

CISA 2025: THE STATE OF AMERICAN CYBERSECURITY FROM A STAKEHOLDER PERSPECTIVE

HEARING
BEFORE THE
SUBCOMMITTEE ON
CYBERSECURITY AND INFRASTRUCTURE
PROTECTION
OF THE
COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 23, 2023

Serial No. 118–4

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

52–262 PDF

WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas	BENNIE G. THOMPSON, MISSISSIPPI, RANKING MEMBER
CLAY HIGGINS, Louisiana	SHEILA JACKSON LEE, Texas
MICHAEL GUEST, Mississippi	DONALD M. PAYNE, JR., New Jersey
DAN BISHOP, North Carolina	ERIC SWALWELL, California
CARLOS A. GIMENEZ, Florida	J. LUIS CORREA, California
AUGUST PFLUGER, Texas	TROY A. CARTER, Louisiana
ANDREW R. GARBARINO, New York	SHRI THANEDAR, Michigan
MARJORIE TAYLOR GREENE, Georgia	SETH MAGAZINER, Rhode Island
TONY GONZALES, Texas	GLENN IVEY, Maryland
NICK LALOTA, New York	DANIEL S. GOLDMAN, New York
MIKE EZELL, Mississippi	ROBERT GARCIA, California
ANTHONY D'ESPOSITO, New York	DELIA C. RAMIREZ, Illinois
LAUREL M. LEE, Florida	ROBERT MENENDEZ, New Jersey
MORGAN LUTTRELL, Texas	YVETTE D. CLARKE, New York
DALE W. STRONG, Alabama	DINA TITUS, Nevada
JOSH BRECHEEN, Oklahoma	
ELIJAH CRANE, Arizona	

STEPHEN SIAO, *Staff Director*

HOPE GOINS, *Minority Staff Director*

NATALIE NIXON, *Chief Clerk*

SEAN JONES, *Legislative Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CARLOS A. GIMENEZ, Florida	ERIC SWALWELL, California, <i>Ranking Member</i>
MIKE EZELL, Mississippi	SHEILA JACKSON LEE, Texas
LAUREL M. LEE, Florida	TROY A. CARTER, Louisiana
MORGAN LUTTRELL, Texas	ROBERT MENENDEZ, New Jersey
MARK E. GREEN, MD, (<i>ex officio</i>)	BENNIE G. THOMPSON, Mississippi (<i>ex officio</i>)

CARA MUMFORD, *Subcommittee Staff Director*

MOIRA BERGIN, *Minority Subcommittee Staff Director*

ALICE HAYES, *Subcommittee Clerk*

CONTENTS

	Page
STATEMENTS	
The Honorable Andrew R. Garbarino, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	1
Prepared Statement	3
The Honorable Eric Swalwell, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	4
Prepared Statement	5
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement	7
WITNESSES	
Ms. Tina Sherman, Director, Critical Infrastructure Protection and Transportation Security, U.S. Government Accountability Office:	
Oral Statement	8
Prepared Statement	10
Mr. Drew Bagley, Vice President and Counsel, Privacy and Cyber Policy, CrowdStrike:	
Oral Statement	14
Prepared Statement	16
Ms. Heather Hogsett, Senior Vice President, Technology and Risk Management, Bank Policy Institute:	
Oral Statement	22
Prepared Statement	24
Mr. Marty Edwards, Vice President, Operational Technology Security, Tenable:	
Oral Statement	27
Prepared Statement	29
APPENDIX	
Question From Chairman Andrew R. Garbarino for Tina Won Sherman	53
Question From Chairman Andrew R. Garbarino for Marty Edwards	53

CISA 2025: THE STATE OF AMERICAN CYBER- SECURITY FROM A STAKEHOLDER PER- SPECTIVE

Thursday, March 23, 2023

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

The subcommittee met, pursuant to notice, at 10 a.m., in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino [Chairman of the subcommittee] presiding.

Present: Representatives Garbarino, Gimenez, Ezell, Lee, Luttrell, Swalwell, Jackson Lee, Carter, and Menendez.

Also present: Representatives Green and Thompson.

Chairman GARBARINO. The Committee on Homeland Security on Cybersecurity and Infrastructure Protection will come to order.

The purpose of this hearing is to receive testimony from a panel of experts and industry leaders who will provide their perspectives on CISA to the subcommittee through the lens of its stakeholders. These witnesses will help the subcommittee explore how the agency has gotten to where it is today and provide ideas to help mature the agency by 2025 and beyond.

I now recognize myself for an opening statement.

I would like to thank the Members of the subcommittee and our witnesses for joining us for our first hearing on the Cybersecurity Infrastructure Protection subcommittee of the 118th Congress. I am honored to continue the great work we started in the subcommittee last Congress, this time as Chairman. We are here today to discuss a key agency to our homeland security, the Cybersecurity and Infrastructure Security Agency, or CISA, within the Department of Homeland Security.

CISA has a critical mission set. It is tasked with administering Federal cybersecurity requirements, supporting private-sector cybersecurity, engaging with the Sector Risk Management Agency, and ensuring the physical security of our critical infrastructure. Today, we will focus specifically on the cyber aspects of CISA's mission. CISA has a direct impact on securing critical infrastructure, Federal agencies, and our way of life. It is an agency built on partnerships, and those partnerships with stakeholders play an important role in furthering CISA's mission. So today we will hear from some of those stakeholders to understand CISA's strengths, weaknesses, and where it needs to go in the future.

In recent years, the United States has experienced a deluge of high-profile cyber incidents, from Solar Winds to Colonial Pipeline, to Log4shell vulnerability. Our cyber defenses, work force, and processes have been put to the test, and CISA has been at the center of every response. These incidents have elevated cybersecurity issues across the country and highlighted the importance of securing both Federal and critical infrastructure networks.

As a result of the evolving cyber threat landscape, Congress has asked a lot of CISA from Day 1 and expected it to succeed. The reality is that CISA is still a young agency, it was created in 2018, and since then it has grown exponentially. Since fiscal year 2019, Congress has nearly doubled CISA's annual budget from \$1.68 billion in fiscal year 2019 to \$2.9 billion in fiscal year 2023, and we are now looking at fiscal year 2024 request of \$3.1 billion. This level of funding would be a lot for even a large, mature department to handle.

Congress has also given CISA significant new authorities, including the responsibility of establishing a cross-sector incident reporting rule making and the authority to persistently hunt for threats on Federal networks without prior agency approval. Properly executed, these new authorities and resources will help CISA accomplish its mission.

This Congress, our subcommittee will conduct rigorous oversight of CISA to ensure those new authorities are implemented appropriately and CISA is a responsible steward of taxpayer dollars. We need to take a step back and allow CISA to get a handle on their new responsibilities and ask pointed productive questions about its efforts. Like CISA is a partnered industry to help them improve their cyber posture, Congress should be a partner to CISA to help the agency mature and reach its full potential.

We have four distinguished witnesses to kick off our efforts. Each witness brings a different perspective on CISA and its partnerships. With these witnesses, we will examine CISA's role as the Nation's risk manager and how it balances that role with its responsibilities as a Sector Risk Management Agency for 8 sectors. We will consider the proper role for regulation while balancing security and collaboration with CISA as a partner to industry. We will also delve into CISA's Federal network programs as well as external efforts as a partner with private sector to improve critical infrastructure cybersecurity, particularly through the Joint Cyber Defense Collaborative.

Sounds like a lot we are doing today.

Additionally, we will discuss CISA's effort to secure operational technology, or OT, an important aspect of critical infrastructure mission.

If I did not comment on the need to address the cyber work force shortage that both the Federal Government and many industry partners across the 16 critical infrastructures face, none of these efforts that I have outlined today will be possible without a fully-equipped cyber work force. I look forward to discussing the ways in which we can address the over 700,000 cyber work force gap that exists today.

I am looking forward to a thoughtful and productive conversation about CISA and how it could improve and grow in the future. It

is imperative that CISA succeed in its important mission. I look forward to working with my colleagues to find bipartisan ways to ensure that it does.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

I'd like to thank the Members of the subcommittee and our witnesses for joining us for our first hearing of the Cybersecurity and Infrastructure Protection subcommittee of the 118th Congress. I'm honored to continue the great work we started in this subcommittee last Congress—this time, as Chairman.

We are here today to discuss a key agency to our homeland security: the Cybersecurity and Infrastructure Security Agency, or CISA, within the Department of Homeland Security. CISA has a critical mission set. It is tasked with administering Federal cybersecurity requirements, supporting private-sector cybersecurity, engaging with the sector risk management agency community, and ensuring the physical security of our critical infrastructure. Today, we will focus specifically on the cyber aspects of CISA's mission.

CISA has a direct impact on securing critical infrastructure, Federal agencies, and our way of life. It is an agency built on partnerships—and those partnerships with stakeholders play an important role in furthering CISA's mission. So today, we will hear from some of those stakeholders to understand CISA's strengths, weaknesses, and where it needs to go in the future.

In recent years, the United States has experienced a deluge of high-profile cyber incidents, from SolarWinds, to Colonial Pipeline, to the Log4Shell vulnerability. Our cyber defenses, workforce, and processes have been put to the test, and CISA has been at the center of every response. These incidents have elevated cybersecurity issues across the country and highlighted the importance of securing both Federal and critical infrastructure networks.

As a result of the evolving cyber threat landscape, Congress has asked a lot of CISA from Day 1, and expected it to succeed. The reality is that CISA is still a young agency; it was created in 2018 and since then, it has grown exponentially. Since fiscal year 2019, Congress has nearly doubled CISA's annual budget, from \$1.68 billion in fiscal year 2019 to \$2.9 billion in fiscal year 2023. We're now looking at the fiscal year 2024 request of \$3.1 billion. This level of funding would be a lot for even a large, mature department to handle.

Congress has also given CISA significant new authorities, including the responsibility of establishing a cross-sector incident reporting rule-making and the authority to persistently hunt for threats on Federal networks without prior agency approval. Properly executed, these new authorities and resources will help CISA accomplish its mission.

This Congress, our subcommittee will conduct rigorous oversight of CISA to ensure those new authorities are implemented appropriately and CISA is a responsible steward of taxpayer dollars. We need to take a step back and allow CISA to get a handle on their new responsibilities and ask pointed, but productive, questions about its efforts. Like CISA is a partner to industry to help them improve their cyber posture, Congress should be a partner to CISA to help the agency mature and reach its full potential.

We have four distinguished witnesses to kick off our efforts. Each witness brings a different perspective on CISA and its partnerships. With these witnesses, we will examine CISA's role as the Nation's Risk Manager and how it balances that role with its responsibilities as a Sector Risk Management Agency, or SRMA, for 8 sectors. We will consider the proper role for regulation while balancing security and collaboration, with CISA as a partner to industry. We will also delve into CISA's Federal network programs as well as external efforts as a partner with the private sector to improve critical infrastructure cybersecurity, particularly through the Joint Cyber Defense Collaborative. Additionally, we will discuss CISA's efforts to secure operational technology, or OT: an important aspect of its critical infrastructure mission.

Finally, I would be remiss if I did not comment on the need to address the cyber workforce shortage that both the Federal Government and many industry partners across the 16 critical infrastructure sectors face. None of these efforts that I've outlined today would be possible without a fully-equipped cyber workforce, and I look forward to discussing ways in which we can address the over 700,000 cyber workforce gap that exists today.

I am looking forward to a thoughtful and productive conversation about CISA and how it could improve and grow in the future. It's imperative that CISA succeed in

its important mission and I look forward to working with my colleagues to find bipartisan ways to ensure that it does.

Chairman GARBARINO. I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for his opening statement.

Mr. SWALWELL. Thank you. I thank the Chairman and congratulate the Chairman and his staff for taking over this subcommittee. I look forward to working with you, Mr. Chairman.

There are a lot of topics that come before this committee where you will see passionate debate between both sides, mostly earnest, substantive, but here, I don't think there is much daylight between the two of us as far as what our cybersecurity threats are and the resolve that the two of us have to meet them.

For me, particularly in my Congressional district, with so many people who work in high tech with two national laboratories, to also make sure that we can deploy awareness and technologies to small businesses in an affordable way. You know, 10 years ago, when I first came on this committee, you had to be this tall to be a target of a serious ransomware attack. Today, small businesses, thousands of small businesses, are being hit every single day. So it is part of my goal on this committee to work with the Chairman to make sure that we can really harden the defenses, especially for critical infrastructure, but especially small businesses.

I want to thank the witnesses for participating today and also our staff who prepared this hearing.

The Cybersecurity and Infrastructure Protection subcommittee has a strong bipartisan support in bipartisan collaboration. Just, again, I look forward—as this is the first committee hearing of the year—to working with the Chairman and his staff and his Members as we pursue that.

But speaking of CISA, as the Chairman pointed out, we have nearly doubled since 2019 CISA's budget. When we established it 4.5 years ago, we envisioned the agency as a sophisticated cybersecurity and infrastructure organization. Thanks to bipartisan work on this subcommittee and the full committee, it has matured rapidly and growing more capable of meeting our Nation's complex and diverse threat environment. All of us have been impressed by what CISA has been able to accomplish so far. However, as the Chairman referenced, we need to work to support the agency as it continues to adapt to the cybersecurity needs of our Federal Government, critical infrastructure sector, and private enterprises, especially small businesses.

From election security to ShieldsUP, CISA has demonstrated an ability to dynamically surge resources to counter emerging threats and collaborate strategically with the private sector. Looking ahead, Director Easterly has set ambitious goals to modernize CISA's Federal network security programs, to tactically engage with entities whose resilience matters most to our national security, and to drive adoption of secure by design and secure by default. At the same time, CISA is in the process of implementing the Cyber Incident Reporting Bill, is in the second year of the State and Local Cyber Grants Program, and is executing on a range of new authorities.

As we speak, this week they are hosting the inaugural Planning Summit for the Joint Cyber Defense Collaborative, also known as JCDC, which was established in August 2021. Everyone who I have spoken to about JCDC has told me and our staff of its importance to ensuring productive collaboration between CISA and the private sector. JCDC has enabled rapid information sharing among Government and private-sector partners following Russia's invasion of Ukraine, and it was critical to addressing the Log4j vulnerability. But JCDC has existed for a year-and-a-half without a charter or concrete criteria for membership, all of which are essential for the JCDC to provide enduring value. A number of people have asked me, how do we get into JCDC?

Toward that end, in the coming weeks, I plan to introduce legislation to clarify the activities of the JCDC to improve on its successes and increase its impact. CISA is also in the process of growing its support for operational technology security by continuing implementation of the Cyber Century Program and the Industrial Control Systems Cybersecurity Training Act, which I introduced and was signed into law last year.

I say this to make the point that while CISA pursues the ambitious agenda set by its leadership, it must also effectively execute its existing obligations, including to promote the great training and educational resources provided by CISA that are widely utilized across industries.

Two principles drove Congress' work last year in the subcommittee, an increase to the Federal Government's visibility of malicious cyber activity, and second, pushing resources to entities most vulnerable to cyber attacks.

As we approach oversight this Congress, we must ensure the laws we have enacted deliver concrete security value and preserve the trust we have built with the private sector to advance critical cybersecurity policy and work with CISA to address gaps.

CISA's collaboration with the private sector is essential to both its Federal network and critical infrastructure activities. I am glad we are kicking off this Congress by hearing from some of CISA's most active partners. The testimony from our witnesses today will play a key role in the on-going oversight of CISA moving forward.

With that, again, welcome to the witnesses, and thank you, Mr. Chairman, for convening us.

[The statement of Ranking Member Swalwell follows:]

STATEMENT OF RANKING MEMBER ERIC SWALWELL

MARCH 23, 2022

Good morning. Before I begin, I would like to congratulate my friend from New York, Mr. Garbarino, on becoming Chairman of the subcommittee. I am confident that we will be able to continue this subcommittee's tradition of bipartisanship under your leadership.

The Cybersecurity and Infrastructure Protection Subcommittee has a strong history of productive collaboration and, as a result, has enacted meaningful legislation to provide cybersecurity grants to State and local governments; enhanced cybersecurity education and training programs; strengthen Federal network security; and improved our ability to understand and address threats to operational technology.

In short, this subcommittee's commitment to bipartisanship has increased capacity and reduced risk for both the public and private sectors. I look forward to building on that record with you this Congress, Mr. Chairman.

Since 2019, Congress has nearly doubled CISA's budget and expanded its authorities significantly.

When Congress established CISA 4½ years ago, we envisioned the agency as a sophisticated cybersecurity and infrastructure protection organization. Thanks to bipartisan work on this subcommittee, and the full committee, CISA has matured rapidly, and growing more capable of meeting the challenges of our complex and diverse threat environment.

I am impressed by what CISA has been able to accomplish so far, and will always work to support the agency as it continues to adapt to the cybersecurity needs of our Federal Government, critical infrastructure sector, and private enterprises.

From election security to "Shields Up" campaign, CISA has demonstrated an ability to dynamically surge resources to counter emerging threats and collaborate strategically with the private sector.

Looking ahead, Director Easterly has set ambitious goals to modernize CISA's Federal network security programs, tactically engage with entities whose resilience matters most to our national security and our economy, and drive adoption of secure-by-design and secure-by-default.

I look forward to learning more about how CISA will work with Congress, its partners in the Executive branch, and the private sector to get the buy-in necessary for success.

At the same time, CISA is currently in the process of implementing the cyber incident reporting bill, is on the second year of the State and local cyber grants program, and is executing on a range of new authorities.

As we speak, CISA is hosting the inaugural planning summit for the Joint Cyber Defense Collaborative (JCDC), which was established in August 2021.

Everyone I have spoken to about JCDC has told me about its importance to ensuring productive collaboration between CISA and the private sector. The JCDC enabled rapid information sharing among Government and private-sector partners following Russia's invasion of Ukraine and it was critical to addressing the Log4j vulnerability.

But JCDC has existed for a year-and-a-half without a charter or concrete criteria for membership—all of which are essential for the JCDC to provide enduring value.

Toward that end, in the coming weeks, I plan to introduce legislation to clarify the activities of the JCDC to improve on its successes and increase its impact.

CISA is also in the process of growing its support for operational technology security by continuing implementation of the CyberSentry program and the Industrial Control Systems Cybersecurity Training Act, which I introduced and was signed into law last year.

I say this to make the point that while CISA pursues the ambitious agenda set by its leadership—some of which will require this committee to provide new resources and authorities—it must also effectively execute its existing obligations, including to promote the great training and educational services provided by CISA are widely utilized across industries.

Last Congress, two principles drove the subcommittee's work: First, an increase to the Federal Government's visibility of malicious cyber activity and second, pushing resources to entities most vulnerable to cyber attack. As we approach our oversight this Congress, we must ensure the laws we've enacted deliver concrete security value, preserve the trust we built with the private sector to advance critical cybersecurity policy, and work with CISA to address gaps in capacity.

My district is home to countless technology companies, so I know the value the private sector adds to the Federal Government's cybersecurity efforts.

CISA's collaboration with the private sector is essential to both its Federal network and critical infrastructure activities, and I am glad that we are kicking off the Congress by hearing from some of CISA's most active partners.

The testimony from our witnesses today will play a key role in our on-going oversight of CISA moving forward.

With that, I thank our witnesses for being here today and I look forward to their testimony.

I yield back.

Chairman GARBARINO. Thank you, Ranking Member Swalwell.

I have to say we had a lot of wins on this committee the last 2 years, and I am really looking forward to working with you. A lot of bipartisan wins. So I think we're going to be able to do a lot together.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 23, 2023

Good morning. I want to congratulate Chairman Garbarino and Ranking Member Swalwell on their first hearing as the leaders of the subcommittee.

As Ranking Member Swalwell observed in his opening statement, this subcommittee has an impressive record of bipartisan action.

I commend former Chairwoman Clarke on everything she accomplished last Congress with then-Ranking Member Garbarino—from Cyber Incident Reporting legislation to the State and local cybersecurity grant program.

I sincerely hope that this Congress the Chairman and Ranking Member will continue the strong tradition of seeking common ground to advance critical security policy.

I am proud of the organization CISA has become over the past 4½ years, thanks in large part to the work of this committee.

It has matured into a powerful convener of public and private-sector capacity, with an ability to rapidly shift focus in response to national security dynamics.

Like Ranking Member Swalwell, I am enthusiastic about CISA's potential, but want to strike the right balance between continuing to grow CISA's authorities and making sure that it can execute the missions and objectives Congress has already authorized.

I am also concerned that CISA's important work on cybersecurity may have come at the cost of a diminished focus on its obligations related to the physical security of critical infrastructure.

As our world becomes more interconnected and the line between cyber and physical security continues to blur, we must redouble our efforts on ensuring our critical infrastructure is resilient to all threats.

In that vein, new goals in one of CISA's divisions cannot come at the cost of diminishing capacity in another.

I am interested in learning more about Director Easterly's plans to work with Sector Risk Management Agencies (SRMA) to identify and provide enhanced support to "target-rich, cyber-poor" entities, and I hope that in doing so, CISA considers the overall resilience.

On a related note, I am concerned about a proposed funding cut for the Infrastructure Security Division and how it could impact CISA's ability to effectively serve as an SRMA for 8 critical infrastructure sectors and partner with other SMRAs across government.

Ensuring that CISA has the resources and expertise to fulfill its cross-sector and SMRA obligations is essential to building national resilience, and I will be interested to learn what more this committee can do to grow that capability at CISA.

Finally, this committee passed landmark pieces of cybersecurity legislation last Congress, and now it is our responsibility to ensure that they are implemented as Congress envisioned.

Toward that end, I will be interested to understand how the private-sector witnesses have engaged with CISA as it works to draft the cyber incident reporting rule and how multiple incident reporting requirements could impact incident response.

I am also interested in perspectives on the implementation of the State and local cybersecurity grant program, how it is improving security across the country, and how we can maintain this progress moving forward.

Stakeholder perspectives are critical to this committee's work, and I thank the witnesses for being here today.

I look forward to the testimony, and I yield back the balance of my time.

Chairman GARBARINO. I am pleased to have a distinguished panel of witnesses before us today on this very important topic. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Chairman GARBARINO. Let the record reflect that the witnesses have answered the affirmative.

Thank you. Please be seated.

I would now like to formally introduce our witnesses.

Tina Won Sherman is a director in the Government Accountability's Office Homeland Security and Justice Team. She oversees work on the protection of the Nation's critical infrastructure assets and the security of the U.S. Transportation system. She has also been here quite a few times. We always enjoy having her. In her over 20 years of experience—20 years of tenure at—at GAO, she has done extensive work on CISA's role as the Nation's risk manager and how it balances that role with its responsibilities as a Sector Risk Management Agency for 8 sectors themselves.

Ms. Sherman has also led reviews—has also led reviews on a range of issues including telecommunications, transportation, and defense, and served in GAO's Office of Congressional Relations.

Drew Bagley is the vice president and counsel for privacy and cyber policy at CrowdStrike, where he is responsible for leading CrowdStrike's data protection initiatives, privacy strategy, and global policy engagement. He serves on the Europol Advisory Group on Internet Security, the U.S. Department of State's International Digital Economy and Telecommunication Advisory Committee, and the Domain Name System Abuse and Institute's Advisory Council. Prior to joining CrowdStrike, Mr. Bagley served in the Office of General Counsel at the Federal Bureau of Investigation. He will offer an important perspective on CISA's internal to Federal network program and value insight as a participant in CISA's Joint Cyber Defense Collaborative work.

Heather Hogsett is a senior vice president for technology and risk strategy for BITS at the Bank Policy Institute. In this capacity, Ms. Hogsett represents a heavily-regulated critical infrastructure sector, the financial sector. Before joining BPI, Ms. Hogsett served as staff director for Federal relations at the National Governors Association, where she oversaw NGA's Federal legislative agenda and activities on cybersecurity, homeland security and defense, emergency management, and Veterans Affairs.

Her experience with Government and within the financial sector will help us understand the proper role for regulation and where CISA fits in as a partner to industry.

Finally we have Mr. Marty Edwards, the deputy chief technology officer for operational technology at Tenable. Prior to joining Tenable Mr. Edwards served as the global director of education at the International Society of Automation, as well as the longest-serving director of the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team. He brings a wealth of knowledge about critical infrastructure and technology security and will be able to speak to CISA's efforts to support the community as well as provide a perspective on CISA's JCDC.

I thank all the witnesses for being here today.

I now recognize Ms. Sherman for 5 minutes to summarize her opening statement.

STATEMENT OF TINA SHERMAN, DIRECTOR, CRITICAL INFRASTRUCTURE PROTECTION AND TRANSPORTATION SECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. SHERMAN. Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, I am pleased to be testifying before the subcommittee today on this important topic.

As the subcommittee is keenly aware, cyber and physical attacks on critical infrastructure are on the rise, with hospitals, schools, and electricity substations all having been recent targets. Few of us are immune to the impact of these attacks, which can have debilitating effects on the assets and systems that underpin our daily lives and also have significant financial and sometimes life-threatening implications.

Strengthening the public- and private-sector partnership to address this national security priority, the agency I work for, GAO, has been reviewing Federal efforts to secure critical infrastructure for over 2 decades and has placed protecting cyber critical infrastructure on our high-risk list in 2003.

The Cybersecurity and Infrastructure Security Agency, CISA, within the Department of Homeland Security, serves as the national coordinator for critical infrastructure security. In this role, CISA is responsible for coordinating Federal actions to protect the Nation against risks to this infrastructure, as well as foster collaboration between the public and private sector to share information and respond to incidents. CISA also defines how sector risk management agencies should carry out their responsibilities and ensure that they have the guidance and support needed to effectively engage with owners and operators, those in State, local, Tribal, and territorial governments and other stakeholders.

Sector risk management agencies, or SRMAs, are the Federal departments with subject-matter expertise in one or more of the 16 critical infrastructure sectors and are responsible for leading, facilitating, and supporting critical infrastructure programs and activities in coordination with CISA. They are also uniquely positioned to partner with other government entities in the private sector. The Fiscal Year 2021 National Defense Authorization Act codified their responsibilities and also required GAO to review implementation of these responsibilities every 4 years through 2034.

The administration's recently-issued National Cybersecurity Strategy calls on SRMAs to serve as a key player in ensuring critical infrastructure security and resilience. Yet, several important efforts to strengthen these agencies' ability to effectively support their sectors are under way without completion. This includes the rewrite of Presidential Policy Directive 21 for Critical Infrastructure Security, along with updates to the National Infrastructure Protection Plan and all 16 sector-specific plans.

The report GAO issued last month also found that CISA could assist SRMAs in implementing their responsibilities through additional guidance as well as improved communication and coordination. For example, CISA does not have a standardized approach for agencies to estimate costs or make requests for resources, does not consistently measure the maturity and effectiveness of the agencies, has created but not yet filled liaison positions with them, and does not obtain regular feedback on their partnerships. We recommended CISA establish milestones and time lines to complete these steps, which we believe would help guide and ensure a consistent level of effort across SRMAs to safeguard our Nation and its people.

I want to thank my team in preparing me for this hearing and to the subcommittee for including me today in this important and timely discussion.

[The prepared statement of Ms. Sherman follows:]

PREPARED STATEMENT OF TINA WON SHERMAN

THURSDAY, MARCH 23, 2023

CRITICAL INFRASTRUCTURE PROTECTION.—TIME FRAMES TO COMPLETE CISA EFFORTS WOULD HELP SECTOR RISK MANAGEMENT AGENCIES IMPLEMENT STATUTORY RESPONSIBILITIES

GAO-23-106720

Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee: Thank you for the opportunity to discuss our work on Sector Risk Management Agencies (SRMAs)—departments or agencies, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise to a sector. My testimony today summarizes the findings from our February 2023 report entitled *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*.¹ That report examined new responsibilities for SRMAs and the Department of Homeland Security's role in coordinating SRMA activities.^{2 3}

Events have demonstrated how disruption or destruction of the Nation's critical infrastructure could have debilitating effects. In particular, the 2021 cyber attack on the Colonial Pipeline disrupted the Nation's largest fuel pipeline, and an extreme weather event in Texas caused wide-spread power and water outages.⁴ Such events also illustrate how the Nation's critical infrastructure assets and systems are often interconnected with critical infrastructure in other sectors and the internet, making them more vulnerable to attack. Protecting critical infrastructure is a national security priority because it provides essential functions—such as supplying water, generating energy, and producing food—that underpin American society.

The Cybersecurity and Infrastructure Security Agency Act of 2018 assigned the Cybersecurity and Infrastructure Security Agency (CISA) the responsibility to coordinate a national effort to secure and protect against critical infrastructure risks.⁵ As such, the Secretary of Homeland Security designated the director of CISA as the national coordinator for critical infrastructure security and resilience. CISA provides a variety of cyber and infrastructure security capabilities and services to Federal and non-Federal organizations, including assessments and analysis, capacity building, expertise and guidance, and security operations (e.g., incident response).

At the Federal level, SRMAs are responsible for leading, facilitating, or supporting the security and resilience programs and associated activities within their designated critical infrastructure sector.⁶ The private sector owns and operates the ma-

¹ GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-105806 (Washington, DC: Feb. 7, 2023).

² 6 U.S.C. § 665d.

³ The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 outlined these new SRMA responsibilities.

⁴ In May 2021, we issued a WatchBlog post addressing the Colonial Pipeline attack and the Federal Government and private-sector response. See <https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic>.

⁵ Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2(a), 132 Stat. 4168, 4169 (codified at 6 U.S.C. § 652). The act renamed the Department of Homeland Security's National Protection and Programs Directorate as CISA and outlined CISA's responsibilities.

⁶ 6 U.S.C. § 651(5). Presidential Policy Directive-21 (PPD-21) previously called these agencies Sector-Specific Agencies. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified Sector-Specific Agencies as SRMAs. In 2013, PPD-21 categorized the Nation's critical infrastructure into 16 sectors with at least one Federal agency designated as SRMA for the sector, although the number of sectors and SRMA assignments are subject to review and modification. Those designations are still in effect. See 6 U.S.C. § 652a(b). Additionally, some sectors have subsectors, such as the Education subsector within the Government Facilities sector, with the Department of Education having a lead sector risk management role for the subsector.

jority of critical infrastructure. Therefore, it is vital that the public and private sectors work together to protect assets and systems.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) includes a provision for GAO to report on the effectiveness of SRMAs in carrying out responsibilities set forth in the act. Our February 2023 report and my statement today addresses: (1) How the fiscal year 2021 NDAA changed sector risk management agency responsibilities, and the actions these agencies reported taking to address them; and (2) the extent to which CISA identified and undertook efforts to help sector risk management agencies implement their responsibilities set forth in the fiscal year 2021 NDAA.

To address these objectives, we analyzed the fiscal year 2021 NDAA and relevant policy directives, collected written responses from SRMAs for all 16 sectors using a standardized information collection tool, reviewed other DHS documents, and interviewed CISA officials.⁷ Additional information about our scope and methodology can be found in our February 2023 report. Our work was performed in accordance with generally accepted Government auditing standards.

FISCAL YEAR 2021 NDAA EXPANDED SRMA RESPONSIBILITIES, AND AGENCIES HAVE ACTIONS UNDERWAY TO ADDRESS THEM

The fiscal year 2021 NDAA expanded SRMA responsibilities previously outlined in Presidential Policy Directive–21 (PPD–21) and added risk assessment and emergency preparedness as responsibilities not previously included in the directive for SRMAs.⁸ Specifically, prior to the fiscal year 2021 NDAA, PPD–21 included the following four SRMA responsibilities: (1) Serve as a Federal interface for the prioritization and coordination of sector-specific activities; (2) carry out incident management responsibilities; (3) provide, support, or facilitate technical assistance and consultations for sectors to support risk management activities; and (4) support the Secretary of Homeland Security by sharing information on sector-specific critical infrastructure. The fiscal year 2021 NDAA expanded the sector coordination, incident management, risk management, and information-sharing responsibilities found in PPD–21 by adding specific activities for SRMAs to carry out within these areas. For example, the fiscal year 2021 NDAA requires SRMAs to conduct sector coordination activities, including serving as the day-to-day Federal interface for the prioritization and coordination of sector-specific activities; serving as Federal Government coordinating council chair; and participating in cross-sector coordinating councils, as appropriate.

Expanded responsibilities.—In response to the expanded responsibilities required by the fiscal year 2021 NDAA described above, some SRMAs reported having actions under way to address these responsibilities. SRMA officials for 4 of the 16 critical infrastructure sectors reported adapting activities related to sector coordination, incident management, risk management, or information sharing to address their responsibilities in the act. For example, as SRMA in the health care and public health sector, Department of Health and Human Services officials reported coordinating an effort to analyze the department’s existing cyber authorities to identify and mitigate any gaps, as well as developing a cyber-incident response plan.

Additionally, some SRMA officials also reported that activities they established prior to the enactment of the fiscal year 2021 NDAA already address the responsibilities outlined in the act. For example, SRMA officials from the Department of Energy and the Environmental Protection Agency, representing the energy sector

⁷Three critical infrastructure sectors have co-SRMAs. When co-SRMAs responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include either of them in the sector count and noted the disagreement.

⁸CISA and the other SRMAs also have roles related to emergency preparedness efforts under the National Preparedness Goal and the National Response Framework. PPD–8 directed the Secretary of Homeland Security to develop a national preparedness goal, which defines the core capabilities necessary for emergency response to specific types of incidents. The National Response Framework is a guide to how the Nation responds to disasters and emergencies of all types. The most recent edition of the framework identifies 15 emergency support functions that serve as the Federal Government’s primary coordinating structure for building, sustaining, and delivering response capabilities. According to the framework, existing infrastructure plans and coordination mechanisms such as SRMAs and councils provide strong foundations for strengthening incident response plans and capabilities. As part of the National Infrastructure Protection Plan, the critical infrastructure sectors and SRMAs have developed sector-specific plans. For more information, see Department of Homeland Security, *National Response Framework*, 4th ed. and GAO, *Emergency Preparedness: Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps* [Reissued on December 9, 2015], GAO–15–20 (Washington, DC: Dec. 4, 2014).

and water and wastewater systems sector respectively, reported that they already address the responsibilities outlined in the fiscal year 2021 NDAA.

Finally, as an SRMA for 8 of the 16 sectors, CISA described established activities that address sector coordination, incident management, risk management, and information sharing. Specifically, CISA officials reported that CISA's Stakeholder Engagement Division focuses on developing relationships with industry and Government in CISA's sectors by meeting with Sector Coordinating Councils and issuing advisories and analysis reports to partners.

Added responsibilities.—To address the added risk assessment and emergency preparedness responsibilities required by the fiscal year 2021 NDAA, SRMA officials for 5 of the 16 critical infrastructure sectors described how they plan to take new actions to address the risk assessment responsibilities outlined in the fiscal year 2021 NDAA. For example, as SRMA in the communications sectors, DHS officials reported plans to develop and maintain a communications risk register that includes cybersecurity risks to emergency communications infrastructure. SRMA officials for 15 of the 16 critical infrastructure sectors also stated that they had conducted risk assessment activities prior to their inclusion in the fiscal year 2021 NDAA.⁹

With regard to emergency preparedness responsibilities, SRMA officials for 6 of the 16 critical infrastructure sectors described how they plan to take new actions to address the emergency preparedness responsibilities outlined in the fiscal year 2021 NDAA. For example, as SRMA in the financial services sector, Department of the Treasury officials reported enhancing a tabletop exercise program, developing a functional exercise platform to improve cybersecurity exercises, and refining incident management and crisis communication tool kits. SRMA officials for all 16 critical infrastructure sectors also stated that they had conducted emergency preparedness activities prior to their inclusion in the fiscal year 2021 NDAA.

Implementation challenges.—SRMA officials cited two challenges in implementing their responsibilities: (1) The voluntary nature of private-sector participation in SRMA activities, and (2) limited or no dedicated resources for SRMA duties. According to SRMA officials, these challenges pre-dated the enactment of the fiscal year 2021 NDAA. Additional challenges SRMA officials identified included coordination issues related to inaccurate SRMA point-of-contact lists and government coordinating council and sector coordinating council membership lists, and limited technical cybersecurity expertise. Our past work describing other DHS functions has highlighted the importance of maintaining accurate and up-to-date contact information for the sharing of information.¹⁰

Participation in SRMA critical infrastructure protection efforts is voluntary, which SRMA officials for 11 critical infrastructure sectors reported as a challenge to conducting their responsibilities. For example, they reported that this affected their ability to stay apprised of issues in the sector and to collect information. SRMA officials reported that these challenges existed prior to the fiscal year 2021 NDAA and they generally expected them to continue.

SRMA officials also stated that they face challenges because they have limited or no dedicated resources to implement their responsibilities. SRMA officials for 13 of the 16 sectors, including those with and without dedicated resources for SRMA activities, stated that they planned to request additional resources to help them implement their fiscal year 2021 NDAA responsibilities.

CISA HAS IDENTIFIED AND UNDERTAKEN EFFORTS TO HELP SRMAS, BUT DOES NOT HAVE MILESTONES AND TIME LINES TO COMPLETE THEM

CISA has identified and undertaken some efforts that could help SRMAs implement their fiscal year 2021 NDAA responsibilities. In November 2021, CISA reported on several on-going and planned efforts to help SRMAs implement these responsibilities and to clarify Federal roles and responsibilities for cybersecurity and

⁹As the co-SRMAs in the government facilities sector, both DHS Federal Protective Service and General Services Administration officials did not describe conducting prior risk assessment activities. They stated that prior to the fiscal year 2021 NDAA, non-CISA co-SRMAs were not required to conduct risk assessments for their sector and did not have the authority to require their Federal and non-Federal partners to provide responses or submit information for such assessments.

¹⁰See GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, DC: Feb. 1, 2017). SRMA officials said they expected CISA to possibly address this challenge if it established consistent communication mechanisms in response to the fiscal year 2021 NDAA. According to CISA officials, CISA has efforts under way to address issues related to inaccurate points of contact lists.

infrastructure security actions across the Federal Government.¹¹ In addition, CISA officials described various efforts to help SRMAs implement their fiscal year 2021 NDAA responsibilities, including:

Define maturity and effectiveness metrics.—CISA officials told us in October 2022 they expect to develop a methodology and metrics to measure the maturity and effectiveness of SRMAs in implementing responsibilities outlined in the fiscal year 2021 NDAA. For example, in its November 2021 report, CISA recommended that the Federal Senior Leadership Council conduct a sector-by-sector assessment of SRMA partnership participation.¹² CISA officials told us in March 2022 that these efforts could include both standardized metrics to measure effectiveness across all sectors, and sector-specific metrics.

Develop standardized budget guidance.—In its November 2021 report, CISA officials identified a need to develop a baseline cost estimation tool for SRMAs.¹³ According to the report, this tool would provide SRMAs a baseline estimate of resource needs, and could be tailored to each SRMA. CISA also proposed implementing a consistent resource request process across the SRMAs, which could help address the challenges associated with their resource limitations, as previously discussed. According to CISA officials, this budget formulation tool would allow SRMAs to request sufficient resources to implement their fiscal year 2021 NDAA responsibilities.

Create sector liaison positions.—In August 2022, CISA officials told us they created liaison positions focused on fostering CISA’s relationship with SRMAs. According to CISA officials, these liaisons will help CISA respond to the responsibilities outlined in the fiscal year 2021 NDAA by enhancing communication and coordination with SRMAs, triaging information in response to incidents, and responding to requests for information.

Enhance the Federal Senior Leadership Council.—The Federal Senior Leadership Council provides a forum for coordination and communication among agencies with critical infrastructure responsibilities, including SRMAs. The council coordinates implementation of SRMA responsibilities as well as other initiatives related to protecting critical infrastructure. According to CISA officials, the Federal Senior Leadership Council is intended to be one of the primary ways CISA will coordinate actions to implement the fiscal year 2021 NDAA across the Federal Government.

Develop a standardized feedback process.—CISA officials told us in June 2022 that they are developing a process to conduct standardized surveys of critical infrastructure stakeholders and plan to use the results to conduct assessments. They said surveys allow them to measure the outcome of sector efforts by collecting information from partners on their intent to take action based on the information, tools, or capabilities provided to them, which they said is important due to the voluntary nature of sector partnerships.

Update the 2013 National Plan and sector-specific plans.—CISA officials told us in March 2022 that the updated National Infrastructure Protection Plan (National Plan) will clarify SRMA responsibilities in response to the fiscal year 2021 NDAA. The National Plan is a key guidance document that provides the overarching national approach for critical infrastructure protection. CISA officials stated that the National Plan will be the “cornerstone” to guide SRMAs as they implement their responsibilities. According to CISA officials, the updated National Plan will: (1) Include a revised approach to critical infrastructure protection, (2) provide information on SRMA responsibilities set forth in the fiscal year 2021 NDAA, (3) clarify Federal roles and responsibilities for sector risk management, and (4) outline how Government and industry should coordinate to identify and mitigate threats to critical infrastructure. The 2013 update of the National Plan responded to new policy in PPD–21, including an explicit provision that DHS update the National Plan to implement the new directive. CISA officials told us they would not make further updates to the National Plan until the review of PPD–21 is completed.

Further, CISA officials stated in October 2022 they plan to provide additional guidance to SRMAs on how they should update their sector-specific plans. CISA officials told us that the updated sector-specific plans should describe how the sector will implement the updated National Plan, along with efforts tailored to the sector’s unique characteristics. CISA officials told us they expected to issue an updated sec-

¹¹In response to the fiscal year 2021 NDAA, CISA reviewed the framework for securing critical infrastructure and submitted a report to the President and Congressional committees that made recommendations. According to CISA officials, they met with and collected feedback from SRMAs while preparing this report. According to CISA officials in January 2023, the President officially approved the recommendations in the 9002(b) report, and initiated the process to re-write PPD–21. CISA, *Fiscal Year 2021 National Defense Authorization Act: Section 9002(b) Report*, (Nov. 12, 2021).

¹²CISA, Section 9002(b) Report, 42.

¹³CISA, Section 9002(b) Report, 5.

tor-specific plan template 3 to 6 months after the release of the updated National Plan for SRMAs to use in collaboration with their sector partners. Further, they told us that the sector-specific plans would likely take 1 year to develop.

Although CISA has identified and started a number of efforts to help SRMAs implement their fiscal year 2021 NDAA responsibilities, CISA does not have milestones and time lines to complete its efforts. According to selected characteristics from GAO's *Key Questions to Assess Agency Reform Efforts*, Government reform efforts should have milestones and time lines to track implementation progress, which can also provide transparency about the progress of reforms.¹⁴

CISA officials said they had not established milestones and time lines to complete CISA's efforts because the agency has prioritized defining its own role as national coordinator. For example, as of October 2022, CISA officials said they were in the process of developing ways to implement CISA's new authorities under the fiscal year 2021 NDAA, which requires SRMAs to carry out their responsibilities in coordination with the CISA director and consistent with DHS strategic guidance.

We recognize that CISA's efforts to address its fiscal year 2021 NDAA responsibilities are linked to its efforts to mature in its role as national coordinator. However, SRMA officials for all 16 critical infrastructure sectors reported that CISA had not yet provided guidance to help the agencies implement their fiscal year 2021 NDAA responsibilities. Establishing milestones and time lines, and updating them when necessary, to accomplish its efforts to support SRMAs, would help ensure CISA completes them in a timely manner.

We recommended, and DHS concurred, that the director of CISA establish milestones and time lines for its efforts to provide guidance and improve coordination and information sharing that would help SRMAs implement their fiscal year 2021 NDAA responsibilities, and ensure the milestones and time lines are updated through completion.¹⁵ As of March 2023, the agency has not yet implemented the recommendation. CISA officials stated that the administration's Homeland and Critical Infrastructure Resilience Interagency Policy Committee is in the process of updating PPD-21. Once it is completed, CISA will work to establish the milestones and time lines needed to develop guidance on improving coordination and information sharing.

However, as of March 2023, CISA had not developed milestones and time lines to complete its efforts. CISA officials stated that they could not provide a specific time line for issuing the updated National Plan until the administration completes a review of PPD-21. CISA officials stated that the Federal Senior Leadership Council has started the Sector Analysis Working Group, which is an interagency consensus-based group that will recommend a new sector designation structure and corresponding SRMA designations. CISA officials reiterated that they plan to issue guidance on improving coordination and information sharing.

Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

Chairman GARBARINO. Thank you, Ms. Sherman.

I now recognize Mr. Bagley for 5 minutes to summarize his opening statement.

STATEMENT OF DREW BAGLEY, VICE PRESIDENT AND COUNSEL, PRIVACY AND CYBER POLICY, CROWDSTRIKE

Mr. BAGLEY. Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, thank you for the opportunity to testify.

Today, nation-states, criminal enterprises, and hacktivist groups use sophisticated means to exploit unsophisticated vulnerabilities

¹⁴ GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, DC: June 13, 2018).

¹⁵ GAO-23-105806. GAO has a large body of work examining aspects of critical infrastructure protection and has made over 80 recommendations to SRMAs relevant to the responsibilities outlined in the fiscal year 2021 NDAA. These recommendations involved sector risk management and assessing sector risk, sector coordination and facilitating the sharing of information regarding physical security and cybersecurity threats, and incident management and contributing to emergency preparedness efforts. As of December 2022, agencies had yet to implement 58 of these recommendations. For more information on these recommendations, see appendix II in GAO-23-105806.

to conduct espionage, breach privacy, and disrupt infrastructure. This is why it's so important to continually evolve in how we prevent, detect, and respond to cyber attacks.

At CrowdStrike we have a unique vantage point on cybersecurity threats and the innovation necessary to prevent them. We work with CISA on key programs and initiatives. We help CISA and other government agencies. We have been involved with JCDC since its inception. We also consume CISA's advisories and are a key technology provider for its stakeholder groups like Critical Infrastructure Entities.

This hearing is timely for several reasons. CISA has matured within a number of operational and planning functions. Major transitions are taking place in Federal cybersecurity, with an emphasis on zero trust adoption. Geopolitical conditions stemming from Russia's war in Ukraine and heightened competition with China have worsened the threat environment. With respect to information sharing and collaboration, the formation of JCDC in August 2021 was a key development. Since then, JCDC has created a platform for key players in industry and Government to voluntarily work toward common goals.

While we defer to CISA leadership to describe key outcomes, CrowdStrike values best time and expertise in the JCDC community, and we look forward to continued shared efforts to promote better cybersecurity.

As JCDC matures, we believe the effort can continue to improve. First, consider approaches that stratify or segment membership to maintain trust. Second, strengthen administrative customer relationship management practices. To their credit, JCDC leadership and staff have been proactive about seeking feedback from participants. Like any start-up, we anticipate continued iteration as the group matures into its full potential.

Importantly, cybersecurity outcomes vary substantially across sectors. I've provided a brief overview in my written remarks.

There remains a gap in cybersecurity performance between the haves and the have-nots, which threat actors continue to exploit and which CISA cannot solve alone. To this end, we are pleased to see reference in the new National Cybersecurity Strategy to shifting the burden for cybersecurity to those best positioned to mitigate risks.

As a community, we should no longer tolerate certain software vendors externalizing the costs of, or worse, nakedly monetizing insecure software. While this policy concept must be made more concrete, a reasonable first step is ensuring that we're not rewarding vendors that cause harm. The Government can lead by example, leveraging its own procurement power. This is clearly a productive area for continued Congressional oversight.

I'd like to offer a few key recommendations.

First, the entire field must become more responsive in adapting to lessons learned. Unfortunately, cyber attacks with the potential for systemic implications take place with increasing regularity. Key lessons of recent breaches include: Utilize managed security services, adopt cloud-based solutions, and employ zero trust. We must approach regulation deliberately and harmonize to the greatest extent possible. We must use care in advancing new requirements,

use formal, open commenting periods, and use principles-based requirements rather than compliance-based approaches. And critically, Federal agencies, particularly regulators, must walk the walk on cybersecurity.

Third, as a community, we must focus more attention on national incident response capacity. JCDC should continue developing community response plans, and CISA should incorporate JCDC contributions and forthcoming revisions to the National Cyber Incident Response Plan. If the Chinese threat actors responsible for the Microsoft Exchange hacking campaign in 2021 had deployed ransomware at scale, large segments of the American economy could have been paralyzed. A CISA-administered program to retain outside providers for emergency incident response had entities of systemic importance.

Last, we must empower defenders with cutting-edge cyber defense capabilities. Too often, defenders are hobbled with ineffective technologies. Those with leading solutions are energized with radically improved morale. Our idea, one idea, is to consider using tax mechanisms to speed adoption of key technologies for small businesses.

Ultimately, CISA and its stakeholders must continue working together collectively to prevent, detect, and respond to cyber attacks.

Thank you for the opportunity to appear here today, and I look forward to your questions.

[The prepared statement of Mr. Bagley follows:]

PREPARED STATEMENT OF DREW BAGLEY

MARCH 23, 2023

Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, thank you for the opportunity to testify today. We are at a pivotal moment in the cybersecurity challenges posed to our country. Today, nation-states, criminal enterprises, and hacktivist groups alike can leverage sophisticated means to exploit unsophisticated vulnerabilities to conduct espionage, breach privacy, and wreak havoc on critical infrastructure, government systems, and businesses throughout the country. We are at a point where the stakes of defensive stagnation pose increasing risks in the face of threat actors' innovation. This is why it's so important to continually evolve in how we prevent, detect, and respond to cyber attacks.

Throughout my career, I have seen first-hand the challenges and opportunities of improving American cybersecurity from my work in the private sector, Government, and academia. For nearly a decade, at CrowdStrike, a leading cybersecurity company, I have had a front-row seat to cybersecurity innovation while building our privacy and public policy programs and advising customers around the globe. Prior to that I worked at the intersection of law and technology in the FBI's Office of the General Counsel. I previously taught at universities in the United States and Europe, and currently serve as an adjunct professor in American University's cybersecurity policy program. I have been asked to speak here today from a stakeholder perspective. Accordingly, my testimony is informed not only from my experience but also by my continued engagement with Government agencies through formal and informal advisory roles, including as a member of CISA's Joint Cyber Defense Collaborative (JCDC).

At CrowdStrike, we have a unique vantage point on cybersecurity threats and the innovation necessary to stop them. We not only protect 15 of the largest 20 banks in the United States but also provide our cybersecurity technology and services to thousands of small- and medium-sized businesses. This means that it is not only possible for small organizations to leverage the same cybersecurity technologies as complex multinational enterprises but that it is becoming more common.

Increasingly, fundamental aspects of cybersecurity program design are applicable everywhere—including for the on-going transformation in U.S. Federal cybersecurity.

CrowdStrike works with CISA in a variety of ways across key programs and activities. We were one of the original plank holders of JCDC and remain active members to this day. We provide cyber threat intelligence and cybersecurity technology offerings to CISA that help it defend not only its own networks but those of some other Government departments and agencies as well. Last, we are a consumer of CISA's advisories and a key technology provider for its other stakeholder groups, like critical infrastructure entities.

KEY DEVELOPMENTS

This hearing is timely for three key reasons. First, over the past couple of years CISA has reached its stride across a number of operational and planning functions (described in more detail below). Second, major transitions are taking place in Federal cybersecurity overall, with an emphasis on security program modernization and Zero Trust Architecture. CISA is a key actor and implementer in these areas. Third, geopolitical conditions have yielded a worsening cyber threat environment overall. Russia's war in Ukraine and heightened competition with China are just two of several active examples where risks are mounting.¹

Now is an impactful time to review the state of cybersecurity overall and evaluate CISA's considerable progress and contributions.² As DHS and CISA leadership and Members of this committee prepare jointly to realize the vision of CISA 2025,³ we can identify fruitful areas for continued development, alignment, and investment, where appropriate.

THE STATE OF CYBERSECURITY

Cybersecurity outcomes vary substantially across different sectors. Different sectors face different threats, have different constraints and capacities, and have different tolerances to risk or disruptions. To this end, I'd like to survey the state of cybersecurity across a few key CISA partner segments.

Federal Civilian Executive branch (FCEB).—Going back 20 years, Federal Government agencies often had considerable cybersecurity strengths relative to their private-sector counterparts. However, as time went on and cyber attacks increasingly occurred without the use of malware, parts of the private sector met and exceeded FCEB cybersecurity performance by adjusting to new realities. In some instances, Government IT standards and controls failed to evolve at the rapid pace of innovation within the commercial IT and cybersecurity space. Large Federal Cybersecurity programs (e.g., National Cybersecurity Protection System (NCPS) or EINSTEIN, and the Continuous Diagnostics and Mitigation Program (CDM)) set ambitious goals aimed to standardize and scale approaches to Government cybersecurity, but even with considerable investment over the years, that aim remains unmet.

Over the past several years, however, the Federal cybersecurity community has made some significant strides. Recent developments are trending positively with the embrace of key cybersecurity concepts like centralized visibility of IT infrastructure to detect and respond to incidents. Significantly, E.O. 14028 on *Improving the Nation's Cybersecurity*⁴ mandated the use across the FCEB of key best practices, like enhanced logging, as well as now-baseline technical solutions like Endpoint Detection and Response (EDR). The release of the Office of Management and Budget's *Federal Zero Trust Strategy*⁵ in January 2022 was another key decision enforcing the use of sound approaches, like increased adoption of cloud-based technologies, credential management practices,⁶ and defensible IT architectures. Even as implementation continues, these initial efforts are yielding positive results.

CISA plays an essential role in strengthening FCEB cybersecurity. As recently as a couple of years ago, CISA had just a few programs (e.g., NCPS, CDM, Trusted

¹ See Adam Meyers, *Testimony on Securing Critical Infrastructure Against Russian Cyber Threats*, House Homeland Security Committee (March 30, 2022) (How Russia-nexus adversaries use cyber attacks and recommendations for U.S. readiness), <https://docs.house.gov/meetings/HM/HM00/20220405/114553/HHRG-117-HM00-WState-MeyersA-20220405.pdf>.

² See *CISA Strategic Plan 2023–2025*, CISA (September 2022), https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf.

³ See *CISA 2025 Overview*, Committee on Homeland Security, House of Representatives (October 13, 2022), <https://homeland.house.gov/cisa-2025/>.

⁴ See *Executive Order on Improving the Nation's Cybersecurity*, The White House (May 12, 2021), <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

⁵ See *M-22-09 Memorandum for the Heads of Executive Departments and Agencies*, Executive Office of the President, Office of Management and Budget (January 26, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>.

⁶ See *7 TYPES OF IDENTITY-BASED ATTACKS*, CrowdStrike (January 10, 2023), <https://www.crowdstrike.com/cybersecurity-101/identity-security/identity-based-attacks/>.

Internet Connections (TIC)) and a few authorities (e.g., Emergency Directives, Binding Operational Directives⁷) to meet this mandate. But the Solarium Commission's recommendation as enacted by Congress to formally elevate CISA to become the operational CISO of the FCEB, including by providing Government-wide, proactive cyber threat hunting capabilities, considerably strengthened CISA's tool kit. Further, actions taken by CISA to implement E.O. 14028, particularly with regard to the EDR program, are helping to realize this vision.

The stakes are high. The FCEB continues to be a key target of threat actors that seek to do harm to the United States. Friends and allies continue to look to the U.S. Government as a model for how to organize their own Government cybersecurity efforts. Importantly, the Government must lead by example on cybersecurity. CISA's efforts to strengthen security across the other entities (e.g., critical infrastructure or State and local governments) will lack credibility if the FCEB is poorly secured.

Large Enterprises.—On balance, the most sophisticated large enterprises in the United States have seen stronger cybersecurity outcomes in recent years, even as threats evolve and multiply. Over the past year, we've observed an increase in vulnerability reuse and increased reliance on access brokers to facilitate initial infiltration into target organizations. We've also witnessed increased targeting of—and mounting costs from—breaches of legacy infrastructure.⁸ Supply chain attacks, which can be targeted but also used to breach many dependent organizations in a single campaign, remain a key concern.

Some large commercial enterprises have greater flexibility and stronger security budgets than other entities, and thus serve as an important proving ground for new technologies, practices, and architectures. From this, recent innovations like Zero Trust and cloud-native EDR have become today's cybersecurity essentials. In the near future, we should expect more attention from other sectors on emerging enterprise security concepts like Extended Detection and Response (XDR), identity threat protection,⁹ as well as continued adoption of managed security services (discussed in more detail below).

Small- and Medium-sized Businesses (SMB).—These entities include everything from the family-owned corner store in each of our communities to start-ups creating new technologies that could change the world. These companies operate off of very different templates but nevertheless share two key features. First, resources are scarce. Second, a multi-day business disruption might well destroy the company. Resource scarcity means there's no place for complex cyber defenses, and few if any 'spare cycles' for participation in demanding or time-consuming information sharing initiatives. Sensitivity to disruption means these organizations are particularly vulnerable to ransomware and "lock-and-leak" attacks.

Among the most positive developments in this space in recent years is the growing affordability and accessibility of managed security services, as well as managed threat hunting services. Organizations increasingly look to professional providers to manage the overwhelming majority of defense actions—under tight service level agreements—24 hours a day, 7 days a week, 365 days a year.

State, Local, Tribal, and Territorial (SLTT) Entities.—Over the past few years, SLTT entities have faced a withering threat environment, most notably from criminal ransomware actors. Materially all SLTT entities face budgetary and personnel constraints, and rely upon critical legacy applications and IT infrastructure. Nevertheless, over that same time horizon, cybersecurity outcomes within the sector have diverged significantly. As Members of this committee know well, many SLTT organizations faced severe incidents and events, and in some instances citizens suffered disruption of key services.

Counterintuitively perhaps, over this time frame the most forward-leaning States and cities were meaningfully further ahead than most of the FCEB in centralizing and modernizing defenses. This was generally achieved through a key service provider—typically a Department of Technology—implementing and managing transformative technologies like EDR and other important security concepts and practices. In addition to leveraging a centralized provider, these States often had no inflexible security program that acted as a barrier to experimentation and technology

⁷See *Cybersecurity Directives*, Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/news-events/directives>.

⁸See *2023 Global Threat Report*, CrowdStrike (2023). <https://www.crowdstrike.com/global-threat-report/>.

⁹See Andrew Harris, *CrowdStrike Falcon Identity Threat Protection Added to GovCloud-1 to Help Meet Government Mandates for Identity Security and Zero Trust*, CrowdStrike (June 1, 2022), <https://www.crowdstrike.com/blog/how-falcon-identity-threat-protection-helps-meet-identity-security-government-mandates/>.

adoption. In addition, community-oriented support efforts, such as those led by the Center for Internet Security, have been a key part of stronger defenses.

The State and Local Cybersecurity Improvement Act, which passed into law in the Infrastructure Investment and Jobs Act of 2021 was a positive step in ensuring State and local governments have the funding needed to centralize and modernize cyber defenses. We appreciate former subcommittee Chairwoman Clarke, Chairman Garbarino, and other Members of the committee for their leadership on this important issue.

Critical Infrastructure.—Most critical infrastructure owners and operators face the same set of hardships outlined above: Severe threat environment, personnel and budget constraints, and legacy applications and IT infrastructure. But they have the added challenges of complex Operational Technology (OT) that in some instances is obsolete and/or esoteric. In addition to these conditions there is increased interest from policy makers in regulatory measures designed to enhance cybersecurity.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law in March 2022, which strengthens reporting obligations for critical infrastructure players, is the most meaningful step to date.¹⁰ CIRCIA's authors—notably Members and key staff on this Committee—recognized these risks and included two key provisions. The first is a Cyber Incident Reporting Harmonization Council that should reconcile duplicative or conflicting regulations. The second is a generous time line for CISA to articulate particulars (like thresholds) in a clear and straightforward manner. CISA has solicited stakeholder feedback to those ends, to which we, and many others in the community, were happy to contribute ideas and suggestions.¹¹

International.—Although somewhat beyond the scope of this hearing, we should take a moment to reflect on international cybersecurity. U.S. allies' public sector organizations, laws, and policy debates tend to reflect somewhat developments here in Washington. This is an incredible leadership opportunity. Efforts like the International Counter Ransomware Initiative¹² serve as a good example for how to use this influence to strengthen the cybersecurity ecosystem globally. Across relevant areas of law and policy, we should embrace interoperable approaches that simplify collaboration between governments, NGO's, and industry players. In addition, the United States should be receptive to areas where other countries have identified helpful policies. These include, for example, policies that support the start-up ecosystem, and national privacy laws that simplify data protection and the cross-border data flows integral for modern cybersecurity.¹³

PUBLIC-PRIVATE COLLABORATION

The Joint Cyber Defense Collaborative (JCDC).—Information sharing in the cybersecurity space is a complex topic and long-standing policy priority. For two decades, various information-sharing efforts—narrow and broad; informal, quasi-official, and official; ad hoc and enduring—have arisen from a desire within the cybersecurity community to do more. While the Cybersecurity Act of 2015 sought to address this problem head-on,¹⁴ structural impediments to comprehensive sharing and collaboration remain.¹⁵ And as a practical matter, we are unlikely to identify a “silver bullet” solution to a problem with this many complexities. However, the formation of JCDC in August 2021 was a key development in promoting sharing and collaboration. In the time since, JCDC has created a platform for key players in industry and Government to voluntarily work toward common goals.

¹⁰ See *Public Law 117–103, Division Y, Cyber Incident Reporting for Critical Infrastructure Act—Consolidated Appropriations Act*, 117th Congress (March 15, 2022). <https://www.congress.gov/bills/117/congress/house-bill/2471/text>.

¹¹ See *CrowdStrike Response to RFI on Cyber Incident Reporting for Critical Infrastructure Act* (November 14, 2022), <https://www.crowdstrike.com/wp-content/uploads/2023/02/RFI-Incident-Reporting-for-Critical-Infrastructure-Act-of-2022.pdf>.

¹² See *International Counter Ransomware Initiative 2022 Joint Statement*, The White House (November 1, 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/>.

¹³ See Drew Bagley, *Data Protection Day 2023: Misaligned Policy Priorities Complicate Data Protection Compliance*, CrowdStrike (January 27, 2023), <https://www.crowdstrike.com/blog/data-protection-day-2023-misaligned-policy-priorities-complicate-data-protection-compliance>.

¹⁴ See *Public Law 113–113, Division N, Cybersecurity Act of 2015*, 114th Congress (December 18, 2015), <https://www.congress.gov/bills/114/congress/house-bill/2029/text>.

¹⁵ See George Kurtz, *Questions for the Record—Hearing on the Hack of U.S. Networks by a Foreign Adversary*, Senate Select Committee on Intelligence (February 23, 2021) (How the private sector has promoted practical information sharing), <https://www.intelligence.senate.gov/sites/default/files/documents/qfr-gkurtz-022321.pdf>.

While we would generally defer to CISA Leadership to describe key outcomes, we can say that CrowdStrike values the partnership opportunity. We continue to invest time and expertise in the JCDC community, and we look forward to continued, shared efforts to promote better cybersecurity.

As JCDC matures, we believe the effort can continue to improve. Two suggestions:

- *Consider approaches that stratify or segment membership to maintain trust.*—As the group expands, JCDC leadership should account for the possibility that some members may become less willing to share details about sensitive issues. JCDC has addressed this concern by maintaining clear direct channels of communication with participants, and creating ad hoc working groups with a subset of members. These are important measures, but additional subgroup governance may help promote more active and applied sharing. Articulating long-term aims for membership composition may also be of value.
- *Strengthen administrative Customer Relationship Management (CRM) practices.*—This would ensure consistent notification of participant stakeholders about upcoming opportunities, events, engagements, etc. A designated partner “JCDC relationship owner” should be able to flexibly add or remove corporate participants from various JCDC workstreams to facilitate participation from particular personas (e.g. according to function, experience, protocol, etc.).

To their credit, JCDC leadership and staff have been proactive about seeking feedback from participants. We have provided suggestions along these lines to them directly and believe it is taken seriously. Like any “start-up,” we anticipate continued iteration as the group matures into its full potential.

Ecosystem.—CISA contributes to the cybersecurity ecosystem in a variety of other ways. Support to key partners in the SLTT community; advice and tools for enhancing infrastructure, Industrial Control Systems (ICS), and OT security; alerts and notifications for IT security, particularly around emerging vulnerabilities; and leadership on workforce topics all contribute to better cybersecurity outcomes. Each of these issue areas is complex and requires specific expertise. CISA’s contributions in this realm continue to mature and become more valuable over time.

There remains a gap in cybersecurity performance between the “haves” and the “have-nots,” which threat actors continue to exploit and which CISA cannot solve alone. To this end, we are pleased to see reference in the new National Cybersecurity Strategy to shifting the burden for cybersecurity to those best positioned to mitigate risks. This includes, where appropriate, holding platform providers accountable for the security of their products.¹⁶ As a community, we should no longer tolerate certain software vendors externalizing the costs of—or worse, nakedly monetizing—insecure software applications.¹⁷ While this policy concept must be made more concrete, a reasonable first step is ensuring that we’re not rewarding vendors that cause harm. To this end, the Government can lead by example by using its own procurement power to shape market dynamics. This is clearly a productive area for continued Congressional oversight.

RECOMMENDATIONS

1. The entire field must become more responsive in adapting to lessons learned. Unfortunately, cyber attacks with the potential for systemic implications take place with increasing regularity. However, organizations are uneven in adopting key lessons, from new security controls and mitigations to more secure architectures. From our vantage point, key lessons of recent breaches include:

- Use managed security services where practical to augment internal security staff and attain responsive and comprehensive security coverage.
- Adopt cloud-based IT systems and where possible, leverage cloud-based security tools to achieve scalability and speed.
- Employ Zero Trust Architecture, with emphasis on identity threat protection, to defend an increasingly diffuse IT infrastructure and radically reduce lateral movement during breach attempts, bringing us closer to cyber and mission resiliency.

2. We must approach regulation deliberately and harmonize to the greatest extent possible. Even as CIRCIA advances through rule making, independent regulators

¹⁶ See *National Cybersecurity Strategy*, page 20. The White House (March 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

¹⁷ For one example of a persistent security issue, see George Kurtz, *Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence (February 23, 2021) (Extended discussion on emerging cybersecurity controls and practices), <https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf> p. 5.

are pursuing new obligations¹⁸ and the National Cybersecurity Strategy fore-shadows additional actions at the sector-level.¹⁹ Each of these measures is well-intended, but taking place simultaneously and with different stakeholders. At best, they will close long-standing gaps and strengthen national resilience.

At worst, they risk yielding burdensome, distracting, and costly compliance obligations without additional security gains. Optimizing for the former is among the most important challenges the cybersecurity policy community faces at this time. Our hope is that continued collaboration between potential regulators and/or muscular harmonization efforts will help avert worse outcomes. The best advice we can offer is:

- Be deliberate about advancing new requirements;
- Provide formal commenting periods for stakeholders to contribute views;
- Use principles-based requirements rather than burdensome and inflexible compliance-based approaches;
- Include provisions to regularly review and if necessary modify, update, or deprecate requirements or controls based on developments in the threat environment or technology ecosystem;
- The DHS Cyber Incident Reporting Council established under CIRCIA should operate with vigor, and work to clearly identify and reduce duplicative reporting; and
- Set the goal of all Federal agencies showcasing cybersecurity best practices with a particular emphasis on those that regulate cybersecurity “walking the walk.”

3. As a community, we should focus more attention on national incident response capacity. JCDC should continue coordinating and developing community response plans and CISA should weigh potential JCDC contributions for the purposes of forthcoming revisions to the National Cyber Incident Response Plan (NCIRP).²⁰ If the Russian threat actors responsible for the major supply chain attack or the Chinese threat actors responsible for the Microsoft Exchange hacking campaign in 2021 had deployed ransomware or pseudo-ransomware at scale, large segments of the American economy would have been paralyzed. A CISA-administered program to retain outside providers for emergency incident response to attacks at entities of systemic importance could be of tremendous value in a future contingency.²¹ This could mitigate crippling impacts and ensure CISA had the ability to orchestrate response activities and maintain insight into findings in real time.

4. We must empower defenders with cutting-edge cyber-defense capabilities. Defenders with leading solutions are energized with radically improved morale. Too often, defenders are hobbled with inefficient and ineffective technologies. When these inevitably fail, they begin to feel like little more than a punching bag for adversaries, and that their best efforts are for naught. But when people are empowered, they can see their impact each day and can remain focused on the importance of their mission. To the extent that this committee can promote access to better tools, that will absolutely strengthen cybersecurity outcomes. For the FCEB, this means the full adoption of technologies mandated in E.O. 14028 like EDR and, ultimately, better access to managed security services to augment staff. To highlight another opportunity, we believe it’s time to have a more serious conversation as a community about using tax mechanisms to speed adoption of key technologies in the SMB space.²²

5. The community must attract and retain top cybersecurity talent. The level of talent in our field—across industry and Government—is deeply inspiring. Based on our experience, the central motivator for people in the field is a sense of mission. A key challenge we have as a community is overburdened staff leading to burnout, a concern that underpins some of my previous comments on leveraging managed services and mitigating time-consuming and ineffective compliance obligations. Fur-

¹⁸ See *TSA issues new cybersecurity requirements for airport and aircraft operators*, Transportation Security Administration (March 7, 2023), <https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft>.

¹⁹ Even prior to CIRCIA and recent efforts, data breach victims commonly faced more than 50 different reporting requirements in the United States alone, with additional international obligations in many cases.

²⁰ See *National Cybersecurity Strategy*, page 12. The White House (March 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

²¹ See Robert Sheldon, *Testimony on Protecting American Innovation*, Senate Select Committee on Intelligence (September 21, 2022), <https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf>.

²² See Robert Sheldon, *Testimony on Protecting American Innovation*, Senate Select Committee on Intelligence (September 21, 2022), <https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf>.

ther, aligning roles to each organization's key missions—and in the case of Government authorities—helps people recognize the uniqueness of their contributions. A second challenge is expanding recruitment efforts to grow additional talent. To this end, I was pleased to announce during my participation at a White House Summit last month that CrowdStrike would soon launch an emerging leaders program focused on diverse candidates.²³ We must continue efforts to fuel the cybersecurity talent pipeline.

CISA's evolution is the culmination of non-partisan efforts under four consecutive Presidential administrations, and CISA has received numerous new key authorities and increases in funding over the past several years. Ultimately, in each passing year it is important to ask whether the U.S. Government is better able to prevent, detect, and respond to cyber attacks. Accordingly, I am pleased to see this committee has identified key oversight areas in the CISA 2025 initiative to put CISA on track to fully implement those authorities and fulfill the mission Congress has entrusted it with. CrowdStrike looks forward to continuing and building upon its trusted relationship with CISA, and playing our part in empowering it to effectively carry out its mission.

Thank you for the opportunity to appear in front of you today, and I look forward to your questions.

Chairman GARBARINO. Thank you, Mr. Bagley.

I now recognize Ms. Hogsett for 5 minutes to summarize your opening statement.

STATEMENT OF HEATHER HOGSETT, SENIOR VICE PRESIDENT, TECHNOLOGY AND RISK MANAGEMENT, BANK POLICY INSTITUTE

Ms. HOGSETT. Chairman Garbarino, Ranking Member Swalwell, honorable Members of the subcommittee, thank you for inviting me to testify.

I'm Heather Hogsett, senior vice president of technology and risk strategy for BITS, which is the technology policy division of the Bank Policy Institute.

BPI is a nonparty research and advocacy organization representing the Nation's leading banks. Through our technology division, we work with our members on cyber risk management and critical infrastructure protection, as well as fraud reduction, regulation, and innovation. We greatly appreciate this committee's leadership and the opportunity to provide perspective on the role of CISA in defending our Nation.

Financial institutions are increasingly under cyber attack by foreign nations and criminal groups seeking to undermine the functioning of the U.S. economy. Our sector takes these risks seriously and has strong relationships with the Treasury Department, our Sector Risk Management Agency, as well as CISA, the National Cyber Director's Office, the FBI, the Secret Service, and also our regulators.

Since being established, CISA has played a vital coordination role during the COVID-19 pandemic to keep critical infrastructure up and running. It also played a key role in the response to Solar Winds, Log4j, ransomware attacks, and on-going geopolitical tensions with Russia. Throughout these efforts, CISA has improved its information sharing and with faster declassification of threat information, including a significant increase in publications and threat

²³ See Readout: Office of National Cyber Director Hosts Roundtable on "The State of Cybersecurity in the Black Community", The White House Briefing Room (February 28, 2023), <https://www.whitehouse.gov/oncd/briefing-room/2023/02/28/readout-office-of-national-cyber-director-hosts-roundtable-on-the-state-of-cybersecurity-in-the-black-community/>.

alerts combined with recommended mitigation measures, tool kits and other support services. Importantly, our members want to emphasize that CISA is also uniquely positioned to address longer-term strategic planning and cross-sector mitigation that would be particularly valuable for more mature sectors like financial services.

As CISA continues to evolve, we encourage a focus on three areas.

First is implementing the Cyber Incident Reporting for Critical Infrastructure Act. Last year, this committee led efforts, which BPI supported, to pass cyber incident reporting legislation requiring companies to report ransomware payments and cyber incidents to CISA. Implementing the new law is a significant undertaking that CISA must get right from the outset. It requires extensive coordination with critical infrastructure agencies, other Government agencies, and independent regulators. As a critical infrastructure sector that has had mandatory cyber reporting requirements for more than 20 years, ensuring that the new rules are harmonized with current requirements is also a key area of focus. As CISA formulates the new rules, it should ensure that definitions, time lines, thresholds, and required incident information are aligned with existing requirements and designed to avoid interfering with response and mitigation activities at an affected entity.

Second, CISA should work with industry to identify and prioritize national systemic risks. Last year CISA received funding to develop a new systemically-important entity designation. Financial institutions are very supportive of efforts to identify and prioritize critical infrastructure assets that are most important to our national security. However, it is vital that CISA clarify what it intends to accomplish with a new designation and how it relates to existing efforts, including the Section 9 list, national critical functions, and sector-specific systemic risk designations like Systemically Important Financial Institutions or SIFIEs. CISA should avoid duplication and leverage sector-specific work like ours to create a framework and methodology for identification of cross-sector risks and critical dependencies.

Finally, CISA should support cross-sector collaboration and joint planning. CISA's role as national coordinator puts it in a unique position to support collaboration between critical infrastructure sectors and the Government to reduce risk and disrupt threats. The Joint Cyber Defense Collaborative was helpful in bringing together industry and Government partners to improve visibility and communication, particularly in response to the Russian invasion of Ukraine. This response-oriented focus, however, has not fulfilled the need for longer-term strategic planning across Government agencies and with the private sector. As authorized by Congress, CISA was charged with creating a Joint Cyber Planning Office to develop plans for cyber defense operations and coordinated actions that public and private-sector entities could take to protect, mitigate, and defend against malicious cyber attacks. We have not seen the JCDC engage in this type of proactive planning, but continue to believe this would be beneficial for financial institutions and other more mature sectors.

Although not addressed to date, but noted in CISA's recent strategy, we believe that building the organizational foundation for sustainable cyber defense operations and focusing on the most critical needs of the Nation is of highest priority and would be the most critical accomplishment CISA could undertake at this time.

On behalf of BPI, we look forward to continuing to work with this committee and with CISA, and I'm happy to answer any questions you may have.

[The prepared statement of Ms. Hogsett follows:]

PREPARED STATEMENT OF HEATHER HOGSETT

MARCH 23, 2023

Chairman Garbarino, Ranking Member Swalwell and Honorable Members of the subcommittee, thank you for inviting me to testify. I am Heather Hogsett, senior vice president of technology and risk strategy for BITS, the technology policy division of the Bank Policy Institute (BPI).

BPI is a nonpartisan policy, research, and advocacy organization representing the Nation's leading banks. BPI members include universal banks, regional banks, and major foreign banks doing business in the United States. BITS, our technology policy division, works with our member banks as well as insurance, card companies, and market utilities on cyber risk management and critical infrastructure protection, fraud reduction, regulation, and innovation.

I also serve as co-chair of the Financial Services Sector Coordinating Council (FSSCC) Policy Committee. The FSSCC coordinates across the financial sector to enhance security and resiliency and to collaborate with Government partners such as the U.S. Treasury and the Cybersecurity and Infrastructure Security Agency (CISA), as well as financial regulatory agencies.

FINANCIAL INSTITUTIONS AND CYBERSECURITY

Banks and other financial institutions are increasingly under cyber attack by foreign nations and criminal groups seeking to disrupt the financial system and undermine the functioning of the U.S. economy. The financial sector takes these risks seriously and has a long history of working across industry and with Government partners to address and manage these risks.

As one of 16 critical infrastructure sectors, the financial industry formed and actively participates in the FSSCC¹ and the Financial Services Information Sharing and Analysis Center (FS-ISAC)²—both of which have served as leading examples other critical infrastructure sectors have sought to replicate. We also lead cybersecurity and operational resilience collaboration through public-private partnerships with our Sector Risk Management Agency (SRMA)—the U.S. Department of the Treasury—the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and importantly with our regulators.

A major part of these industry efforts is focused on in-depth information sharing to accelerate and amplify public-private cooperation. During the nearly two decades of work, we have established exercise programs through the FSSCC and FS-ISAC that have covered a wide range of possible events such as destructive malware, an outage at a large service provider, or a pandemic and addressed managing public confidence during a crisis. More than 40 such exercises have been held to date and have included participants from across the industry, third parties, regulators, the U.S. Treasury Department, DHS/CISA and law enforcement agencies.

In addition to Treasury and CISA, we also work closely with financial regulators to address cybersecurity, third-party, and supply chain risks and promote operational resilience across the sector. This work occurs with individual firms, through trade associations such as BPI, and via joint efforts between the FSSCC and its Government counterpart the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by Treasury and includes 17 Federal and State regulators.³

¹ <https://fsscc.org/>.

² <https://www.fsisac.com/>.

³ www.fbiic.gov.

EXPERIENCES WITH CISA

Since its establishment in 2018 as an operational component of DHS, CISA has taken on an increasingly important role protecting Federal civilian agencies and supporting security and resilience across critical infrastructure sectors. Following the important coordination role CISA filled during the COVID-19 pandemic to keep critical infrastructure working for America, there have been notable improvements in faster declassification and sharing of threat information, including a significant increase in publications, alerts, and joint advisories with other Government agencies such as the FBI and National Security Agency (NSA). These publications have become more frequent, timely, and relevant and included recommended mitigation measures to help critical infrastructure entities better protect themselves, particularly mid-size and smaller entities where the assistance is needed most. For example, CISA's recommended mitigations and tool kits to help entities protect themselves during the response to Solar Winds, Log4j, and the ransomware attack against Colonial Pipeline were welcome for their timeliness and actionable nature. By creating a centralized repository for this information CISA has also made it easier for companies to quickly find and access relevant information and resources.

Its efforts to help raise awareness and promote baseline cybersecurity practices across all critical infrastructure sectors have been a welcome focus that will help reduce risk and improve national resilience. CISA also deserves credit for fostering collaboration and coordination across Government entities including the banking industry and other critical infrastructure. Its work to date has built the foundation for trusted relationships and very importantly created resources to support those sectors that are resource-constrained and in the earlier stages of building their cyber risk management programs.

The preparation and response to the Russian invasion of Ukraine highlight a number of these accomplishments. As tensions rose and the United States prepared for Russian aggression and the potential for retaliatory attacks, CISA's senior leadership, along with senior leaders at Treasury, DHS and the FBI, was in regular communications with financial institutions and organizations like the FSSCC, FS-ISAC and the Analysis and Resilience Center for Systemic Risk (ARC). CISA created the "Shields Up" campaign to raise awareness and urge critical infrastructure companies to shore up their defenses and actively share suspicious information with the Government to provide an early warning of attacks. During this time, CISA created a new bi-directional communication mechanism to provide for near-real-time information sharing among trusted partners in both industry and Government that had never previously been done. This coordination role was invaluable for our industry and others and provided a streamlined mechanism to exchange threat information and share timely updates to those operating some of the Nation's most critical infrastructure.

EVOLVING FOR THE FUTURE

Looking ahead, it will be important for CISA to establish a clear path for maturing and scaling its operations, including ensuring these programs and initiatives have stakeholder input and will continue despite future changes in leadership. A number of the efforts to date have been in response to current cyber threats, which was and continues to be important, but CISA is also uniquely positioned to address longer-term strategic planning and cross-sector risk mitigation that will be particularly valuable for mature sectors. As CISA continues to evolve, we encourage a focus on the following areas:

- *Cyber Incident Reporting and Harmonization—Supporting Response and Recovery.*—Last year, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, requiring critical infrastructure companies to report ransomware payments and cyber incidents to CISA. BPI supported this legislation which we believe will help improve national cyber defense by providing CISA and other Government agencies with timely and relevant information to assess and analyze cyber threats across sectors, improve the alerts and security services CISA provides and ultimately provide earlier warning of potential attacks so companies can better defend themselves. Under the law, CISA must conduct a rulemaking process, seek input from stakeholders, and develop the necessary systems and processes to collect, analyze, and share reported information while ensuring strong data security and protection measures are in place.

As CISA crafts rules under CIRCIA, it is also required to harmonize the new requirements with existing regulatory reporting to avoid conflicting, duplicative, or burdensome requirements. Given the comprehensive set of cybersecurity and

incident notification rules⁴ that financial institutions already comply with, harmonizing and aligning the new rules will be important to ensure cyber defenders can maintain focus on protecting the firm rather than complying with multiple Government reporting requirements.

This is a significant undertaking that CISA must get right from the outset and will require extensive coordination with critical infrastructure entities, SRMAs, other Government agencies and independent regulators. As a critical infrastructure sector that has had mandatory cyber reporting requirements for more than 20 years and has invested significant time and resources into harmonizing and driving toward regulatory convergence, this is a key area of focus. CISA should ensure that definitions, time lines, thresholds, and required incident information are aligned with existing requirements and designed to avoid interfering with response and mitigation at an affected firm.

BPI recommends that CISA build a streamlined reporting system that accomplishes the following: (1) Allows an impacted firm to report incident information once and have it shared, as appropriate, with SRMAs, regulators, and law enforcement agencies; (2) provides CISA with timely and relevant information useful to assessing trends, improving analysis, and the development of alerts, tools, and services that can be provided to critical infrastructure companies; and (3) maintains its role as a trusted channel for information and communications, preserving privacy and confidentiality while supporting the response and recovery of an impacted entity.

- *Identification and Prioritization of National Systemic Risks.*—Identifying critical infrastructure assets that are most important to our national security would help prioritize resources and guide public-private collaboration to prevent or mitigate threats and prepare for potential response and recovery needs.

Financial institutions have existing designations such as the Systemically Important Financial Institution designation that stems from the Dodd-Frank Act of 2010 and requires firms to adopt enhanced measures for security and resilience and includes additional oversight and examination by financial regulators. Many of these firms are also included in the Section 9 process, established by Executive Order 13636 in 2013 and managed by DHS, which recognizes firms where a cyber incident could result in “catastrophic regional or national effects on public health or safety, economic security, or national security.”

Similarly, in 2019, CISA created a list of 55 National Critical Functions that are functions “so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”⁵ CISA is in the process of working with SRMAs to decompose or analyze these further. At the same time, CISA is developing a new designation for Systemically Important Entities (SIEs) and was appropriated an increase of \$1.9 million for the creation of an SIE Program Office.

Financial institutions are very supportive of efforts to better identify and prioritize cross-sector risks; however, the current approach appears disjointed and opaque, making it challenging for industry to provide input or information that might be helpful. Past proposals to create an SIE or Systemically Important Critical Infrastructure (SICI) designation would have duplicated existing designations and requirements on financial institutions, diverting resources from defending against threats to regulatory compliance.

As CISA continues this work, we encourage greater transparency and clarity in the approach, what it intends to accomplish, and how an SIE designation fits with related areas of work such as the Section 9 list, NCFs and sector-specific systemic risk designations such as SIFI. CISA should not only avoid duplication or overlap with other systemic designations and their requirements but also leverage work that has already been done in the more mature critical infrastructure sectors. Financial institutions have worked through the ARC to analyze financial sector systemic risks and are ready to work with CISA to develop a framework for assessing risks and critical dependencies across sectors.

- *Fostering Cross-Sector Coordination and Operational Collaboration.*—CISA’s role as national coordinator for critical infrastructure security puts it in a unique position to support collaboration among more mature sectors and the Government to reduce risk and disrupt threats. Since 2017, the financial, energy, and communications sectors have conducted joint planning and exercises to address cyber threats that could impact or cascade across the three sectors.

⁴<https://staging4.bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/>.

⁵<https://www.cisa.gov/national-critical-functions>.

CISA supported the creation of the “tri-sector” working group which is a good example of fostering and enabling collaborative efforts.

CISA’s Joint Cyber Defense Collaborative (JCDC) was helpful in bringing together industry and Government partners to improve visibility and communication in response to geopolitical tensions and the Russian invasion of Ukraine. This response-oriented focus, however, has not fulfilled the need for longer-term strategic planning across Government agencies and the private sector. As originally authorized by Congress,⁶ CISA was charged with creating a Joint Cyber Planning Office (JCPO) to develop plans for cyber defense operations and coordinated actions that public- and private-sector entities could take to protect, mitigate, or defend against malicious cyber attacks. To date, we have not seen the JCDC engage in the type of planning directed by Congress but continue to believe this would be beneficial for financial institutions and other more mature sectors.

The recently released National Cybersecurity Strategy recognizes that the private sector has growing visibility into adversary activity and calls for enhancing public-private operational collaboration to disrupt adversaries.⁷ Through our relationship with Treasury as our SRMA, we have robust partnership and dialog. Treasury is establishing a cyber collaboration center to facilitate greater opportunity for firms to exchange Classified and un-Classified information and facilitate discussion around threat actor activity and vulnerabilities. Other parts of Government have created similar centers such as the NSA’s Cybersecurity Collaboration Center. Plans to create a cross-sector equivalent or otherwise foster collaboration and exchange among these efforts would be valuable and CISA could play a helpful role.

SUSTAINING PROGRESS AND BUILDING CAPABILITIES

We are at a defining juncture in CISA’s development, similar to any start-up at this stage, where achieving scale matters. As Congress intended and supported with funding, CISA must refine its focus and apply resources carefully to be successful. Now that CISA has established its presence, developed communications and outreach capabilities, and designed tools and services to improve near-term resilience, it should shift its approach to expand management capabilities, add operational expertise and establish processes that will be the foundation for sustained leadership on immediate tactical response matters as well as longer-term, proactive planning and support that will benefit even the most cyber-mature sectors like financial services.

Successful implementation of CIRCIA, including harmonizing its reporting requirements to optimize protection and response and streamline coordination, will serve as a cornerstone for the future of public-private partnerships and should be a top priority. Similarly, developing the means to identify and prioritize the highest risks by sector and across sectors will refine CISA’s focus and support more secure and resilient outcomes for the Nation.

This is no small task and requires CISA to focus on building organizational consistency and rigor, hiring and retaining experienced staff, and sourcing support from sectors that have well-established security, resilience and, in the financial services case, regulatory standards that can be leveraged.

We are committed to working with CISA to support its continued development and look forward to the opportunity to engage in future national risk mitigation efforts.

Chairman GARBARINO. Thank you, Ms. Hogsett.

I now recognize Mr. Edwards for 5 minutes to summarize his opening statement.

STATEMENT OF MARTY EDWARDS, VICE PRESIDENT, OPERATIONAL TECHNOLOGY SECURITY, TENABLE

Mr. EDWARDS. Chairman Garbarino, Ranking Member Swalwell, and Members of the committee, thank you for the opportunity to testify before you today on CISA and the state of American cybersecurity.

⁶William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. Pub. L. 116–283, Sec 1715.

⁷National Cybersecurity Strategy, March 2023, p. 15.

I am Marty Edwards, deputy chief technology officer for operational technology at Tenable, the leading cybersecurity exposure management company, with 43,000 customers world-wide, including just about every Federal department and many critical infrastructure providers.

From Russia's invasion of Ukraine to the Colonial Pipeline incident, we're operating in a heightened threat landscape. CISA, the National Coordinator for Critical Infrastructure Security and Resiliency, and Congress have recognized the need to prioritize critical infrastructure security. Under Director Jen Easterly's leadership, CISA has taken significant steps to strengthen the U.S. cyber posture, including through prioritizing public-private partnerships, enhancing strategic collaboration, and developing new cybersecurity initiatives in favor of greater security and resiliency, which were emphasized the recent National Cyber Security strategy.

This includes addressing the security of IT and OT system Convergence operational technology, or OT, is the hardware used in manufacturing, utilities, and critical infrastructure industries. But while today's technology are implemented to improve efficiencies, the convergence of these technologies between IT and OT makes OT susceptible to many new threat vectors. Successful OT attacks can impact human safety and damage physical equipment, making this a national security imperative. Public-private-sector collaboration, including CISA's Joint Cyber Defense Collaborative, of which Tenable is a proud alliance partner, is essential to building resilient and robust converged IT-OT environments and enabling collaboration on a range of issues.

To combat the growing cyber threats, the White House tasked the President's National Security Telecommunications Advisory Committee with examining key challenges to securing converged IT-OT systems. I co-ed this Convergence Subcommittee Working Group to produce a report to the President which found that despite having the technology and the expertise to secure these systems, organizations still lack visibility into their OT environments.

To strengthen the cybersecurity posture of the U.S. Government-owned and -operated OT systems with relatively low risk, the NSTAC report recommends three key steps for the U.S. Government, including No. 1, issue a binding operational directive that requires Federal agencies to maintain a real-time, continuous inventory of all OT systems and assets, including any interconnectivity to other systems.

No. 2, develop guidance on procurement language for OT products and services to incentivize and prioritize cybersecurity capabilities. Existing technology products and services should be secure by design, especially those that support critical infrastructure.

And third, prioritize the development and implementation of interoperable, technology-neutral, vendor-agnostic information-sharing mechanisms to enable real-time information sharing between the U.S. critical infrastructure stakeholders. We should not allow for learned helplessness by Federal Government agencies or by private industry. There is too much at stake for organizations to remain negligent and not take the most basic steps to improve their cybersecurity posture.

From Tenable's perspective, Congress has the opportunity to enhance U.S. preparedness by establishing baseline cybersecurity standards of care and ensuring that CISA is adequately resourced to support its critical mission.

Oh, that's interesting, I don't have the rest of my page here. Sorry about that.

Many critical operating environments lack a formal, systemic approach to risk assessments, let alone the continuous visibility required for critical services and high-value targets. In these instances, policy guidance can help drive improved risk management practices and foster innovation.

Thank you again, Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee for your attention to these important bipartisan issues, your continued assessment of the work CISA is doing to help keep Americans safe, and for the opportunity to testify here today.

I look forward to working with you to secure our Nation's cyber assets and answer your questions.

[The prepared statement of Mr. Edwards follows:]

PREPARED STATEMENT OF MARTY EDWARDS

MARCH 23, 2023

INTRODUCTION

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and Members of the subcommittee, thank you for the opportunity to testify before you today on the Cybersecurity and Infrastructure Security Agency (CISA) and the state of American Cybersecurity.

My name is Marty Edwards and I am the deputy chief technology officer for operational technology (OT) and internet of things (IoT) at Tenable, a cybersecurity exposure management company that provides organizations, including the Federal Government, with an unmatched breadth of visibility and depth of analytics to measure and communicate cybersecurity risk. My expertise is in OT and Industrial Control System (ICS) cybersecurity, and my work with Tenable has focused on furthering Government and industry initiatives to improve critical infrastructure security. In collaboration with industry, Government, and academia, Tenable is raising awareness of the growing security risks impacting critical infrastructure and of the need to take steps to mitigate those risks. I also recently served as the staff lead under Tenable co-founder Jack Huffard in the development of the Report on Information Technology (IT)/OT Convergence Report¹ issued by The President's National Security Telecommunications Advisory Committee (NSTAC). Prior to joining Tenable, I worked in industry as an industrial control systems engineer and as a program manager at the U.S. Department of Energy's Idaho National Laboratory focused on cybersecurity. I was the longest-serving director of the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which is now part of CISA.

ABOUT TENABLE

Tenable is headquartered in nearby Columbia, Maryland, and has 1,900 employees globally and approximately 43,000 customers world-wide. Tenable is publicly traded on the NASDAQ and is the world's leading provider of vulnerability management capabilities. We believe cybersecurity is foundational to making better and more strategic decisions. Our goal is to eliminate blind spots and help organizations prioritize which actions they can take to most efficiently reduce exposure and loss.

Tenable empowers organizations of all sizes to understand and reduce their cybersecurity risk. For the Federal Government specifically, Tenable provides the most widely-deployed vulnerability management solution, serving just about every depart-

¹ President's National Security Telecommunications Advisory Committee, "Information Technology and Operational Technology Convergence Report," https://www.cisa.gov/sites/default/files/publications/NSTAC%20ITOT%20Convergence%20Report_508%20Compliant_0.pdf.

ment and agency. Our solutions are also broadly used by State and local governments to manage cybersecurity risk.

THE CURRENT STATE OF OT/CRITICAL INFRASTRUCTURE/FEDERAL CYBERSECURITY

Over the past few years, we have seen a dramatic increase in the frequency of successful cyber attacks against U.S. public and private-sector organizations and have experienced new threats targeting our critical infrastructure. New ransomware and extortion groups routinely exploit known vulnerabilities to gain access into organizations, with at least 31 new groups discovered from November 2021 to October 2022, resulting in ransomware attacks intensifying, exposing reams of data and accounting for over 35 percent of data breaches.²

In February 2021, a water treatment plant in Oldsmar, Florida, was breached when attackers attempted to poison the water supply.³ Just months later, a ransomware attack against Colonial Pipeline shut down operations for 6 days, prompting the President of the United States to issue a state of emergency.⁴ Following Russia's invasion of Ukraine last year, and increased threats of malicious activity against the United States and our allies, CISA and other law enforcement agencies took swift steps to warn Governors, public-sector partners and critical infrastructure providers to harden their cyber defenses, including through the "Shields Up" initiative.⁵

Just this month, a breach of D.C. Health Link, the health insurance exchange which serves Members of Congress and their staff, resulted in the on-line exposure of personal data of more than 56,000 customers.⁶ While unfortunate, this breach is not surprising as health care was the No. 1 sector targeted by ransomware attacks last year with 472 breaches, followed by the public administration sector, which includes governments, towns, and municipalities with 162 breaches.⁷

When it comes to reducing cyber risk, organizations world-wide find themselves restricted by deeply entrenched people, process, and technology issues. An orientation toward reactive, incident-focused cybersecurity practices means preventive tasks are often relegated to nothing more than a compliance exercise. Teams are measured by how many vulnerabilities they've remediated, rather than by how effectively they've reduced their organization's exposure.

The siloed nature of cybersecurity, especially between IT and OT teams—each with their own, sometimes contradictory, goals—exacerbates the problem. It is nearly impossible for cybersecurity leaders to obtain a unified and contextual view of their exposure using the existing tools at their disposal. The processes involved—which often require cybersecurity teams to convince their counterparts in IT, cloud, and Development Operations (DevOps) to take necessary security precautions—are fraught with opportunities for error and conflict. The siloed nature of the many preventive security tools offered by cybersecurity vendors means there's no way to determine how much exposure any given weakness actually represents at any given time. The reason? Security pros using siloed tools are unable to determine the relationships among users, systems, and software. Without a unified and contextual view of their environments, security professionals cannot realistically identify the objective security truths that indicate their exposure to risk.

These issues are not new. While applying basic cyber hygiene can reduce exposure, it's long been challenging for organizations to achieve with existing preventive tools. What is new is the expanding complexity of the modern attack surface. Modern IT infrastructure encompasses multiple cloud systems, numerous identity and privilege management tools, multiple web-facing assets along with operational technology (OT) and internet of things (IoT) systems and software.

Today's IT environment brings with it numerous opportunities for misconfigurations and overlooked assets. The lack of a unified and contextual view of users, systems, and software means security teams cannot effectively evaluate what's happening across the attack surface. Competing business interests often mean speed and uptime are favored over security.

²Tenable, "2022 Threat Landscape Report," https://static.tenable.com/marketing/research-reports/Research-Report-2022_Threat_Landscape_Report.pdf.

³ABC News, "Florida city's water treatment system hacked by 'intruder,' investigators say," <https://abcnews.go.com/US/florida-citys-water-treatment-system-hacked-intruder-investigators/>.

⁴NPR, "What We Know About The Ransomware Attack On A Critical U.S. Pipeline," <https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline>.

⁵U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Shields Up," <https://www.cisa.gov/shields-up>.

⁶Roll Call, "House, Senate members affected in DC Health Link breach to total 21," <https://rollcall.com/2023/03/14/house-senate-members-affected-in-dc-health-link-breach-total-21>.

⁷Ibid 2.

Government officials and private-sector leaders are paying increasing attention to critical infrastructure vulnerabilities, particularly those brought on by the convergence of IT and OT technologies. Since the late 1960's, OT has been part of manufacturing, utilities, and other critical infrastructure sectors, and has been considered technology "safe" from attacks because most OT devices were not connected to outside networks. However, in today's modern facilities, these devices are no longer air-gapped and are now in many cases exposed to the internet—and to the threat of cyber attacks.⁸

The combination of IT and OT systems makes OT systems susceptible to the same risks of malware and threats that IT systems face today. Between the two: OT has different performance requirements than IT; OT systems serve a specific purpose while IT systems serve a wide variety of technologies; and OT systems have a life cycle of a decade or more while IT systems are much shorter. This creates different priorities between IT security professionals and OT system operators within organizations. While IT security practices can inform OT security requirements, the OT systems require more specialized solutions which address the performance requirements of the system.⁹

Securing IT and OT systems and their convergence has become a national security imperative. Public-private-sector collaboration to address cyber threats is essential to building resilient and robust converged IT/OT environments. CISA is the national coordinator for critical infrastructure security and resilience and, as the administration's National Cybersecurity Strategy emphasizes, it must enhance strategic collaboration and scale public-private partnerships in favor of greater security and resiliency.¹⁰

Given the heightened threat landscape, CISA and Congress have started to recognize the need to prioritize critical infrastructure security and have begun making much-needed investments. CISA is working to guide the Nation's State and local governments, critical infrastructure providers, and other private-sector organizations, and Federal entities, to strengthen their cyber defenses. In Congress, the House Committee on Homeland Security-led efforts to include a \$1 billion State and local cybersecurity grant program in the Infrastructure Investment and Jobs Act. The program will help State, local, Tribal, and territorial governments safeguard these vital systems from future attacks.

CISA 101

CISA was established on November 16, 2018, to defend and secure our Nation's cyber space and build a resilient and robust critical infrastructure for the American people. As a relatively new Federal agency, CISA has made strides in elevating cybersecurity and infrastructure security as national security issues. Unlike other well-established Federal organizations, CISA is working at start-up speed to keep American organizations ahead of growing and constant cyber threats.

There has been significant activity under Director Jen Easterly's leadership to strengthen the U.S. cyber posture, including prioritizing public-private partnerships, developing new cybersecurity initiatives and implementing cybersecurity policies proposed by Congress and the administration.

Joint Cyber Defense Collaborative (JCDC)

CISA established the Joint Cyber Defense Collaborative (JCDC) to lead "integrated public-private sector cyber defense planning, cybersecurity information fusion, and dissemination of cyber defense guidance to reduce risk to critical infrastructure and National Critical Functions."¹¹ Tenable is a proud Alliance Partner of the JCDC, which has enabled us to collaborate with CISA across a range of cybersecurity issues and challenges, to provide strategic insights and operational response acumen. Managing vulnerabilities is essential to secure critical IT and OT infrastructure and the work done by JCDC and CISA promotes the prioritization of network security. In fact, known vulnerabilities dating as far back as 2017 were so

⁸Tenable, "Operational Technology (OT) Security: How To Reduce Cyber Risk When IT and OT Converge," <https://www.tenable.com/source/operational-technology>.

⁹President's National Security Telecommunications Advisory Committee, "Information Technology and Operational Technology Convergence Report," <https://www.cisa.gov/sites/default/files/publications>.

¹⁰The White House, "National Cybersecurity Strategy," <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

¹¹U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Joint Cyber Defense Collaborative," https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet_508C.pdf.

prominent in Tenable's 2022 Threat Assessment Report findings that they occupied the top spot in the 2022 list of the top 5 vulnerabilities.¹²

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA)

Following passage and implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA), CISA began development of cyber incident reporting regulations as required by the new law.¹³ Timely cyber incident reporting—both from critical infrastructure entities to CISA and from CISA to its industry stakeholders—enables rapid identification, remediation, and proactive defense against these and similar incidents. CISA's commitment to working with industry stakeholders to develop thoughtful, effective, and balanced reporting requirements will further strengthen the cybersecurity of our Nation's critical infrastructure.

As part of the regulatory development process, Tenable provided CISA with input as the agency developed its cyber incident reporting regulations required by CIRCA. Among its input, Tenable proposed the following three primary recommendations to effectively improve threat and incident situational awareness:

1. That CISA request contextual details about the specific vulnerability exploited in the cyber incident and actionable information about the nature of the incident, including tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs).
2. That CISA share this information, utilizing the traffic light protocol with a trusted group of cybersecurity stakeholders, such as JCDC Alliance Partners.
3. That actionable information sharing across the critical infrastructure sectors would enable owners and operators to help defend their organizations against and respond to cyber attacks.

Binding Operational Directives (BOD)

CISA also has authority to issue Binding Operational Directives (BOD), which are compulsory directions to Federal, Executive branch, departments and agencies for purposes of safeguarding Federal information and information systems.¹⁴ In 2021, CISA issued BOD 22–01, which requires Federal agencies “to remediate vulnerabilities in the KEV catalog within prescribed time frames.”¹⁵ The Known Exploited Vulnerabilities (KEV) catalog is maintained by CISA and helps organizations prioritize remediation of listed vulnerabilities and reduce the opportunities for threat actors to compromise systems.

Following recommendations to conduct asset inventories of OT systems included in last year's NSTAC Report to the President, CISA issued BOD 23–01 to require Federal agencies to improve asset visibility and vulnerability detection on Federal networks.¹⁶ To provide additional visibility into the variety of assets that make up the modern attack surface and help agencies understand the full scope of their cybersecurity risk, BOD 23–01 mandates continuous and comprehensive asset visibility. The BOD focuses on two core activities that are essential to maintaining a successful cybersecurity program:

- Asset discovery
- Vulnerability enumeration.

By mandating continuous and comprehensive asset visibility, BOD 23–01 will ensure that Federal agencies have the necessary foundation to maintain a successful cybersecurity program.

This directive applies to all IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols. It builds on BOD 22–01 and outlines new requirements for cloud assets, IPv6 address space, and operational technology (OT) in an effort to reduce cyber risk.

Cross-Sector Cybersecurity Performance Goals (CPGs)

In 2021, the Biden administration issued the National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems, outlining initiatives in the electricity, pipeline, water, and chemical sectors, and calling for

¹² Ibid 2.

¹³ U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA),” <https://www.cisa.gov/topics/cyber-threats-and-advisories>.

¹⁴ 44 U.S.C. § 3552(b)(1). U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “Binding Operational Directive 23–01,” <https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01>.

¹⁵ U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “Reducing the Significant Risk of Known Exploited Vulnerabilities,” <https://www.cisa.gov/known-exploited-vulnerabilities>.

¹⁶ Ibid 9.

the development of cross-sector cybersecurity performance goals for critical infrastructure.¹⁷

Last October, CISA released its Cross-Sector Cybersecurity Performance Goals (CPGs), based on relevant categories and subcategories of the NIST Cybersecurity Framework (CSF), to address some of the Nation's most frequent and impactful cybersecurity risks. The CPGs also emphasize OT security and how it is often overlooked and under-resourced.¹⁸ By offering IT/OT cybersecurity guidance, CISA's CPGs create a baseline set of cybersecurity practices and benchmarks for critical infrastructure operators to measure and improve their cyber posture. Earlier this week, CISA released stakeholder-based updates to the CPGs that are more strongly aligned with the functions, categories, and subcategories of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is widely utilized by critical infrastructure owners and operators and the greater alignment of the CPGs will make them more accessible to these entities.

Pillar One of the administration's new National Cybersecurity Strategy builds on this notion of establishing cybersecurity best practices and expanding the use of minimum cybersecurity standards, such as the adoption of basic cyber hygiene and secure-by-design principles. This reinforces that IT/OT convergence will continue to be a security issue for years to come, and organizations need a plan to address these challenges.¹⁹

Tenable was pleased that CISA incorporated input from multiple critical infrastructure industry stakeholders, including relevant sector-coordinating councils (SCCs) in the development of the CPGs, ensuring they were aligned with the NIST CSF. We are also encouraged to see the administration emphasize similar approaches to mitigate cybersecurity risk in its National Cybersecurity Strategy. Baseline cybersecurity requirements or standards of care for critical infrastructure, which align with CISA's Cross-Sector Cybersecurity Performance Goals, international standards, and the NIST CSF, drive better cybersecurity and a more resilient ecosystem.

Secure-by-Default

In recent months, CISA has spearheaded efforts to shift the security burden from consumers to putting the onus on manufacturers to ensure built-in security is a feature of all technology products, especially those that support critical infrastructure. Director Easterly stated, "the leaders of technology manufacturers should explicitly focus on building safe products, publishing a roadmap that lays out the company's plan for how products will be developed and updated to be both secure-by-design and secure-by-default."²⁰ Likewise, CISA launched the Ransomware Vulnerability Warning Pilot program to help identify vulnerabilities in critical infrastructure systems and inform owners to take action before a potential cybersecurity incident occurs.²¹ In conjunction with the other initiatives CISA has developed, these efforts will work to advance the Nation's cybersecurity resiliency.

SEPARATION OF DUTIES/INDEPENDENT ASSESSMENTS OF SOFTWARE

Similar to the Sarbanes-Oxley Act of 2002 requirement for firms to separate their auditing function from their consulting function, "separation of duties" in cybersecurity is necessary to prevent conflicts of interest, misaligned incentives, and increased security risks. The U.S. Securities and Exchange Commission states that an auditor is not capable of exercising objective and impartial judgment if a relationship with or service provided by an auditor "(a) creates a mutual or conflicting interest with their audit client; (b) places them in the position of auditing their own

¹⁷The White House, "National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems," <https://www.whitehouse.gov/briefing-room/statements-releases>.

¹⁸U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.

¹⁹The White House, "National Cybersecurity Strategy," <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

²⁰U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "The Cost of Unsafe Technology and What We Can Do About It," <https://www.cisa.gov/news-events/news/cost-unsafe-technology-and-what-we-can-do-about-it>.

²¹U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "CISA Announces Ransomware Vulnerability Warning Pilot," <https://www.cisa.gov/news-events/alerts/2023/03/13>.

work . . . ”.²² CISA should apply the Sarbanes-Oxley “separation of duties” principles to cybersecurity and prohibit the provider responsible for developing and/or running software programs from also testing its security, conducting security audits, or reporting on its security.

WHAT’S NEXT: CISA 2025

CISA has worked to enable organizations and critical infrastructure providers to understand, manage, and reduce their cybersecurity risks, but there is still much work to be done. Naturally, as the agency evolves, there is a significant need for continued improvements to strengthen our cybersecurity efforts and to address the many unique needs of the critical infrastructure sectors.

While some of the 16 identified critical infrastructure sectors²³ have a high degree of cybersecurity preparedness, strong risk understanding and risk management practices, and very strong security programs, others are woefully ill-prepared. New technology investments represent great efficiency opportunities, like the move to smart factories and smart cities, but these shifts can introduce real gaps in security. Continued digital transformation, increasingly interconnected IT and OT systems, and an expanding cyber attack surface will require enhancements to security and resiliency. Critical infrastructure providers must be prepared to address tomorrow’s cyber threats and it is CISA’s responsibility to support them in that effort.

Zero Trust Architecture

The White House issued a Federal Zero Trust Architecture (ZTA) Strategy in January 2022, requiring agencies to implement Attack Surface Management (ASM) as part of their ZTA by the end of fiscal year 2024. The memorandum states, “to effectively implement a zero trust architecture, an organization must have a complete understanding of its internet-accessible assets so that it may apply security policies consistently and fully define and accommodate user workflows.”²⁴ ASM enables organizations to identify assets and look for vulnerabilities from the outside in, from the attacker’s perspective, and will give agencies complete asset discovery, increase awareness of what is on their networks, and improve vulnerability management.

The memorandum further states, “for agencies to maintain a complete understanding of what internet-accessible attack surface they have, they must rely not only on their internal records, but also on external scans of their infrastructure from the internet.”²⁵ Ultimately, organizations cannot take a ‘trust no one’ approach on a device if they do not know the device exists; however, ASM enables that visibility.

As agencies look to comply with the White House’s ZTA strategy by moving toward a zero trust architecture and taking a ‘trust no one’ approach to security, the security of an agency’s underlying user identity and privilege management system itself comes into play. To ensure identity systems are secure, agencies need to be able to identify everything in their complex Active Directory (AD) environment, predict what matters to reduce risk, and eliminate attack paths before attackers exploit them. Effective management of AD users and privileges allows agencies to take a proactive approach to address and mitigate future cyber threats.

NSTAC IT/OT Convergence Report

In response to growing cybersecurity threats to the critical infrastructure upon which Americans depend, the White House tasked The President’s National Security Telecommunications Advisory Committee (NSTAC) with conducting a multi-phase study on “Enhancing Internet Resilience in 2021 and Beyond.”²⁶ The subcommittee for the second phase of the study was charged with developing the NSTAC Report to the President on IT/OT Convergence.²⁷ I co-lead the subcommittee’s working group to produce this report. The report identifies three opportunities for the Federal Government:

- to help relevant stakeholder communities execute a secure convergence of IT and OT cybersecurity;

²²The U.S. Securities and Exchange Commission, “Audit Committees and Auditor Independence,” <https://www.sec.gov/oca/audit042707>.

²³U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “Critical Infrastructure Sectors,” <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

²⁴The White House, “Federal Zero Trust Architecture (ZTA) Strategy,” <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>.

²⁵Ibid 24.

²⁶President’s National Security Telecommunications Advisory Committee, “NSTAC Fact Sheet,” <https://www.cisa.gov/resources-tools/resources/presidents-nstac-fact-sheet>.

²⁷Ibid 9.

- to examine the key challenges of securing converged OT systems against threats that emerge from IT network connections; and
- to identify emerging approaches to increase OT resiliency to these threats.

The subcommittee received briefings from more than 30 subject-matter experts across Government and private industry. First, the subcommittee heard from Government owners and operators of OT systems and policy makers focused on IT and OT cybersecurity; second, we heard from critical infrastructure owners and operators of converged IT/OT environments and original equipment manufacturers; and third, we heard from cloud service providers, integrators, and cybersecurity vendors.

NSTAC Report Findings

On August 23, 2022, NSTAC approved the Report to the President. The report findings revealed several consistent themes highlighting that the convergence of IT and OT systems is not a new issue. As a Nation, we have not prioritized securing IT/OT interconnected systems, despite having the technology and knowledge readily available. Even in 2022, the report found organizations lack visibility into their OT environments, which is exacerbated by the traditional silos within which OT and IT personnel operate. The current siloed approach demonstrates a need to promote harmonization through a unified structure to better manage shared responsibility to secure converged environments.²⁸

Stakeholders also rarely take the opportunity to proactively “build in” security where appropriate and opt instead to “bolt-on” security in OT environments after the fact, costing organizations valuable time and resources to recover from cyber incidents and unpatched vulnerabilities.

Businesses, organizations, and governments need to share the responsibility of building a more sustainable cybersecurity model to create ecosystems that take a secure-by-design approach to ensure the long-term cybersecurity resiliency of our country—a point Director Easterly and CISA Executive Director Eric Goldstein recently emphasized.²⁹

NSTAC Recommendations to Improve Critical Infrastructure Security

Based on the findings, the subcommittee developed 15 Presidential, strategic, and actionable recommendations to address the many concerns expressed to the subcommittee through the briefing phases. Amongst the 15 recommendations, the subcommittee identified 3 consequential recommendations for the President to strengthen the cybersecurity posture of U.S. Government-owned and -operated OT systems that should be prioritized.

The report first recommends that CISA issue a Binding Operational Directive (BOD), similar to what Section 1505 of the Fiscal Year 2022 National Defense Authorization Act (NDAA) requires for the Department of Defense (DoD), that requires Executive civilian branch departments and agencies to maintain a real-time, continuous inventory of all OT devices, software, systems, and assets within their areas of responsibility, including an understanding of any interconnectivity to other systems. An up-to-date inventory should be required as part of each department’s or agency’s annual budget process.

Once Federal agencies clearly understand the vast and interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions about how to prioritize their cybersecurity budgets to best protect the most consequential of those assets.

Second, CISA should develop guidance on procurement language for OT products and services, and for products and services that support converged IT/OT environments, to incentivize the inclusion of risk-informed cybersecurity capabilities, including for supply chain risk management. This guidance should also help organizations understand best practices for bolt-on security for legacy OT devices that are difficult or expensive to replace.

CISA should work with the General Services Administration (GSA) to require the inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the Federal Government. There should also be a mechanism for both private-sector users of the procurement guidance and public sector agencies, which must follow the new requirements, to provide feedback and lessons learned to aid the community.

Finally, the NSC, CISA, and the Office of the National Cybersecurity Director (ONCD) should prioritize developing and implementing interoperable, technology-neutral, vendor-agnostic information-sharing mechanisms to enable real-time sharing of sensitive collective-defense information between authorized stakeholders in

²⁸ Ibid 9.

²⁹ Foreign Affairs, “Stop Passing the Buck on Cybersecurity,” <https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity>.

volved with securing U.S. critical infrastructure. This should include breaking down the artificial barriers for sharing controlled unclassified information, both within the U.S. Government and between Government and other key, cross-sector stakeholders.

Additional recommendations in the report to secure U.S. OT infrastructure call on CISA and the ONCD to clearly articulate roles and responsibilities for Federal agencies that support critical infrastructure and other industry stakeholders. Concurrently, CISA should work with the Office of Management and Budget (OMB) to develop key IT/OT convergence cybersecurity performance indicators and implementation time lines for agencies and hold agency heads accountable. Furthermore, the ONCD, in partnership with CISA, should facilitate an interagency study that evaluates conflicting regulations for OT operators to identify opportunities to streamline OT cybersecurity regulation.

Based on the subcommittee briefings, it was evident that the Federal Government has historically underfunded OT cybersecurity. Fortunately, the Infrastructure Investment and Jobs Act (IIJA) has created numerous grant programs that include cybersecurity as an allowable expense, presenting an opportunity for the ONCD and CISA to collaborate with Sector Risk Management Agencies (SRMA) to ensure that cybersecurity is a priority item in any grant application. Of note, the State and Local Cybersecurity Grant Program (SLGCP) appropriates \$1 billion in grant funding over the next 4 years to help advance OT cybersecurity. Tenable has been leading efforts to educate eligible entities on how to apply for grant funding and implement cybersecurity solutions that address the growing threats and risks to their information systems.³⁰

Binding Operational Directive 23–01

As previously mentioned, last October CISA issued Binding Operational Directive (BOD) 23–01, calling on Federal civilian departments and agencies to “make measurable progress toward enhancing visibility into agency assets and vulnerabilities,” aligning with NSTAC’s IT/OT Convergence Report recommendations.³¹

BOD 23–01 mandates continuous and comprehensive asset visibility, focusing on two core activities essential to maintaining a successful cybersecurity program: asset discovery and vulnerability enumeration. According to BOD 23–01, “continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage cybersecurity risk. Accurate and up-to-date accounting of assets residing on Federal networks is also critical for CISA to effectively manage cybersecurity for the Federal Civilian executive branch (FCEB) enterprise.”³² Federal agencies need comprehensive visibility into their assets and vulnerabilities across their organizations to protect against external unknowns.

Enumerating OT assets, critical infrastructure and vulnerabilities present unique challenges to Federal agencies. Compared to the IT environment, where patching, upgrading, and replacing systems is standard, an OT environment typically requires working with legacy technologies. To prioritize remediation efforts, agencies need a detailed view of OT and IT assets in the OT environment and the ability to map connections between devices and identify high-risk assets.

To ensure FCEB systems and agencies operating those systems meet said requirements, Congress should appropriate funding to implement CISA’s BOD 23–01, enabling agencies to maintain an updated inventory of assets, identify software vulnerabilities, track how often an agency enumerates its assets, and share information with CISA’s Continuous Diagnostics and Mitigation Program (CDM) Federal Dashboard. Pursuant to BOD 23–01, the scope of this implementation encompasses all reportable OT as well as IT assets.

POLICY RECOMMENDATIONS

Congressional action should not allow for “learned helplessness” by Federal Government agencies or private industry. There is too much at stake for individuals and organizations to remain negligent and not take even the most basic steps to improve their cyber posture.

Tenable recommends the following steps that Congress should implement to enhance the cyber preparedness of U.S. critical infrastructure:

- *Establish baseline cybersecurity requirements or standards of care for critical infrastructure that align with CISA’s Cross-Sector Cybersecurity Performance*

³⁰ H.R. 368—117th Congress (2021–2022): Infrastructure Investment and Jobs Act. (2021, June 4). <https://www.congress.gov/bills/117/congress/house-bill/3684/text>.

³¹ U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “Binding Operational Directive 23–01,” <https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01>.

³² Ibid 31.

Goals, international standards, and the NIST CSF, based on effective cyber hygiene and preventive security practices.—Basic cyber hygiene for critical infrastructure operators includes continuous understanding of what assets are on networks, ensuring strong identity and access management, scanning for and patching known vulnerabilities, and implementing incident detection and response capabilities. Pillar One of the recently-released National Cybersecurity Strategy calls for baseline cybersecurity requirements for critical infrastructure providers. The CISA Cross-Sector Cybersecurity Performance Goals, based on the NIST CSF, are an excellent resource for industry and Sector Risk Management Agencies to utilize in the development of baseline requirements and standards of care.

- *In its oversight of CISA implementation of CIRCIA, Congress should ensure that CISA:* is adequately resourced to ingest the wealth of information that will be shared by critical infrastructure entities; will request and share anonymized data on the types of vulnerabilities that were exploited and the attack paths that adversaries followed after infiltrating target networks; and provides actionable information through trusted partners, such as JCDC Alliance Partners, to provide cyber situational awareness to the broader critical infrastructure ecosystem to enable entities to protect themselves against on-going and potential attacks.
- *Require Independent Assessments of IT Management Software.*—CISA should apply the Sarbanes-Oxley “separation of duties” principles to cybersecurity and prohibit the provider responsible for developing and/or running IT management software from also conducting its exposure management or otherwise testing its security, conducting security audits, or reporting on its security.
- *Continue implementation of the NSTAC IT/OT Convergence Report policy recommendations.*
 - *Direct Federal civilian agencies to inventory their OT assets and provide OT asset and vulnerability information to the CDM Dashboard.*—CISA has already taken steps to address this obstacle through BOD 23–01, but Congress should reinforce the need to gain visibility into these mission-critical environments so we can understand the scale of cybersecurity challenges and begin to systematically address the serious risk. The foundation for every security framework, whether IT or OT, always begins with visibility into the assets for which you are responsible. Achieving this visibility is a significant step forward for Federal departments and agencies to protect their critical IT and OT assets against evolving cybersecurity threats.
 - *Develop enhanced OT-specific cybersecurity procurement language.*—Public and private-sector OT requests for proposals and procurement processes seldom require the inclusion of risk-informed cybersecurity capabilities for products and services. Updating procurement language guidance will help asset owners specify that cybersecurity be built into products and projects rather than bolted on as an afterthought. Including cybersecurity in both government and private-sector procurement vehicles will significantly enhance the resilience of critical infrastructure systems.
 - *Implement standardized, technology-neutral, real-time interoperable information-sharing mechanisms to promote the sharing of sensitive information across agencies and to break the traditional siloed approach.*—Cyber attacks often target multiple critical infrastructure sectors and attackers have the ability to move at machine speed to compromise multiple industrial sectors. Our defenses need to match this threat and it is imperative for our critical infrastructure sectors to securely communicate with each other to get the right information to the right person, at the right time, in a standardized, technology-neutral way, in order to leverage cyber threat and vulnerability information from the broader critical infrastructure ecosystem.
- *Ensure CISA and FCEB agencies are adequately resourced to implement BOD 22–01 and BOD 23–01 policy recommendations.*—Protecting our Nation’s cybersecurity means knowing what’s on our networks and maintaining it in good working order, which includes conducting an inventory of OT assets and prioritizing remediation of known vulnerabilities. If an organization does not know an asset exists, it cannot scan it for vulnerabilities. With the issuance of BOD 23–01, Federal agencies need comprehensive visibility into their assets and vulnerabilities across their organization. This includes:
 - External unknowns
 - Cloud workload and resources
 - Operational technology
 - Network infrastructure and endpoints
 - Web application

- Identity systems.
- *Ensure sufficient funding for CISA and the Office of the National Cyber Director to ensure they can meet mission requirements.*—Our company supported the creation of the Office of the National Cyber Director and applauded efforts to stand up and staff the new office. The threats to Federal networks and critical infrastructure are growing at a significant rate, and CISA must serve as an effective coordinator to strengthen security in these environments. Congress should see the fiscal year 2024 appropriations for CISA as a new baseline number, which should grow at a rate commensurate with the needs of the mission.
- *Support and strengthen value-added engagement between the private sector and public sector.*—The JCDC, of which Tenable is a member, is bringing together representatives from private industry and key Government agencies to drive strategic planning and incident response capabilities. This type of operational Government-industry engagement has been a positive step forward and we urge Congress to continue supporting and strengthening the JCDC's alignment.
- *Accelerate deployment of Zero Trust including Active Directory and Attack Surface Management.*—Congress should provide Federal agencies with the resources needed to implement Cyber Executive Order 14028 to modernize and strengthen our collective cyber defenses, recognizing that Zero Trust is a philosophy that dictates systems design and operation, not a singular product.
- All Government systems must incorporate Active Directory security to ensure least privileges for user identities, and to scan for misconfigurations that can be exploited to gain access to Active Directory and monitor for on-going suspicious and high-risk activities within Active Directory.³³
- *Attack Surface Management*, which continuously scans the internet to discover, inventory, classify, and monitor an organization's IT infrastructure, will give agencies complete asset discovery, increase awareness of what is actually on their networks, and will improve vulnerability management.

CONCLUSION

There are fundamental steps all Federal agencies and critical infrastructure sectors must take—from knowing what's on their network and how those systems are vulnerable to addressing known exposures, and from controlling user access and privileges to managing critical systems that are interconnected—that will make it harder for bad actors to compromise interconnected IT and OT systems.

Many critical operating environments lack a formal systemic approach to risk assessments and processes, let alone the continuous visibility expected for critical services and high-value targets. These formal processes are desperately needed as rapid increases in access and interconnectivity dramatically increase risk. In these instances, policy guidance for transparency and standards of care can help drive improvements in risk management practices and at the same time foster innovation.

Thank you Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and Members of the subcommittee for your attention to these important issues and continued assessment of the work CISA is doing to keep Americans safe. I appreciate the work this committee is doing to elevate cybersecurity with bipartisan support. Thank you for the opportunity to testify today and I look forward to working with you to secure our Nation's cyber assets.

Chairman GARBARINO. Thank you, Mr. Edwards.

Members will be recognized by order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I now recognize myself for 5 minutes.

Ms. Sherman, Congress has increased CISA's budget from \$1.68 billion to \$2.9 billion in a couple of years. This is a big increase, even for a mature department. In your experience analyzing CISA more broadly since its inception, how has this increase in budget changed CISA's coordination assistance to the private sector?

Ms. SHERMAN. CISA, a few years back as it was stood up and then subsequently within a couple of years, undertook a reorganization. As a function of that reorganization, there was movement

³³U.S. Department of Commerce, "NOAA Inadequately Managed Its Active Directories That Support Critical Missions," <https://www.oig.doc.gov/OIGPublications/OIG-22-018-A.pdf>.

within the agency to kind-of reshape different offices and the roles that they played.

I think GAO, we took a look at the reorganization and at that time made a number of recommendations with respect to both coordination within CISA and coordination between CISA sector risk management agencies, State and local entities, and the private sector, and a number of those recommendations still remain open. So, in part, the additional budget that the agency has been receiving over time and how it's using those funds is really important as it's thinking about implementing not only the recommendations that we made, but being able to implement an effective organization to be able to address cybersecurity issues and infrastructure security issues, the different parts of its mission. But it remains a challenge because it has a lot of priorities on its plate and it also is at, I think, a difficult position with challenges with respect to the cybersecurity work force as well and being able to fill positions within the agency.

So we continue to monitor and watch the efforts that they have undertaken, but it's a daunting task in a lot of ways.

Chairman GARBARINO. I am not going to ask you for the list of recommendations they haven't fulfilled yet right now, but if you can get that to us, that would be great to have for the upcoming hearing we are going to have with Director Easterly.

Ms. SHERMAN. Absolutely.

Chairman GARBARINO. I just want to ask, has CISA's sector risk management agency capabilities matured at a similar rate to its budget or budget growth or?

Ms. SHERMAN. That's an interesting question. We cannot say for certain. Part of that is with our current review, or the review that we just recently completed and issued a report on, we attempted to try to get an understanding and spoke with all the sector risk management agencies to understand exactly what their maturity levels are and the extent to which they've been affected in their roles. But CISA doesn't have a very good handle on what that looks like. In fact, we heard that directly also from those agencies themselves. Part of the recommendation that we made was to be able to establish milestones and time lines to implement some of the efforts they have under way, one of which is being able to better understand and assess maturity and effectiveness of those agencies.

Chairman GARBARINO. Thank you very much.

Ms. Hogsett, I want to move over to you now. I am fortunate to not only to serve as Chairman of this committee, but as a member of Financial Services. I look forward to working with BPI and other financial service industry stakeholders on cyber issues.

But I want to ask you, how has the authorization—I think you mentioned a little bit in your opening statement—how has the authorization of new reporting requirements like the Cyber Incident Reporting for Critical Infrastructure Act, changed your sector's relationship with CISA?

Ms. HOGSETT. Thank you for the question.

So I think our relationship with CISA right now we have a very good relationship. CISA has been able to establish itself as a trusted partner not only for our sector, but a variety of others. So I think the voluntary information sharing that they have today will

be improved with implementation of the new Incident Reporting rules. But it is really important throughout that process that CISA look at the existing regulations. We within the financial sector have several that are all sort-of happening at the same time and impacting a firm in a really challenging way.

So just by way of example, we from a regulatory perspective have an incident notification rule to notify our primary regulators within 36 hours that a significant event may have occurred. Then the reporting to CISA after that with more detail within 72 hours, which the benefit of that will help CISA have a better view of the threats and what's happening out there to improve its ability to support critical infrastructure. So we very firmly believe that this is important work. But then for us now and other companies who fall under the Securities and Exchange Commission, we are also then potentially facing about a day later a public notification of those same incidents and challenges which will undermine some of the work that has been done by our regulators and by CISA.

So we think that CISA is in an important role to really move forward and get this right. There is a requirement to streamline those requirements which we stand ready to assist and engage with them to help make that happen. It will be a key challenge and I think most importantly, the fact that CISA is not a regulator will be helpful in this effort.

Chairman GARBARINO. I appreciate that.

My time has expired, so I now call—I will start with other questions. OK, sure.

I now recognize Representative Carter for 5 minutes.

Mr. CARTER. Mr. Chairman, thank you very much, Ranking Members—Member rather. Thank you all for being here.

Ms. Hogsett, in your submitted testimony you emphasize that in order for there to be successful implementation of CIRCIA, it is critically important that these agencies harmonize for their reporting requirements to optimize protection and response, a streamlined coordination. Let's take a step back here and see how private-sector entities, specifically the banking sector, for which you are an expert, can speak to how the private sector assesses cyber risk internally, how they ensure the risk assessments that they utilize are objective, independent, and reliable.

Ms. HOGSETT. So financial institutions have a variety of different requirements that we need to meet with our regulators. So we have—just at the Federal level we have, for instance, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, all of whom look at cyber risk management practices, they look at third-party risk management, they look at how you architect your systems for operational resilience. So what firms do internally is we have actually what we refer to as a three lines of defense model, in essence, where you have your front-line cyber defenders doing a lot of work, you will have a second line, which is independent of that and will look at those policies and programs and challenge them internally, and then you have a third line internally, which is internal audit, which will then do all of that same work again from yet another independent perspective. Then we have for the largest institutions, they have an on-site examiner sitting in their headquarters work-

ing with them day in and day out. So there was an on-going oversight relationship there. So it's a very complex interwoven set of rules and requirements that we work with every day.

Mr. CARTER. What input do you get from outside with that, do you?

Ms. HOGSETT. So firms will bring in outside security consultants to do additional review, things like penetration testing, to sort-of test how good their defenses are from a variety of different angles. They will assess themselves independently against things like the NIST Cybersecurity framework. That happens alongside and in addition to the regulatory oversight that happens. All of that gets reported up to senior management and the board of directors level for regular conversation and action.

Mr. CARTER. So with technology moving as fast as it does, as you evaluate the risk, the pace at which the bad guys, if you will, are getting technology to undermine systems, how are we doing with keeping pace with the outside forces that we have to manage?

Ms. HOGSETT. It is absolutely a challenge and it is one reason why you need to ensure that any rules put in place are flexible and can be adaptable over time, because the threats do change. So we have layered defense models. Zero trust was mentioned earlier, that's one of multiple things that we will employ. The challenge there is in the regulatory structure to be nimble and get that right and not dictate that something has to be protected a certain way or with a certain type of technology. Because I think that's where you can run into challenges. You need that flexibility and that ability to be nimble in how you're protecting your organization.

Mr. CARTER. Thank you.

Ms. SHERMAN, presently FISMA requires annual audits of Federal Government entities to conduct cybersecurity compliance and risk assessment. Their inspector general or an independent auditor can conduct this for them. This ensures reliability of the information that they share with CISA, it ensures accountability. What can be done to ensure that this reliability and accountability with private-sector entities as information-sharing reporting requirements expand?

Ms. SHERMAN. With respect to the ability to ensure reliability of the data and information sharing, I think it's important. We've been talking today so far about the partnerships and the relationships not only between CISA and the sector risk management agencies but between the sector risk management agencies and all of the other critical infrastructure entities that they rely on the owners and operators, the SLTTs and others in the private sector. That partnership is critical in order to be able to bring and be able to receive reliable information.

But that comes from a place of trust, which can be challenging sometimes, to be able to acquire that type of information on a regular basis and again, have that flow of information in order be able to really kind-of understand what actions are being taken and also how the specific sectors are carrying out their work in order to be able to improve cybersecurity.

The partnerships working to strengthen those partnerships would help to encourage trust and would contribute to building the

information sharing or improve the information sharing in order to have more reliable data.

Mr. CARTER. Thank you.

Chairman GARBARINO. The gentleman yields back.

I now recognize my friend from Florida, Mr. Gimenez for 5 minutes questioning.

Mr. GIMENEZ. Thank you, Mr. Chairman.

As the Chairman of the committee's Transportation and Maritime Services Subcommittee, I have a distinct interest in transportation and maritime cybersecurity.

So in light of what happened in the Colonial Pipeline a couple of years ago, Mr. Bagley, have you seen any improvements in our posture, in our ability to stop these kind of attacks, ransomware, and others in the future in our pipelines?

Mr. BAGLEY. Thank you for the question.

Vast improvement from a technological standpoint in terms of the capabilities available, as well as the ability for those cyber have-nots to be able to acquire sophisticated defensive cybersecurity technologies in recent years. However, there is still a great disparity between those who are deploying these technologies, like endpoint detection and response, zero trust architecture, identity protection and whatnot and those who are not.

However, one of the things that we've seen as a positive development in recent years has been the call to action from Executive Order 1428, which calls out the very same cybersecurity technologies that are successful by many large entities in the private sector. In CISA's efforts to expand use of these technologies within Federal Government as well as within critical infrastructure entities, is one where we're still in the early stages, but so far we are seeing the technology proliferated more. I think that that's important because right now we're really in a war of innovation against adversaries. Adversaries traditionally had to have some sort of technological ability themselves and now we're in an era in which literally there are access brokers that sell credential access to victim organizations, we're in an era in which there is not only ransomware, but ransomware as a service. Meaning a threat actor does not actually have to develop the ransomware themselves or even operate it in many cases in order to deploy it and target it. So that's where the threatscape has changed in recent years and yet the defensive capabilities are fortunately improving.

Mr. GIMENEZ. So are you saying that you have, like, rent-a-cyber attack?

Mr. BAGLEY. That's correct, Congressman. It is now possible not only for ransomware, but for other types of services, such as if a threat actor wants to do data leak extortion whereby they infiltrate a victim organization, exfiltrate data, hold it ransom, and perhaps leak some of it subject to a ransom or purely for embarrassment and destruction of that organization's reputation, they're able to do so without actually being able to code themselves or even have the infrastructure because they can rent it in the same way that we use different services today or the same way we pay for our monthly services as consumers.

Mr. GIMENEZ. Where are the vast majority of these companies for rent? Where are they located?

Mr. BAGLEY. These threat actors are located throughout the world. Our reporting certainly shows that naturally there are a lot of threat actors based in Eastern Europe and in Russia who run some of these ransomware-as-a-service operations. But they're proliferated throughout the world.

Mr. GIMENEZ. The ones that are operating out of Russia, is it your thought that they are wink, nod, et cetera? They are allowed to operate in Russia by the Russian government? If the Russian government wanted to shut them down, could they?

Mr. BAGLEY. From what we've seen, we've certainly seen use of nation-states, including Russia, utilizing and leveraging the capabilities of Ecrime actors to carry out state goals and means. That's certainly the case with Russia.

Mr. GIMENEZ. What about China?

Mr. BAGLEY. China traditionally targets just about every sector. Recently, we released our Global Threat Report and in it what we saw from the data that we've analyzed is that China has targeted just about every sector, not only in the United States, but also more broadly around the globe for its aims.

Mr. GIMENEZ. Does anybody attack China?

Mr. BAGLEY. I imagine there are others who might be able to answer that on behalf of the U.S. Government, but certainly cyber attacks are rampant everywhere.

Mr. GIMENEZ. Look, in a nuclear age, we have mutually assured destruction, which kind-of kept the peace. So do you find that the Russians and maybe the Chinese and those bad actors are operating with impunity? Is that your opinion?

Mr. BAGLEY. Well, what we see is that you not only have nation-state actors to contend with in the modern era, but you also have Ecrime groups which will run by their own rules, as well as hacktivist organizations, which will be motivated by specific aims related to issues.

Mr. GIMENEZ. OK, thank you very much. My time is up. Thank you.

Chairman GARBARINO. The gentlemen yields back.

I now recognize Mr. Menendez for 5 minutes for questioning.

Mr. MENENDEZ. Thank you, Mr. Chairman, for communing us here today, thank you to our witnesses, and to our Ranking Member.

In recent years, communities across the country have been impacted by the spike in ransomware attacks. Last year, as part of the bipartisan infrastructure law, Congress provided \$1 billion over 4 years in new grants to improve the cybersecurity of State and local governments.

Mr. Edwards, as State and local governments seek to utilize this new strength in their cybersecurity, how should they prioritize their cybersecurity investments? Do you believe additional support for State and local cybersecurity will be necessary going forward?

Mr. EDWARDS. Thank you very much for your question.

In general, my perspective is that we should look at those systems that have the highest risk to society. In my perhaps not-so-humble opinion, that usually falls to these operational technology systems that operate things like power grids, pipelines, and other infrastructure that's critical. I think that both the U.S. Federal

Government and State and local governments have done a reasonably good job of prioritizing what I would call information technology, or IT, security over the years, right. But we certainly are behind in investing in protection of these critical systems that are investor control system applications or other operational technology applications.

I think when it comes to funding for the States, that seems to be a good mechanism that we use in our country to ensure that the State and local governments have the adequate types of programs that they need to run. I think that cybersecurity is going to benefit, for example, from the cybersecurity language that was inserted into the Infrastructure and Jobs Act and things like that.

So I see some positive trends with regards to funding at the State and local level. They do need to, I think, move beyond—some of the other witnesses talked about going in to do an assessment of a facility or a system. We used to do that kind-of on a periodic basis. You'd go in and hire a consultant and do an assessment once a year or once every 3 years and it would satisfy your compliance requirements. I don't think that we can live in that world anymore. We need to move to continuous visibility so that we know what's happening on those networks at all times, rather than waiting for somebody to come in in 2 years to tell us that we were hacked a year-and-a-half ago.

Thank you for your question.

Mr. MENENDEZ. No, I appreciate your answer.

Mr. Bagley, you have mentioned a couple of times the cybersecurity have and have-nots. We are still clearly trying to come up with a cohesive system to address our greatest, highest-risk assets. Talk to us about some of the challenges in scaling up cybersecurity protections for all different segments of our industries, economy, folks of different size who want to implement cybersecurity best practices, but No. 1, have an allocation of resource challenge and No. 2, I think the director also mentioned the cybersecurity work force. Are we training enough people?

So, sort-of a two-part question, but would love to get your thoughts on those items.

Mr. BAGLEY. Thank you for the question.

One of the recent positive developments that we've seen is that managed service providers are able to augment existing security programs or sometimes completely replace security in an organization that would not otherwise be able to afford to have its own security program. One of the advantages of modern managed service providers is that managed service providers can bring the very same sorts of cybersecurity best practices that are currently called upon in the U.S. Government today, such as endpoint detection and response as well as proactive threat hunting.

One of the things that managed service providers can bring is scale, meaning that a small organization that might not be as well-resourced, a cybersecurity have-not, could easily utilize a managed service provider instead of building its own security program, whereas if we look back not that many years ago when we looked at the cybersecurity haves and have-nots, the have-nots would not have the capabilities of building their own security program. It

might not have an alternative, and today there exists an alternative.

I think that's something that can be highly effective and I think that that can be highly effective too when we look at the SLTT space and we look at the broader Federal Government space and think about shared services models. So for example, with CISA, with its newer powers as a CISO, CISA is able to bring to bear cybersecurity capabilities to Government agencies that traditionally have lacked the same resources as their larger counterparts. This trend is one that we see in the private sector as well.

Mr. MENENDEZ. Appreciate it. Four seconds. I will yield back the remainder of the time, but do want to hopefully eventually get everyone's thoughts either in writing, but about the challenges that we are seeing from a work force perspective and what we could at the Federal Government to ensure that we are aiding and developing that work force so we can meet these challenges with a robust system.

I do apologize for going over, Chair.

Chairman GARBARINO. Not a problem.

The gentlemen yields back.

I now recognize my friend from Mississippi, Mr. Ezell, for 5 minutes of questioning.

Mr. EZELL. Thank you, Mr. Chairman.

As a former sheriff with decades of experience fighting to protect the people and communities in Brown, South Mississippi, I am eager to join the Cybersecurity and Infrastructure Protection Subcommittee to combat the threat of the malicious cyber actors.

Mr. Bagley, you have talked today about how JCDC aims to connect private industry with Federal partners such as DoD, the intelligence community, and law enforcement. In your role. Can you describe how JCDC interacts with local law enforcement?

Mr. BAGLEY. Thank you for the question.

From my perspective as a stakeholder in JCDC, from what we've seen is we've seen it's very issue-oriented. So, for example, if there is an issue, such as certainly what we saw come to bear with Log4j, where CISA was rallying all members to come together, bring information, share information, and consume information, we've certainly seen involvement at all level of government and what—where JCDC can share information. Specifically, in terms of how local law enforcement is prioritized within the apparatus of JCDC, I would defer to CISA leadership, but we've certainly seen involvement across industry and across government in JCDC.

Mr. EZELL. Do you think the balance between CISA's asset response and the FBI's threat response activities has been successful?

Mr. BAGLEY. I think that there are certainly different missions at play. One of the strengths of JCDC is that it's not trying to necessarily define a brand-new mission for all stakeholders, but instead be a centralized place where stakeholders with different missions can come and cooperate. So naturally, the FBI, having an interest in law enforcement and focusing on seeking justice for victims, is one where the FBI obviously has ad hoc relationships with partners. But I think the strength is the FBI can bring its expertise to JCDC and similarly JCDC and its mission as a civilian

agency focused on cybersecurity for regulated entities as well as a convener of public and private partnerships, can utilize that expertise and the expertise of others. I think that naturally strengthens the dynamic, especially if we think about having the system in place in the events of big events, such as the Log4shell, Log4j event.

Mr. EZELL. Thank you.

I want to move on the importance of leveling the playing field to ensure there is active participation from a mix of large- and small-sized companies. What can CISA do to be more business-friendly in order to increase participation?

Mr. BAGLEY. I think that as JCDC grows in its structure, I think it's important to put into place different structures so that as it expands there can be different working groups that might be well-suited for organizations of different sizes or organizations focused on different topics in general. So I think that's one way.

I think also CISA, what we've seen in recent years is CISA has certainly demonstrated its ability to serve as a clearinghouse for certain types of information and proliferate that information to the community. I think that's another one where there is an awareness component in addition to, of course, a resource component when we think about the cybersecurity haves and the have-nots. I think CISA has an important role to play and that it has been playing in recent years with regard to raising awareness not only about cybersecurity threats, but also cybersecurity resources and capabilities. I would expect that that would continue to grow and expand and be for the benefit of smaller entities.

Mr. EZELL. Thank you for your answer.

Mr. Chairman, I yield back.

Chairman GARBARINO. The gentleman yields back.

I now recognize the Ranking Member for 5 minutes of questioning.

Mr. SWALWELL. Great.

Ms. Sherman, GAO has made a number of recommendations related to how CISA can improve its support to critical infrastructure and sector risk management agencies. Can you just prioritize those recommendations?

Ms. SHERMAN. What I would want to do is I would want to highlight actually in our recently-issued report from last month, we included a section in the report where we outlined all outstanding open recommendations that we had made to sector risk management agencies, specific to critical infrastructure, of which there are many. There are challenges in prioritizing those recommendations, but what we would say with respect to CISA is that it's important for CISA to take in the near-term, a set of following actions. We think that there's gaps in guidance that the agency could provide. In part, this has to do with the national plan and being able to update the national plan and the sector-specific plans. We understand that there's a pause essentially that's going on with a lot of the sector management agencies because of the PPD-21 rewrite, but we think that CISA can be taking action in the interim to position themselves to be able to update those plans expeditiously once the rewrite is completed.

We also feel that there could be opportunities, of course, to be able to standardize the set of approaches in order to really understand—harking back to what we were talking about a little bit before, how mature and how effective these agencies are in their efforts. So we would want CISA to prioritize being able to collect that information.

I think finally, that feedback loop of really being able to understand what the relationships are like between the sector and all of their partners, look at those existing partnerships, getting a recognition of what's working and perhaps what's not and where improvements can be made.

Mr. SWALWELL. Great.

Exactly the cogent answer I would expect from a fellow government and politics degree holder from the University of Maryland.

Ms. SHERMAN. I noticed that. Thank you.

Mr. SWALWELL. Go Terps.

Ms. SHERMAN. Go Terps.

Mr. SWALWELL. Mr. Edwards, can I also ask you, JCDC has a new dedicated unit focused on industrial control system security. What should we expect to see from the JCDC ICS?

Mr. EDWARDS. Yes, thank you for your question.

It certainly is a fairly new initiative that the JCDC has taken on to build a dedicated group, or a tiger team, I guess, of sorts, for industrial control systems. I think I agree with my other witnesses here that have stated that in order to be successful, the JCDC is going to have to be able to break some of these topics down in all discussions, rather than having every discussion happen with the entire group, right. This is going to be a scalability challenge of sorts, right, where we can't solve every problem with everybody in every room, we have to break these into smaller digestible pieces. So I believe that we will see a lot of good information come out of the JCDC ICS group or OT group.

The other thing I believe that is important that CISA can work on here is with regards to the CIRCIA, incident risk reporting. That information, when it comes in and is analyzed, needs to be disseminated to technology service providers such as represented here, so that we can build the coverage to detect those threats or those weaknesses in those systems in a timely fashion. So we're eager to work with CISA and the JCDC construct on how to best make this into a machine-readable, real-time, information-sharing platform.

Mr. SWALWELL. Great.

Building off of Mr. Menendez's point at the end of his questioning, Mr. Edwards, what is your assessment of the current state of our Nation's OT cybersecurity work force? What can the Federal Government do to ensure that OT cybersecurity skills are prioritized in any work force development training?

Mr. EDWARDS. Yes, it's a very complex problem, right. So you have sort-of this overlap between cybersecurity professionals who typically come from business colleges or degrees, they've come up through the business side of a corporation or an enterprise, and the operational technology people such as myself come from an engineering background, and many of the engineering schools, the curricula is such that there's no more room to put in there to talk

about cybersecurity, they're going through the physics and the basics of an engineering discipline. So I think that in some cases, the educational institutions themselves are somewhat challenged with how to put this in.

Another thing that I believe is that we have a little bit of a chicken or the egg problem, right. As the NSTAC report stated, we believe that the United States actually has the technology and actually has the knowledge base to solve these problems. We just haven't manifested it at scale. So I think things like the NICE Framework, that are coming out with work force development, that are focusing more on OT, are good initiatives, and we should continue to invest there.

Mr. SWALWELL. Great. Thank you.

I yield back.

Chairman GARBARINO. The gentlemen yields back.

I now recognize Ms. Lee from Florida for 5 minutes of questioning.

Ms. LEE. Thank you, Mr. Chairman.

In my former role as Florida's secretary of State elections, I worked extensively with CISA in securing our elections infrastructure. CISA was a key partner to State and local elections officials. I look forward to our work together to ensure that we are advancing cybersecurity across all of the critical infrastructure sectors.

My questions, I would like to begin with you Ms. Sherman, and specifically in the subject of elections and election security, since it has been designated part of our critical infrastructure. First this, because CISA has become such an important part of assisting and aiding State and local election officials, would you describe for me some of the things that you think are working well there? Or if there are other places where CISA needs additional support or resources from Congress to make sure that you can do that job effectively?

Ms. SHERMAN. So the election security sector is in some respects, I think, just a little over 5 years old and the subsector-specific plan that guides it also is somewhat outdated. So for the last election, guidance was put out by the Subsector Coordinating Council to ensure that there was a more kind-of relevant, timely understanding of efforts and to be able to kind-of fill that gap—or in the absence of an updated plan.

In the recent review that we carried out, we did hear from individuals that we spoke with, officials that we spoke with, and actually as part of the priorities work for last year that we had carried out with CISA, that the agency has done a good job of sharing election-specific information that's general, so kind-of Nation-wide threats to consider, but that there was an interest and a desire for and a need for more locally-tailored information. So the information they had was limited along those lines and they were looking for more.

We also heard that with respect to day-of capabilities and ability to have kind-of a quick response for incidents that occur, that CISA should build their capacity along those lines as well.

Ms. JACKSON LEE. You just touched on something that is another area of interest for me, and that is specifically the incident response capability. At present is CISA able to meet the call when

that is coming in or are you receiving a larger number of requests for that more hands-on critical incident response than you can provide?

Ms. SHERMAN. I can only speak to the conversations and the information that we had and collected during the course of our specific review. But that is something that we had heard from election officials, that there was a concern that the agency did not necessarily have those capabilities in place to be able to quickly address an incident that might occur, and they were looking to work and partner with CISA to help build that capacity.

Ms. JACKSON LEE. Do you have any thoughts—another feature I think of the approach to securing infrastructure is a need for CISA to work collaboratively with other Federal law enforcement partners. Any feedback for us about how that is going or any input about how the relationships with other Federal law enforcement partners are productive or could use additional enhancements?

Ms. SHERMAN. We didn't collect any information specific to the relationship between law enforcement and the election in the course of our review, so I can't speak in detail to that. But I can talk to the fact that local officials also pointed to limited awareness and conversations or dialog at the Federal level and that they wanted to see more of that as well.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

I yield back.

Chairman GARBARINO. The gentlelady yields back.

I will now move into a second round of questions.

I recognize myself for 5 minutes of questioning.

Chairman GARBARINO. Ms. Hogsett, the Biden administration released its new National Cybersecurity Strategy. The strategy rightly emphasizes the need to harmonize regulations to avoid duplication and overly burdensome requirements, but the implementation plan will be key to demonstrating how they actually plan to achieve harmonization.

What sorts of aspects will you look for in the eventual implementation plan to deconflict requirements?

Ms. HOGSETT. We've actually started discussing implementation with the National Cyber Director's Office because this is such a critical issue for us to get right.

The challenge that we in financial services face, and certain other sectors will as well, is the fact that most of our regulators are independent. So no matter what CISA may put out, it's still up to them, in essence, whether they will follow that and align. We are lucky that three of our primary regulators collaborate with each other and have done a lot of work to sort-of streamline and align their requirements where they can. I know they're participating in some of these Government conversations right now, but that's like 3 out of 9, for instance, that we have to work with across our sector.

So it's really important for us. Actually something where Congress could help, I think is encourage when it comes to cybersecurity. Given the importance of getting it right, given the work force challenges that we've just been discussing, we are frankly hearing increasing concern from our member firms that the regulatory and Government reports are placing a strain on the existing staff. We

have some figures that folks are spending anywhere from 30 to 40 percent of their time not focused on the day-to-day protective mission that is so important that they need to do instead, they're focusing on compliance matters. That's a challenge and that can't continue as we layer on new and additional requirements, which, each on their own, can be very beneficial, but when you layer them together, it's a real challenge.

So our hope and the discussion that we've started having with the White House is how can we get to sort-of this idea of regulatory reciprocity where one regulator might accept another's work, where can you create even an 80 percent solution where you align on the core things that various regulators and Government agencies would want, and then you're just doing some additional pieces above that. That's the conversation that we're looking forward to contributing to and is critically important for us.

Chairman GARBARINO. Appreciate that answer.

Then I know everybody talks about we are going to have a separate hearing just on work force if we need to.

I did want to ask you this before when we were talking about the incident reporting, the legislation and the rule-making that is going on, with the implementation we have heard about how there is no private-sector work force, there are a lot of people. Does CISA have the proper amount of work force for a proper implementation of the incident reporting language, in your opinion?

Ms. HOGSETT. It's a very good question. I'm not sure. What we would hope to see at this point is one or two people are in an office set-up that we can go to on a regular basis to have a dialog. That's what we do with our regulators. We would like to see CISA set that up. It was good that they put out a request for information. We certainly responded to that. They did a series of sort-of listening sessions. But there are so many—I mean, as you know, the 16 critical infrastructure sectors, each of them is so unique. For those that have regulations, even those regulations, whether you're talking from an OT or an IT perspective, they can be very different. So we think and would love support to have CISA set up more on-going dialog so we can kind-of help them jointly problem-solve to make sure they get this right.

Chairman GARBARINO. I appreciate that answer.

I just have one final question for Mr. Bagley.

I understand CISA, through the JCDC plans to update the National Cyber Incident Response Plan. In your view, where does CISA's role start and stop in terms of incident response and support of the private sector?

Mr. BAGLEY. Well, I think we have to think about what the stakes are today. What we've seen in recent years with some of the high-profile systemic cyber attacks that JCDC in fact has responded to, like the Log4j incident, is that they could have been so much worse. So one of the things we have to anticipate, and that should certainly be considered in that planning, is how we as a Nation would deal not just with currently-designated infrastructure, but how would we deal with some sort of victim that in a specific context is fundamentally important and that them being hit by, say, disruptive or destructive ransomware would be catastrophic for the country. That's where it's important to be able to have that

flexibility to respond, to rally both the public and private sector together to ensure that we have the capacity.

One of the things that we see in the private sector is that the way complex multinational organizations or large U.S. organizations respond is by ensuring that they have playbooks ahead of time as well as the actual resources on retainer, such as incident response firms. I think for CISA to be able to scale up, they must consider not only their own organic capacity, but those of private partners as well.

Chairman GARBARINO. Thank you.

I am out of time.

I now recognize the Ranking Member, Mr. Swalwell, for his second round of 5 minutes.

Mr. SWALWELL. Great. Thank you, Chair.

Ms. Hogsett, wanted to get the benefit of your wisdom on a recent banking crisis that especially hit my area, that is Silicon Valley Bank. We are still taking an MRI to this to see exactly what happened. But one thing that was different in this “run on the bank” than any other was the speed at which it happened. Of course, in the digital age, the speed at which you can move money is different than having to wait on the phone or wait in line in past crises. But we are also looking at the role that on-line chatter and on-line panic and rumors led to this run on the bank. I have sent a letter to the SEC with my colleague Brad Sherman asking them as well to look at whether there was a short that took place that was followed by any sort of on-line manipulation of the market.

But have you all at the Bank Policy Institute, just in the realm of cyber, looked at whether there was a potential cyber incident around the run on Silicon Valley Bank?

Ms. HOGSETT. We have not. I think it's early stages, so I would be getting ahead of, I think, all of us who want to get to a better sense for what happened and where were the deficiencies.

It's an interesting point, though, around the role of social media. We actually saw this with Colonial Pipeline, to provide another example, where the initial reports were that there were going to be sufficient gas supply. But when it hit the news, human behavior kicked in and you had in essence, like what we saw with the run on a bank, you had a run on gas stations. So it's a new era where we need to think about how do we communicate and involving social media. Treasury is our sector risk management agency and we have actually recently re-looked at our communications plans, including among large banks, the trade associations, our information-sharing analysis center, and Treasury's role with the regulators as to at various points in time based on certain scenarios when might it make sense for the Treasury Secretary to put something out and do exercise that. So can't respond specifically to the SVB example, but we are carefully watching that, so.

Mr. SWALWELL. Did that incident at Silicon Valley Bank, though, did it give you concern that a foreign adversary or a hacktivist could seize on a bank crisis like that and use on-line information or disinformation to try and manipulate a result or to cause further chaos?

Ms. HOGSETT. We did not see indicators of that with this recent issue. However, the potential for mis-, dis- and mal-information is

very real and that is something that CISA has done some work on. We've contributed to that. It is something that firms need to consider and our firms internally for their own response playbooks think about those dynamics as they plan for when do you notify your board internally, if it hits the media, what then? It makes the response that much more complex, quite frankly, to think about it that way.

Mr. SWALWELL. Great. Thanks, Ms. Hogsett.

Mr. Bagley, how can CISA give JCDC the structure and clarity it needs to sustain momentum over time and how can we do that without losing the flexible, agile features that make it successful today?

Mr. BAGLEY. Thank you for the question.

I think one of the things that's very important is for CISA to ensure that as JCDC grows, it's growing with intention, with deliberation, and with a bit more structure. So that's not to say that there's one ideal size for JCDC. Certainly there are strengths to the fact that there are more members bringing more capabilities, but the more that CISA can actually structure with purpose and with theme different working groups, I think that can lead to certain advantages and certain efficiencies. Just as any organization that's going from start-up to scale needs to adjust and reorganize, I think that is the case with JCDC today. So it would be more structure and more working groups. Great.

Mr. SWALWELL. Great.

Chairman GARBARINO. Thank you very much.

The gentleman yields back.

I thank the witnesses for the valuable testimony and the Members for their questions. We got a lot of information today and we are going to have to digest this and hopefully get some answers from Director Easterly when she comes in. I talked about we are going to have, I think, a future hearing on work force. I think we should have one on IT-OT. I mean, there is some really important stuff that was brought up to you today.

The Members of the subcommittee may have additional questions for the witnesses and we would ask the witnesses to respond to these in writing.

Pursuant to the committee rule VII(D), the hearing record will be held open for 10 days.

Without objection, this subcommittee stands adjourned.

[Whereupon, at 11:21 a.m., the subcommittee was adjourned.]

A P P E N D I X

QUESTION FROM CHAIRMAN ANDREW R. GARBARINO FOR TINA WON SHERMAN

Question. From GAO's perspective, are you satisfied with the level of innovation seen from CISA and its industry partners as they evolve to meet advanced persistent threats to Federal agency IT systems? Or are we still doing things the same way as 5 years ago?

Answer. Response was not received at the time of publication.

QUESTION FROM CHAIRMAN ANDREW R. GARBARINO FOR MARTY EDWARDS

Question. The NSTAC report discusses the many benefits as well as risks of IT and OT convergence. Will we always be faced with this trade-off between efficiency and security? Are there any steps organizations can take to mitigate the security risks while still enjoying the benefits of digital transformation?

Answer. Response was not received at the time of publication.

