale of say 1 to 10, where do you think we are right now in getting that information out for the small businesses to understand what CISA is really doing?

Mr. GOLDSTEIN. Sir, I think it is asymmetric across sectors. I think that there are some sectors, for example, the energy sector, where there are of course a lot of electric co-ops or municipal utilities that are smaller. I think CISA's work in cooperation with the energy department has really done an important job in driving an understanding of risks and an understanding of controls. I think if we look across other sectors, for example, thousands upon thousands of small water utilities in this country, I think we have work to do to make sure that we are identifying all possible means of communication and collaboration to, as my co-witness noted, raise an understanding of the risk in the first instance, so that organizations don't, for example, just plug a device into the internet without understanding the risk thereof, and we are driving adoption of the reg controls and security measures that are done in a way that is considering the unique attributes of OT environment and the requirements for availability and operational risk therein.

Mr. CLYDE. Thank you. Thank you very much for that.

Now, Mr. Gipson, in your testimony, you said from our decades-long work in building and testing more than 50 nuclear reactors in the high desert of Idaho Falls, the Idaho National Lab has developed a deep understanding of OT and cybersecurity engineering processes needed to secure systems and provide critical function assurance.

With proper safeguards in place, and one of those being operational technology security, nuclear reactor energy is, you know, one of the most clean and reliable sources of electricity in the world. Having that incredible amount of experience in, you know, building over 50 nuclear reactors, would you agree that nuclear reactor energy is perfectly safe with the proper safeguards in place?

Mr. GIPSON. Well, I will caveat it with saying I am not a nuclear engineer or a scientist, but, yes, modern nuclear reactors are incredibly safe. Their design is nothing like the nuclear reactors of the past.

Mr. CLYDE. OK, great. Do you think we need more nuclear reactor capability in this country?

Mr. GIPSON. So, once again, away from my area of expertise. Yes. Having that baseline generation available in a clean and reliable source like nuclear is an incredible opportunity to take advantage of and really there is not technical reason why we shouldn't move out rapidly.

Mr. CLYDE. Well, I will tell you, you know, in Georgia we have two nuclear plants coming on-line in Plant Vogtle just literally months away, just—early next year the second plant, just a few weeks away from the first plant and I am really excited about that.

Chairwoman CLARKE. The gentleman's time has expired.

Mr. CLYDE. Thank you and I yield back.

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentleman from New York, Mr. Torres.

Mr. TORRES. Thank you, Madam Chair. Good to see you again, Mr. Goldstein.

The Federal Government must not only preach but also practice cybersecurity, it must lead by example. So with that in mind, does the Federal Government have full visibility in to the OT assets it owns and operations?

Mr. GOLDSTEIN. Thank you, sir. Wonderful to see you as well.

The Federal Government is making extraordinary strides in getting visibility across the IT and OT landscape. The key to this is our Continuous Diagnostic and Mitigation, or CDM, program which has been supported by Congress for many years and provides really two key elements. First, it funds cybersecurity tools for all Federal Civilian Executive Branch agencies to enable that asset visibility and understand the state of assets, configurations, and vulnerabilities, and then also provide CISA an on-going feed to what we call our Federal dashboard to get visibility into the State of assets across the Federal Civilian Executive Branch. In part by President Biden's cybersecurity Executive Order last year, we have made extraordinary progress and now have increasingly high confidence in the state of asset visibility across Federal agencies. Now, we are still working every day to identify gaps in that coverage, make sure that we are catching what we call shadow IT, instances of IT and OT assets that might be missed by on-going——

Mr. TORRES. It sounds like the answer is no, you don't have full visibility. I am curious pursuant to NSTAC's recommendation, is CISA willing to invoke its binding operational directive to mandate visibility into Federal OT assets or?

Mr. GOLDSTEIN. Sir, we have better visibility than we have ever had in the history of the Federal Government. What I would say is any organization conclusively saying they have absolute confidence, I don't think any entity would say that, but we have better visibility than we have had. We are making progress every day on——

Mr. TORRES. But are you willing to invoke the authority you have to mandate visibility?

Mr. GOLDSTEIN. Unequivocally we will use every authority at our disposal to make sure that we have the visibility we need.

Mr. TORRES. You noted earlier that the National Security Memorandum on improving critical infrastructure requires you and NIST to set both cross-sector and sector specific performance goals. What are time lines for finalizing both of those goals?

Mr. GOLDSTEIN. Yes, sir. We are planning to release the next iteration of the baseline performance goals in October during cybersecurity awareness month. We are really excited about this opportunity first to get these goals out in the community and help owner-operators start using them for their risk management, but also to keep getting feedback.

Mr. TORRES. What is the time table?

Mr. GOLDSTEIN. We are releasing the baseline goals in October, sir, and then from that point we are going to start working on the sectoral goals. We are going to——

Mr. TORRES. Is there a time table for finalizing the sectoral goals, or?

Mr. GOLDSTEIN. We are going to do them in tranches, sir. So we are going to start off with a few sectors off the bat. I think the time frame is going to differ by sector. We will see some sectors where the baseline goals may largely be sufficient, those will be finalized faster. Other sectors that have more unique technologies may take longer. But as to the baseline goals, this will be deeply collaborative in coordination with the private sector and our partners across the inter-agency.

Mr. TORRES. Now, as you know well, there are 16 sectors of critical infrastructure, and in addition to partnering with sector risk management agencies, CISA itself is a SRMA. Remind me how many agencies or sectors fall within your portfolio?

Mr. GOLDSTEIN. Eight, sir.

Mr. TORRES. Eight?

Mr. GOLDSTEIN. Yes, sir.

Mr. TORRES. Is that manageable given the constraints of your agency? There are some agencies that only have one sector to oversee, you have eight of them.

Mr. GOLDSTEIN. Yes, sir. CISA has unique capacity for both cyber and physical risk management. It is of course the calling and mission of our agency, and so we do work closely to support and enable further maturation of each sector for which we are the SRMA.

Mr. TORRES. Of the eight sectors, which one would you identify is the most target-rich and resource-poor?

Mr. GOLDSTEIN. Sir, there is a variety. I would note certainly sectors like the dam sector, like critical manufacturing, given its diversity, and even emergency services are sectors where we know that adversaries have expressed interest. A need for maturation is of course on-going.

Mr. TORRES. I have read the press releases about the 100 days cybersecurity sprints, but it seems like there is no real transparency around them. There has been no reporting regarding the results of these sprints.

So what have been the—do you intend to report the failures and successes of these sprints or the lessons learned from them?

Mr. GOLDSTEIN. So, sir, because the sprints derived from the President's NSM, I will defer to the White House for any reporting.

What I will say in this forum is we have seen different successes for each sprint based upon the diversity of entities involved in each. So as one example, for our pipeline sprint we saw that sprint derive much deeper collaboration between major pipeline companies the Federal Government. We have now stood up within the

Joint Cyber Defense Collaborative a new cyber defense planning effort with the Nation's largest pipelines that we would not have been able to achieve without the catalyzing force of these cybersecurity sprints.

For the water sprint, we were able to get an increasing number of companies signed up for our voluntary cyber hygiene vulnerability scanning services and were able to get more water entities interested in and signed up for CyberSentry.

So we at CISA certainly are seeing benefit and value from these sprints, but the value is different inherently based upon the different nature of the entities involved for each.

Mr. TORRES. I see my time has expired, so.

Chairwoman CLARKE. I thank the gentleman from New York.

The Chair now recognizes for 5 minutes the gentleman from Mississippi, Mr. Guest.

Mr. GUEST. Thank you, Madam Chairman.

I first want to thank both of you individuals for joining us today for this hearing.

Mr. Gipson, in your written testimony that you submitted, I think you did a great job summarizing the difference between the risk associated with IT and OT technology. For those who may be watching this hearing who may be, as I am at times, technologically challenged, can you kind-of walk through that since they don't have the benefit of what I have in front of me of the differences and the risk associated with those different systems. Very quickly.

Mr. GIPSON. Of course. Thank you for the opportunity again.

So as I ran through in my testimony, the IT and OT are different in a number of ways, specifically the ones I wanted to highlight was that IT is typically upgraded to replace every 3 to 5 years, software and firmware is frequently updated and patches are routinely installed, whereas with operational technology, because that is designed to in many cases last decades, those systems are often only updated every—whenever there is a noticeable failure. So very large difference in how modern the systems are.

When it comes to the standardization, there is existing guidance, cybersecurity best practices widely available for IT that many practitioners are trained in, whereas with operational technology, that simply does not exist.

Then finally, when it comes to cybersecurity tools, I mentioned discovery tools, but it is not only that, it is the ability to do things like intrusion detection, network analysis, widely available on the information technology side, but still very rare on the operational technology side. So there is a lot that still needs to happen to mature not only the practice of operational technology, but all of the support that goes with it that will come from industry. That needs to happen in parallel with training that operational technology, cybersecurity work force and training many others involved in critical infrastructure on what to know about cybersecurity.

Mr. GUEST. Then you continue on page 3 and you talk about vulnerabilities, specifically I believe to OT systems. You talk about vulnerabilities being inherent in the systems themselves, but you say that they are also introduced by adversaries through supply chain operations.

Can you talk a little bit about supply chain operations and how adversaries are able to exploit systems through that mechanism?

Mr. GIPSON. Yes. So when I speak of inherent vulnerabilities, that is what comes in, a piece of hardware, a piece of software, poor design, poor coding, mistakes people make, things that are errors that we didn't know at the time the device or service was created. They are inherent to the product.

Externally introduced is something that an adversary does to put a vulnerability into a product. That can happen anywhere along the supply chain. At the point of manufacture an adversary can introduce a vulnerability into a component or a system. At the point of shipping, an adversary can do that same thing. So along that supply chain are equipment, the component in the systems sometimes are exposed to adversaries who can manipulate them and introduce those vulnerabilities. Then likewise, because not everything in any system is developed in-house, there are other products that are introduced and incorporated into systems as they are designed and built. Each of those products has that same exposure to supply chain vulnerabilities.

So it is a remarkably difficult problem to know the entire supply chain, let alone secure the entire supply chain for a system.

Mr. GUEST. There have been recent efforts by Congress to move some of those manufacturers of some of these critical components back to the United States. As we see that legislation becomes successful, as we see these companies move back from foreign nations, particularly China, back to the United States, do you think that that will help with this supply chain issue that you have referred to here in your report?

Mr. GIPSON. I believe that will help. That is one piece of what needs to be done to help better secure the supply chain. It is a broad-based large problem, an issue that needs to be widely addressed.

Mr. GUEST. Thank you.

Madam Chairman, I believe I am out of time, so I will yield back.

Chairwoman CLARKE. I thank the gentleman from Mississippi.

We are going to enter into a second round of questioning at this time. This is a very important subject matter, something that we are trying to wrap our brains around and you two have the expertise to really get us where we need to be in terms of our vision for what we can do here from the Committee on Homeland Security.

So as I said in my statement, I believe we need to revamp our playbook for securing OT and the common baseline performance goals that CISA is developing might create a foundation to do just that, but only if CISA gets it right by working with the stakeholders to make sure that goals are effective, translated across sectors, and address the unique needs of OT operators.

So let me just ask, Mr. Goldstein, what mechanisms does CISA have in place to engage with stakeholders and solicit feedback? Is CISA proactively seeking new untapped stakeholder groups who may have novel insight to share?

Mr. GOLDSTEIN. Yes, ma'am, absolutely.

As you note, very correctly, the baseline performance goals are voluntary by intent and design and the only way that organizations will use these goals to advance their own risk management and

drive investment toward the most important security outcomes is if they are seen as credible, as valid, as helpful.

The only way we can achieve that is through a collaborative process in development. We have gone through two rounds of robust stakeholder feedback, both of which included public review. We received, remarkably, over 2,000 comments on the cybersecurity performance goals and held a variety of workshops, including both for sectoral partners and the general public, as well as listening sessions across our stakeholder groups.

Now, the point you raise, ma'am, is really important because one goal here we had was to make sure that we are getting input not just from the stakeholders who we talk to at CISA everyday, but also a diversity of individuals and groups with unique views. So we reached out uniquely to our international partners, to academia, to researchers, to owner-operators, device manufacturers, integrators, entities, across the spectrum.

Really importantly here, even after we released the next iteration of the baseline performance goals, our work on these goals isn't done, because we understand that as organizations begin to use these baseline goals in practice, they are likely to have observations and feedback that will help us make these even more useful. So our intent is to leave the door open for feedback on these baseline goals and actually do a fairly agile revision and update cycle so we can keep getting input and keep improving these again so organizations can use these on a voluntary basis with frameworks, like the NIST cybersecurity framework, to advance their risk management and measurement thereof.

Chairwoman CLARKE. It is good to hear that there is on-going exchange taking place, because this is an ever-evolving threat and need to really keep up to speed.

Now, for the sprints, CISA is in a supporting role to the sector research management agencies. How does CISA adjust that support based on the capacity and expertise of each SRMA?

Mr. GOLDSTEIN. Yes, ma'am.

So CISA is a source of expertise and cybersecurity risk reduction services, two critical sectors with and through the various SRMAs. As you know correctly, the level and type of support that we offer varies not only by the SRMA, but also by the sector itself. So in the context of the cyber sprints directive by the President's National Security Memorandum, for sectors, for example, like the pipeline sector, where many organizations have well-resourced security programs, you know, our level of support was different and actually providing, you know, more guidance, more coordination, and now really moving toward on-going operational collaboration to help more quickly identify and respond to emerging threats, risks, and vulnerabilities.

Conversely, for the water sector, given the over 50,000 water entities in this country, many of which are dramatically resource-constrained in cybersecurity, our role is really different. Our role is thinking through how we can help them provide capabilities, provide services, or for public entities, through our new SLTT Cyber Grant Program, actually provide them resources to improve their programs. So the heterogeneity of sectors does call for a different

level of support from CISA depending on the partners we are working with.

Chairwoman CLARKE. Then, finally, I know CISA wants to expand the CyberSentry to new partners. What is stopping you from doing that faster?

Mr. GOLDSTEIN. Yes, ma'am.

So the expansion of CyberSentry is on-going. We have gotten wonderful feedback on this program from the partners who are on board today, with the support of Congress, both resourcing and authorizing the program in the past year. We will be expanding throughout fiscal year 2023. We do want to be thoughtful and rigorous about the entities to whom we expand to make sure that they meet our requirements for consequentiality and risk and also that they are able to make best use of this program in conjunction with the commercial solutions that they already have deployed.

Chairwoman CLARKE. Very well.

We have been joined by one of our colleagues who wasn't with us in the first round but is now here with us, Mr.—Ranking Member, I am just going to—yes. I am going to—the Chair now recognizes for 5 minutes the gentleman from Kansas, Mr. LaTurner.

Mr. LATURNER. Thank you, Madam Chair. I appreciate it.

With the increase in prevalence of internet of things devices and connections between OT and IT systems, the cyber risk faced by our Nation will surely grow. I am sure we all heard from constituents about this threat and about attacks that have crippled vital businesses in our districts. In Kansas, 10 FSB officers hacked into a nuclear power plant in my district in 2017, and while they did not gain access to the cyber systems that operate the facility, the attack makes clear the importance of increasing our cybersecurity capability so that utilities can operate as a partner for the defense of the Nation.

In order for utilities to perform that role as expected by Government, they need timely and actionable information that they can take and respond to effectively. I appreciate the work that both CISA and INL are doing to meet those needs of industry and would like to thank each of our witnesses for being here today and sharing your expertise.

Mr. Gipson, you shared in your testimony about the importance of cyber physical test environments, like INL's control environment laboratory resource. How can industry partners like the nuclear plant in my district better leverage test ranges, like CELR?

Mr. GIPSON. Thank you. It is a wonderful thought.

The CELR, or that test range, think of that as a scaled version of a representative test range where practitioners, individuals can learn how to secure the operational technology while simultaneously seeing the physical system that is being controlled. So this is done at a scaled-down model size.

Now, it is wonderful because it helps see and visualize not only the cyber activity but also the physical results of any cyber mitigation. Now, it is even better if those same sorts of activities can be done at life-size scale. At Idaho National Lab we have that life-size scale. You know, the place is big, it is 890 square miles. That is 13 times the size of Washington, DC. We have a test bed for electricity, a small water test bed, some other things. But there is no

mechanism right now to open that up to public use without specific funding, either by private entities or more often, more normally, the Government.

Mr. LATURNER. I appreciate that.

I understand INL hosts an ICS community of practice that brings together ICS professionals across the Government, academia, and the industry. Is this group focused on the energy sector specifically?

Mr. GIPSON. No. ICS, industrial control system, community of practice is broader and it welcomes practitioners from all sectors. It is over a couple of hundred participating members now that is driving the maturation and training of ICS among those practitioners.

So that is an opportunity for collaboration that is easily grown as more learn of its existence and how it can benefit them.

Mr. LATURNER. Talk to me—I don't have a ton of time left, but it is so important—what efforts are under way with the COP on work force development and increasing the talent pipeline in OT cybersecurity?

Mr. GIPSON. So this is where Idaho National Lab spends a lot of effort. The training and development of that cybersecurity, and especially the operational technology cybersecurity work force. There are a variety of classes offered that can be attended either in-person or virtually that allow the hands-on learning of what it takes to secure critical infrastructure.

As I mentioned earlier, one of the great things about the offerings is that it allows the collaboration, and in many cases forces the collaboration beyond what the operational technology cybersecurity person normally does. That is critical to being able to secure cyber physical systems.

Now, in addition to those courses that are available to anyone—CISA funds many of those—through the development of courses for particular sponsors, like those within the Department of Defense and other areas, and in those cases we try to train the trainer so that it can be easily grown and expanded upon.

Mr. LATURNER. Thank you.

I yield back, Madam Chair.

Chairwoman CLARKE. I thank the gentleman.

I now recognize our Ranking Member, the gentleman from New York, Mr. Garbarino, for any additional questions he may have.

Mr. GARBARINO. Thank you, Chairwoman.

Again, thank you to the witnesses for being here today.

Mr. Gipson, can you speak—we have—I don't think we have touched on it really at all today, but can you speak in greater detail about National Lab's Malcolm Tool and, you know, how are CISA and other organizations, Government organizations utilizing this and other tools like this?

Mr. GIPSON. Thank you for that.

Malcolm, for those who aren't familiar, is an open-source analysis framework. The beauty of that is it is open source. Anyone can download the code, it is available on GitHub, and it allows those practitioners in cybersecurity to have a tool set to be able to better analyze that operational technology network data.

So as I mentioned in my testimony, these types of tools are widely available for IT cybersecurity professionals and analysts, but not so much on the OT side. So with CISA's funding, that Malcolm capability has been made available to everyone in the world.

Mr. GARBARINO. Is there room for a tool like this to go to the OT side? Is that possible or not really?

Mr. GIPSON. No, in fact Malcolm is available for the OT side. I mean emphasize that while there are many tools available from vendors to analyze IT data, not as many on the OT side. This is where Malcolm fills a gap and can help those analysts manipulate the data to be used in other IT available tools.

Mr. GARBARINO. Mr. Goldstein, is there a way—how do we get more people to use this tool and similar tools like it? I mean is it something that we just need to educate people of its existence and then hopefully they use it? Or what thoughts do you have?

Mr. GOLDSTEIN. Yes, absolutely.

So just to echo the good points of my co-witness, developing these sorts of open-source tools that meet specific security needs of the ICS and OT community is a key effort for both CISA and our colleagues at INL. So, you know, Malcolm is a wonderful tool. There are more to come. We continue to evaluate requirements and then develop and release as open source new tools that fulfill known gaps in the community.

To your point, sir, these tools are not useful if they are not being used. So part of our effort is to make sure that through efforts like INL's ICS community of practice, but also through groups that we sponsor at CISA, like the ICS joint working group that every year puts together thousands of practitioners around the world in this pace, as well as frankly being out there on the conference circuit, speaking at the events like the S4 Conference every year and making sure that we are evangelizing the usefulness of these tools to organizations and practitioners. That is really key so that they can actually drive down risk in practice.

Mr. GARBARINO. Would it make sense to make this—we have this as you said the State and local grant applications, could CISA require to be able to get access to these grants utilization of some of these tools as part of the application? Would that help it expand use?

Mr. GOLDSTEIN. Certainly we are thinking carefully through how we can utilize the grant program in the future to incentivize adoption of the right security measures and controls for many organizations that will be utilizing our grant programs. There are likely more foundational investments that will help them get to the point where they can use a tool like Malcolm more effectively.

Mr. GARBARINO. I appreciate both your answers on this and look forward to hearing about more tools in the future.

So thank you very much and I yield back.

Chairwoman CLARKE. I thank the gentleman, our Ranking Member, for his questions.

We have been joined by some additional colleagues and I want to give them an opportunity to ask their questions at this time.

So the Chair now recognizes the gentlelady from Texas, Ms. Sheila Jackson Lee, for her questions at this time.

Ms. JACKSON LEE. Madam Chair, I am passing at this time. Thank you.

Chairwoman CLARKE. Very well.

I will then recognize the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Madam Chair.

I want to thank our witnesses for their testimony today and what they are doing to better secure the country in cyber space. I deeply appreciate your efforts.

I wanted to follow up on a discussion that had taken place a little while ago about using binding operational directive authority requiring executive civilian branch departments and agencies to inventory the OT assets under their control as the NSTAC recommended in its related report to the President on IT OT convergence.

So my question is how well-resourced is CISA to support compliance with such a directive and integrate agency information about OT assets into its responsibilities as the operational lead for Federal cybersecurity?

Mr. GOLDSTEIN. Thank you, sir. Of course, a privilege to see you as always.

I will answer that in two parts. At the outset, the way that we have designed our continuous diagnostic and mitigation program is that agencies have the tools and have the connectivity with CISA's Federal dashboard to provide that asset visibility, both at the agency level and at a more aggregated level to CISA with the ability for CISA also to do deeper analytics into what we call object-level data, the characteristics of specific devices running on a network. We have a robust team at CISA focused exclusively at drafting, issuing, but then ensuring adherence to our binding operational directives. One key threshold criteria for issuance of a directive under our authorities at CISA is an assessment of our ability to measure adherence and ensure appropriate escalation with agencies if adherence does not meet our requirements.

So as we evaluate the use of our authorities to ensure appropriate asset visibility across both IT and OT assets, that will be top of mind. Our sense is today that we do have the technology and governance in place to enable that adherence if and when we do utilize such authorities.

Mr. LANGEVIN. OK. Thank you for clarifying that.

Of course finding solutions to the OT visibility problem should not exclude private-sector critical infrastructure owners and operators. To both of our witnesses, I wanted to ask, what are some of the major impediments right now facing critical infrastructure owners and operators and their Federal partners in cataloging OT assets and instances of IT-OT convergence? What can Congress do to help overcome those impediments?

Mr. GOLDSTEIN. Yes, sir, I will offer a thought and certainly welcome views from my co-witness.

You know, at the outset, a through line throughout this hearing has been the important differences between IT management and IT cybersecurity versus the control systems and OT environment. I think one example of this is for most IT practitioners and cybersecurity professionals, you know, IT asset management is considered

to be a foundational enabler of cybersecurity. To that end, there are a variety of tools and solutions in place to enable that visibility. Transposing those sorts of tools directly onto control systems and OT environments is non trivial and in fact may not be fit for purpose given the unique aspect of control systems and OT environments.

Additionally, the individuals or teams accountable for IT asset management in a given organization may be quite different from the ones who are managing the OT environment. So two key steps are to ensure that there a resolutions available for OT asset management that take into account the unique attributes of control systems and operational technology and that there is convergence between the teams, the individuals who are accountable for asset management to ensure that IT security and OT security are considered together given the unique linkages between those environments.

Mr. LANGEVIN. OK. Thank you.

Let me turn now finally to OT cybersecurity work force development. Critical infrastructure cybersecurity, especially as it pertains to the security of the industrial control systems requires a work force with specific skills that aren't always identical for those needed for traditional IT cybersecurity.

So to be sure traditional IT cybersecurity skills are valuable for a critical infrastructure cybersecurity operator to have, but equally importantly I think those operators must have an understanding of the engineering principles underlying specific ICS devices and the systems they control, as well as the knowledge of how to maintain physical and environmental safety in the operation of such devices. Have you seen challenges in this critical infrastructure owners and operators ability to attract ICS cybersecurity talent with expertise in each of these areas? Are the opportunities for the Federal Government and Congress specifically to support the development of these skills across the ICS cybersecurity work force?

Mr. GOLDSTEIN. Yes, sir. This absolutely is an area of urgent focus and concern. My co-witness outlined some of the important work from Idaho National Labs to address this delta, but certainly we know that our Nation is facing a real workforce crisis in the cybersecurity work force generally. As you well note, sir, these specialized skills to operation control systems or OT cybersecurity environment are even more specialized and require an understanding not only of cybersecurity but also of the unique operational considerations that are inherent in control systems and OT.

CISA is working closely with partners, including INL, including our colleagues at DOE, to provide curricula, courses, hands-on training, to address this gap, but we need to do more. Certainly as control systems and OT become more and more ubiquitous and relied upon across sectors, this will be an area where the Federal Government, the private sector, academia, and with the support of Congress, we really need to invest and focus.

Mr. LANGEVIN. Very good.

Thank you, Madam Chair. Thank you to our witnesses for their testimony.

I yield back.

Chairwoman CLARKE. So I wish to thank the witnesses for their valuable testimony and the Members for their questions today.

The Members of the subcommittee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

The Chair reminds Members—it looks as though we do have another question from—we are working hybrid here, so I did recognize that our chair—excuse me, Congresswoman Sheila Jackson Lee of Texas is now recognized for 5 minutes. Excuse me. Congresswoman Lee, I think you need to unmute. We can't hear you, can you unmute?

Ms. JACKSON LEE. Can I be heard now?

Chairwoman CLARKE. Yes, you can.

Ms. JACKSON LEE. All right. Well, let me just say that hybrid is certainly helpful, but challenging sometimes.

To the witnesses, let me thank you for your testimony. To Madam Chair, thank you and Ranking Member for very important hearing. Members are detained in other matters and I did want to make sure in this important hearing I raise two questions.

So I would like the witnesses to answer them as they are able to do so.

We have been working with the issue of industrial infrastructure for a very long time. I remember chairing the Transportation Security Committee, which had infrastructure as part of its jurisdiction. Really, in the old days, if you will, we had not reached the level of fear or apprehension about cyber attacks. They were probably more physical attacks as relates to industrial infrastructure. But I would like to ask the level of threat, the level or the rate of threats you think are to America's industrial infrastructure. What level are we at? How can we educate the industrial community—I think some are more informed than others—on the level of threat?

Secondarily, as relates to the work force, are you working with historically Black colleges, Hispanic-serving institutions to help them steer toward programs that would help build the work force?

If those who are able to answer those questions to do so, I would appreciate it. I thank the Chair for her indulgence.

Mr. GOLDSTEIN. Thank you, ma'am.

On the first question, the level of threat facing control systems and operational technology is significant. I will call particular attention to the variety of products that CISA and our partners released during our Shields Up campaign subsequent to Russia's unprovoked invasion of Ukraine, which included advisories focused on threats to, for example, programmable logic controllers, interval power supplies, and similar technology widely used in the ICS and OT context. We know that the consequentiality of an intrusion into these systems is very significant and therefore we must be concerned about steps to ensure their security and resilience under all conditions.

On the second question, ma'am, absolutely. You know, as much as we need to address the cybersecurity work force gap in this country, we need a cybersecurity work force that reflects the diversity of America. So at CISA we are deeply focused on working with HBCUs, with MSIs. We are excited to host our upcoming CISA Cyber Summit in October with a number of HBCUs in the Atlanta,

Georgia area in coordination with those entities to ensure that we have a pipeline that dramatically changes. The diversity of our cyber work force is foundational to our strategy.

Ms. JACKSON LEE. I think I still have a little bit of time.

I think many of us would be very much interested in a summit of that form. Are you suggesting that colleges outside of Atlanta can come? Or otherwise would you reach my office? I think the southwest region sometimes gets overlooked and we have a sizable population of historically Black colleges in the region and would like to offer that region, and Houston in particular, for another site for such a summit. Because this is crucial to help build the platforms of programs that colleges can begin to start with to help assist in the work force development going forward.

Mr. GOLDSTEIN. Yes, ma'am. I am confident that we value the chance to work with HBCUs and MSIs in your district and will certainly follow up with your team.

Ms. JACKSON LEE. Thank you so very much.

Madam Chair, I thank you so very much for this hearing and I yield back.

Chairwoman CLARKE. Before we close, I am going to give one more opportunity. Anyone virtually who has any questions at this time and wishes to be recognized?

Very well.

With that, I thank you once again. I thank our witnesses for your valuable testimony and the Members for their questions. The Chair reminds Members that the subcommittee record will remain open for 10 business days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:28 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE FOR ERIC GOLDSTEIN

Question 1a. CISA has published a fact sheet supporting and prioritizing the migration to post-quantum cryptography for public and private entities. Given that National Critical Functions (NCFs) are reliant on ICSs, how can Congress support CISA's efforts to provide additional targeted guidance to NCFs that require more aide?

Question 1b. Can CISA provide a list of NCFs that require the most aide based on level of priority?

Question 1c. What additional resources are shared with SRMAs to provide support as the entities transition to post-quantum cryptography?

Answer. The transition to post-quantum cryptography (PQC) requires that the National Institute of Standards and Technology (NIST) standardize the new algorithms that have been developed to resist attack by a cryptographically-relevant quantum computer. These algorithms are not yet standardized and therefore not included in commercially-available systems for ready adoption by critical infrastructure owners and operators. As PQC proceeds through the standardization process at NIST and more PQC algorithms appear in systems that owners and operators can adopt, the Cybersecurity and Infrastructure Security Agency (CISA) will achieve a better understanding of which sectors and functions need greater aid and support to transition to PQC.

CISA and NIST recently held an all-sector call with a large number of critical infrastructure cybersecurity executives to inform them of the upcoming transition to PQC and recommend that they conduct an internal inventory of their current cryptosystems to better understand the scope of what their organizations will need to transition.

CISA has highlighted several National Critical Functions that are dependent on ICS and may benefit from additional support to prepare for and execute the migration to post-quantum cryptography:

- Generate Electricity
- Distribute Electricity
- Transmit Electricity
- Transport Cargo and Passengers by Rail
- Transport Cargo and Passengers by Vessel
- Transport Materials by Pipeline
- Transport Passengers by Mass Transit
- Manage Hazardous Materials
- Manage Wastewater
- Store Fuel and Maintain Reserves
- Exploration and Extraction of Fuels
- Fuel Refining and Processing Fuels
- Manufacture Equipment
- Produce and Provide Agricultural Products and Services
- Produce and Provide Human and Animal Food Products and Services
- Produce Chemicals
- Provide Metals and Materials
- Supply Water
- Provide Internet-Based Content, Information, and Communication Services
- Provide Identity Management and Associated Trust Support Services
- Provide Information Technology Products and Services
- Protect Sensitive Information.

CISA continues to partner closely with NIST, other U.S. Government partners, and private-sector partners to support a smooth transition to post-quantum cryptography, as called for in National Security Memorandum–10, when new standards are available.

QUESTIONS FROM RANKING MEMBER ANDREW R. GARBARINO FOR ERIC GOLDSTEIN

Question 1. A major challenge public and private-sector critical infrastructure owners and operators face is balancing the priorities of enhancing security and modernizing legacy equipment. There are sensitivities around when certain devices on the network can be taken off-line for updates versus when they need to be on-line and operating. With the introduction of new regulations and guidelines related to industrial control system (ICS) modernization and security, organizations are forced to make difficult decisions.

Understanding these difficulties, can you describe how CISA is partnering with its Federal agency partners to provide owners and operators with assistance in market research to better understand what resources are available to assist with these common issues?

Answer. CISA has received substantial input during stakeholder outreach activities in support of the development of cybersecurity performance goals for critical infrastructure that echoes the challenge you have outlined. CISA's primary forum for engaging with interagency counterparts on the topic of modernization is the monthly Control Systems Interagency Working Group. Additionally, CISA leads a Control Systems Working Group that brings together both industry and interagency representatives to talk through ICS challenges. Going forward, CISA intends to use both bodies, as well as the activities associated with our roll-out of the cybersecurity performance goals, as opportunities to both garner feedback and share recommendations and best practices with the community on how to safely and effectively approach modernization.

As an example, CISA has worked with the U.S. Department of Energy (DOE) to support market research, including through publication of recommended considerations for organizations seeking to adopt and deploy ICS/operational technology (OT) monitoring solutions. These recommendations consist of a vendor-agnostic framing of capabilities and feature-sets, which CISA and DOE believe to be most critical in ensuring the procured tool delivers value to the adopter and meaningfully reduces risk to ICS/OT assets.

Another example of support that can aid in market research for ICS investment are the recently published Cybersecurity Performance Goals (CPGs) for Critical Infrastructure. These goals were developed as a minimum baseline of cybersecurity activities for critical infrastructure, that should inform where organizations should prioritize resource investments for the most effective reduction of cyber risk. While the goals themselves are vendor and platform-agnostic, they do inform what practices organizations should be implementing.

Question 2a. Core to CISA's mission is gaining centralized, holistic visibility across Federal Civilian Executive Branch (FCEB) networks. Recognizing that you can't secure what you can't see, the fiscal year 2022 Consolidated Appropriations Act included $65 million in CISA funds for "attack surface management and National vulnerability incident response." The accompanying House report for this funding appropriately recognizes that, "Unlike DoD, CISA remains heavily dependent on manual self-reporting for situational awareness of internet-facing attack surfaces, creating a fractured and inaccurate snapshot of vulnerabilities in the Federal civilian cybersecurity ecosystem." Effective execution of these fiscal year 2022 funds could finally give CISA continuous visibility over the entirety of the internet-facing FCEB attack surface through the eyes of the adversary.

Recognizing Congressional intent, what is CISA's plan to execute the $65 million of fiscal year 2022 funds? How much of those funds have been executed to date?

Question 2b. In line with the direction of the report language, how is CISA evaluating state-of-the-art commercial solutions?

Question 2c. Are the lessons from successes elsewhere in Government standing up similar attack surface management programs being appropriately incorporated into CISA's plans?

Answer. CISA remains appreciative of Congress' on-going support of the Agency's cybersecurity mission, including support of enhanced visibility into threats targeting the internet-facing Federal Civilian Executive Branch attack surface.

CISA has obligated 100 percent of the funds appropriated in fiscal year 2022 for Attack Surface Management (ASM). To date, the agency has executed a portion of the obligated appropriations (~20 percent) to initiate a technology assessment to identify candidate tools to advance CISA's ASM capabilities, specifically in the areas of asset discovery, vulnerability enumeration, domain and subdomain discovery, passive scanning, and web app scanning. In addition to the technology assessment, funding has been executed to bolster CISA's analytic capabilities through enhanced data feeds data analytics, a necessary prerequisite to expansion of our ASM capabilities.

CISA's evaluation has consisted of in-house market research and proof-of-value assessments, coordination with other Federal agencies (including the U.S. Department of Defense (DoD)) who have stood up similar ASM capabilities, and an independent assessment conducted by Lawrence Livermore National Laboratory, which concluded in September.

CISA intends to execute the remainder of the obligated-but-not-yet-expended fiscal year 2022 appropriations to implement state-of-the-art commercial technologies over the duration of this fiscal year to ensure that the agency is providing maximum benefit to our stakeholders, and will continue to coordinate with DoD and other Federal agencies throughout the duration of funding execution and associated capability implementation.

Question 3. How should the adoption of modern "zero trust" architectures and the latest cybersecurity standards be encouraged as ICS and operational technology (OT) systems become more internet-connected?

Answer. Due to the unique design limitation inherent in many ICS and OT assets, full implementation of Zero Trust across ICS and OT environments is especially difficult. Wide-spread utilization is likely not feasible until there is a critical mass of available products and infrastructure that supports such efforts. While wide-spread adoption may be difficult, more mature organizations can likely begin applying Zero Trust concepts to some elements of their infrastructure where possible. CISA continues to leverage our monthly Control Systems Interagency Working Group (CSWG), public-private Control Systems Cybersecurity Working Group (CSCSWG), and our Joint Cyber Defense Collaborative-ICS group to share lessons learned and best practices to accelerate adoption of Zero Trust controls across ICS and OT environments.

Question 4. CISA helps Federal agencies implement the Cybersecurity Executive Order and Federal Zero Trust Strategy to move to more modern, defensible cyber architectures.

How is CISA working to encourage adoption of "zero trust" approaches to cybersecurity by critical infrastructure owners?

Answer. CISA has developed guidance and is planning to establish a Zero Trust program office to lead and support the adoption of Zero Trust in the Federal Civilian Executive Branch. The guidance publications are Cloud Security Technical Reference Architecture (CSTRA) and the Zero Trust Maturity Model (ZTMM), and are intended to address modernization, cloud migration, and zero trust strategies and approaches that can be broadly applied to support Executive Order 14028 and associated strategies and policies.

The CISA Zero Trust Program Office was identified in the National Security and Telecommunications Advisory Committee's Report To The President, Zero Trust and Trusted Identity Management, February 23, 2022. The report provided recommendations that CISA should take to incorporate Zero Trust practices into Federal cybersecurity programs and services. To date, the CISA Cybersecurity Division has initiated planning efforts to support the establishment of the program office with key lines of effort intended to address critical. This work will will be necessary to evolve and mature Zero Trust implementations within Federal agencies.

The CSTRA was co-authored by CISA, Federal Risk and Authorization Management Program, and United States Digital Services and addresses Zero Trust architecture and protections concepts and approaches intended to guide agencies that modernize and migrate applications, data, and services to the cloud. This guidance focuses on cloud hosting environments to ensure that cybersecurity and data protections, as well as monitoring and visibility, are consistent with organizational risk management practices. The ZTMM was developed to support and guide agencies as they develop strategies and implementation plans to transition from perimeter-focused architectures to Zero Trust. The maturity model utilizes five pillars and cross-cutting functions to explain key capabilities to advance and evolve zero trust within on-premise and cloud hosting environments.

Question 5. In July, TSA issued a revised cybersecurity directive for pipelines owners to apply "zero trust" cybersecurity elements to any information technology (IT) or OT system connected to a critical pipeline or facility. Federal agencies are also implementing zero trust architectures following requirements from the Cybersecurity Executive Order.

Should similar zero trust requirements for IT and OT systems be encouraged across all critical infrastructure sectors?

Answer. The disruptive ransomware attack on Colonial Pipeline in May 2021 revealed a continuing significant National security risk with critical vulnerabilities in the pipeline sector that previous voluntary efforts did not sufficiently mitigate. Following the incident, the Transportation Security Administration (TSA) issued two Security Directives mandating that pipeline owners and operators implement sev-

eral critically-important and urgently-needed cybersecurity measures. TSA developed these directives in close consultation with Federal partners, including CISA, the Pipeline Hazardous Materials and Safety Administration, and DOE. TSA is working closely with the pipeline industry to ensure the successful implementation of the measures required by the directives.

While Zero Trust does represent an effective approach to security, and is certainly a strong and growing trend, there are unique considerations to its utilization in OT environments. The most pertinent of these considerations is that many OT assets were originally designed with a focus on safety and reliability with limited focus on security. Therefore, many OT environments likely do not support effective utilization of Zero Trust, at this time. Before adoption can be widely encouraged, the most effective immediate action would likely entail working with OT vendors to recognize Zero Trust as a desired attribute in future product sets. Additionally, Zero Trust is likely too complex of an implementation for many small and medium-sized entities for the time being; it may however, be a more realistic goal state for more mature and better-resourced organizations.

QUESTIONS FROM HONORABLE JAMES LANGEVIN FOR VERGLE GIPSON

Question 1. What are some of the major impediments facing critical infrastructure owners and operators and their Federal partners in cataloguing Operational Technology (OT) assets and instances of Information Technology (IT)/OT convergence, and what can Congress do to help overcome those impediments?

Answer. The convergence of IT/OT is not understood well enough within critical infrastructure owners and operators. From Idaho National Laboratory's (INL's) perspective, we have seen cases where owners and operators were not aware of IT/OT convergence in their systems. More educational training and improved information sharing between public and private-sector partners are needed. INL recommends Congress support these measures in the National Plan and Presidential Policy Director–21 rewrites.

Further, many OT assets do not support the typical tools—like asset identification—commonly used by the IT sector. In fact, many IT tools may negatively impact OT operation because of their interrogation techniques. The commercial and research communities are working to address this problem and further investigation and testing against representative models of common process environments will be needed to achieve higher rates of success of these solutions. We recommend that Congress continue to support development and expansion of Digital Bill of Material (DBOM), to include Software Bill of Material (SBOM) and Hardware Bill of Material (HBOM), as the most promising method to document OT assets.

Question 2. Critical infrastructure cybersecurity, especially as it pertains to the security of industrial control systems (ICS), requires a workforce with specific skills that are not always identical to those needed for traditional IT cybersecurity. To be sure, traditional IT cybersecurity skills are valuable for a critical infrastructure cybersecurity operator to have. But equally importantly, I think those operators must have an understanding of the engineering principles underlying specific ICS devices and the systems they control, as well as the knowledge of how to maintain physical and environmental safety in the operation of such devices.

Have you seen challenges in critical infrastructure owners and operators' ability to attract ICS cybersecurity talent with expertise in each of these areas, and are there opportunities for the Federal Government, and Congress specifically, to support the development of these skills across the ICS cybersecurity workforce?

Answer. There is a Nation-wide shortage of workers with IT cybersecurity skills, and an even larger shortage of workers with OT cybersecurity skills. Asset owners and operators, as well as vendors and others, have had significant challenges in attracting right-skilled workers. In addition to OT cybersecurity courses offered in the private sector, Idaho National Laboratory (INL) continues to develop and offer advanced and tailored OT cybersecurity training. Furthermore, specialized programs, such as the Department of Energy's "Operational Technology Defenders Fellowship," have brought together the right industry and Government stakeholders to develop the knowledge and the relationships to better defend U.S. critical infrastructure. We recommend Congress support expansion of the OT Defender Fellowship to sectors beyond the energy sector and to additional stakeholders.

Further, there is a shortage of OT cybersecurity workers who have working knowledge of the systems and processes their operational technology is controlling. Perhaps even more detrimental to security, there is a shortage of engineers and operators who have a working knowledge of cybersecurity. We recommend Congress expand its support of Cyber-Informed Engineering (CIE) and Consequence-Driven CIE to sectors beyond the energy and defense sectors and to additional stakeholders.

QUESTIONS FROM RANKING MEMBER ANDREW R. GARBARINO FOR VERGLE GIPSON

Question 1. Critical National infrastructure is susceptible to a variety of cybersecurity threats, reliability concerns, aging equipment, and resource limitations. To add to the complexity, grid modernization efforts are well under way with the advent of smart devices, renewable technologies, and cellular connectivity.

How does INL and Cybersecurity and Infrastructure Security Agency (CISA) plan to mitigate a growing threat landscape beyond simply network monitoring and detection?

Answer. Investments continue to be made by Idaho National Laboratory and CISA in developing advanced cybersecurity tools and analysis capabilities that are far beyond "simply network monitoring and detection."

We recommend Congress support a "defense in depth" and "security by design" approach for U.S. critical infrastructure. Additional funding is needed to expand Cyber-Informed Engineering (CIE) and additional test environments are needed at both small-scale and full-scale to develop and demonstrate effective mitigations. Further investments and a build-out of more full-scale and small-scale test ranges will allow high-fidelity research to better understand this growing landscape, as well as provide the needed research environment to develop capabilities and collaborate with asset owners, vendors, and Government to solve this evolving problem.

Question 2. The National Laboratories invest in cutting-edge, innovative technologies aimed at tackling some of the hardest cybersecurity challenges. However, the transition of emerging, desperately-needed technology lacks the funding, sponsorship, and ultimately the deployment to secure the grid.

What strategies and approaches do you recommend at INL to transition technology to the utility sector, like the Constrained Communications Cyber Device?

Answer. Federal agencies must commit to the long-term deployment of the technology and support collaborative projects to pilot and mature them through operational testing with interested private-sector commercialization partners so that technology comes to market. The key barrier facing deployment of laboratory-developed technologies to the utility sector is the "valley of death." This phenomenon happens when funding for initial technology development concludes after a proof-of-concept effort with a technology not yet mature enough for use in critical infrastructure environments. It is often difficult for laboratory researchers to attract funding to mature technology through the maturity cycle, and often the National Laboratories are not the most cost-effective entities to perform that work. However, INL and other National Laboratories are exploring solutions to obtain funding and support to mature these technologies for deployment.

For example, INL, along with Pacific Northwest National Laboratory, Oak Ridge National Laboratory, and Sandia National Laboratories, executed a trial program partnered with the Department of Energy's Office of Technology Transitions (DOE–OTT) and a venture advisory company. In this program, National Laboratories work with the venture advisory company to select technologies within their portfolios that are highly aligned with the growing needs of highly-regulated industries. The venture advisory company establishes an investor network to create start-up companies that can develop the technology toward the maturity needed for deployment in critical infrastructure. The trial of this program was very successful, and DOE–OTT has invested in an additional year of execution. Additional funding focused on leveraging venture capital to mature technologies past the "valley of death" into deployable maturity would hasten the deployment of technologies like the Constrained Communications Cyber Device.

We recommend that Congress fund activities to further mature appropriate technologies to the operational pilot stage and fund activities for the National Laboratories to team with potential private-sector partners to demonstrate, operationalize, and deploy those technologies.