MOBILIZING OUR CYBER DEFENSES: MATURING PUBLIC-PRIVATE PARTNERSHIPS TO SECURE U.S. CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

APRIL 6, 2022

Serial No. 117–51

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

48–050 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

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

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

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

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

MOIRA BERGIN, *Subcommittee Staff Director*
AUSTIN AGRELLA, *Minority Subcommittee Staff Director*
MARIAH HARDING, *Subcommittee Clerk*

CONTENTS

Page

STATEMENTS

The Honorable Yvette D. Clarke, a Representative in Congress From the State of New York, and Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation:
Oral Statement 1
Prepared Statement 3
The Honorable Andrew R. Garbarino, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation:
Oral Statement 4
Prepared Statement 5
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security:
Prepared Statement 6
The Honorable John Katko, a Representative in Congress From the State of New York, and Ranking Member, Committee on Homeland Security:
Oral Statement 30
Prepared Statement 31
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Prepared Statement 6

WITNESSES

Mr. Eric Goldstein, Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security:
Oral Statement 9
Prepared Statement 11
Mr. Robert K. Knake, Deputy National Cyber Director for Strategy and Budget, Principal Deputy National Cyber Director (Acting), Office of the National Cyber Director, The White House:
Oral Statement 16
Prepared Statement 17
Ms. Tina Won Sherman, Director, Homeland Security and Justice, U.S. Government Accountability Office:
Oral Statement 20
Prepared Statement 21

FOR THE RECORD

The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Article, crn.in, April 5, 2022 46
Article, *TechCrunch,* December 10, 2021 48
Article, *New York Times,* July 29, 2021 49
Article, *Washington Post,* March 22, 2022 50

APPENDIX

Questions From Chairman Bennie G. Thompson for Eric Goldstein 55
Questions From Chairwoman Yvette D. Clarke for Eric Goldstein 56

Page

Questions From Honorable Sheila Jackson Lee for Eric Goldstein 57
Questions From Ranking Member John Katko for Eric Goldstein 58
Questions From Honorable Ralph Norman for Eric Goldstein 58
Questions From Chairman Bennie G. Thompson for Robert K. Knake 59
Questions From Chairwoman Yvette D. Clarke for Robert K. Knake 60
Questions From Honorable Sheila Jackson Lee for Robert K. Knake 60
Question From Honorable James R. Langevin for Robert K. Knake 60
Question From Ranking Member John Katko for Robert K. Knake 61
Questions From Chairwoman Yvette D. Clarke for Tina Won Sherman 61
Questions From Honorable Sheila Jackson Lee for Tina Won Sherman 62

MOBILIZING OUR CYBER DEFENSES: MATURING PUBLIC-PRIVATE PARTNERSHIPS TO SECURE U.S. CRITICAL INFRASTRUCTURE

Wednesday, April 6, 2022

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

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

Present: Representatives Clarke, Jackson Lee, Langevin, Slotkin, Garbarino, and Harshbarger.

Also present: Representative Katko.

Chairwoman CLARKE. The Subcommittee on Cybersecurity Infrastructure Protection and Innovation will be in order. The subcommittee is meeting today to receive testimony on mobilizing our cyber defenses, maturing public-private partnerships to secure U.S. critical infrastructure. Without objection, the Chair is authorized to declare the committee in recess at any point.

Good morning, everyone. I would like to thank the witnesses for participating in today's hearing on how we can build a better, more robust framework for protecting our Nation's most critical infrastructure.

As some of you may know, this is not my first time serving as Chair of this subcommittee. The last time I presided over this panel was in 2011 during the 111th Congress. At that time, the Obama administration was working to develop and strengthen many of the policy frameworks we know today, which place DHS at the center of a voluntary, public-private partnership to promote strong cybersecurity across sectors. I have also served as Ranking Member of this subcommittee, working across the aisle to codify many of the those voluntary frameworks and information-sharing regimes. With that backdrop in mind, and with all due respect to the hard work that has been done, I think it is time to be candid about the limits of these voluntary partnerships and authorities.

When I rejoined the subcommittee last year, we were reeling from a massive supply chain attack that gave Russia months of access to some of the most critical networks. We have had to watch from the sidelines as our critical infrastructure, from hospitals and

meatpackers to manufacturers and pipelines, have been crippled by ransomware attacks.

For the past few months, Federal officials, like the ones on our panel today, have been working around the clock to help private-sector owners and operators understand that they may soon be the target of retaliatory Russian cyber attacks. But we have no way of knowing if these operators are hearing those warnings and taking action to shore up their defenses. From where I am sitting, one thing is clear: The United States desperately needs to revamp the playbook it uses for critical infrastructure cybersecurity.

We know that our Nation's critical infrastructure is vulnerable to cyber attacks and the Federal Government has resources it can bring to bear in closing security gaps, but we have been reluctant to make the private sector come to the table. The Federal Government also has the bird's-eye view vantage point to track cyber threats in one sector, then use that information to connect the dots on other malicious activities across sectors. But until recently, we haven't been willing to require critical infrastructure operators to provide that information to CISA.

While the Biden administration has taken some aggressive steps to partner with the private sector in new, innovative ways, we have a long way to go and some big challenges ahead. Fortunately, we know that Congress can still come together to tackle big challenges. Most recently, enacted cyber incident reporting legislation is proof of that.

To get this legislation across the finish line, we had to work across the aisle and with our partners in industry to find a solution that would give CISA the visibility it needs without needlessly burdening victims of a cyber attack. We found a smart, compromise solution there and I have faith that we can do it again here.

My goal today is to get testimony that will help us answer the question what is next? How do we continue to mature the way the Government engages with critical infrastructure, particularly those entities that are the most critical of the critical or, as the Cyber Solarium Commission put it, our systemically important critical infrastructure, or SICI? Do we have a good sense of where these SICI assets are, who is operating them, and how they are being secured?

Once we know who and what they are, what benefits should the Federal Government provide for these entities to help them protect themselves? Importantly, what burdens should they be asked to shoulder in light of their importance to our National security?

This latter part is key. It is not enough to simply identify these most critical entities nor is it consistent with what the Solarium Commission proposed. We need to be able to answer the question what do these companies need to do as a result of their designation? What does the Federal Government need to do for them, whether that is better access to threat intelligence, enhanced operational collaboration, or other priority access to resources and support?

It is not enough to simply make a list of our most vital assets. We need to know how we are going to operationalize it. We have tried this exercise in list-making before, from the National Asset Database to the designation of Section 9 companies. Some of these efforts were costly and labor-intensive, and none of them ever real-

ly lived up to the security gains originally envisioned. The through line for all these efforts is that at some point, Congress or the administration, or both, decided to punt on the question of benefits and burdens. That will not happen on my watch.

I would like to recognize Representative Langevin and Ranking Member Katko for championing this issue and I look forward to continuing to work with them to craft this legislation in a way that avoids the pitfalls of the past. This hearing is an opportunity to help move the ball forward and hear how the administration is thinking about these challenges and working to upgrade its cybersecurity playbook.

I thank the witnesses for participating today and I look forward to a robust discussion.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

APRIL 6, 2022

I would like to thank the witnesses for participating in today's hearing on how we can build a better, more robust framework for protecting our Nation's most critical infrastructure. As some of you may know, this is not my first time serving as Chair of this subcommittee. The last time I presided over this panel was in 2011, during the 111th Congress.

At the time, the Obama administration was working to develop, and strengthen, many of the policy frameworks we know today—which place DHS at the center of a voluntary, public-private partnership to promote strong cybersecurity across sectors. I've also served as Ranking Member of this subcommittee, working across the aisle to codify many of those voluntary frameworks and information-sharing regimes.

With that backdrop in mind—and with all due respect to the hard work that's been done—I think it's time to be candid about the limits of these voluntary partnerships and authorities.

When I rejoined the subcommittee last year, we were reeling from a massive supply chain attack that gave Russia months of access to some of our most critical networks. We've had to watch from the sidelines as our critical infrastructure—from hospitals and meatpackers to manufacturers and pipelines—have been crippled by ransomware attacks.

For the past few months, Federal officials—like the ones on our panel today—have been working around the clock to help private-sector owners and operators understand that they may soon be the target of retaliatory Russian cyber attacks. But we have no way of knowing if these operators are hearing those warnings and taking action to shore up their defenses. From where I'm sitting, one thing is clear, the United States desperately needs to revamp the playbook it uses for critical infrastructure cybersecurity.

We know that our Nation's critical infrastructure is vulnerable to cyber attacks—and the Federal Government has resources it can bring to bear in closing security gaps. But we've been reluctant to make the private sector to come to the table. The Federal Government also has the bird's-eye view vantage point to track cyber threats in one sector, then use that information to connect the dots on other malicious activity across sectors. But until recently, we haven't been willing to require critical infrastructure operators to provide that information to CISA.

While the Biden administration has taken some aggressive steps to partner with the private sector in new, innovative ways—we have a long way to go, and some big challenges ahead. Fortunately, we know that Congress can still come together to tackle big challenges. My recently-enacted cyber incident reporting legislation is proof of that.

To get this legislation across the finish line, we had to work across the aisle, and with our partners in industry, to find a solution that would give CISA the visibility it needs without needlessly burdening victims of a cyber attack. We found a smart, compromise solution there—and I have faith we can do it again here. My goal today is to get testimony that will help us answer the question—what's next?

How do we continue to mature the way the Government engages with critical infrastructure—particularly those entities that are the "most critical of the critical"? Or, as the Cyber Solarium Commission put it, our "Systemically Important Critical

Infrastructure," or SICI? Do we have a good sense of where these SICI assets are, who's operating them, and how they're being secured?

And, once we know who and what they are—what benefits should the Federal Government provide for these entities to help them protect themselves? Importantly, what burdens should they be asked to shoulder, in light of their importance to our National security?

This latter part is key. It is not enough to simply identify these "most critical" entities—nor is it consistent with what the Solarium Commission proposed. We need to be able to answer the question: What do these companies need to do as a result of their designation? What does the Federal Government need to do for them—whether that's better access to threat intelligence, enhanced operational collaboration, or other priority access to resources and support?

It's not enough to simply make a list of our most vital assets—we need to know how we're going to operationalize it. We've tried this exercise in 'list-making' before—from the National Asset Database, to the designation of "Section 9" companies. Some of these efforts were costly and labor-intensive, and none of them ever really lived up to the security gains originally envisioned. The through line for all these efforts is that at some point, Congress, or the administration, or both, decided to punt on the question of benefits and burdens. That will not happen on my watch.

I would like to recognize Representative Langevin and Ranking Member Katko for championing this issue, and I look forward to continuing to work with them to craft this legislation in a way that avoids the pitfalls of the past. This hearing is an opportunity to help move the ball forward and hear how the

Administration is thinking about these challenges and working to upgrade its cybersecurity playbook.

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

Mr. GARBARINO. Thank you, Chairwoman Clarke, for calling this hearing today and thank you to the witnesses. I appreciate you being here to discuss how we can bridge the gap between public and private stakeholders and to discuss on-going efforts to identify and secure systemically important critical infrastructure.

It is no secret that we are facing an unprecedented level of cyber attacks against our Nation's critical infrastructure. Recent breaches, like Colonial Pipeline and SolarWinds, among others, are sobering reminders of the devastation attacks can cause to our economic and National security.

Additionally, yesterday's full committee hearing provided us with a stern reminder that cyber threats posed by foreign adversaries are only becoming more potent. Potential for malicious Russian cyber activity as well as attacks by other adversarial nations, like China, Iran, and North Korea, is only increasing. Congress must continue to facilitate public and private partnerships that are able to meet and repel these threats.

Cyber space is seemingly endless and the Federal Government's visibility to monitor incidents is limited. While Congress recently took an important step by codifying our subcommittee's incident reporting framework at CISA, there is more that can be done.

The vast majority of our Nation's critical infrastructure is owned and operated by the private sector. Therefore, information sharing between these stakeholders and the Federal Government is necessary to effectuate meaningful change. We need a process for the Federal Government to identify which infrastructure is systematically important and we need a plan for the private sector to protect those assets.

Earlier in this Congress, I joined with my colleagues Mr. Katko and Ms. Spanberger in introducing bipartisan legislation, Securing Systemically Important Critical infrastructure Act. The bill author-

izes CISA to designate certain entities of critical infrastructure as systemically important. By designating key elements, the Federal Government will signal to the private sector the assets that they should specifically prioritize in order to secure our Nation's critical sectors. As an original cosponsor of this effort I am confident that this is the best path forward.

I am pleased to have an expert panel of witnesses here today to hear their perspectives on this initiative. We must create the foundation for strong public-private collaboration without adding additional regulatory burdens for the industry.

I would like to say a quick note of thanks to CISA's Region 2 team for joining me last week for a successful cybersecurity webinar for critical infrastructure partners in my district. It is information sharing like this, coupled with cyber incident reporting and systemically important critical infrastructure designation, that will be instrumental in hardening our cyber defenses.

I look forward to hearing from our witnesses on how we can best move forward. Thank you again, Chairwoman.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW R. GARBARINO

Thank you, Chairwoman Clarke, for calling this hearing today. I appreciate our witnesses being here to discuss how we can bridge the gap between public and private stakeholders, and to discuss on-going efforts to identify and secure systemically important critical infrastructure.

It is no secret that we are facing an unprecedented level of cyber attacks against our Nation's critical infrastructure. Recent breaches like Colonial Pipeline and SolarWinds, among others, are sobering reminders of the devastation that attacks can cause to our economic and National security.

Additionally, yesterday's full committee hearing provided us with a stern reminder that the cyber threats posed by foreign adversaries are only becoming more potent. The potential for malicious Russian cyber activity, as well as attacks by other adversarial nations like China, Iran, and North Korea, is only increasing. Congress must continue to facilitate public and private partnerships that are able to meet and repel these threats.

Cyber space is seemingly endless, and the Federal Government's visibility to monitor cyber incidents is limited. While Congress recently took an important step by codifying our subcommittee's incident reporting framework at CISA, there is more that can be done. The vast majority of our Nation's critical infrastructure is owned and operated by the private sector. Therefore, information sharing between these stakeholders and the Federal Government is necessary to effectuate meaningful change.

We need a process for the Federal Government to identify which infrastructure is systemically important and we need a plan for the private sector to protect those assets.

Earlier this Congress, I joined my colleagues Mr. Katko and Mrs. Spanberger in introducing bipartisan legislation, the Securing Systematically Important Critical Infrastructure Act. The bill authorizes CISA to designate certain entities of critical infrastructure as systemically important. By designating key elements, the Federal Government will signal to the private sector the assets that they should specifically prioritize in order to secure our Nation's critical sectors. As an original co-sponsor of this effort, I am confident that this is the best path forward.

I'm pleased to have an expert panel of witnesses here today to hear their perspectives on this initiative. We must create the foundation for strong public-private collaboration without adding additional regulatory burdens for industry.

I'd like to say a quick note of thanks to CISA's Region II team for joining me last week for a successful cybersecurity webinar for critical infrastructure partners in my district. It's information sharing like this, coupled with cyber incident reporting, and systemically important critical infrastructure designation, that will be instrumental in hardening our cyber defenses.

I look forward to hearing from our witnesses on how we can best move forward.

Thank you again, Chairwoman.

Chairwoman CLARKE. I thank the Ranking Member, Mr. Garbarino.

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

[The statements of Chairman Thompson and Honorable Jackson Lee follow:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

APRIL 6, 2022

This Congress has been marked by a series of high-profile cyber incidents, from SolarWinds to Colonial Pipeline to JBS. We have been forced to evaluate our current approach to critical infrastructure security and how the Federal Government and private sector collaborate. Our oversight revealed that we spend too much time examining challenges to effective public-private partnerships and are too slow to take bold action to address them—that is, unless Chairwoman Clarke is leading the charge.

I want to applaud Chairwoman Clarke for the recent passage of the Cyber Incident Reporting for Critical Infrastructure Act. This critical legislation will position CISA to help its private-sector partners detect and disrupt malicious cyber campaigns sooner and provide enhanced situational awareness to inform strategic security investments. A mandatory cyber incident reporting framework is long overdue.

I want to thank the Chairwoman for working with private-sector stakeholders, the administration, and our colleagues in the Senate to get it right. I would also like to thank Ranking Member Katko and Subcommittee Ranking Member Garbarino for their efforts to get this important legislation across the finish line. Despite this progress, we must do more to maximize the cybersecurity benefits of public-private collaboration.

Yesterday, we heard from representatives from critical infrastructure sectors—including financial services and water—regarding how they are working with the Federal Government to strengthen cyber defenses and build resilience. Although there were similarities in the witnesses' testimonies—both stressed the value of continuous two-way engagement between the Federal Government and the private sector—there were notable differences.

The financial services sector is well-resourced, regulated, and capable of actioning both Classified and un-Classified information. In contrast, the water sector is under-resourced, largely unregulated, and would benefit from concise, properly contextualized security guidance.

In short, while the financial services sector has the resources and capacity to engage in operational collaboration with the Federal Government, the water sector is still working to establish a stronger security baseline. Similar disparities exist across the 16 critical infrastructure sectors, and the Federal Government must tailor its approach to partnership accordingly.

In doing so, it must prioritize collaboration with the private sector with the understanding that not all critical infrastructure is equally critical. Efforts to identify the most "critical of the critical" infrastructure are nothing new. But previous efforts—from the Section 9 designation to the National Asset Database—have fallen short.

As we work to identify the most significant critical infrastructure and define the associated benefits and burdens, we must leverage lessons learned. Before I close, I want to thank Congressman Jim Langevin and Ranking Member Katko for their commitment to modernizing how the Federal Government engages with critical infrastructure. I look forward to working with them to refine and advance their approaches.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

APRIL 6, 2022

Chairwoman Clarke, and Ranking Member Garbarino, thank you for holding today's hearing on "Mobilizing our Cyber Defenses: Maturing Public-Private Partnerships to Secure U.S. Critical Infrastructure."

I thank today's witnesses:
- Mr. Eric Goldstein, executive assistant director for cybersecurity, Cybersecurity and Infrastructure Security Agency;
- Mr. Robert K. Knake, deputy national cyber director for strategy and budget & principal deputy national cyber director (acting), Office of the National Cyber Director; and
- Ms. Tina Won Sherman, director, Homeland Security and Justice, Government Accountability Office (Republican Witness).

I thank each of you for bringing your expert view of the cyber threats against our Nation's critical infrastructure.

The USA PATRIOT Act of 2001 defines CI as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, National economic security, National public health or safety, or any combination of those matters.

This hearing allows Members the opportunity to assess Federal efforts to mature collaboration with critical infrastructure owners and operators as they work to defend their networks and build resilience.

The hearing is an opportunity to learn about existing partnerships between the public and private sectors regarding critical infrastructure protection, and what can be done to encourage greater collaboration to protect the most critical infrastructure from cyber threats.

To address the current threat landscape, the Federal Government needs to rethink the way that it engages with key critical infrastructure partners—the "most critical of the critical."

That starts by developing a clear understanding of critical functions and points of failure across the country—but that is not where it ends.

The most important aspect of critical infrastructure is that it is essential to modern American life and strong link to economic competitiveness.

Electricity, clean drinking water, functioning dams, spillways, levies, transportation, and food production are all under the heading critical infrastructure.

The House Committee on Homeland Security has the responsibility of providing for the cybersecurity of Federal civilian agencies as well as the to secure the Nation's 16 critical infrastructure sectors from cyber and other threats.

The list of critical infrastructure has expanded to include election systems following cyber incidents targeting election systems leading up to the 2016 National Elections.

We know the threats that computing devices and systems face, which are almost too numerous to count:
- Bot-nets;
- Ransom-ware;
- Zero-Day Events;
- Mal-ware;
- Denial-of-Service Attacks;
- Distributed Denial-of-Service Attacks;
- Pharming;
- Phishing;
- Data Theft;
- Data Breaches;
- SQL Injection;
- Man-in-the-middle attack.

This list is not exhaustive, but it does make clear the scope of the threat and why the United States can no longer rely solely on the resources of critical infrastructure owners and operators to secure assets absent Federal guidance and resources.

This is why I introduced the Cybersecurity Vulnerability Remediation Act was introduced and passed the House during the 115th and 116th Congresses and has been updated again in the 117th Congress to meet the ever-evolving nature of cyber threats faced by Federal and private-sector information systems and our Nation's critical infrastructure.

This bill, which was included in the National Defense Authorization Act for fiscal year 2022, goes significantly further than the first Cybersecurity Vulnerability bill that I introduced in the 115th Congress, to address the instance of Zero-Day Events that can lead to catastrophic cybersecurity failures of information and computing systems.

H.R. 2980, the Cybersecurity Vulnerability Remediation Act:
- Changes the Department of Homeland Security (DHS) definition of security vulnerability to include cybersecurity vulnerability,
- Provides the plan to fix known cybersecurity vulnerabilities,

- Gives the Department of Homeland Security the tools to know more about ransomware attacks and ransom payments, and
- Creates greater transparency on how DHS will defend against and mitigate cybersecurity vulnerabilities and lays the road map for preparing the private sector to better prepare for and mitigate cyber attacks.

The bill requires a report that can include a Classified annex, which I strongly recommend to the Secretary of DHS so that it can be available should the agency elect to engage private-sector entities in a discussion on cyber attacks and breaches targeting critical infrastructure.

This bill is needed because the Nation's dependence on networked computing makes us vulnerable to cyber threats.

Soon I will be introducing 3 cybersecurity critical infrastructure bills to address many of the issues associated with cyber vulnerabilities found in the infrastructure our communities and that our Nation depends on.

The focus I have had on cybersecurity and critical infrastructure is to protect against a crippling "Zero-Day Event."

A Zero-Day Event describes the situation that network security professionals may find themselves when a previously unknown error or flaw in computing code is exploited by a cyber criminal or terrorist.

The term "Zero-Day Event" simply means that there is zero time to prepare a defense against a cyber attack.

When a defect in software is discovered then network engineers and software companies can work to develop a "patch" to fix the problem before it can be exploited by those who may seek to do harm.

Because vulnerabilities can be used by adversaries it is important that this sensitive information be managed securely so details are not routinely made available neither to the public nor to Congress.

Congress must do its job by providing the necessary leadership that moves the Nation from an unrealistic moat-and-drawbridge cybersecurity posture to one that is agile.

Vulnerabilities of computing systems are not limited to intentional attacks, but can include acts of nature, human error, or technology failing to perform as intended.

I am particularly concerned that so many jurisdictions rely on critical infrastructure that is inadequately maintained for physical and cybersecurity threats.

Cybersecurity threats to critical infrastructure (CI) have accelerated rapidly in recent years.

The U.S. framework for securing CI, set forth in Presidential Policy Directive 21 (PPD–21) and reinforced in statute, designates the Department of Homeland Security (DHS), through the Cybersecurity and Infrastructure Security Agency (CISA), to lead Federal efforts to secure critical CI across 16 diverse sectors, in coordination with designated Sector Risk Management Agencies (SRMAs) for each sector.

However, these partnerships are largely voluntary, and most CI in the United States is privately-owned.

High-profile cyber attacks such as SolarWinds and Colonial Pipeline have renewed questions about whether the voluntary partnership model is sufficient to address the current threat landscape.

This is particularly true in light of recent elevated threats from Russia, which may seek to use malicious cyber attacks to retaliate for U.S. sanctions following their invasion of Ukraine.

Because the majority of critical infrastructure is owned and operated by the private sector, CISA has limited visibility into malicious cyber activity on their networks, absent voluntary reporting and information sharing.

Moreover, although in the past the Federal Government has attempted to establish a mechanism to identify and track those assets and entities most critical to regional and National security, it has failed to define its relationship with those entities in a way that would yield meaningful security benefits.

The Biden administration has shown a willingness to move away from voluntary partnerships and toward a more regulatory model, but there are challenges in understanding how such a regime might work, and the entities to which it would apply.

This step is long overdue because of the nature of critical infrastructure.

A failure in critical infrastructure would have wide-spread consequences far beyond the scope of the critical infrastructure service delivery area.

For this reason, there must be more accountability on the part of owners and operators and greater Federal agency engagement regarding the cybersecurity of these entities.

I look forward to the testimony of today's witnesses.

Thank you.

Chairwoman CLARKE. I now welcome our panel of witnesses. First, I would like to welcome Mr. Eric Goldstein, the executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency. Previously, Mr. Goldstein was the head of cybersecurity policy, strategy, and regulation at Goldman Sachs. Mr. Goldstein also served at CISA's precursor agency, the National Protection and Programs Directorate, for several years.

Second, I would like to welcome Mr. Robert Knake. Mr. Knake is currently the deputy national cyber director of strategy and budget and the acting principal deputy national cyber director in the Office of the National Cyber Directorate. During the Obama administration Mr. Knake served as the director of cybersecurity policy at the National Security Council.

Finally, I would like to welcome Dr. Tina Won Sherman, who is the director of homeland security and justice at the U.S. Government Accountability Office, GAO. Dr. Sherman manages work on the protection of the Nation's critical infrastructure assets and the security of the United States transportation system. During her tenure, Dr. Sherman has led reviews on a range of critical issues, including telecommunications, transportation, and defense.

Without objection, the witnesses' full statements will be inserted into the record. I now ask that our witnesses will summarize their statements for 5 minutes, beginning with Mr. Goldstein.

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

Mr. GOLDSTEIN. Thank you so much. Chairwoman Clarke, Ranking Member Garbarino, it is really a privilege to be here today testifying on behalf of CISA, the Cybersecurity and Infrastructure Security Agency.

This hearing occurs, of course, in the backdrop of Russia's unjust and tragic invasion of Ukraine and the on-going risk of malicious cyber activity. This subcommittee is to be commended on taking the time to examine CISA's role as our Nation's cyber defense agency and the manner in which we catalyze operational collaboration between Government and the private sector. This operational collaboration is foundational to our success as an agency and our shared goals of rapidly advancing cybersecurity across the country. We recognize at CISA that no individual organization, public or private, has the visibility or the ability alone to manage cybersecurity risk. So our goal is to change the traditional models of public-private collaboration and move to a new paradigm of public and private operational collaboration where we can scale more effectively to meet the risks that we are facing both today and into the future.

Even as we evolve toward this model, we have already shown the benefits of true operational collaboration where Government partners and the private sector are working side-by-side. I look forward to speaking a bit more about our successes in this area and our work yet to come.

The core of our operational collaboration efforts at CISA are through our Joint Cyber Defense Collaborative, or the JCDC, which was established by Congress to serve as the focal point for proactive planning and domestic cyber defense across Government and the private sector. In its short history, the JCDC has already pioneered several real innovations.

The first is bringing together representatives from the core cyber operational agencies—CISA, FBI, NSA, U.S. Cyber Command—with partners across critical sectors—the Nation's largest technology companies, energy companies, financial institutions—to sit side-by-side in a virtual environment, exchanging information, developing mitigations, and then sharing information to protect the broader cybersecurity community. We initiated this sort of work with the vulnerability in the Log4j software library and we are now scaling it as part of our broader shields of effort in response to the Russian invasion of Ukraine, where our goal is to bring together the best and most effective capabilities across Government and the private sector so we can quickly learn about threat activity and mitigations, and then share it more broadly to protect the country.

We are also deeply focused on the JCDC as a locus of proactive planning. Looking briefly at our work around the Russian invasion of Ukraine, in December we developed a joint public-private cyber defense plan. We exercised this plan in January. When the invasion occurred, we moved into execution, bringing together our partners across Government and the private sector to exchange information and collaborate at scale. We are showing through this work the value of the JCDC and operational collaboration in taking information into insights into action, all underpinned by proactive planning that brings together Government and the private sector as coequal partners through this work. We were gratified to hear in the subcommittee's hearing yesterday many of our partners in the private sector reflect the value of this partnership and the work that we have done, even as we mature going forward.

But, of course, while our core goal is ensuring that every American organization has the information and tools needed to protect their enterprises and customers against cyber risks, our core goal is ensuring the continuity and resilience of National critical functions. For this reason, at CISA we are focused on identifying the systemically important entities, or SIEs as we call them, which, if degraded, would cause debilitating systemic or cascading impacts to National critical functions. We are engaged today in a rigorous effort to identify these entities, understand how they support National critical functions, and think creatively about how we can work collaboratively to build our operational collaboration and support these entities to reasonably assure the continuity of National critical functions under all conditions.

We are grateful for the support of the subcommittee, including Mr. Katko and Mr. Langevin, at helping us advance these efforts. I am looking forward to conversation yet to come as we evolve this critical and essential work.

It goes without saying that our Nation is facing unprecedented cybersecurity risk, but we are deepening our relationships, we are deepening the effectiveness of our collaboration and our services, and working across Government, our allies, and the private sector.

With the support of Congress we are confident that we will make the difference we need to manage risk to our country.

Thank you again for the privilege of appearing today. Very much looking forward to your questions.

[The prepared statement of Mr. Goldstein follows:]

PREPARED STATEMENT OF ERIC GOLDSTEIN

APRIL 6, 2022

Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding our efforts to evolve our partnerships with the private sector to enable true operational collaboration.

In our globally interconnected world, our critical infrastructure and American ways of life face a wide array of serious risks with significant real-world consequences. Today, the critical functions within our society are built as "systems of systems," complex designs with numerous interdependencies and systemic risks that can have cascading effects. This trend has yielded significant gains in efficiency and productivity, but also provides the opportunity for nation-state actors and criminals to potentially undermine our National security, economic prosperity, and public health or safety.

The risks we face today are complex and dispersed, both geographically and across a variety of stakeholders. They are challenging to assess and difficult to address. Consequently, we must recognize that threats to our digital infrastructure are not bound by National borders. Rather, our critical infrastructure is integrated into a larger global cyber ecosystem requiring us to be at the constant ready.

This committee is well aware of CISA's broader domestic role as the operational lead for Federal cybersecurity, and as the National coordinator for critical infrastructure security and resilience. The importance of CISA's mission and role has been clearly reflected during the war in Ukraine, as we have led the Nation's efforts across Government and the private sector to prepare for potential malicious cyber activity by Russian actors.

Critical to our success, and at the heart of CISA's mission, is partnership and collaboration. Securing our Nation's cyber and critical infrastructure is a shared responsibility and has never been more important than it is today. Neither Government nor the private sector have the knowledge or resources to do it alone. At CISA, we are challenging traditional ways of doing business and are actively working with our Government, industry, academic, and international partners to change the paradigm from traditional public-private partnerships to public-private operational collaboration at scale. Operational collaboration is foundational for effective critical infrastructure security and resilience. Timely, trusted information fusion among stakeholders is essential.

In the past year, CISA has made significant strides in this respect, particularly through the establishment of the Joint Cyber Defense Collaborative (JCDC) and our CISA Cybersecurity Advisory Committee (CSAC). These groups are examples of CISA's agency-wide dedication to operational collaboration and deep partnership, which is imbued across our mission divisions. By leveraging the expertise and unique authorities of Government and the private sector, CISA is better-positioned to connect with our stakeholders in industry and Government to share resources, analyses, and tools. This in turn helps our stakeholders build their own cyber, communications, and physical security and resilience. The net effect is a stronger Nation, better positioned to contend with the myriad threats we face to our cybersecurity and critical infrastructure.

As we strive to make progress in the security of our Nation's critical infrastructure through our various partnership initiatives, we are not looking to duplicate the efforts of the private sector. Instead, CISA is looking for ways we can add value, such as bringing experts from Government and industry together, compiling a broader holistic view of the cyber landscape, and sharing information across sectors to ultimately make our Nation's critical infrastructure resilient against malicious cyber activity.

Our work has taken on increased urgency subsequent to Russia's unprovoked invasion of Ukraine. CISA has been working closely with our critical infrastructure partners over the past several months to ensure awareness of potential threats. We have been providing additional resources, guidance, and support for months, and reiterated this call for critical infrastructure to adopt a heightened security posture in light of President Biden's statement that intelligence shows Russia may be ex-

ploring options for potential cyber attacks. As part of our broader "Shields Up" effort, we developed and published a variety of resources, including guidance for organizations, corporate leaders and CEOs, individuals, ransomware response, and a list of additional resources, multiple joint Cybersecurity Advisories (CSAs), mitigation guidance, including recent products on securing satellite communications and uninterruptible power supply devices, and a dedicated Technical Guidance web page with mitigation guidance and resources from CISA, the JCDC and other partners. Our goal with all of these efforts is to serve as a comprehensive resource for information about mitigations for the Russian cyber threat.

JOINT CYBER DEFENSE COLLABORATIVE (JCDC)

Given that the vast majority of our Nation's critical infrastructure is owned and operated by the private sector, the early warnings of a cyber attack affecting U.S. organizations are more likely to be identified by a private company rather than the Government. The private sector plays a vital role in working with CISA to improve our Nation's cybersecurity by helping to ensure that we are aware of new campaigns or intrusions so we can protect other possible victims.

Critical to CISA's effort to build better operational collaborative channels is the JCDC, which leverages authorities granted in the fiscal year 2021 NDAA, among other authorities, and was launched by CISA in August 2021 to lead collaborative, public, and private-sector cyber defense planning, cybersecurity information fusion and analysis, and the purposeful dissemination of cyber defense guidance to reduce cyber risks to the Nation's critical infrastructure and the impact to our National Critical Functions (NCF).

Today, the JCDC is a collection of more than 25 private-sector companies working with CISA and other Federal Government cybersecurity partner agencies—including DHS Office of Intelligence and Analysis, FBI, NSA, U.S. Cyber Command, the U.S. Secret Service, and relevant Sector Risk Management Agencies (SRMA)—to understand and respond to cyber threats. The diversity and unique capabilities of JCDC partners provides increased visibility and insight into the threat landscape and enables JCDC to develop plans and exercises against the most serious threats.

The JCDC model reflects the reality that no one entity can secure cyber space alone. Collaboration across JCDC partners results in action across an expansive set of cybersecurity stakeholders throughout the Nation and the globe.

By leveraging and unifying the respective capabilities, authorities, and expertise of the JCDC's partners, CISA is creating a proactive, rather than reactive, capability for the Government and private sector to work together to drive down risk even before an incident occurs. Should another incident like the compromises affecting SolarWinds Orion, Microsoft Exchange Server, or Colonial Pipeline occur, the strengthened connective tissue among our partners will allow for a more unified response.

The JCDC operating model relies on regular analytic and data exchanges to enable common situational awareness and equip public and private-sector partners to take risk-informed coordinated action for our collective defense. Simply put, the work of the JCDC is about seeing the dots, connecting the dots, and collectively driving down risk to the Nation at scale. This alignment strengthens our mutual resilience and ability to address immediate and impending cyber incidents. Collaborative insights gleaned from the JCDC are then rapidly shared across the broader cybersecurity community, including through our Cybersecurity Information Sharing and Collaboration Program and through a broad ecosystem of Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs).

In its short history, the JCDC has strengthened the lines of communication between industry and the Federal Government to improve real-time information sharing, planning, and exercising. For example, when CISA issued its emergency directive in response to the Log4j vulnerability, CISA leveraged the JCDC, establishing a senior leadership group within the the organization to coordinate collective action and ensure shared visibility into both the prevalence of the Log4j vulnerability and threat activity. By bringing together key Government and private-sector partners via the JCDC, including the agency's partners at the FBI and the NSA, CISA was able to ensure that the country's strongest capabilities were brought to bear in an integrated manner against the threat.

Having built trust and strengthened relationships with our partners during our response to the Log4j incident, the JCDC was well-prepared to respond to the current dynamic threat environment amidst rising geopolitical tensions related to the Russia-Ukraine war.

To ensure domestic resilience against potential cyber attacks in response to the Russia-Ukraine war, the President designated the Department of Homeland Secu-

rity as the Lead Federal Agency (LFA) for domestic preparedness and response related to the current crisis. Secretary Mayorkas then established a Unified Coordination Group (UCG) and appointed CISA's executive director to serve as the senior response official to ensure Federal unity of effort across the U.S. Government. The stand-up of the UCG formalized the work CISA had been doing for months with Sector Risk Management Agencies (SRMAs) to inform stakeholders of the heightened threat environment, and conduct intelligence-based threat briefs for SRMA partner agencies, Sector and Government Coordinating Councils, and participants from the private sector and State and local community. In addition, CISA is working with FEMA, SRMAs, and other Federal partners to manage downstream physical consequences of potential cyber attacks. The Russia-Ukraine crisis has brought on a whole-of-Government and whole-of-Nation preparedness effort

More broadly with the private sector though, the JCDC has served as a critical forum to implement standing operational collaboration channels.

For example, CISA developed a Russia-Ukraine crisis plan with our JCDC partners that lays out phases and objectives of operational coordination between the U.S. Government and our private-sector partners amidst escalating geopolitical tensions. In mid-February, we conducted a tabletop exercise of this plan with our interagency and private-sector partners. We are using the plan as tensions escalate to guide and align our collective operational posture and support our ability to esynchronize defensive actions to mitigate harmful impacts to U.S. critical infrastructure from Russian cyber operations. In the wake of distributed denial-of-service (DDoS) and destructive malware attacks affecting Ukraine and other countries in the region, we are working very closely with JCDC and international cyber defense partners to understand and rapidly share information on these on-going malicious cyber activities.

Moreover, JCDC's collaborative channels have allowed CISA to exchange technical information about recent incidents in Ukraine and conduct real-time analysis with interagency and industry partners. Further still, the JCDC established additional information-sharing mechanisms with the Nation's largest energy and financial companies, in coordination with the appropriate SRMAs, allowing CISA to provide additional early warning about Russian activity against U.S. institutions and exchange-related threat information and defensive measures.

We recognize that many critical infrastructure partners or SLTT governments find it challenging to identify resources for urgent security improvements. In response, JCDC has worked with our partners to compile a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This catalog includes CISA's own services, open-source tools, and free offerings from private-sector entities, including our JCDC partners. The catalog includes resources like malware and antivirus protection systems, vulnerability assessment solutions, tools that test password strength, distributed denial-of-service protection services and intelligence from several leading cybersecurity companies. This is particularly impactful for small businesses and SLTT organizations who are target-rich and resource-poor.

Going forward, we continue to build and mature the JCDC construct. We are particularly focused on advancing our capability to create, exercise, and execute joint cyber defense plans. Upcoming planning efforts focus on the energy sector and collaboratively supporting defense of the Nation's election infrastructure. The JCDC has demonstrated the promise of a new model for public-private operational collaboration: Joint cyber planning—including deliberate and crisis action plans—through collaboration across the public and private sectors to prepare for and address the Nation's most pressing cyber risks, combined with integrated and institutionalized testing and assessments to continuously measure and improve the effectiveness of cyber defense planning and capabilities.

Through these collaborative efforts, we will enable common situational awareness, information fusion, and analysis that equips public and private partners to take risk-informed coordinated action. This journey is not CISA's alone. Rather, we are embarking on a rapid evolution in concert with our partners across the inter-agency and private sector, with a shared goal of advancing our Nation's security and resilience at scale.

SYSTEMICALLY IMPORTANT ENTITIES (SIE)

Through our operational collaboration efforts, we have learned that prioritization is essential. By focusing on systemic risks, growing interdependencies within and across sectors and our evolving reliance on information and communications technology (ICT), we will more effectively reduce the potential of cascading impacts asso-

ciated with the failure of these technologies that could threaten our National and economic security.

In March 2020, the Cyberspace Solarium Commission proposed a "designation of critical infrastructure entities that manage systems and assets whose disruption could have cascading, destabilizing effects on U.S. National security, economic security, and public health and safety."[1] At CISA, we are operationalizing this concept by developing approaches to identify Systemically Important Entities (SIE). These are entities that own, operate, or otherwise control critical infrastructure, prioritized based on indicators of systemic importance and the potential impact that their disrupted or corrupted functions will have a debilitating, systemic or cascading impact on our country's critical infrastructure and related NCFs, National security, National economic security, public health, public safety, or some combination thereof.

As the private sector owns and operates a vast majority of the Nation's critical infrastructure, partnerships like JCDC, CSAC, and others that foster integrated, collaborative engagement and interaction are essential to maintaining critical infrastructure security and resilience. Therefore, identifying systemically important private-sector firms, in addition to SLTT and other public entities, is paramount to prioritizing the partnerships CISA establishes and maintains to reduce risk to critical infrastructure.

To aid in this identification, CISA established an SIE effort within the National Risk Management Center (NRMC) to develop the SIE concept in order to prioritize CISA's delivery of services to those entities. CISA's SIE effort, which seeks to support and respond to partners and stakeholders across the Federal Government, private industry, and SLTT governments, will be the central body responsible for coordinating across CISA, DHS, and the interagency to manage stakeholder engagement with systemically important entities. Additionally, CISA is sponsoring work by the Homeland Security Operations Analysis Center (HSOAC) to develop a prototype analytic capability to identify SIEs at scale. By using advanced data-analytic techniques that evaluate entities based on their network centrality and sector revenue, we will be better able to identify and assess an SIE's importance across the NCFs and close gaps in their risk profiles.

Identifying SIEs is more than just a naming and mapping exercise. By identifying SIEs we will be better positioned to understand the true landscape of institutions and systems whose disruption could have cascading and systemic effects to our critical infrastructure and related NCFs. This knowledge will better position us to prioritize these entities for CISA services and capabilities and identify mature entities whose partnership can help the Nation reduce systemic risk to our cyber and critical infrastructure.

While we are committed to growing our capacity to collaborate and share information, CISA and our Federal partners are limited in our ability to influence private-sector functions, such as complex supply chains, that are an increasing source of cyber risk. Fortunately, SIEs can help set expectations for acceptable activities and behavior by employing effective supply chain security risk management practices.

CISA will prioritize partnership and engagement with the SIE community and provide recommendations for addressing the emerging challenges of systemic risk. We particularly would benefit from specific input from partners regarding our efforts to improve our understanding of systemic risk.

The SIE program is of critical importance. While we are committed to protecting all of the Nation's critical infrastructure, not all infrastructure is created equal. Assets and systems that are of such vital importance to our security require prioritized protection in collaboration with the private sector. In some cases, individual companies can reduce risk because they own or operate a significant portion of the assets and systems. CISA's efforts to begin the identification process of systemically important entities represents a vital, and necessary, first step in that process.

CISA CYBERSECURITY ADVISORY COMMITTEE (CSAC)

Even as we work through the JCDC to collaborate around urgent risks of today and develop cyber defense plans to address those risks still ahead, we must also learn from diverse minds across the cybersecurity community to advance CISA's strategic maturation. To achieve this goal, we recently launched the CISA Cybersecurity Advisory Committee (CSAC), a key authority granted in the National Defense Authorization Act (NDAA) for fiscal year 2021.

The CSAC was established with the purpose of bringing together strategic thinkers with diverse expertise and insights to examine issues and create recommenda-

[1] United States of America. (2020). *Cyberspace Solarium Commission, Final Report.* p. 138. Retrieved from *https://www.cybersolarium.org/reports-and-white-papers*.

tions related to the development, refinement, and implementation of policies and programs that will help to advance the cybersecurity mission of CISA as well as strengthen the cybersecurity of the United States. In December 2021, Director Easterly appointed 23 leading experts on cybersecurity, technology, risk management, privacy, and resilience from across industry, academia, and Government to serve as the CSAC's initial members. The diversity of the committee's members emphasizes the need for an "all hands on deck" approach to secure our digital networks.

CSAC members advise, consult with, report to and make recommendations to the Director on the development, refinement, and implementation of policies, programs, planning, and training pertaining to CISA's cybersecurity mission. The committee will examine and make recommendations on a variety of topics collectively aimed at strengthening CISA and more broadly reshaping the cyber ecosystem to favor defense. These topics include growing the cyber workforce; reducing systemic risk to National critical functions; combating misinformation and disinformation impacting the security of critical infrastructure; and turning the corner on cyber hygiene by raising the baseline of security throughout the cyber ecosystem to advance an environment that favors the defender by better aligning Government and private-sector efforts to build resilience and improve cyber hygiene at scale. In addition, the CSAC recently established a new Technical Advisory Council, a subcommittee of the CSAC, with some of the most accomplished individuals in the cybersecurity community to provide CISA with expert insights into advancing our collaboration with the research community and ensuring that our programs reflect leading technology practices.

Building on the momentum from the committee's inaugural meeting in December, the CSAC convened again just this past week on March 31. Protecting the Nation's critical infrastructure depends on a unified effort and we remain committed to ensuring that we have the right strategy in place to prepare for, respond to, and mitigate cybersecurity threats to our Nation's critical systems. CISA looks forward to the recommendations made by the committee Members and the subsequent subcommittees.

CYBER SAFETY REVIEW BOARD (CSRB)

A continuous learning culture is critical to staying ahead of the increasingly sophisticated cyber threats we face in today's complex technology landscape. Recognizing this need, President Biden's Executive Order 14028 on Improving the Nation's Cybersecurity directed DHS to establish a Cyber Safety Review Board (CSRB) to review significant cyber incidents to ensure that the Nation fully understands and learns from significant cyber events that may threaten us all.

The CSRB serves a deliberate function to review major cyber events and make concrete recommendations that would drive improvements within the private and public sectors. As a uniquely constituted advisory body, the CSRB will focus on learning lessons and sharing findings with the President, and with others who can benefit from them, as appropriate.

The private sector has a significant role to play in providing visibility, validation, and insight into how cyber events emerge and which short and long-term improvements can stave off future, similar events, and incidents. The CSRB—composed of 15 highly-esteemed cybersecurity leaders from the Federal Government and the private sector—provides a unique forum for collaboration between Government and private-sector leaders who will deliver strategic recommendations to the President and the Secretary of Homeland Security.

CONCLUSION

Our Nation is at a turning point in cybersecurity. We must continue to work together, by deepening our operational collaboration and ensuring we have the plans and policies in place now, to defend against new and changing cyber threats going forward. Recent incidents and the on-going threat of malicious Russian cyber activity provide a stark reminder about the vulnerability of our country's critical infrastructure. The need for increased risk sharing and distribution between the Government and private sector is clear.

The cyber ecosystem is a shared space with shared responsibilities and shared benefits, with every organization gaining from the interoperability, scale, and resilience of the internet and networked technologies. As a result, every organization must invest in protecting it. Together we can address the risks we all face. CISA's public and private-sector programs provide novel collaborative venues for diverse entities to evolve their relationships.

Now is the time to act—and CISA is helping to lead our National call to action. We will deepen our partnerships with critical infrastructure partners, enhance our

visibility into National cybersecurity, and drive targeted action to reduce vulnerabilities and detect our adversaries. In collaboration with our Government partners, critical infrastructure entities, our international allies, and with the support of Congress, we will make progress in addressing this risk and maintain the availability of critical services to the American people under all conditions.

Chairwoman CLARKE. Thank you for your testimony, Mr. Goldstein. I now recognize Mr. Knake to summarize his statement for 5 minutes.

STATEMENT OF ROBERT K. KNAKE, DEPUTY NATIONAL CYBER DIRECTOR FOR STRATEGY AND BUDGET, PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR (ACTING), OFFICE OF THE NATIONAL CYBER DIRECTOR, THE WHITE HOUSE

Mr. KNAKE. Thank you, Chairwoman Clarke. Thank you, Mr. Garbarino, and thank you, Mr. Katko, for being here today. I very much appreciate the opportunity. It is very good to be back before this committee in my new role as deputy national cyber director in the Office of the National Cyber Directorate.

So, we are the new kids in school and we are working closely with our colleagues at CISA. We are working very closely with our colleagues throughout the interagency and with our colleagues at the National Security Council in order to bring together a more cohesive effort on the part of the Federal Government when we are working with the private sector. So, that is what we are here for.

So, today you will hear me say a lot of things that sound almost like what you might hear from Ms. Sherman. We are reviewing, we are evaluating, we are supporting rather than we are directing or we are operationalizing some activity. That is the role of CISA, that is the role of Eric Goldstein, and the SRMAs, Sector Risk Management Agencies.

So, with that said, what I would like to talk about is in terms of the maturing public-private partnership, first, I think we really need to recognize how far we have actually come, particularly in the last few years. We have gone from a partnership that was fundamentally about having meetings between public policy officials and companies, and public policy officials and organizations, to one in which we have operational collaboration that, in some cases, is side-by-side, shoulder-to-shoulder, but, even more importantly, has been virtualized so that people at large companies can engage with the private sector, with the Government, and can do it in real time from where they were. This is a massive lead that the JCDC has really enabled over the last year. We are really seeing the benefits of that maturation as we confront the Russia threat.

So, as we look to mature, we first need to recognize that we really have come a significant way. My hat is off to this Congress for giving the resources, the authorities, and looking at the organization of CISA and the SRMAs in order to make sure that we have got the right players on the field and they have got the right resources to do their jobs.

So, where do we go from here I think is the big question? The Russia threat I think, as Eric has said, is really providing a focus. It is making sure that every single day we are improving our connectivity with the private sector, that when problems happen they are getting resolved. That if, for instance, somebody calls our office and says we have an issue, we can't find the right place to

plug into the Government, we don't say, great, we will take that, we will stand up a new body at the White House to do it. No, we say, OK, I am going to get on the phone with Eric or, better yet, our engagement team is going to get on board with the JCDC and say how do we plug these guys in? That is happening every single day. So that improvement is something that we very much want to see continue as we face this Russia threat.

I think Eric has given a very good encapsulation of what the JCDC does. Let me talk a little bit more about what we are doing with the Sector Risk Management Agencies, which we see as a vital partner in this effort.

Many people have used the football analogy and I will use it here. If you have got the quarterback at CISA, you got to make sure you have strong players on the rest of the field, and that is where the SRMAs come in. Our office is evaluating, in partnership with those SRMAs, what are their capabilities? What are the resources they need? What are the gaps and how can we help fill them?

Crucial to that we have heard from every private sector company we talked to is to make sure that we can provide the one thing that private companies can't do on their own, which is intelligence. Only the U.S. Government can collect intelligence and only the U.S. Government can provide it back. So, that is a major focus of our efforts.

There is a great model here that the defense industrial base is engaged in with DOD. We think we can replicate it. The key is to build some connectivity between CISA and the SRMAs and the private sector, so we can really scale these great efforts. I think we are well on our way to that.

Finally, as I think we look at the concept of the systemically important entities, it is fairly clear to us that DHS has the authorities to do the work they have done today. We are working with them to see are there other things you would like to do? Are there authorities you don't have in order to either identify, but, more importantly, provide support to or set performance goals with, tailored performance goals with those entities? So that is the last piece of what we are looking at in the very near term.

Thank you for the opportunity to testify. I am looking forward to the discussion.

[The prepared statement of Mr. Knake follows:]

PREPARED STATEMENT OF ROBERT K. KNAKE

APRIL 6, 2022

Chairwoman Clarke, Ranking Member Garbarino, distinguished Members of the subcommittee, thank you for the privilege to appear before you today. It's an honor to appear alongside CISA's executive assistant director for cybersecurity Eric Goldstein. I am eager to share with you what the Office of the National Cyber Director (ONCD) is doing to mature the public-private partnership with industry to better secure critical infrastructure from cyber intrusions, including destructive cyber attacks. The Biden-Harris administration continues to strengthen our cybersecurity defenses and prepare our Nation with unprecedented focus, and the ONCD is proud to work alongside our interagency partners in these efforts.

The President has taken aggressive action to secure the Nation's critical infrastructure and is prepared to use every tool to deter, disrupt, and when appropriate, respond to cyber attacks against our homeland. In May 2021, the President issued Executive Order 14028, mandating extensive cybersecurity measures for the Federal Government to ensure we are leading by example. The ONCD, working with our

partners at the Office of Management and Budget (OMB) and the National Security Council, is conducting implementation oversight of Executive Order 14028, to ensure continued progress on fulfilling the Order's requirements.

Since the fall 2021, as Russian President Vladimir Putin escalated his aggression against Ukraine, the Biden-Harris administration has worked to provide extensive briefings and advisories to U.S. businesses and individuals regarding potential threats and the cybersecurity measures they can put in place to protect themselves. CISA, the FBI, the National Security Agency's Cybersecurity Directorate—and, in many cases, our international partners—have issued numerous threat advisories outlining Russia's malicious intent and activities in cyber space and outing their tools and infrastructure. The professionals in our intelligence community have done outstanding work in exposing Putin's nefarious plots, while our cyber defenders continue to ensure strategic warnings are paired with actionable steps for companies and the American public to defend themselves.

Recognizing the unique risks presented in cyber space for the conflict to spill out of Ukraine and onto our shores, the Federal Government has also partnered with industry on tabletop exercises, bringing important critical infrastructure stakeholders—including CEOs—together to operationalize collaboration and prepare for various scenarios. Paired with Classified intelligence read-ins and aggressive declassification efforts, these exercises help enhance resilience and coherence among our private-sector partners, Federal departments, and agencies. The administration has also been able to leverage relationships developed through public-private action plans under the President's Industrial Control Systems Cybersecurity Initiative to enhance the cybersecurity posture of the electricity, pipeline, and water sectors.

On March 21, 2022, the President reiterated his warning about potential cyber attacks from Russia against critical infrastructure and urged companies to harden cyber defenses immediately and deploy best practices. The Government and private sectors must also continue to work together to build National resilience and productively collaborative to address and defeat the evolving cyber threats we face. The administration has prioritized stronger cybersecurity controls for critical infrastructure sectors where we have authority to do so and is creating innovative public-private partnerships and initiatives to enhance cybersecurity across all our critical infrastructure. Congress has partnered with us on these efforts, and we appreciate the bipartisan work of this committee to require companies to report cyber incidents to the U.S. Government. These efforts have become even more critical as we assess evolving intelligence that Russia may be exploring options for potential cyber attacks on U.S. critical infrastructure.

The ONCD is helping to execute the Biden-Harris administration's cyber agenda by, among other things, working to improve public-private collaboration in cybersecurity. Through strategic engagements with stakeholders, the ONCD is establishing and maintaining relationships to enhance knowledge sharing and strategic coordination and collaboration. ONCD is working with the NSC, other White House components, and relevant agencies to harness the once-in-a-generation scope and scale of the Infrastructure Investment and Jobs Act to build infrastructure that is future-proofed and resilient to cyber threats, with standards and policy frameworks necessary for a durable cyber foundation.

As we work with industry to invest in the resiliency of our infrastructure, we remain committed to rapidly improving our collaboration with industry to address today's cyber threats.

We work closely with our Federal partners, including CISA, OMB, the Department of Justice, including the FBI, the National Institute of Standards and Technology (NIST), and Sector Risk Management Agencies (SRMAs) to expand engagement and partnership opportunities across sectoral lines and increase collaboration.

CISA has a central role to play in building our capacity for collaboration with the private sector. I expect that EAD Goldstein will highlight CISA's on-going efforts in this area to mature collaboration and improve cybersecurity, but let me highlight one critical success. CISA leveraged the authority entrusted to it by Congress to establish the Joint Cyber Defense Collaborative (JCDC), an organization that brings together representatives from Government and industry collaborating to identify threats, develop crisis response plans, and foster the relationships needed to quickly share information and respond to malicious cyber incidents. The JCDC has already had some early successes, most notably by bringing Government and the private sector together to respond to the Log4j vulnerability. Building resilience to potentially catastrophic cyber incidents will require an unprecedented level of planning, information sharing, and operational collaboration. Efforts to connect Government and industry experts, such as the JCDC, can identify and address threats far more effectively than can any single organization operating alone.

Equally important, however, is the role of SRMAs, each a vital component of the Federal Government's capacity to assist private-sector entities in improving cybersecurity. SRMAs have statutory responsibilities to work with their sectors on a day-to-day basis and help surface information relevant to other sectors and are vital for managing National risk. Agencies like the Department of Energy, the Department of the Treasury, and others are partnering closely with industry to share information, drive risk management activities, and collaborate to reduce risk.

Sector Coordinating Councils and organizations like ISACs and ISAOs have been proven to be useful mechanisms for information sharing, but we need to mature the policies and procedures for strengthening collaboration. NSA's Cybersecurity Collaboration Center, in partnership with the Defense Industrial Base Sector, is an example of the power of bringing together cyber threat experts and network defenders to enable more secure Department of Defense (DoD) and defense industry platforms and systems.

Resourcing SRMA functions, including those resident at CISA, is key to achieving the Federal coherence that is central to the strategic intent of the ONCD. ONCD is beginning an initiative to review the cyber capabilities and resources of SRMAs and understand the requirements to operationalize SRMAs so that they can better collaborate in cyber defense.

As part of this review, ONCD is examining current authorities and a pilot program that can be used to mature these efforts. We are also examining how we can improve internal Government capacity to collect and share threat intelligence with these entities.

We also need to strengthen our efforts to coordinate law enforcement capabilities with private-sector entities to combat botnets, ransomware, and other malicious activity. The Department of Justice, including the FBI, has enjoyed a string of successes in disrupting ransomware operations. ONCD is reviewing opportunities to create linkages to further mature the ability to coordinate these efforts with private-sector entities that may be targeted by threat actors or have information or capabilities that can support Government action.

Congress, Presidential policy, the Department of Homeland Security, and SRMAs have long recognized the need to identify critical infrastructure that if successfully targeted by adversaries could cause disproportionate harm to the American people and the U.S. economy. Section 9 of Executive Order 13636 requires the Secretary of Homeland Security to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or National security. In March 2020, the Cyberspace Solarium Commission proposed a "designation of critical infrastructure entities that manage systems and assets whose disruption could have cascading, destabilizing effects on U.S. National security, economic security, and public health and safety." These entities support National Critical Functions and are of heightened interest to nation-state adversaries. Given the potential consequences of a cyber incident impacting a Section 9 entity, there is a vested interest of both the Federal Government and the private sector to improve the security and resilience of these entities.

The administration supports the general concept of identifying systemically important entities that own, operate, or otherwise control critical infrastructure. ONCD is evaluating how to enhance the Federal Government's capacity to reduce the risk to National Critical Functions posed by adversaries against the entities that own and operate our most important systems and assets and to understand and improve their resiliency to cyber attacks. Specifically, we are examining authority and capacity to provide prioritized support to, and opportunities to collaborate with, these entities, as well as the possibility for tailored obligations required on designated entities. Additionally, CISA is currently developing a plan and time line for the rulemaking required under the Cyber Incident Reporting for Critical Infrastructure Act, or "CIRA". We look forward to working with Congress to ensure that any potential framework for systemically important entities is complementary to CIRA and other on-going efforts across the administration.

Finally, one of the most important things that we can do to mature the public-private partnership to secure U.S. critical infrastructure is to make sure we are extracting lessons learned from cyber incidents and implementing those lessons as rapidly as possible. The Biden-Harris administration created the Cyber Safety Review Board (CSRB) modeled after the National Transportation Safety Board with the goal of reviewing significant cyber incidents with this purpose in mind. Established in accordance with Section 5 of Executive Order 14028, the Board brings together Government and private-sector leaders to analyze significant cybersecurity incidents, generate lessons learned, and produce concrete recommendations to avoid future crises. Director Inglis proudly serves on the Board, which is currently undertaking a review of the vulnerabilities in the Log4j library that came to light last

December. I am also actively engaged in the review. Importantly, following this first review, the CSRB will review its own processes and develop plans for improving future reviews.

With the continued support of the President and the Congress, the Office of the National Cyber Director is committed to building robust relationships with industry and our interagency partners to enhance the security and resilience of our Nation's cyber ecosystem. Thank you for the opportunity to testify before you today, and I look forward to your questions.

Chairwoman CLARKE. Thank you for your testimony, Mr. Knake. I now recognize Dr. Sherman to summarize her statement for 5 minutes.

STATEMENT OF TINA WON SHERMAN, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. SHERMAN. Chairwoman Clarke, Ranking Member Garbarino, Ranking Member Katko, Members of the subcommittee, I am pleased to be here today to discuss our Nation's critical infrastructure alongside witnesses from two key Federal entities in this space.

As evidenced by yesterday's testimonies on Russian cyber threats and in the Comptroller General of the United States' comments in front of the House Appropriations Committee protecting the assets, systems, and networks that underpin our daily lives is a pressing and monumental task. We must safeguard not only our oil and gas pipelines, our water, and food manufacturing facilities, but also our cell towers and satellites, our financial and health institutions, and more from cyber and other attacks that occur almost daily.

The owners and operators of this infrastructure, many of whom are in the private sector, work closely with the Federal Government to implement measures that help prevent those attacks not only from foreign adversaries, but from domestic actors and insider threats. Regardless of their origins, the threats are real and require urgent action.

The agency I represent, GAO, has reported on critical infrastructure protection in response to Congressional interest for many years. In 1997, GAO first designated information security as a Government-wide high-risk area and, in 2003, expanded that area to include critical infrastructure protection. Since 2021, we have issued reports on several areas where urgent action is needed. This includes CISA's transformation initiative following its 2020 reorganization, its prioritization efforts and role in supporting the 16 critical infrastructure sectors, and Sector Risk Management Agencies' implementation of NIST's cybersecurity framework, to name a few.

One of the repeated themes that cuts across this work is the continued need to improve collaboration between the Government and the private sector. The diffuse and voluntary nature of the critical infrastructure landscape continues to pose a range of challenges to this community, from implementing security standards and effectively analyzing risks to sharing threat-related information and providing timely support and guidance to stakeholders.

The relatively new Federal entities, both CISA and ONCD, are uniquely positioned to play a significant role in protecting our Nation's critical infrastructure. Collaboration is essential and we have recommended to the Department of Homeland Security that it

strengthen efforts between public and private partners. While the Department has communicated to us that they are taking steps to implement our recommendations, we urge them to do so even more expeditiously to protect our economy, public health and safety, and National security from any future attacks.

Thank you for holding this hearing and for inviting me to participate in this conversation this morning.

[The prepared statement of Ms. Sherman follows:]

PREPARED STATEMENT OF TINA WON SHERMAN

WEDNESDAY, APRIL 6, 2022

GAO HIGHLIGHTS

Highlights of GAO–22–105973, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The Nation's critical infrastructure consists of physical and cyber assets and systems that are vital to the United States. Their incapacity or destruction could have a debilitating impact on security, National public health and safety, or National economic security. Critical infrastructure provides the essential functions—such as supplying water, generating energy, and producing food—that underpin American society. Protecting this infrastructure is a National security priority.

GAO first designated information security as a Government-wide high-risk area in 1997. This was expanded to include protecting: (1) Cyber critical infrastructure in 2003 and (2) the privacy of personally identifiable information in 2015.

This statement discusses DHS's efforts to address critical infrastructure security. For this testimony, GAO relied on selected products it issued from September 2018 to March 2022, including GAO–21–236 and GAO–22–104279.

What GAO Recommends

GAO has made various recommendations to strengthen critical infrastructure security efforts, with which DHS has agreed. DHS has implemented or described planned actions to address these recommendations.

CRITICAL INFRASTRUCTURE PROTECTION.—DHS ACTIONS URGENTLY NEEDED TO BETTER PROTECT THE NATION'S CRITICAL INFRASTRUCTURE

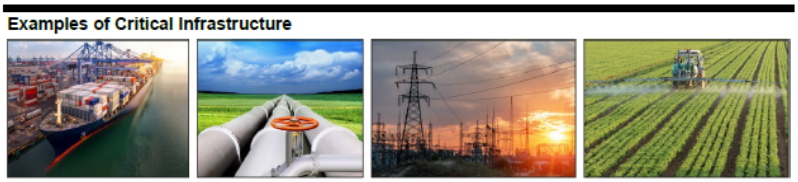
What GAO Found

To improve critical infrastructure security, key actions Department of Homeland Security (DHS) needs to take include: (1) Strengthening the Federal role in protecting the cybersecurity of critical infrastructure and (2) improving priority-setting efforts.

Strengthen the Federal role in protecting the cybersecurity of critical infrastructure.—Pursuant to legislation enacted in 2018, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS was charged with responsibility for enhancing the security of the Nation's critical infrastructure in the face of both physical and cyber threats. In March 2021, GAO reported that DHS needed to complete key activities related to the transformation of CISA. This includes finalizing the agency's mission-essential functions and completing workforce planning activities. GAO also reported that DHS needed to address challenges identified by selected critical infrastructure stakeholders, including having consistent stakeholder involvement in the development of related guidance. Accordingly, GAO made 11 recommendations to DHS, which the Department intends to implement by end of 2022.

Improve priority-setting efforts.—Through the National Critical Infrastructure Prioritization Program, CISA is to identify a list of systems and assets that, if destroyed or disrupted, would cause National or regional catastrophic effects. Consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007, CISA annually updates and prioritizes the list. The program's list is used to inform the awarding of preparedness grants to States. However, in March 2022, GAO reported that 9 of 12 CISA officials and all 10 of the infrastructure stakeholders GAO interviewed questioned the relevance and usefulness of the program. For example, stakeholders questioned the current relevance of the criteria used to add critical infrastructure to the Prioritization Program list. In 2019, CISA pub-

lished a set of 55 National critical functions of the Government and private sector considered vital to the security, economy, and public health and safety of the Nation (see figure). However, most of the Federal and non-Federal critical infrastructure stakeholders that GAO interviewed reported being generally uninvolved with, unaware of, or without an understanding of the goals of the framework for its critical functions. GAO made recommendations to DHS in its March 2022 report to address these concerns, such as ensuring stakeholders are fully engaged in the framework's implementation, and DHS agreed with the recommendations.



Source: (L to R) anekoho/stock.adobe.com, Sergiy Serdyuk/stock.adobe.com, yelantsevv/stock.adobe.com, Federico Rostagno/stock.adobe.com. | GAO-22-105973

Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee: Thank you for the opportunity to contribute to today's discussion on Federal perspectives to secure the Nation's critical infrastructure.[1] As you know, the Nation's critical infrastructure consists of physical and cyber assets and systems that are vital to the United States. Their incapacity or destruction could have a debilitating impact on security, National economic security, or National public health and safety.[2] Critical infrastructure provides the essential functions—such as supplying water, generating energy, and producing food—that underpin American society. Protecting this infrastructure is a National security priority.

We have long stressed the urgent need for effective cybersecurity to protect critical infrastructure, as underscored by increasingly sophisticated threats and frequent cyber incidents.[3] Recent events—including the ransomware attack that led to a shutdown of a major U.S. fuel pipeline, cyber threat actors who obtained unauthorized access to a U.S. water treatment facility in an attempt to increase the amount of a caustic chemical that is used as part of the water treatment process, and a cyber attack campaign again U.S. Government agencies and other entities—have illustrated that the Nation's critical infrastructure continues to face growing cyber threats.[4] Because the majority of critical infrastructure is owned and operated by the private sector, it is vital that the public and private sectors work together to protect these assets and systems.

My remarks today will focus on DHS's efforts to strengthen the Federal role in protecting the cybersecurity of critical infrastructure and improving its priority-setting efforts. This statement is based on the results of our prior work, which includes the reports and testimonies that we cite throughout this statement, issued from September 2018 to March 2022. Detailed information about the scope and methodology for our prior work can be found in the products cited throughout this statement.

We conducted the work on which this statement is based in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

[1] The term "critical infrastructure," as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, National economic security, National public health or safety, or any combination of these. 42 U.S.C. § 5195c(e).

[2] 242 U.S.C. § 5195c(e).

[3] See, for example, GAO, *Cybersecurity and Information Technology: Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas,* GAO–21–105325 (Washington, DC: July 28, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO–21–288 (Washington, DC: Mar. 24, 2021).

[4] For more information regarding such recent events, see GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks,* GAO–21–594T (Washington, DC: May 25, 2021). Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

BACKGROUND

Information systems supporting Federal agencies and our Nation's critical infrastructure—such as transportation systems, communications, education, energy, and financial services—are inherently at risk. Compounding the risk, systems and networks used by Federal agencies and our Nation's critical infrastructure are also often interconnected with other internal and external systems and networks, including the internet. Examples of critical infrastructure are shown in figure 1.

The Department of Homeland Security (DHS) coordinates the overall Federal effort for National critical infrastructure protection.[5] This effort spans across the 16 Federally-designated sectors and prioritizing available resources to the most critical infrastructure can enhance our Nation's security, increase resiliency, and reduce risk.[6] Our prior work has cited DHS actions to identify and assess risk to critical infrastructure. For example, we reported in March 2022 on DHS's Cybersecurity and Infrastructure Security Agency's (CISA) programs to prioritize assets and systems for protection efforts.[7] Specifically, we evaluated the National Critical Infrastructure Prioritization Program (NCIPP), which, consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007, annually prioritizes critical infrastructure based on the consequences associated with the disruption or destruction of those assets.[8] The program's list is used to inform the awarding of preparedness grants to States. We also examined CISA's National Critical Functions framework, which consists of 55 National Critical Functions, which are the functions of Government and non-Governmental entities 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. Our prior findings on both the NCIPP and National Critical Functions framework are discussed later in this statement.

Source: (L to R) anekoho/stock.adobe.com, Sergiy Serdyuk/stock.adobe.com, yelantsevv/stock.adobe.com, Federico Rostagno/stock.adobe.com. | GAO-22-105973

GAO Has Previously Identified Four Major Cybersecurity Challenges Facing the Nation

To underscore the importance of this issue, we have designated information security as a Government-wide high-risk area since 1997.[9] In 2003, we added the protection of critical infrastructure to the information security high-risk area, and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.[10]

In our high-risk updates from September 2018 and March 2021, we emphasized the critical need for the Federal Government to take 10 specific actions to address

[5] The Homeland Security Act of 2002 created DHS and gave the agency responsibilities for coordinating National critical infrastructure protection efforts. See generally Pub. L. No. 107–296, tit. II, 115 Stat. 2135, 2145.

[6] Federal policies identify 16 critical infrastructure sectors: Chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; Government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[7] GAO, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing,* GAO–22–104279 (Washington, DC: Mar. 1, 2022)

[8] Originally developed in 2006, the NCIPP identifies critical infrastructure that would result in National-level consequences if disrupted or destroyed, resulting in Classified lists of specific assets, clusters, and systems. The NCIPP annually prioritizes critical infrastructure based on the consequences associated with the disruption or destruction of those assets. To conduct this work, CISA coordinates a voluntary effort with States and other partners to identify, prioritize, and categorize high-priority critical infrastructure.

[9] GAO, *High-Risk Series: Information Management and Technology,* HR–97–9 (Washington, DC: Feb. 1997). GAO maintains a high-risk program to focus attention on Government operations that it identifies as high-risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[10] GAO, *High-Risk Series: An Update,* GAO–15–290 (Washington, DC: Feb. 11, 2015) and *High-Risk Series: An Update,* GAO–03–119 (Washington, DC: Jan. 2003).

4 major cybersecurity challenges that the Federal Government faces.[11] These challenges are: (1) Establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing Federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.

Federal Law and Policy Establish Requirements for Critical Infrastructure

Federal law and policy establish roles and responsibilities for the protection of critical infrastructure, discussed below in chronological order.

- *Presidential Policy Directive 21*.—In February 2013, the White House-issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience,* to specify critical infrastructure responsibilities.[12] Among other things, the order designated 9 Federal sector-specific agencies with lead roles in protecting critical infrastructure sectors. The lead agencies coordinate Federally-sponsored activities within their respective sectors. The policy also directed DHS to coordinate with lead agencies to develop a description of functional relationships across the Federal Government related to critical infrastructure security and resilience. The policy further provided that DHS, in coordination with lead agencies, to conduct an analysis and recommend options for improving public-private partnership effectiveness.
- *Executive Order 13636*.—In February 2013, the White House-issued Improving Critical Infrastructure Cybersecurity, Executive Order 13636, which called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing.[13] To do so, the order established mechanisms for promoting engagement between Federal and private organizations. Further, the order directed DHS, with help from the lead agencies, to identify, annually review, and update a list of critical infrastructure sectors for which a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or National security.
- *National Institute of Standards and Technology (NIST) Cybersecurity Framework*.—Executive Order 13636 directed NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of standards, procedures, and processes.[14] Further, the order directed the lead agencies, in consultation with DHS and other interested agencies, to coordinate with critical infrastructure partners to review the cybersecurity framework. The agencies, if necessary, should develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.
  In response to the order, in February 2014, NIST first published its framework—a voluntary, flexible, performance-based framework of cybersecurity standards and procedures. The framework, which was updated in April 2018, outlines a risk-based approach to managing cybersecurity that is composed of three major parts: A framework core, profiles, and implementation tiers.[15] The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes.
- *Cybersecurity and Infrastructure Security Agency Act of 2018*.—The November 2018 act established CISA,[16] within DHS, and gave it responsibility to coordinate a National effort to secure and protect against critical infrastructure risks. To implement this legislation, CISA undertook a three-phase organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.
- *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*.—The act established roles and responsibilities for lead agencies, known as sector risk management agencies, in protecting the 16 critical infrastructure agencies.[17] According to the act, among other things, the lead agencies

---

[11] GAO–21–288 and GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO–18–622 (Washington, DC: Sept. 6, 2018).

[12] The White House, *Presidential Policy Directive/PPD–21: Critical Infrastructure Security and Resilience,* (Washington, DC: Feb. 12, 2013).

[13] Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

[14] The Cybersecurity Enhancement Act of 2014 authorized NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure. 15 U.S.C. § 272(c)(15). The *Framework for Improving Critical Infrastructure Cybersecurity* represents that voluntary set of standards.

[15] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Washington, DC: April 2018).

[16] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, 132 Stat. 4168, 4169, (Nov. 16, 2018) (codified at 6 U.S.C. § 652). The act renamed the DHS National Protection and Programs Directorate as CISA.

[17] The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 states that the term "sector risk management agency" replaces the term "sector-specific agency"

are required to: (1) Coordinate with DHS and collaborate with critical infrastructure owners and operators, regulatory agencies, and others; (2) support sector risk management, in coordination with CISA; (3) assess sector risk, in coordination with CISA; (4) coordinate the sector, including by serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities; and (5) support incident management, including supporting CISA, upon request, in asset response activities.

The act also established the Office of the National Cyber Director within the Executive Office of the President.[18] Among other responsibilities, the Director is to serve as the principal advisor to the White House on cybersecurity policy and strategy, including coordination of implementation of National cyber policy and strategy.

In June 2021, the Senate confirmed a director to lead this new office. In October 2021, the National Cyber Director issued a strategic intent statement, outlining a vision for the Director's office and the high-level lines of efforts it intends to focus on, including National and Federal cybersecurity; budget review and assessment; and planning and incident response, among others.[19]

- *Executive Order 14028*.—In May 2021, the President issued, Improving the Nation's Cybersecurity, Executive Order 14028, that was prompted, in part, by malicious cyber campaigns that threaten the public and private sectors.[20]

DHS ACTIONS URGENTLY NEEDED TO PROTECT CRITICAL INFRASTRUCTURE

Over the last several decades, we have emphasized the urgent need for the Federal Government to improve its ability to protect against cyber and other threats to our Nation's critical infrastructure. In our recent work, we emphasized the need for the Federal Government to address major cybersecurity challenges through critical actions. These actions include the need for DHS to strengthen its role in protecting the cybersecurity of critical infrastructure. In addition, as we reported in March 2022, DHS's CISA should take actions to improve its priority-setting efforts for the protection of critical infrastructure.[21]

DHS Needs to Strengthen Its Role in Protecting the Cybersecurity of Critical Infrastructure

The Federal Government has been challenged in working with the private sector to protect critical infrastructure. We have made recommendations aimed at strengthening DHS's role in critical infrastructure cybersecurity, including by: (1) Enhancing the capabilities and services of CISA and (2) ensuring that Federal agencies with sector-specific responsibilities are providing their sector partners with effective guidance and support.

DHS Needs to Complete CISA Transformation Activities

The importance of clear cybersecurity leadership extends beyond the White House to other key Executive branch agencies, including DHS. Federal legislation enacted in November 2018 established CISA within the Department to advance the mission of protecting Federal civilian agencies' networks from cyber threats and to enhance the security of the Nation's critical infrastructure in the face of both physical and cyber threats. The act elevated CISA to agency status; prescribed changes to its structure, including mandating that it have separate divisions on cybersecurity, infrastructure security, and emergency communications; and assigned specific responsibilities to the agency.[22]

To implement the statutory requirements, CISA leadership launched an organizational transformation initiative. In March 2021, we reported that CISA had completed the first two of the three phases of its organizational transformation initia-

---

in the Homeland Security Act of 2002. The act amends the Homeland Security Act of 2002 and sets out sector risk management agency responsibilities within this critical infrastructure framework. Pub. L. No. 116–283, § 9002, 134 Stat. 3388, 4768.

[18] Pub. L. No. 116–283, § 1752, 134 Stat. at 4144 (codified at 6 U.S.C. § 1500).

[19] The White House, *A Strategic Intent Statement for the Office of the National Cyber Director* (Washington, DC: Oct. 28, 2021).

[20] Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021).

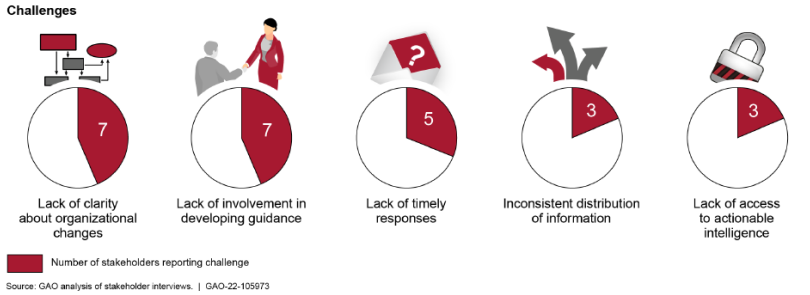
[21] GAO–22–104279.

[22] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, § 2,132 Stat. 4168, 4169, (codified at 6 U.S.C. § 652). The act renamed the DHS National Protection and Programs Directorate as CISA.

tive.[23] Specifically, we noted DHS had not fully implemented its phase three transformation, which included finalizing the agency's mission-essential functions and completing workforce-planning activities by December 2020.

We also found that of 10 selected key practices for effective agency reforms we previously identified, CISA's organizational transformation generally addressed 4, partially addressed 5, and did not address 1. Further, we reported on a number of challenges that selected Government and private-sector stakeholders had noted when coordinating with CISA, including a lack of clarity surrounding its organizational changes and the lack of stakeholder involvement in developing guidance. Although CISA had activities under way to mitigate some of these challenges, it had not developed strategies to, among other things, clarify changes to its organizational structure. Figure 2 below describes the coordination challenges identified by private-sector stakeholders.

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors



To address these weaknesses, we made 11 recommendations to DHS. The Department concurred with our recommendations and, as of September 2021, reported that it intends to fully implement them by the end of calendar year 2022. Implementing these recommendations will better position CISA to ensure the success of its reorganization efforts and carry out its mission to lead National efforts to identify and respond to cyber and other risks to our Nation's infrastructure.

Sector Risk Management Agencies Need to Ensure Effective Guidance and Support

Since 2010, we have made about 80 recommendations for various Federal agencies to enhance infrastructure cybersecurity. For example, in February 2020, we recommended that agencies better measure the adoption of the NIST framework of voluntary cyber standards and correct sector-specific weaknesses. Specifically, we found that most sector risk management agencies were not collecting and reporting on improvements in the protection of critical infrastructure as a result of using the framework across the sectors.[24] We concluded that collecting and reporting on these improvements would help the sectors understand the extent to which sectors are better protecting their critical infrastructure from cyber threats.

To address these issues, we made 10 recommendations—one to NIST on establishing time frames for completing selected programs—and 9 to the lead agencies, to collect and report on improvements gained from using the framework. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. However, as of November 2021, none of the recommendations had been implemented. Until the lead agencies collect and report on improvements gained from adopting the framework, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructure from threats will be largely unknown. We reiterated these recommendations in a February 2022 report.[25]

---

[23] GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation,* GAO–21–236 (Washington, DC: Mar. 10, 2021).

[24] GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements,* GAO–20–299 (Washington, DC: Apr. 9, 2020).

[25] GAO, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance,* GAO–22–105103 (Washington, DC: Feb. 9, 2022).

We have also frequently reported on the need for lead agencies to enhance the cybersecurity of their related critical infrastructure sectors and subsectors—such as transportation systems, communications, energy, education, and financial services.[26]

CISA Should Improve its Priority-Setting Efforts

CISA and Critical Infrastructure Stakeholders Do Not Find the NCIPP Useful

In our March 2022 report, CISA and other critical infrastructure stakeholders we spoke with told us that the NCIPP's results were of little use. In addition, the stakeholders raised concerns with the program, which included the relevance of the program's criteria given the current threat environment, limited State participation, and lack of use among critical infrastructure stakeholders.[27]

Relevance of NCIPP criteria, given current threat environment.—We reported in March 2022 that CISA and other stakeholders questioned the present-day relevance of the criteria for adding critical infrastructure to the NCIPP list. To be included on the NCIPP's Level 1 list (its highest consequence list), an asset's destruction or disruption must meet minimum specified consequence thresholds for at least two of the following four categories: Economic loss, fatalities, mass evacuation length, and degradation of National security.[28]

Senior officials with CISA, as well as other Federal, State, and private-sector officials we spoke with said that the consequence thresholds for these criteria did not reflect the current threat environment, which focuses more on cyber attacks and extreme weather events. The threat environment also focuses on vulnerabilities or attacks that can affect multiple entities within a short period. In this scenario, the consequences related to a single asset, entity, system, or cluster may not reach NCIPP thresholds, but the aggregate impacts may be Nationally significant, according to CISA officials.

Limited State participation.—As part of the NCIPP process, we found in our March 2022 report that State homeland security agencies identify relevant critical infrastructure—both public and private—and nominate those assets for inclusion on the NCIPP list.[29] However, CISA data showed that since fiscal year 2017, no more than 14 States (of 56 States and territories) provided new nominations or updates to the program in any given fiscal year.

Lack of use among critical infrastructure stakeholders.—Critical infrastructure stakeholders, including Protective Security Advisors (PSAs) and Cybersecurity Advisor (CSAs),[30] we interviewed for our March 2022 report also questioned the NCIPP's

---

[26] GAO–21–288. See also GAO, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses,* GAO–21–105263 (Washington, DC: July 27, 2021); GAO, *Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices,* GAO–20–404 (Washington, DC: Apr. 3, 2020); GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector,* GAO–20–104462 (Washington, DC: Nov. 23, 2021); GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid,* GAO–19–332 (Washington, DC: Aug. 26, 2019); GAO, *Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems,* GAO–21–81 (Washington, DC: Mar. 18, 2021); GAO, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K–12 Schools from Cyber Threats,* GAO–22–105024 (Washington, DC: Oct. 13, 2021); and GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts,* GAO–20–631 (Washington, DC: Sept. 17, 2020).

[27] GAO–22–104279.

[28] CISA coordinates a voluntary effort with States and other partners to identify, prioritize, and categorize high-priority critical infrastructure as either Level 1 or Level 2 based on the possible consequences to the Nation in terms of our factors—fatalities, economic loss, mass evacuation length, and degradation of National security. According to DHS, the overwhelming majority of the assets and systems identified through the NCIPP are categorized as Level 2. Only a small subset of assets meet the Level 1 consequence threshold—those whose loss or damage could result in major National or regional impacts similar to the impacts of Hurricane Katrina or the September 11, 2001, attacks. The precise consequence thresholds for inclusion on the NCIPP list are information that DHS has designated as "for official use only." We did not include the specific thresholds in this report so that we could publically present the results of our work.

[29] GAO–22–104279.

[30] CISA offers government (Federal, State, local, Tribal, and territorial), private sector, and other critical infrastructure stakeholders a suite of programs and services to identify and mitigate risks to infrastructure security. These include infrastructure and cybersecurity services, some of which are carried out by CISA's PSAs and CSAs. PSAs are operators with expertise in physical security protection, and CSAs are cybersecurity specialists responsible for helping to bolster owners' and operators' cybersecurity capabilities. Both types of advisors use their respective assessment tools to work with critical infrastructure stakeholders to help make critical

Continued

usefulness.[31] These stakeholders noted that the data were not accurate, relevant, consistent, or reflective of infrastructure risk. For example:

- *PSAs and CSAs*.—Three of the 12 PSAs and CSAs we spoke with reported using the NCIPP list to a limited degree when planning annual outreach to some facilities. However, these same officials (as well as the other 9 we spoke with) all questioned the list's accuracy and relevance. For example, one CSA said that the current NCIPP list was missing key assets that needed protection because the current criteria to be included on the list were outdated.
- *Sector Risk Management Agencies*.—None of the 4 Sector Risk Management Agency officials we contacted reported regularly using the NCIPP list.[32] Sector Risk Management Agency officials raised a number of issues with the results, leading them to not rely on the list for risk management purposes. For example, officials from one Sector Risk Management Agency said their department had a copy of the list, but it was generally not something they referred to regularly or used in their efforts. Officials felt that the types of infrastructure on the list were not consistent across regions.
- *State homeland security agencies*.—Only 1 of the 6 State homeland security agencies we contacted reported regularly using the NCIPP list.[33] State homeland security agency officials questioned the list's accuracy, and most said that they did not use the list to inform risk communication or influence decisions.

Given the evolving risk landscape and CISA and the critical infrastructure community's recognition of the NCIPP's limitations, we made two recommendations to CISA regarding NCIPP: (1) That the agency improve its NCIPP process to better reflect current threats and (2) the agency should seek input from States that have not provided recent updates on identifying critical infrastructure. DHS concurred with the recommendations and described initial actions under way or planned in response to our report, with completion expected by September 2023.

Limited Understanding of National Critical Functions Framework May Pose Challenges

We reported in March 2022 that CISA's National Risk Management Center published a set of 55 critical functions in spring 2019 as part of its new National Critical Functions framework.[34] According to CISA officials, since 9/11, the complexity and interdependency of critical infrastructure has expanded significantly. While the NCIPP has historically focused on protecting physical assets within the context of the 16 critical infrastructure sectors, primarily from acts of terrorism, the framework reflects a shift in risk management. The shift emphasizes resilience—maintaining and restoring the Nation's essential services and customary conveniences—along with hazards and threats that are increasingly cross-cutting in nature, particularly around cybersecurity and natural disasters. The complete list of functions is shown in figure 3.

---

infrastructure more resilient. CSAs and PSAs operate across CISA's 10 regions. CSAs and PSAs we interviewed were from Regions 2, 3, 4, 5, 7, and 8. We also interviewed the CISA Regional Coordinator from Region 10 for contextual information on the regional coordinator role; however, this interview is not included in our overall total number of regional stakeholder interviews, which include only the PSAs and CSAs.

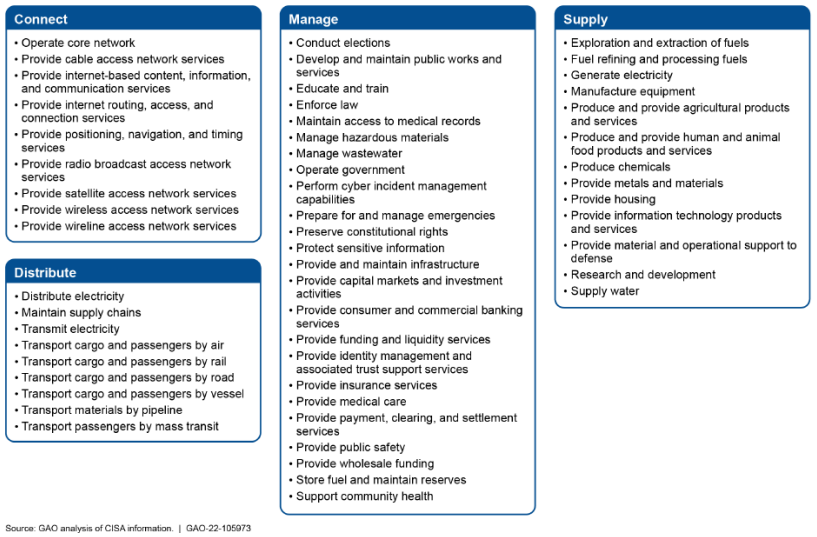
[31] GAO–22–104279.

[32] Sector Risk Management Agencies we interviewed were the Department of Energy (energy sector), Environmental Protection Agency (water sector), and CISA (both the critical manufacturing and IT sectors).

[33] One State homeland security official said that while data on the NCIPP was problematic, his State did refer to the NCIPP each year to inform the State's grant allocation methodology.

[34] GAO–22–104279.

Figure 3: Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions



Source: GAO analysis of CISA information. | GAO-22-105973

Seven of 25 critical infrastructure stakeholders we met with were aware of and supportive of CISA's new direction and had positive feedback on the National Critical Functions; however, most of the Federal and non-Federal critical infrastructure stakeholders we interviewed reported being generally uninvolved with, unaware of, or not understanding the goals of the framework. Specifically, stakeholders did not understand how the framework related to prioritizing infrastructure, how it affected planning and operations, or where their particular organizations fell within the framework.

For example, 8 of the 25 officials we interviewed said that communication from CISA headquarters regarding the National Critical Functions framework needed improvement. Industry officials from 1 of the 4 sectors we met with said that their sector's members were trying to cooperate with CISA and provide data when CISA requested it but said that the requests were often broad or their goals unclear. Officials from one State homeland security agency said that CISA often shares complex and academic presentations about sophisticated risk modeling and visualizations; however, officials said they felt those presentations were too complicated and, therefore, they did not know how they were supposed to use the information.

Five of 6 CISA regional CSAs—who are responsible for reducing cybersecurity risks to the Nation's critical infrastructure—were also not using or did not understand how the National Critical Functions would affect their stakeholders, despite some of the functions having a cyber and IT focus. For example, one advisor said that they and their stakeholders—organizations for which he provides cybersecurity assessments—are bombarded with information. The advisor stated that they have not had time to understand the National Critical Functions framework, which they believed was more focused on physical security, rather than cybersecurity. The PSA and CSA in one region said that there was no prioritization within the 55 critical functions, making everything equally critical. Accordingly, the officials said they did not have a clear sense of what they—or DHS broadly—should prioritize. In response, CISA officials stated that stakeholders with local operational responsibilities were the least likely to be familiar with the National Critical Functions. These functions were conceived to improve the analysis and management of cross-sector and National risks. Still, CISA officials acknowledged the need to improve connection between the National Critical Functions framework and local and operational risk management activities and communications.

As we stated in our March 2022 report, helping to ensure that stakeholders understand the goals of the framework and are involved in its implementation could

aid CISA in its future infrastructure protection efforts.[35] We therefore recommended that CISA ensure that stakeholders are fully engaged in the implementation of the National Critical Functions framework. DHS concurred with the recommendation and described initial actions under way or planned in response to our report, with estimated completion by October 2022.

In summary, cyber attacks, physical attacks, and other threats facing the Nation's critical infrastructure require an effective and coordinated public-private response. CISA has undertaken a wide range of efforts to identify and prioritize nationally significant critical infrastructure. However, as our previously-reported findings and recommendations indicate, urgent action is needed and CISA should take steps to improve and further these efforts. By taking steps to ensure that is process for identifying and prioritizing critical infrastructure accounts for current threats and meets the needs of all States, CISA and its partners could have a more relevant and useful understanding of critical infrastructure risk.

Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

Chairwoman CLARKE. Thank you, Dr. Sherman, for your testimony this morning. The Chair now recognizes the Ranking Member of the full committee, the gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Thank you, Madam Chair, for giving me the time to speak today, and thank you all for being here. It is a most important topic. I thank you, Mr. Garbarino, for holding this important hearing, as well.

The public-private partnership that CISA maintains are integral to its ability to protect the Nation from cybersecurity threats. Yesterday's full committee hearing which we had in this room showed us that CISA's work in this space is excelling, but there is always room for improvement. We must work to ensure that CISA maintains the tools, resources, and relationships that it needs to protect our Nation's critical infrastructure.

I have worked diligently, as well as my colleagues have, to ensure that CISA's adequately resourced in terms of funding, authorities, and work force, but we can't overlook the importance of the close and trusted relationships that CISA has developed with the private sector. It is just outstanding what you have done and we have got to keep that going. Those relationships is what allows the agency to collect and disseminate timely and valuable threat information in a trusted manner.

Despite the passage of the cyber incident reporting legislation this year, which I think is a critical piece of legislation, which Madam Chair was a lead on, we can't lose sight of the value of those voluntary relationships. For example, last year, CISA took an important step forward by leveraging the authorities provided in the fiscal year 2021 NDAA to establish the Joint Cyber Defense Collaborative, or JCDC. As the committee discussed yesterday, the JCDC has served as a force multiplier for our Nation's cybersecurity and it is wholly dependent on the voluntary relationship framework.

Last year, I introduced the Securing Systemically Important Critical Infrastructure Act to allow CISA to efficiently allocate its resources by establishing a thoughtful, transparent, stakeholder-engaged process to identify what truly constitutes critical infrastructure. This methodical identification process would be accom-

[35] GAO–22–104279.

panied by a prioritization of benefits for those entities deemed SICI. For the first time this effort would move CISA away from the current first-come first-served approach model by establishing a true risk-based approach to Federal cyber assistance.

While there are conflicting opinions between my colleagues and myself on the right direction for SICI, I think we can all agree that allowing CISA to maintain its close partnerships with the private sector is the keystone to its long-term success and the cybersecurity of our Nation.

I look forward to exploring these issues further with our witnesses today and I thank you again for being here. I thank, again, Chairwoman Clarke and Ranking Member Garbarino for your work on these issues. With that, I yield back.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

Thank you, Chairwoman Clarke and Ranking Member Garbarino for holding this important hearing today.

The public-private partnerships that CISA maintains are integral to its ability to protect the Nation from cybersecurity threats.

Yesterday's full committee hearing showed us that CISA's work in this space is excelling, but there is always room for improvement.

We must work to ensure that CISA maintains the tools, resources, and relationships it needs to protect our Nation's critical infrastructure.

I've worked diligently to ensure that CISA is adequately resourced in terms of funding, authorities, and workforce, but we can't overlook the importance of the close and trusted relationships that CISA maintains.

Those relationships are what allows the agency to collect and disseminate timely and valuable threat information.

Despite the passage of Cyber Incident Reporting legislation this year, we can't lose sight of the value of those voluntary relationships.

For example, last year, CISA took an important step forward by leveraging the authorities provided in the fiscal year 2021 NDAA to establish the Joint Cyber Defense Collaborative, or "JCDC."

As the committee discussed yesterday, the JCDC has served as a force multiplier for our Nation's cybersecurity, and it is wholly dependent on the voluntary relationship framework.

Last year, I introduced the Securing Systemically Important Critical Infrastructure Act to allow CISA to more efficiently allocate its resources by establishing a thoughtful, transparent, stakeholder-engaged process to identify what truly constitutes critical infrastructure.

This methodical identification process would be accompanied by prioritization of benefits for those entities deemed SICI. For the first time, this effort would move CISA away from the current first-come, first-served model by establishing a true risk-based approach to Federal cyber assistance.

While there are conflicting opinions on the right direction for SICI, I think we can all agree that allowing CISA to maintain its close partnerships with the private sector is the keystone to its long-term success, and the cybersecurity of our Nation.

I look forward to exploring these issues further with our witnesses. Thank you again for being here, and thank you, Chairwoman Clarke and Ranking Member Garbarino, for your work on these issues.

Chairwoman CLARKE. I thank our Ranking Member, Mr. Katko, for his opening statement. I want to thank our witnesses for their testimony.

I will remind the subcommittee that we will each have 5 minutes to question the panel. I now recognize myself for questions.

As I mentioned in my opening, with cyber incident reporting legislation behind us, I want to use this hearing to talk about what is next. The Solarium Commission recommended a new designation for entities that are the most critical of the critical or systemically important to our National security, which would come with bene-

fits, such as threat intelligence, and burdens, like security requirements.

Mr. Goldstein, broadly speaking, does CISA support the concept of codifying this designation as the Solarium Commission described it with benefits and burdens for designees or is CISA envisioning a different approach?

Mr. GOLDSTEIN. Thank you, ma'am. Prioritization is foundational to our ability to protect the country against both cyber and physical threats. Within CISA today we are focused on developing a list of what we call systemically important entities that are critical to National critical function, these sorts of services upon which Americans depend every day to go about their daily lives. Based upon this prioritization effort, we will be more effectively able to drive operational collaboration with those organizations that have the ability, the scale, the visibility to drive down risk for the Nation and prioritize our provision of services and develop new services that are most effectively tailored to support those entities that are most critical to our country.

Our work in developing this systemically important entity list aligns closely to the definition and the approach proposed by the Solarium Commission. Our focus importantly here is on entities, who are the organizations with whom we need to partner. But the underlying philosophy of prioritization as an enabler of collaboration and an enabler of risk reduction is one in which we are wholeheartedly focused.

Our priority today is ensuring that we understand these prioritized entities and we can work within our current voluntary model to ensure that we are driving operational collaboration and provision of services to drive down risk to these entities and the National critical functions that they support. We very much look forward to updating the subcommittee and your staff on our progress in developing this list and working with you going forward to ensure we have the authorities and resources to make the best use of this prioritization.

Chairwoman CLARKE. Mr. Knake, as Congress considers this new designation, what are some of the competing priorities and tradeoffs? For instance, is the goal to cement long-term operational partnerships with key partners or is it more about developing a dynamic methodology that can be used as threats evolve, whether that is a pandemic, a hurricane, or a war in Eastern Europe?

Mr. KNAKE. Thank you for the question. I think we want to look at, and I think this aligns very well with where CISA is and the National Risk Management Center is, on the ability to both have a dynamic list based on current threats as well as an understanding of what are the entities that are on a consequence base the most essential and the most important? So, what we have seen as we work through the pandemic, what we have seen as we work through the threat from Russia, is CISA and the NRMC have been able to move quite rapidly to say here are the organizations that are most affected by this emerging threat, who are most at risk.

At the same time, a much smaller list is needed and exists of those systemically important entities that are really just consequence-driven, that no matter what the vulnerabilities are or the threats are, we need to make sure that they have got the protec-

tions in place so the American people can be assured that the services and the functions they provide will continue. So, I don't think it is necessarily an either/or.

Chairwoman CLARKE. Dr. Sherman, this is not the first time we have tried to identify our most significant infrastructure. Can you talk about some of the challenges GAO has uncovered with respect to maintaining these lists and making sure they are relevant and useful? How important is it that we go into this with a clear sense of the goals and security outcomes we are trying to achieve?

Ms. SHERMAN. Ensuring that the list is valued or perceived as valued, relevant, and useful by stakeholders, both within Government and the private sector, is critical. Yes, goals and strategies are also key.

Based on our work, actually both in 2013 and the work that we recently carried out in 2022, there were similar themes that we identified with respect to the list that emerges from the National Asset Database. The first one is concerns not only from external private-sector stakeholders, but within the Federal Government, as well, that the assets on the list are not reflective of current threats, most importantly cyber attacks. Therefore, again, to be able to demonstrate the value of that list, it is important to make sure that it is current, relevant, and useful.

Then finally, with respect to goals and strategies, it is absolutely important to make sure that it is transparent and clear in terms of what the endpoint is for having a list. Let us prioritize how it will be used and working backward to make sure those goals and strategies are met.

Chairwoman CLARKE. Thank you. Before I yield back I want to know how critical it is that as you begin rolling up your sleeves on cyber incident reporting, we do everything you can to expedite this rulemaking, recognizing, of course, that we also need to allow for ample stakeholder consultation and regulatory harmonization.

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

Mr. GARBARINO. Thank you, Chairwoman. Mr. Goldstein, you were just talking about the voluntary relationship model and JCDC, I think, is a great example of what has been going on. Have you run into any hurdles in building this out? If so, how can we help?

Mr. GOLDSTEIN. Thank you, sir. The collaboration that we have seen through the Joint Cyber Defense Collaborative has been nothing short of remarkable. In the course of our Nation's response to the Russian invasion of Ukraine, we have operational collaboration virtual environment through the JCDC with our Nation's largest and most important technology companies, energy firms, financial entities, and those organizations were identified based upon their criticality, really a leading example of the sort of operational collaboration that we can drive through efforts like the identification of systemically important entities.

What we have seen, and this was reflected in yesterday's hearing in the full committee, is the best way of incentivizing voluntary collaboration is for the Government to show value, the Government to be at the table cohesively as a co-equal partner across all of the dif-

ferent agencies that have different equities in this space, with CISA serving as the convening platform, as the lead for domestic cyber defense. Then providing our partners in the private sector with both the platform and the opportunity to exchange information and get real value in return.

We have seen remarkable improvements even in the last 6 months in this kind of effort and we are excited for the maturation to come.

Mr. GARBARINO. That is great to hear. Do you think that these partnerships with the companies, the private sector being so willing to work with us and have this partnership, should we be concerned that these relationships might change if CISA takes more of a regulator role, if we turn it into a regulator? Is that a concern that you have heard from the private sector?

Mr. GOLDSTEIN. Certainly CISA's role in the current space as a trusted partner in cybersecurity, where our goal is solely to catalyze and improve cybersecurity as a voluntary partner, is one that is invaluable. That is a relationship that we work very hard to preserve and advance with partners across sectors.

Mr. GARBARINO. The Chairwoman mentioned it. The Chairwoman mentioned when she talked about the importance for rulemaking, especially with the new cyber incident reporting bill, but systemically critical infrastructures, you know, making sure that list up to date, as Dr. Sherman said, do you have the resources to be able to do both right now? Do you need more? Can you tell us what CISA needs?

Mr. GOLDSTEIN. So, we are deeply grateful for the work of Congress and this committee for providing CISA with additional resources in the recently-passed omnibus and working with us to ensure that we have a growth trajectory that aligns with the breadth of our National mission. Certainly we know that the cyber and physical security risks facing our country continue to get more grave and we look forward to working with the committee to ensure that in future years our growth continues on the appropriate pace so that we can effectively address the threats we are facing.

Mr. GARBARINO. But you feel like you will be able to get both done?

Mr. GOLDSTEIN. Today we are able to execute the mission ahead of us in the immediate future, but certainly we will want to continue to work together to ensure that we continue to meet the risk.

Mr. GARBARINO. Great. Dr. Sherman, you mentioned in your opening statement that you have a list of items that you want the agency and DHS to take up and you are hoping to implement them quickly. What is on the list? What recommendations do you have?

Ms. SHERMAN. Sure. So, based on the recent report and the comments I made in response to Chairwoman Clarke, it is important to ensure that the list that is prioritized as a function of the National Asset Database reflects current threats. We also believe that stakeholder input is increased. We feel like it is important to make sure that State and local governments, as well as the private sector, are able to more proactively share their perspective in terms of nominations and removals as part of the list, the prioritization list.

One of the things that we had found actually over the past 5 fiscal years is that in any given fiscal year there were no more than 14 States that provided input to CISA related to the prioritized list. We think that is for several reasons, one of which is that they don't find value in the list because it is not reflective of what they think is truly important. They don't believe that the different types of infrastructure that are included on the list are consistent across States. They have raised concerns that—with respect to how the list is actually used and how meaningful it really is for them.

So, we definitely believe that increased stakeholder is important, as well.

Mr. GARBARINO. I appreciate that and I am out of time, so I yield back. Thank you, Chairwoman.

Chairwoman CLARKE. I now recognize the Ranking Member of the full committee, the other gentleman from New York, Mr. Katko, for his questions at this time.

Mr. KATKO. The other gentleman. Thank you very much, Madam Chair. Thank you all for your testimony.

I must say at the outset, Mr. Knake, I was thinking when you were talking about how good it is to have a National cyber director finally in place again and someone that can be the coach of the whole field here. I am very pleased with what is going on there and the relationship Inglis has with the various subsets, one of which is CISA.

Mr. Goldstein, I can't say enough how encouraging it is to see that CISA is developing those really trusted and treasured partnerships with the private sector. It is so critical to their mission. The more we can develop that trust and the trusted exchange of information, by far we are going to make this whole cyber landscape safer. So, it is in that vein that I have a couple of questions for you.

Obviously, we are all concerned about infrastructure in general and systemically important critical infrastructure in particular given the threat that Russia now poses, an increased threat. So, I wonder if you can give us an update on the current State of the effort to define SICI, as you will, which is not the best acronym, by the way. I know that is why CISA came up with the PISCES acronym and I want to figure out what the two are. So, why don't you explain to us what the two are and how they work together? Maybe give us, after that, give us a little bit of the private-sector input, if you would.

Mr. GOLDSTEIN. Thank you, sir. Of course. At CISA, through our National Risk Management Center, we are currently focused on developing our list of systemically-important entities, and these are organizations that own, operate, or otherwise control critical infrastructure that, if degraded, would have debilitating systemic or cascading impact on our National security or——

Mr. KATKO. So, just to interrupt you just for a second, I think that is so important because if all critical infrastructure is systemically important than nothing is, right? So, we have to take the most critical of the critical. Is that basically the effort we are trying to do here?

Mr. GOLDSTEIN. Yes, sir.

Mr. KATKO. OK. Well, go ahead.

Mr. GOLDSTEIN. Importantly, sir, there are a few important nuances with the definition that we are utilizing at CISA. The first, as I mentioned at the outset, is our focus on entities because we need to figure out the organizations with whom we are partnering. So focusing on entities allows us to use this prioritization to actually drive collaboration and drive provision of services to those organizations we need to help.

The second important aspect is this idea of cascading effects or systemic impact, which means that we can look at some of these smaller organizations, organizations in the supply chain that are deeply critical, but actually might not be—might not have as much revenue or market share as others in a given sector.

The third piece, which really is critical, is the tie to National critical functions, the services upon which the American people and businesses rely every day to go about our daily lives. By tying the entity list to National critical functions, that then lets us do the rigorous analysis to figure out how do we keep these functions at the end of the day available and resilient? Which really is why we are all here.

Today, our National Risk Management Center has developed a rigorous methodology to decompose our National critical functions into a list of systemically important entities. That work is on-going and our goal here is for this to be both a rigorous and strongly methodological approach, but also one that is transparent and gets input from our partners in Government and the private sector to ensure, to Ms. Sherman's very well-taken point, that we have—that the list is understood and credible by those organizations who are so designated on the list.

Mr. KATKO. Yes, so if you could just drill down a little bit more on the private sector input. What is the nature and quality of the input you are getting from them right now or asking for?

Mr. GOLDSTEIN. So, thus far, we are still at the fairly early stages of that process. We are beginning to reach out through our sector fora to get input on the methodology and the process. As this work evolves and we generate the underlying lists for National critical functions, we do intend to do robust engagement with our sector partners with whom we work so closely to ensure that both the methodology is understood and the outputs therefrom.

Mr. KATKO. OK, great. Thank you very much and I appreciate that. I really strongly encourage you to continue your collaborative effort with the private sector.

Mr. Knake, is there anything you want to add to that? Your microphone, please.

Mr. KNAKE. I am sorry, sir. Just that we are working very closely with CISA as we try and understand what additional authorities they may need in order to further this work. I think we have a good sense of where they are today and what they have been able to do under current authority. We need to work with them to identify are there additional authorities that would help them do that kind-of deeper level identification you are discussing?

Mr. KATKO. Thank you very much. I know I am out of time, but I just want to say, Ms. Sherman, the work that your office does. Please keep it up because your input is very valued and I wanted

to let you know that even though I didn't have time to ask you a question.

I yield back. Thank you very much.

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

The Chair now recognizes for 5 minutes the gentlewoman from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. Let me thank the Chair very much for this hearing and the Ranking Member, as well, and the committee. Let me pose questions.

As I listened to Ranking Member Katko's question, let me ask all three, starting with Mr. Goldstein and then following Mr. Knake and Ms. Won Sherman. I would appreciate it if they were brief because I have a series of questions, but I really would like to know the gaps in the authorities that have impeded previous efforts to identify and boost the security of critical infrastructure.

We have been on a long journey on this and we certainly have been on a long journey as it relates to finding out about critical infrastructure. I remember doing this in the early 2000's and looking at water and other forms of the electric grid, but really looking at it from probably a very naive perspective.

What is happening now? What impedes you from having the fullest comprehensive review on this vast critical infrastructure subjected now to dangerous operators, such as those housed in Russia?

Mr. GOLDSTEIN. Thank you, ma'am. Congress, led by this committee, has done an extraordinary job over the past few years of providing CISA with new and robust authorities for us to conduct our mission as the Nation's lead for domestic cyber defense, whether that is establishing the Joint Cyber Defense Collaborative last year, whether it is providing the authority to establish mandatory incident reporting requirements this year, or even, going a few years back, providing us the ability to issue subpoenas to identify the operators of vulnerable devices or protect information shared with us.

Ms. JACKSON LEE. Let me interject to say that I want to go—I thank you for recognizing that I would like to ensure that we know what else we need to do.

Mr. GOLDSTEIN. Yes, ma'am. At this point today, we are focused on fully implementing the authorities that we have been provided, including those that were just recently provided this year through the Congress and good work of this committee. Very much looking forward to working with this committee and your staffs to ensure that any gaps or impediments as they emerge are rapidly identified and we can work with Congress to address them.

Ms. JACKSON LEE. All right. Does anyone have any specifics that have not answered, Mr. Knake or Ms. Won Sherman?

Mr. KNAKE. Thank you. Thank you, Congresswoman. What I would add is it is a gap, but we don't necessarily know at this point

whether it needs to be filled, so I want to be careful in making this point.

Right now, DHS wouldn't have the capacity to do what might be called a census. They wouldn't have the capacity to go out to critical infrastructures, say provide us this information back, and then we will evaluate it. Now, whether they need that authority, whether they need that information is an open question. They have got a lot of other data sources that they can pull on to identify critical infrastructure at this point. So I think it is an open question as to whether or not that kind of census-like activity would really actually be important.

Ms. JACKSON LEE. I think that is an important point you made.

Let me just change the question for you, Ms. Won Sherman, and ask about the narrative dealing with Russia and the example of Colonial Pipeline. They were housed in Russia, obviously. The Russian government at that time indicated that they as a government were not involved. But in light of the horrors in Ukraine and the seemingly ramping up on the Russian government's sort-of negative operations that may include cyber attacks that they have done in other countries, what do we need to do here in the United States domestically?

Ms. SHERMAN. One area I would like to speak to has to do with CISA's role as the National coordinator for the Sector Risk Management Agencies. This is a space that we are starting to look more into at GAO. You know, at this stage we believe that CISA has several opportunities to be able to more proactively engage with those Sector Risk Management Agencies. As a Sector Risk Management Agency itself for multiple sectors, to be able to bring them along in terms of implementing and carrying out their responsibilities from the fiscal year 2021 NDAA, and to be able to improve the information sharing as well as coordination within the sector and across all of the sectors to ensure that there is a more informed understanding of the key issues in the various sectors, especially in the lifeline sectors and those specific to the concerns that you are raising here with respect to Russia.

Ms. JACKSON LEE. Thank you very much. Thank you, Madam Chair. I yield back.

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentlewoman from Tennessee, Mrs. Harshbarger.

Mrs. HARSHBARGER. Thank you, Chairwoman. Thank you, witnesses, for being here today. I do have a question for Mr. Knake.

As we are all aware, there is a new incident reporting law on the books, but that doesn't mean we can lose sight of the importance of the voluntary relationships between CISA and the private sector. I guess my question is, should Congress be considering any additional incentives that could be used to enhance the two-way dialog between the Federal Government and owners and operators of critical infrastructure?

The reason I ask that is I have multiple companies within my district, when I go visit, they tell me they have been—had cyber attacks and been hacked multiple times. They just go ahead and pay the ransomware and don't report that to the FBI. So, there is probably reasons that they don't report that. Of course, they don't want their customer base to think they can't protect their informa-

tion or stockholder—you know, the stocks go down and they don't want to be hauled in front of Congress.

But tell me what you are doing to make that a better private partnership with these Government entities, sir.

Mr. KNAKE. Thank you for the question. It is a really important one.

I believe as part of that bill one of the things that CISA was instructed to do that we are part of is to establish a new ransomware task force that is going to look at these issues. So I believe we are on a fairly tight time line to get that stood up and to start figuring out how we can make sure that ransomware is treated as the National security priority that it is and that our Government, which is often very focused on these large systemically important entities that affect the entire Nation is providing support, is providing services, and is providing incentives to those smaller businesses that are really the backbone of the economy.

So that ransomware task force, which Congress has mandated that we will play a large role in and that CISA will lead, is absolutely essentially to that activity.

Mrs. HARSHBARGER. Well, it absolutely is. We were in the SCIF talking about the cyber threats from Russia and one of my colleagues asked how will we know when we are hit? They said, well, we will know when it—when we are hit. So, is there anything we can do to preemptively stop it?

You know, I think about and I talk about TBA in my district and how they—you know, I talked to their CEO and how they protect the TBA system basically from attacks as far as the grid or EMP and things like that. But cyber is a very big threat and they said they had—they were protected. So, you know, it is a little bit worrisome that you won't know until it happens.

In the first hearing I was ever in, you remember that we had 9 different Government agencies hacked and they didn't even know it. We had Microsoft and FireEye and SolarWinds, and I am like what can we do to protect these private companies and our own Government? It is worrisome. Anybody have a response?

Mr. GOLDSTEIN. Yes, ma'am. I will offer a few points on that great question about it.

The first is we really collectively need to push a cultural change in how we think as a country about cyber incident reporting. It is terrific and Congress has provided CISA with the authority to mandate reporting. But even in lieu of that requirement or while that requirement is being executed, the rulemaking organizations need to understand the value of reporting incidents to the Federal Government, which is, of course, first so that the U.S. Government can offer assistance if needed, but it is also so that we can help understand the breadth of campaigns and contain them before other organizations are victimized.

That is why at CISA we have had our Shields Up campaign for months now, really evangelizing this perspective that if you see anything unusual in your networks, tell the U.S. Government, tell CISA, so that we can help understand is this actually a leading indicator of a foreign adversary campaign? Also why at CISA—it was wonderful to hear Mr. Garbarino talk about his meeting with our Region 2 colleagues. Because we have regional representatives

throughout the country who every day are knocking on doors, physically and virtually, and explaining the value of proactively voluntary reporting. Again, CISA is not a regulator in this space and so our goal exclusively is to ensure that organizations know how to protect themselves and to help identify intrusions, so we can help safeguard others.

Mrs. HARSHBARGER. OK. Well, thank you for that answer. With that, I will yield back.

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Good morning. Madam Chair, can you hear me OK?

Chairwoman CLARKE. Yes, we can.

Mr. LANGEVIN. Very good. Well, I want to thank you, Madam Chair, for hosting this very important hearing. I want to thank our witnesses for their testimony today and the exceptional work you are doing in protecting our Nation's cybersecurity.

Let me just associate myself with the remarks from the Ranking Member in complimenting CISA and how closely you are working with private-sector entities to make sure that they are secure. Also I applaud you for the work you have done under Director Easterly's leadership and Director Goldstein in standing up the Shields Up Program to make sure that we are prepared for any blowback and threats from Russia.

So, let me start with Mr. Knake. So, I believe that, you know, one important factor in considering SICI or other public-private cybersecurity partnerships is the degree to which those partnerships need to be shaped by the cybersecurity maturity of the entities that are involved. So, a critical infrastructure entity's in-house cybersecurity capability will affect really the utility of different kinds of assistance the Government can provide.

You know, for many resource-constrained critical infrastructure entities, technical assistance and other CISA services can be extremely valuable. But other critical infrastructure entities have a much higher degree of cybersecurity maturity, including many of those that I would construe as systemically important critical infrastructure. For those entities, the return on investment of technical assistance would be lower whereas access to more actionable cyber threat intelligence to inform their own defenses would be more helpful.

So, Mr. Knake, how is ONCD thinking about this issue in the context of promoting operational collaboration with systemically important critical infrastructure?

Mr. KNAKE. Thank you, Congressman. That is a great question.

I think you are right. If you look at a lot of the systemically important entities, these are very well-resourced organizations for cybersecurity. They purchase many of the services that CISA could provide to them. That is not where they are looking for support. They have got their own red-teaming capability. They have got their threat hunting capability. It is probably more important for CISA to deploy those resources strategically to the organizations that are important or systemically important, but don't have the kind of budget, let us say, some of these larger entities do.

When we talk to these large systemically important entities the thing that they really do emphasize is that intelligence piece. What is the one thing that they are not allowed to do, right? They cannot go out and collect foreign intelligence in the way that the U.S. intelligence community can. That would be illegal for them to do. They understand that, but yet they see the need to collect that kind of threat intelligence, have it shared with them, have it operationalized by them. So, I think that is the critical important piece here.

What we are looking at is what are the opportunities to really move that into real time? How can we move from situations in which we are saying come down to the SCIF at the FBI office wherever you are located and we will give you a brief, to how can we get this out to you in a secure form that you can use to protect your network? There is a lot that we can do, there is a lot that we have done to declassify data, to push it out broadly, push it out widely on the internet. I applaud what CISA's done in that regard.

But we are really trying to look at how could we actually, with these systemically important entities, really bring them into some kind of collaborative environment where we could trust that that environment is secure and this kind of information can be shared?

Mr. LANGEVIN. Yes. That is why I think the joint collaborative environment which the Solarium Commission has recommended and which is a top priority for me this year was to create that common tool set for sharing information in real time and understanding context.

But for both of you, based on testimony we have heard today, it is clear that CISA's systemically important entities effort is engaged in a rigorous identification process, but the next steps of what to do with the list appear less clear to me than the Solarium Commission's vision of SICI, which recalls for specific benefits and obligations to SICI entities. So, while an accurate identification process is important, we must also have a clear picture of the policies and strategies that will govern and strengthen the partnership between Federal Government and our most critical infrastructure entities.

So, for Mr. Knake and Mr. Goldstein, if CISA develops a list of systemically important entities, what does the administration plan to do with it? How would those factors, like cyber maturity, as we discussed today, play a role in where and how the Government would prioritize its efforts to partner with critical infrastructure owners and operators?

Mr. GOLDSTEIN. Yes, sir. Thank you for that question. As ever, thank you for your leadership on this critical issue.

We are focused on utilizing the SIE list for two main purposes. In the first instance recognizing that on value, such a list is that its applicability will evolve over time as the risk environment changes apace. But the first is to use it to drive operational collaboration and bring together organizations across sectors, across National critical functions into the Joint Cyber Defense Collaborative to enable that sort of risk-reduction efforts that we are already doing with highly critical entities across three sectors in the context of the Russian invasion of Ukraine. As the SIE effort expands, we will be able to do that prioritized collaboration more effectively.

The second piece is focusing on supply chains with these key SIE entities to ensure, to Rob's very well-taken point, if an organization doesn't need U.S. Government risk-reduction services, we can understand their dependencies and their supply chains to reduce their risk going forward.

Chairwoman CLARKE. The gentleman's time has expired.

Mr. LANGEVIN. Thank you, Madam Chair.

Chairwoman CLARKE. The gentleman's time has expired. Thank you, too, Mr. Langevin, for all of your dedication and hard work in this space.

The Chair now recognizes for 5 minutes the gentlewoman from Michigan, Ms. Slotkin.

Ms. SLOTKIN. Thanks very much, Madam Chair. Thanks for being here. I echo my comments that Representative Langevin, Representative Katko are two Members who have a ton of in-depth knowledge on cyber and it is really difficult to think of both of them not here next term.

I wanted to take kind-of a 40,000-foot view for a second. You know, I think, unfortunately, what I hear from people in my district more often than not is they have no idea, you know, who in the U.S. Government is protecting them from cyber attack. They feel like they are on the front lines, that they are being attacked all the time, and their Government—they just don't know like who is the 9–1–1 call? What does it look like, these folks who are protecting me or trying to protect me? They know what a police officer looks like. They know what someone in the military looks like. So, I would just put a note in that we need to also communicate to the American public, not just within Washington circles, kind-of what we do, what you all do to protect people.

But I want to talk about two sectors that we haven't talked about very much. One is the agriculture sector and second is K through 12 schools. In the ag sector, obviously JBS, the ransomware attack last year, was a really big deal. I come from a district with a ton of farmers and it was like the first thing on their mind when I brought the Secretary of Agriculture last summer.

So, my understanding is there is not an ISAC or like a community of folks that are focused on cybersecurity in the ag world. Can you tell me briefly, first and foremost, what you are doing and what reassurance we can give farmers that our food security systems are protected and being looked at?

Then second, K though 12, it is just amazing. You get 10 superintendents from my district together. Every single one of them has been the victim of a ransomware attack. Every single one of them is desperate for tools to protect our kids' data.

So, tell me what we are doing in those two sectors, please, if you could.

Mr. GOLDSTEIN. Certainly. Both great questions. Regarding the food and ag sector, you know, certainly the ransomware intrusion affecting JBS put in stark relief the impacts that a cyber intrusion on the food and ag sector could have on the availability of the food supply to the American people. You know, I actually personally met this week with a number of the largest meat producers in the country and this sector is one that is of paramount importance to our collaborative efforts.

Our goal with the food and ag sectors, as with other sectors, is to work really closely with those organizations and their security leadership that accounts for the preponderance of food production, food distribution, and food supply in this country understand areas of needed improvement or areas where we can help advance their cybersecurity programs and then ensure that they are getting the specific services, tools, and information from CISA and our partners, including USDA, as applicable, to meet them where they are. So our goal with this sector is to really partner with the organizations that contribute to the related National critical functions to ensure that we are providing them with everything we can to shore up their security.

K–12 cybersecurity, ma'am, as you note, is an absolute urgent issue. We know that many K–12 school districts lack the resources and maturity to secure their networks in many cases against sophisticated threats. Congress thoughtfully anticipated this issue in passing the K–12 Cybersecurity Act, which directed CISA to conduct a study on this very issue and assess how we can provide more effective services and tools and information to the K–12 cybersecurity community. That work is on-going. I am very much looking forward to briefing this subcommittee on our conclusions, but this is an area where our regional team members at CISA have so much value because we know——

Ms. SLOTKIN. Yes, I am a cosponsor of that legislation. I think I would offer that our cybersecurity community, which is doing yeoman's work in trying to, you know, gain all these connections with these different sectors, it is one thing to come and testify, it is one thing to kind-of have conversations about what you are doing in a forum like this. I would offer that part of the responsibilities of your agencies is to also communicate out to normal people who have no idea how to keep themselves safe. I would just ask that you maybe look at your budget on this matter and redouble your efforts to communicate to real people who don't understand what you all do and how it protects them and how that should be—how their responsibilities fit into that. Right? Making sure they are doing everything they can on cyber hygiene.

So, thank you for that. Thank you for your work. I yield back.

Chairwoman CLARKE. I thank the gentlewoman for her line of questioning. I wanted to recognize the Ranking Member for a follow-up question. I myself have a few follow-up questions, so I yield to the gentleman from New York, Mr. Garbarino.

Mr. GARBARINO. Thank you, Chairwoman. Are you sure you don't want to go first? Whatever, I can go. OK. Thank you.

Mr. Goldstein, you started answering this question before and Ms. Sherman brought up when she talked about sector risk management coordination and how you are going to work together with these other agencies. I know you have already started, CISA has already started some programs through the Section 9 list and the U.S. Department of Energy has begun initiatives to strengthen resilience in the energy sector. What is CISA's plan to make sure that all the Sector Risk Management Agencies have a say in determining what is systemically critical infrastructure and to make sure everybody is kept up-to-date and, you know, everybody is reading from the same sheet of music?

Mr. GOLDSTEIN. Yes, thank you, sir. The SRMAs are critical partners in really everything we do at CISA. But particularly when we are identifying systemically important entities, SIEs, the SRMAs fill two essential roles.

The first is helping us make sure that the methodology that we are using for identification in the first instance incorporates the relevant expertise from each SRMA, so that we are not underweighting or overweighting different variables that might contribute to getting a suboptimal list for a given National critical function, but then essentially, when we have a list established for a given National critical function, the SRMAs are critical partners in figuring out how do we as a U.S. Government bring together everything that we can offer to improve the security and resilience of entities that are supporting a given NCF.

Critically in this phase, you know, in CISA's as the National coordinator for critical infrastructure's security and resilience and the lead for National cyber defense, that does not mean that we are the sole actor in providing these services and information. The SRMAs, in many cases, have unique sectoral risk management expertise, particularly regarding understanding how a cyber intrusion or physical event could impact the continuity of a National critical function. So by partnering with the SRMAs, we can combined CISA's generally applicable expertise in both cyber and physical security with the sector knowledge of an SRMA. That is the combination that we believe adds real value to set directives.

Mr. GARBARINO. I appreciate that. Just to question Ms. Sherman, do you have any ideas or suggestions on how to make sure that there is no confusion?

Ms. SHERMAN. Sure. Well, maybe two quick points related to the SRMAs. The first, as discussed yesterday during the hearing, there is a range of maturity levels when it comes to Sector Risk Management Agencies, you know, spanning from, for example, you talked about the financial services sector all the way to the water sector and everything in between. So, I think it is important for CISA to be able to work to bring along those less mature sectors and to work with the relevant SRMA in those instances to make sure they have the support and resources and coordination needed.

The other point I wanted to raise actually is around the update to the National plan and the sector-specific plans. The National plan has been in place since 2013 and CISA is actively undertaking an update effort. I think by the end of this year is the goal.

One of the things, some of the conversations that we have had with Sector Risk Management Agencies is that they are holding still and updating their sector-specific plan until the National plan update occurs. So we do think that this is something timely and important for CISA to continue to act on so that those updates and, again, the relevancy and the value of the guidance that's being provided to the sectors and the steps that they need to take will be laid out in those plans and is something that they can act on.

Mr. GARBARINO. Thank you. I yield back.

Chairwoman CLARKE. Thank you, Ranking Member. Mr. Goldstein, I have a couple of clarifying questions before we close.

First, CISA's working to identify systemically important entities. Right now, does CISA have the authority to compel any SIE to share information about security measures they have in place?

Mr. GOLDSTEIN. No, ma'am. At this point, we do not have the authority to compel organizations to share cybersecurity information. Our focus is on building these trusted partnerships in which organizations voluntarily work with us to share information that we need to understand and manage cybersecurity risk.

Chairwoman CLARKE. Does CISA have the authority to compel information about their vendors or supply chains?

Mr. GOLDSTEIN. Currently, we do no have the authority to compel private organizations to provide CISA with information about the vendors or supply chains.

Chairwoman CLARKE. Does CISA have the authority to compel any other information it may need to fully assess an SIE's relative security risk or vulnerability?

Mr. GOLDSTEIN. Today CISA does not have such authority as to compel private organizations. We have narrow authorities, ma'am, as you are aware, for our subpoena authority to compel disclosure of voluntary devices being used by an organization, but certainly not specific to the security controls in place by an SIE. Certainly, those authorities may exist elsewhere in Government, but not within CISA.

Chairwoman CLARKE. So, what kind of information enhance CISA's understanding of National systemic risk?

Mr. GOLDSTEIN. Our approach today is understanding the entities that contribute to the continuity of National critical functions, bringing those organizations in.

I think it is relevant to note here that in our view, the U.S. Government and the private sector has a shared interest in ensuring the continuity and resilience of National critical functions. Thus far, we have shown great success in building trusted partnerships in which we have a shared goal with the private sector to ensure continuity and resilience of NCFs. By building that trust, we are able to catalyze information sharing to the degree needed to execute our mission.

Chairwoman CLARKE. Second, do you anticipate that the concept of SICI or systemically important entities will replace the list of Section 9 entities?

Mr. GOLDSTEIN. We certainly envision the SIE process as an evolution or maturation of the Section 9. We're tying the list to National critical functions and focusing on cascading and systemic impact will be improvement over the Section 9 process and allow us to drive operational collaboration more effectively.

Chairwoman CLARKE. So, do you anticipate a replacement or just sort-of archiving what—how do you sort-of manage all that information?

Mr. GOLDSTEIN. Our goal would be that if we achieve our intended outcomes with the SIE list, that the SIE list would resolve the need for a separate Section 9 list. Ideally, the SIE list will meet the intent of Section 9 of E.O. 13636 and allow us to do even more with the critical prioritization of entities across the country.

Chairwoman CLARKE. If Congress were to codify the concept of SICI or SIEs without also replacing new requirements on des-

ignated—excuse me, also placing new requirements on designated entities, how would that list be different from the existing Section 9 program?

Mr. GOLDSTEIN. So, today our work to develop the SIE list differs in important ways from the Section 9 program, including tying the SIE list back to National critical functions, ensuring that we are encompassing the breadth of critical sector, for example, the IT sector was excluded specifically from the Section 9 program in the underlying Executive Order as well as focusing on cascading and systemic risk so that we are not only identifying the largest entities in the country, but also ones that, by virtue of their unique dependencies or relationships, pose a potential risk to the continuity of National critical functions.

Chairwoman CLARKE. Very well. It is my understanding that we have an additional question or questions from Congresswoman Sheila Jackson Lee of Texas. You are recognized at this time.

Ms. JACKSON LEE. Thank you, Madam Chair. Thank you for this very good hearing.

I would like to ask unanimous consent to introduce into the record several articles: "From SolarWinds to Log4j: The Global Impact of Today's Cybersecurity Vulnerability," April 5, 2022; *Tech Crunch,* "Apple, iCloud, Twitter, and Minecraft Vulnerable to 'Ubiquitous' Zero-Day Flaw"; "Biden Signs an Executive Order Aimed at Protecting Critical American Infrastructure from Cyber Attacks"; and "Biden Warns U.S. Companies to Gear It Up Against Russian Hacks."

Chairwoman CLARKE. So ordered.

Ms. JACKSON LEE. I ask unanimous consent, Madam Chair, to include that in the record.

Chairwoman CLARKE. So ordered.

Ms. JACKSON LEE. Thank you so very much.

Chairwoman CLARKE. So ordered.

[The information follows:]

FROM SOLARWINDS TO LOG4J THE GLOBAL IMPACT OF TODAY'S CYBERSECURITY VULNERABILITIES

By CRN Team—April 5, 2022

By Harish Kumar, Head, Enterprise & Government, Check Point Software Technologies, India & SAARC

http://www.crn.in/columns/from__solarwinds__to__log4j__the__global__impact__of__todays__cybersecurity__vulnerabilities

If the past year has taught businesses anything, it's that the impact of targeted cyber attacks and security vulnerabilities is now, without doubt, universal. From the fallout of the Solar Winds software supply chain attack to the exposed Apache Log4j vulnerability, the case for organizations of all shapes and sizes to have a comprehensive and robust security infrastructure in place has never been stronger, even if they themselves aren't necessarily in the crosshairs.

Many regard the now-infamous SolarWinds breach in late 2020 as a major catalyst for what would become a frenzy of "Gen V" or fifth-generation attacks that persist to this day. Such large-scale, multi-vector attacks have virtually unlimited reach, with devastating security consequences for businesses and governments around the world. A year later, the Apache Log4j vulnerability was exposed, which made it possible for malicious actors to execute code remotely on almost any targeted computer to take control, steal data or even hijack a user's machine to mine cryptocurrency.

The former was an orchestrated attack by an advanced persistent threat group, the latter was an exposed zero-day vulnerability that nobody saw coming. One thing both incidents have in common, however, was that they increased risk and vulner-

ability for businesses in every sector, in every corner of the world. As organizations plot their course through 2022 and beyond, it's never been clearer that cybersecurity is a global issue rather than a local one, and this should be reflected in every cybersecurity strategy moving forward.

THE RISE OF "GEN V" ATTACKS

Gen V attacks are unique in the way that they leverage broad attack surfaces and multiple infection vectors to infiltrate large numbers of organizations, and they are increasing at an unprecedented rate. At a time when businesses and government agencies are expanding their network footprint, adding more endpoint and connected device into their technology mix, the risk of being impacted by a Gen V attack has also never been higher. As outlined in our 2022 Security Report, the SolarWinds breach, which impacted organizations around the world, kickstarted a torrent of supply chain attacks that still plague businesses today. In a year that saw cyber attacks against corporate networks increase by 50 percent across the board, software vendors like SolarWinds experienced the largest year-on-year growth in attacks with an increase of 146 percent. Today's corporate economy is built on an intricate web of software supply chains, which means that with every additional attack on a software vendor, the vulnerability of businesses around the world is further amplified.

FUELLING ATTACKS: THE SUNBURST CATALYST

The SolarWinds software supply chain attack was facilitated by a back door knovm as 'Sunburst', which was added to the SolarWinds Orion system before being distributed to customers globally via a routine update. This gave the APT (advanced persistent threat) group involved covert access to thousands of SolarWinds customers' networks, from government agencies to Fortune 500 companies. Unfortunately, this mode of attack from APT groups is now on the rise. As our report details, the REvil ransomware group targeted multiple managed service providers (MSPs) throughout 2021, and in July managed to embed a malicious software update in IT company Kaseya's patch management and client monitoring tool. Thousands of unsuspecting businesses were impacted, with millions of U.S. dollars demanded in ransom.

Sunburst also likely inspired the attack on Colonial Pipeline, which carries almost half of the fuel consumed by the U.S. East Coast. The nation-state APT group, DarkSide, was allegedly behind the attack, employing a Ransomware-as-a-Service model, meaning it relied on third-party affiliate programs to orchestrate the breach. This is one of the most striking examples to date of how tools used to carry out such attacks are becoming democratized and more widely used, again ramping up the pressure on businesses to guard their perimeters.

While the assets of the REvil ransomware group have since been seized and its ringleaders arrested, you cannot arrest code. Once one threat group make headway with a particular attack, it doesn't take much for an affiliate member to keep that momentum going. Emotet, one of the most dangerous botnets in history, made a return in November 2021 following its takedown a year earlier. It's a trojan primarily spread through links, spam emails, malicious scripts and macroenabled document files, and once it infects a user it can spread like wildfire without detection, stealing banking credentials and financial data from individuals, companies, and governments around the world.

AMBUSHED BY ZERO-DAY VULNERABILITIES

While targeted attacks like the ones outlined above are presenting an increased threat to organizations around the world, so are exploits and vulnerabilities. In December last year, a remote code execution vulnerability was reported in Apache Log4j, the most popular java logging library in the world. This library is embedded in almost all of the services and applications we use in our day-to-day lives, from Twitter and Amazon to Microsoft and Minecraft. Initially used by some threat actors to leverage cryptocurrency mining resources at the expense of their victims, there's no reason an exploit like this couldn't be used for more sophisticated and nefarious attacks. Check Point Research detected approximately 40,000 attack attempts just 2 hours after the Log4j vulnerability was revealed, and a further 830,000 attack attempts 72 hours into the event.

These zero-day vulnerabilities earn their name from their ability to completely blindside businesses, giving them virtually no time to react before they become potential victims. It then becomes a race between threat actors and their ability to exploit the vulnerability, and how quickly businesses can close the gap in their defenses.

GLOBAL THREATS REQUIRE A GLOBAL SOLUTION

The threat climate has changed. The traditional defensive line that businesses can draw between themselves and the rest of the cyber landscape has become blurred to the point that it may as well not exist. Instead of guarding a static perimeter, businesses need to take a more holistic and real-time view of their security infrastructure. Security practitioners need to be able to maintain 360-degree visibility of their entire network, regardless of how far and wide it has been distributed. They also need access to real-time threat intelligence on a global scale, so they can preempt far-reaching zero-day vulnerabilities and targeted software supply chain attacks like the ones outlined above.

Check Point's Infinity platform, for instance, is the only security platform of its kind that offered pre-emptive protection for customers against the Log4j exploit. It's the first modern, consolidated security platform specifically designed to guard against zero-day vulnerabilities and sophisticated fifth-generation attacks across all networks, cloud deployments and endpoints. Part of Infinity's success is its ability to leverage Check Point's ThreatCloud, a real-time global threat intelligence platform that monitors networks around the world for emerging threats and vulnerabilities.

If organizations around the world want to operate safely and securely in 2022 and beyond, they need to start seeing cybersecurity as a global issue rather than a local one, and evolve their security strategies accordingly. Only then will they be able to confidently defend themselves against a threat landscape that knows no bounds and cannot be contained by borders.

If you have an interesting article/experience/case study to share, please get in touch with us at editors@expresscomputeronline.com

---

APPLE ICLOUD, TWITTER, AND MINECRAFT VULNERABLE TO UBIQUITOUS ZERO-DAY FLAW

TechCrunch, Carly Page@carlypage__/1:24 PM EST—December 10, 2021

A number of popular services, including Apple iCloud, Twitter, Cloudflare, Minecraft and Steam, are reportedly vulnerable to a zero-day vulnerability affecting a popular Java logging library.

The vulnerability, dubbed "Log4Shell" by researchers at LunaSec and credited to Chen Zhaojun of Alibaba, has been found in Apache Log4j, an open source logging utility that's used in a huge number of apps, websites and services. Log4Shell was first discovered in Microsoft-owned Minecraft, though LunaSec warns that "many, many services" are vulnerable to this exploit due to Log4j's "ubiquitous" presence in almost all major Java-based enterprise apps and servers. In a blog post, the cybersecurity company warned that anybody using Apache Struts is "likely vulnerable."

Companies with servers confirmed to be vulnerable to Log4Shell attack so far include Apple, Amazon, Cloudflare, Twitter, Steam, Baidu, NetEase, Tencent and Elastic, though there are likely hundreds if not thousands of other organizations affected. In a statement given to TechCrunch, Cloudflare said it has updated systems to prevent attacks, adding that it saw no evidence of exploitation.

Robert Joyce, the director of Cybersecurity at the NSA, confirmed that GHIDRA, a free and open source reverse engineering tool developed by the agency, is also affected: "The Log4j vulnerability is a significant threat for exploitation due to the widespread inclusion in software frameworks, even NSA's GHIDRA," he said.

The Computer Emergency Response Team (CERT) for New Zealand, Deutsche Telekom's CERT, and the Greynoise web monitoring service have all warned that attackers are actively looking for servers vulnerable to Log4Shell attacks. According to the latter, around 100 distinct hosts are scanning the internet for ways to exploit Log4j vulnerability.

Kayla Underkoffler, a senior security technologist at HackerOne, tells TechCrunch that this zero-day highlights the "threat that open source software presents as a growing portion of the world's critical supply chain attack surfaces."

"Open source software is behind nearly all modern digital infrastructure, with the average application using 528 different open source components," Underkoffler said. "The majority of high-risk open source vulnerabilities discovered in 2020 have also existed in code for more than 2 years and most organizations lack direct control over open source software within supply chains to easily fix these weaknesses. Securing this often poorly funded software is imperative for any organization that relies on it."

The Apache Software Foundation has released an emergency security update today to patch the zero-day vulnerability in Log4j, along with mitigation steps for those unable to update immediately. Game developer Mojang Studios has also released an emergency Minecraft security update to address the bug.

Updated with comment from Cloudflare.

https://techcrunch.com/2021/12/10/apple-icloud-twitter-and-minecraft-vulnerable-to-ubiquitous-zero-day-exploit/

BIDEN SIGNS AN EXECUTIVE ORDER AIMED AT PROTECTING CRITICAL AMERICAN INFRASTRUCTURE FROM CYBER ATTACKS

New York Times, July 29, 2021

https://www.nytimes.com/2021/07/28/us/politics/cyber-security-biden-executive-order.html

The effort is a way to get beyond the patchwork of mandates and voluntary action to protect electric utilities, gas pipelines, water supplies, and industrial sites that keep the economy running.

A day after President Biden warned that cyber attacks could lead to a "real shooting war," he signed an executive order on Wednesday aimed at preventing hackings on America's critical infrastructure.

While the order has been in the works for some time, the need was driven home by a series of major ransomware attacks, including against Colonial Pipeline, which provides the East Coast with 45 percent of its gasoline, jet fuel and diesel.

The order was mostly filled with voluntary measures for companies to meet a series of on-line security standards, like encrypting data and requiring two-factor authentication for all users on a system, to stymie hackers who possess stolen passwords. In a call with reporters Tuesday night, a senior administration official said the idea was to develop "cybersecurity performance goals" to assess how prepared each company or utility was.

The effort is a way to get beyond the "woefully insufficient" patchwork of mandates and voluntary actions to protect electric utilities, gas pipelines, water supplies and industrial sites that keep the economy running, the official said.

Such efforts have been tried before, dating to the presidency of George W. Bush. But Mr. Biden is the first president to talk about the issue—almost every week—as a national security imperative. It was the central topic of his meeting in June with President Vladimir V. Putin of Russia. And on Tuesday, visiting the Office of the Director of National Intelligence, Mr. Biden gave a grim assessment of where he believed the constant, short-of-war attacks on the United States, both state-sponsored operations and criminal ransomware, are headed.

"If we end up in a war, a real shooting war with a major power," he told the intelligence officers there, "it's going to be as a consequence of a cyberbreach of great consequence. And it's increasing exponentially—the capabilities."

Mr. Biden's chief challenge now is a lack of authority to mandate changes. He has already imposed security standards on providers of software to the Federal Government, betting that if a company is banned from selling to the government it will also suffer in the commercial marketplace. He has ordered a series of increased protections for Federal agencies, 10 of which were affected by the SolarWinds hacking last year, a broad invasion of the software "supply chain" used by 18,000 companies and governments.

But key elements of American infrastructure are run by private companies and in Colonial Pipeline's case, Russian-speaking hackers brought down the distribution system almost accidentally, after attacking the company's business systems. That was followed by another ransomware attack on JBS, the world's largest beef producer, which paid $11 million to start running again.

For years, many industries have maintained informal organizations that share cyberthreat information or best practices. But there are so many holes in the system that it has been relatively easy for Iran, Russia, China and ransomware groups to find ways to place malicious software in the systems, or initiate attacks that freeze data and make it impossible to operate, as happened to Colonial Pipeline and JBS.

The measures outlined in the new national security memorandum, called "Improving Cybersecurity for Critical Infrastructure Control Systems," are being coordinated by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Commerce Department's unit that sets industrial standards.

BIDEN WARNS U.S. COMPANIES TO GIRD UP AGAINST RUSSIAN HACKS

Washington Post, March 22, 2022

https://www.washingtonpost.com/politics/2022/03/22/biden-warns-us-companies-gird-up-against-russian-hacks/

Welcome to The Cybersecurity 202! I've seen "The Power of the Dog," "Licorice Pizza," "Drive My Car," and "Don't Look Up," so far this year, and I'm not rooting for any of them for Best Picture yet. Is there a better one in the mix?

Below: The online verification firm Okta says there's "no ongoing malicious activity" after hackers claim to access networks connected to the company, and NSO's old owners are fighting in court with its new owners.

The White House has issued its starkest warning that Russia may be planning cyberattacks against critical-sector U.S. companies amid the Ukraine invasion.

There's "evolving intelligence" that the Kremlin is actively exploring its cyberattack options, President Biden said in a statement, warning that companies have a "responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely."

Deputy national security adviser Anne Neuberger described the alert as a "call to action" for companies to raise their cyber defenses, during a White House press briefing. She tied it to a series of U.S. intelligence releases in recent months aimed at shining light on Russian planning.

Biden later warned that he believes a Russian cyberattack "is coming" per CNN's Kaitlan Collins:

Context: The alert comes after Russia has lobbed a series of digital attacks at the Ukrainian government and critical industry sectors. But there's been no sign so far of major disruptive hacks against U.S. targets even as the government has imposed increasingly harsh sanctions that have battered the Russian economy.

The public alert followed classified briefings government officials conducted last week for more than 100 companies in sectors at the highest risk of Russian hacks, Neuberger said. The briefing was prompted by "preparatory activity" by Russian hackers, she aid.

U.S. analysts have detected scanning of some critical sectors' computers by Russian government actors and other preparatory work, one U.S. official told my colleague Ellen Nakashima on the condition of anonymity because of the matter's sensitivity. But whether that is a signal that there will be a cyberattack on a critical system is not clear, Neuberger said.

Neuberger declined to name specific industry sectors under threat but said they're part of critical infrastructure—a government designation that includes industries deemed vital to the economy and national security, including energy, finance, transportation and pipelines. The warning reflects a grave concern that U.S. companies aren't sufficiently prepared to withstand a Russian cyber assault—even after years of concerted pressure from government cyber officials that ramped up even further in the run up to the Ukraine invasion.

Neuberger lamented that foreign hackers continue to regularly crack into companies using known computer bugs that the companies could have patched against if they were more diligent.

"This is deeply troubling," she said. Neuberger compared the companies to New Yorkers that were robbed after leaving their doors unlocked.

The warning also reflects a deep anxiety that companies that have girded their defenses against Russian hacking will let their guards down as the Ukraine conflict drags on.

"The White House is running out of ways to keep the alert levels up for cyber incident responders," Tatyana Bolton, a former Cybersecurity and Infrastructure Security Agency official who now leads cyber programs for the R Street Institute, told me. "It's very difficult to stay on a high level of alert for a long amount of time because we're humans and alert levels go down as time passes."

A second U.S. Government official Ellen spoke with described "fatigue" among industry cyber pros who've been working long hours for weeks on end as part of CISA's "Shields Up" initiative to guard against Russian hacking.

"Since this heightened threat environment started, it's been like 'Shields Up.' So people ask, 'When do we put shields down?'" the official said.

Some industry officials said the Government's latest alert didn't tell them anything they didn't already know.

"I don't see anything new there that we haven't already been informed of," Bill Fehrman, CEO of Berkshire Hathaway Energy and co-chair of the Electricity Subsector Coordinating Council, whose sector was given a classified briefing last week, told Ellen.

"Our defensive postures remain in 'Shields Up' position," he added.

Government only has limited options to make private industry improve their cyber defenses.

Officials have gone into hyperdrive sharing information about cyberthreats and best practices, but mostly lack the authority to compel companies to adopt those practices.

In a handful of industries where government has broader cyber authorities, such as pipelines, its requirements have received a cool reception from industry leaders.

Congress recently passed a bill requiring critical infrastructure firms to alert the government when they're hacked, but even that will take a year or longer to go into effect.

One hope among cyber analysts is that the focus on improving cyber defenses will outlast the current conflict.

"My hope is that the Russia crisis will spur long-term investments in cybersecurity and critical infrastructure resilience," Mark Montgomery, executive director of the congressionally led Cyberspace Solarium Commission, told me. "My fear is it will be treated as it has been [after cyber crises] in the past and forgotten soon thereafter."

The Keys

Okta says no ongoing malicious activity after 'attempt to compromise' third-party contractor

The online verification company stated in a tweet that screenshot photos posted to Telegram by the ransomware hacking gang LAPSUS$ seemed to be related to a January "attempt to compromise the account of a third-party customer support engineer working for one of our subprocessors."

"There is no evidence of ongoing malicious activity beyond the activity detected in January," Okta CEO Todd McKinnon said.

It wasn't clear from the statement how much access the gang had to Okta systems. The hacking gang claimed the screenshots showed internal Okta systems. Okta said in an earlier statement that it was investigating the breach reports.

Okta is used by thousands of companies to verify employees' identities before they access company digital systems making it an especially valuable hacker target.

One of the hacker screenshots purported to be of a dashboard for the cybersecurity company Cloudflare. Cloudflare CEO Matthew Prince said the company was resetting Okta credentials for some users out of an "abundance of caution."

Microsoft is also investigating LAPUS$ claims it breached some of the company's systems. Here's more from CyberScoop's AJ Vicens.

NSO Group's former owners are locked in a court battle with its current owners

The fund that owns NSO is now run by Berkeley Research Group. (Sebastian Scheiner/AP)

The fight stems from an effort to assess how much the embattled spyware company is worth—a valuation that could lead to a big payout for the former leaders of a fund that bought NSO Group in 2019, Stefan Kowski and Bastian Lueken of Novalpina Capital, *Bloomberg News*'s Jonathan Browning reports.

Kowski and Lueken were ousted by the fund's investors in 2021 and replaced with Berkeley Research Group, which currently runs the fund. NSO's value has likely dropped since then, largely due to extensive reporting by *The Washington Post* and 16 media partners that found NSO clients used its Pegasus spyware to hack devices belonging to journalists and activists.

NSO has reportedly mulled shutting down its Pegasus division since then.

"Lawyers for Kowski allege that BRG reneged on a commitment to get the Israeli company fairly valued," Browning writes. "According to emails disclosed in Kowski's filing, BRG responded to say that with NSO shutting down Pegasus, it was therefore 'unfeasible (and was always unworkable)' to conduct an independent valuation."

Iran-linked hackers are trolling the head of Israel's Mossad spy agency

A group of purported Iranian hackers released a document that they said was a stolen 2020 pay stub belonging to Mossad chief David Barnea. The gang said more sensitive leaks were on the way, *Haaretz*'s Omer Benjakob reports. It's not clear if the leaked document is authentic, but it "was intended to disprove Israel's claim that the hack was of an old device belonging to his wife" and therefore not of significance, Benjakob writes.

The group previously published a video showing personal photos, tickets, tax documents and a video clip of Barnea. The Israeli prime minister's office said Barnea's phone wasn't hacked and the "materials in question are old," the *Times of Israel*'s Emanuel Fabian reported.

"Israel believes the hack was revenge for an airstrike in Iran last month, which caused heavy damage to the country's drone network," Benjakob writes.

Hackers have a history of taunting their victims and enemies online, as well as making boisterous claims about their exploits. For example, a hacker taunted top Obama administration officials after he hacked their accounts. And late last year, a hacker appeared to breach an FBI email system to vilify a security researcher.

GOVERNMENT SCAN

Ransomware attacks on the supply chain are national security threat, officials say

U.S. supply chains are struggling even without cyberattacks. (Eric Risberg/AP)

Hacks targeting the U.S. logistics and shipping industries could crush the already struggling supply chain, warned a U.S. Customs and Border Protection intelligence bulletin dated March 7. Much of the bulletin focused on a cyberattack on Seattle logistics firm Expeditors International, though it didn't say who was behind the attack, *Yahoo News*'s Jana Winter reports.

The hacks could also make it tougher to crack down on smuggling. "Large-scale attacks on the logistics industry pose the risk of increased illicit activity through ports of entry due to the shutdowns of computer systems which are essential to CBP processing and security procedures," the bulletin said.

Ms. JACKSON LEE. I am going to go again to CISA and reflect on the testimony that you gave that indicated you made great strides in establishing joint cyber defense, CISA's Cybersecurity Advisory Committee, et cetera. Can you give examples, just point it because I have other questions, of the significant strides that CISA has made in the establishment of this Joint Cyber and the CISA Cybersecurity Advisory Committee?

Then if you would answer is this Joint Cyber Defense Collaborative in authorization language? Would you answer that, please? Thank you.

Mr. GOLDSTEIN. Yes, ma'am, of course. Let me answer the last part first.

So, yes, Congress established a Joint Cyber Planning Office in the National Defense Authorization Act 2 years ago. The JCDC is the maturation the Joint Cyber Planning Office using the same underlying authorization passed by Congress with the leadership of this committee and, of course, Mr. Langevin.

We have had actually remarkable successes with the Joint Cyber Defense Collaborative thus far. Ma'am, I will reference it particularly through the articles you have noted. Around our response to the Log4j software library vulnerability, we brought together, frankly, within hours, many of the largest technology companies in the world to understand what technologies were impacted by the vulnerability, the cyber defense measures that were effective in mitigating the risk of the vulnerability. Then we set up broadly applicable and widely disseminated websites and products that we share with stakeholders across the country, and indeed across the world, driving mitigation of the vulnerability at scale.

We could never have done that work without the insights that we were able to glean and enrich from our private-sector partners in the Joint Cyber Defense Collaborative. We are now doing very similar work, but even more at scale, around the risk of——

Ms. JACKSON LEE. Thank you.

Mr. GOLDSTEIN. Sorry, ma'am?

Ms. JACKSON LEE. Thank you. Ms. Won Sherman, let us go back to my premise about the bad actor that Russia has become, so much so that you can't distinguish between Russia's violence and cyber attacks from the criminals that are lodged in their town. I

want to pursue your line of statements that you made when I asked you previously and your point about that the Federal Government needs to take—needs to include strengthening the Federal role in terms of dealing with the critical infrastructure, strengthening the Federal role in protecting the cybersecurity and critical infrastructure, and improving priority-setting efforts. Having in your mind the backdrop of Russia's rising threat, could you further enhance that comment, please? Ms. Won Sherman.

Ms. SHERMAN. Almost made it through without doing that. Apologies.

Yes, you know, at this stage some of the other findings that we had come across in our review highlighted, for example, some of the challenges with the National critical functions' framework, which looks to have promise and it is great to hear all of the perspective and efforts that have been carried out and are under way as part of that framework.

The concerns that we have identified as part of that particular framework is making sure that there is a clear understanding, both within, again, the Federal Government and all of the levels of Government and the private sector, of exactly what the priority-setting looks like and how the priority-setting is going to actually be carried out, what the goal of the framework is, and what impact there might be on planning and operations. I tie that back to your question related to Russia and the Russia cyber threats and thinking about the various sectors and all of the functions that cut across those sectors and the importance of making sure that the private-sector entities and all of the levels of Government have a clear understanding and awareness of what actions that they would need to take and where they sit in terms of planning and operations.

So it is definitely an area that we have made several recommendations in and we think it is important not only for the broader framework effort, but for some of these very real-time incidents that are occurring.

Ms. JACKSON LEE. Thank you. Madam Chair, I intend to introduce legislation and look forward to working with you around this zero-day potential that has been moving for so many years and now may be even more of a threat.

Thank you for yielding and I yield back. Thank you.

Chairwoman CLARKE. Thank you very much, Congresswoman.

With that, I thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

The Chair reminds Members that the subcommittee record will remain open for 10 business days. Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:27 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR ERIC GOLDSTEIN

Question 1a. In his testimony and responses to Member questions, Mr. Goldstein described the Systemically Important Entity process as an "evolution" or "maturation" of the Section 9 [of Executive Order 13636] list, with a goal of driving "operational collaboration" and understanding Systemically Important Entities' "dependencies and supply chains to reduce their risk going forward."

Is it CISA's/ONCD's goal to codify the framework established in Section 9 of Executive Order 13636?

Question 1b. Section 10 of Executive Order 13636 directed Federal agencies to engage in a review of "the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks," among other things. Did Section 10 of Executive Order 13636 result in the imposition of any new security obligations on Section 9 companies? If so, please describe. If not, why not? In light of the current threat environment, is the administration revisiting the analysis described by Section 10?

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

Question 2a. At the hearing Mr. Goldstein testified: "We certainly envision the Systemically Important Entity (SIE) process as an evolution or maturation of the Section 9 list. We're tying the list to National critical functions, and focusing on cascading a systemic impact will be an improvement over the Section 9 process and allow us to drive operational collaboration more effectively."

Please provide a description of the methodology CISA currently uses to identify SIEs, and describe how it differs from the methodology used in Section 9 designations.

Question 2b. Do you anticipate that tying the Systemically Important Entity list to National Critical Functions will result in a list of entities that differs significantly from the existing list of Section 9 entities? Or do you anticipate that the National Critical Functions analysis will drive analysis of interdependencies among SIEs?

Question 2c. Are there Section 9 entities that you do not believe will identified as Systemically Important Entities because the analysis is tied to National Critical Functions?

Question 2d. As the SIE process continues to evolve, do you anticipate identifying "tiers" of Systemically Important Entities to reflect both an entity's systemic importance and the sophistication with which it can operationally collaborate with the Federal Government?

Question 2e. How many SIEs has CISA currently identified? Please provide a breakdown of such list by sector, the number of SIEs currently enrolled in CISA programs and services, the number of currently engaged in operational collaboration with CISA, and any other information that would be helpful to characterize CISA's current understanding of SIEs.

Question 2f. What information does CISA need in order to fully and accurately identify and understand systemic risks to SIEs, and where does that information originate? What data sources is CISA currently able to leverage to carry out this work, and what data is CISA currently unable to obtain?

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

Question 3a. The Cyberspace Solarium Commission (CSC) recommended Congress codify a new designation for SICI. The concept behind SICI is that certain entities—those that operate our most vital systems and assets—should be granted special assistance from the U.S. Government and should be expected to shoulder additional security and information-sharing requirements befitting their unique status and importance.

If Congress were to create a regime that aligns as closely as possible to the CSC's proposal (i.e., a designation that comes with benefits and burdens), what are the most critical, impactful programs or partnership models that Congress should con-

sider for purposes of mandating participation from designates entities? What types of information should be shared?

Question 3b. Are there authorities CISA currently lacks that it would need if Congress were to decide to mandate such participation, collaboration, or sharing?

Question 3c. Assuming there are no changes to CISA's current funding levels, does CISA have the resources, personnel, and overall capacity to scale up these services beyond what is being offered now—and at what point would additional resources be required to meet heightened demand?

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

Question 4a. As the conversation about SICI evolves, there continues to be confusion about the proper terminology and definitions. The CSC report proposed the term "SICI," but you testified that CISA is instead using the term "Systemically Important Entities," or SIEs.

Please define Systemically Important Entity.

Question 4b. In your view, does this definition differ from the concept of SICI recommended by the CSC? If so, how?

Question 4c. What security objectives does CISA hope the SIE effort will accomplish? Please provide benchmarks and time lines.

Question 4d. Director Easterly has also recently utilized the term "Primary Systemically Important Entities," or PISCES. What differentiates these terms from one another? How do they work together?

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

Question 5. If Congress were to codify the concept of SICI/SIEs without adding any additional requirements on designated entities, how would that list be different from the Section 9 program?

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

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE FOR ERIC GOLDSTEIN

Question 1a. You noted that CISA's understanding of National systemic risk is rooted in the continuity and resilience of NCFs, and that the list of SIEs that CISA is currently identifying would be tied to NCFs. It would seem that, to do this work effectively, CISA would need a fairly granular understanding of critical assets within each region, the vendors they use, the security measures they have in place, and an overall sense of where they sit in the supply chain. However, as you testified, CISA has no authority to compel any organization to turn over this information.

How can CISA purport to understand the universe of assets and entities most critical to regional and National security—and the systemic cyber risks they face—without reliable access to information on the security posture and supply chains of SIEs?

Question 1b. Is there any other information that CISA needs in order to fully assess an SIE's relative security risk or vulnerability?

Question 1c. If Congress were to grant CISA broader compulsory authorities, how might CISA leverage these data streams to better understand and reduce systemic risks?

Question 1d. Would this include an understanding of the security measures critical entities have in place? Their vendors or supply chains? Or any other critical information that could be needed to fully assess an SIE's relative security risk or vulnerability?

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

Question 2. We know that CISA currently maintains a National Asset Database. You noted in your testimony that through your research, you found that no more than 14 States ever provided input to CISA related to the National Asset Database.

What does CISA intend to do to ensure that this stakeholder input from the State and local levels is improved and appreciated?

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

Question 3a. Earlier this year Congress passed legislation requiring certain critical infrastructure owners and operators to report major cyber incidents to CISA pursuant to rules set forth by CISA in an upcoming rulemaking. However, it may take years for these rules to go into effect. Recognizing the urgency of the current threat landscape, Congress also directed CISA to stand up voluntary reporting mechanisms that organizations can use to report cyber incidents and other threat information today, in lieu of formal requirements. CISA has been encouraging entities to report cyber incidents and other anomalous activity through those voluntary channels—particularly in response to potential escalation of Russian cyber threats.

How many voluntary reports has CISA received since this legislation was enacted in March—and from how many entities? Would you characterize this as an uptick in reporting, or is it on par with the past reporting levels?

Question 3b. How would you describe the nature and usefulness of the information CISA is receiving through this voluntary reporting?

Question 3c. How has CISA acted on the information it has received? For instance, has CISA used technical data to detect malicious cyber activity across sectors or inform guidance that can be disseminated broadly?

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

Question 4. In light of the March 21 announcement by the President on the evolving intelligence concerning a potential cyber threat from Russia, and the accompanying White House fact sheet encouraging U.S. critical infrastructure entities, technology and software companies to increasingly incorporate security by design, automation, a Software Bill of Materials and undertake other efforts to improve security of software development, what role do you see for CISA and/or ONCD in ensuring Infrastructure Investment & Jobs Act funding is implemented with the greatest attention paid to the cybersecurity standards and requirements built into it?

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

Question 5. The recent "Shields Up" warnings from CISA reinforce that today's threat landscape demands the most proactive posture possible. What's a recent example of operational collaboration between the private sector and the U.S. Government giving us advanced warning before the Russian military invasion in Ukraine about the nature of Russian cyber aggression we could reasonably expect and the sophistication of those actors?

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

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR ERIC GOLDSTEIN

Question 1a. On page 2 of your testimony, the last paragraph begins: "In the past year, CISA has made significant strides in this respect, particularly through the establishment of the Joint Cyber Defense Collaborative (JCDC) and our CISA Cybersecurity Advisory Committee (CSAC). These groups are examples of CISA's agency-wide dedication to operational collaboration and deep partnership, which is imbued across our mission divisions. By leveraging the expertise and unique authorities of Government and the private sector, CISA is better-positioned to connect with our stakeholders in industry and Government to share resources, analyses, and tools."

Can you give examples of the "significant strides" that CISA has made through the establishment of the Joint Cyber Defense Collaborative (JCDC) and our CISA Cybersecurity Advisory Committee (CSAC)?

Question 1b. Is the Joint Cyber Defense Collaborative in authorization language?

Question 1c. What industries, entities, or institutions are part of the stakeholders who are building their own cyber, communications, and physical security and resilience efforts?

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

Question 2a. On page 3 of your statement, you state that: "Our work has taken on increased urgency subsequent to Russia's unprovoked invasion of Ukraine. CISA has been working closely with our critical infrastructure partners over the past several months to ensure awareness of potential threats."

What are examples of the cause for the increased urgency due to Russia's unprovoked invasion of Ukraine?

Question 2b. How have critical infrastructure owners and operators responded to the call "to adopt a heightened security posture in light of President Biden's statement that intelligence shows Russia may be exploring options for potential cyber attacks. As part of our broader 'Shields Up' effort . . . "?

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

Question 3. In your testimony, on page 3, you say, "The JCDC operating model relies on regular analytic and data exchanges to enable common situational awareness and equip public and private-sector partners to take risk-informed coordinated action for our collective defense." I am aware that at the onset of the Federal Government's focus on getting better collaboration and cooperation from private-sector critical infrastructure owners and operators that there were rough patches.

How would you characterize the cooperation and engagement of private-sector partners?

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

Question 4. You mentioned the critical importance of the Log4j incident in moving stakeholders toward better cooperation. Your testimony states, "having built trust and strengthened relationships with our partners during our response to the Log4j incident . . . ".

How did this incident make the difference in what the program is able to accomplish today?

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

QUESTIONS FROM RANKING MEMBER JOHN KATKO FOR ERIC GOLDSTEIN

Question 1. The administration has identified some sectors, and specifically the energy sector, as at risk from "evolving" Russian cyber threats. How is CISA, as the Sector Risk Management Agency (SRMA) for 9 critical infrastructure sectors, leveraging independent and third-party data, like security ratings, to provide baseline cyber risk assessments to these sectors?

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

Question 2. Does CISA continuously monitor the cyber health of a given sector, or does CISA rely on a different means of assessing the cyber health of a sector? How does CISA leverage new tools and capabilities like security ratings to automate this task, and to see sector-wide cybersecurity risks in real time?

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

Question 3. Can you describe the process and criteria that CISA is using to evaluate endpoint detection and response (EDR) products as it works to fulfill the requirements laid out by EO 14028 for a centrally located EDR initiative? What are CISA's plans to ensure that a clear process is in place and what are the time lines for doing so?

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

Question 4. In light of the March 21 announcement by the President on the evolving intelligence concerning a potential cyber threat from Russia, and the accompanying White House fact sheet encouraging U.S. critical infrastructure entities, technology and software companies to increasingly incorporate security by design, automation, a Software Bill of Materials and undertake other efforts to improve security of software development, what role do you see for CISA and/or ONCD in ensuring Infrastructure Investment & Jobs Act funding is implemented with the greatest attention paid to the cybersecurity standards and requirements built into it?

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

Question 5. DoD has recently launched several initiatives to improve Defense Industrial Base security. DoD is leveraging the same technology that is used to harden the .mil to provide outside-in visibility into the resilience of these industry stakeholders that play equally central roles in our National security.

What are CISA's plans to leverage similar attack surface management capability for a strategic National snapshot and proactive vulnerability notification across the entire critical infrastructure community?

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

QUESTIONS FROM HONORABLE RALPH NORMAN FOR ERIC GOLDSTEIN

Question 1a. This committee has addressed at length the increasing threat that cyber attacks pose to our National security and the privacy and security of American workers and families served by businesses large and small around the country. The concern I'd like to raise is one of regulatory fragmentation. Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act as part of the recent Omnibus to require covered entities to notify CISA of cyber attacks within 72 hours. The problem is that multiple Federal regulators can require firms to notify them of the exact same cyber incident that CISA also requires notification for. For instance, with CISA notification requirements and similar proposed and final cyber incident rulemakings by multiple Federal and State regulators, one firm experiencing a single cybersecurity incident would likely have to notify several different Federal regulators of that same incident right in the middle of a tumultuous period in which covered entities should first and foremost be tending to the interests, privacy, and security of their customers and consumers. This regulatory fragmentation undermines Federal efforts and the efforts of covered entities under the law to respond in real time to and guard against cyber attacks. The Cyber Incident Reporting Act requires the DHS Secretary to lead a Cyber Incident Reporting Council to harmonize Federal reporting requirements and identify opportunities to streamline that reporting process.

How does CISA plan to streamline its cyber incident notification process to avoid regulatory fragmentation and ensure a single Federal notification procedure?

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

Question 1b. How are you going to ensure that covered entities under the law do not have to notify multiple regulators of the same cyber incident in the middle of doing what they need to protect their customers?

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

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR ROBERT K. KNAKE

Question 1a. In his testimony and responses to Member questions, Mr. Goldstein described the Systemically Important Entity process as an "evolution" or "maturation" of the Section 9 [of Executive Order 13636] list, with a goal of driving "operational collaboration" and understanding Systemically Important Entities' "dependencies and supply chains to reduce their risk going forward."

Is it CISA's/ONCD's goal to codify the framework established in Section 9 of Executive Order 13636?

Question 1b. Section 10 of Executive Order 13636 directed Federal agencies to engage in a review of "the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks," among other things. Did Section 10 of Executive Order 13636 result in the imposition of any new security obligations on Section 9 companies? If so, please describe. If not, why not? In light of the current threat environment, is the administration revisiting the analysis described by Section 10?

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

Question 2a. At the hearing Mr. Goldstein testified: "We certainly envision the Systemically Important Entity (SIE) process as an evolution or maturation of the Section 9 list. We're tying the list to National critical functions, and focusing on cascading a systemic impact will be an improvement over the Section 9 process and allow us to drive operational collaboration more effectively."

Please provide a description of the methodology CISA currently uses to identify SIEs, and describe how it differs from the methodology used in Section 9 designations.

Question 2b. Do you anticipate that tying the Systemically Important Entity list to National Critical Functions will result in a list of entities that differs significantly from the existing list of Section 9 entities? Or do you anticipate that the National Critical Functions analysis will drive analysis of interdependencies among SIEs?

Question 2c. Are there Section 9 entities that you do not believe will identified as Systemically Important Entities because the analysis is tied to National Critical Functions?

Question 2d. As the SIE process continues to evolve, do you anticipate identifying "tiers" of Systemically Important Entities to reflect both an entity's systemic importance and the sophistication with which it can operationally collaborate with the Federal Government?

Question 2e. How many SIEs has CISA currently identified? Please provide a breakdown of such list by sector, the number of SIEs currently enrolled in CISA programs and services, the number of currently engaged in operational collaboration with CISA, and any other information that would be helpful to characterize CISA's current understanding of SIEs.

Question 2f. What information does CISA need in order to fully and accurately identify and understand systemic risks to SIEs, and where does that information originate? What data sources is CISA currently able to leverage to carry out this work, and what data is CISA currently unable to obtain?

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

Question 3a. The Cyberspace Solarium Commission (CSC) recommended Congress codify a new designation for SICI. The concept behind SICI is that certain entities—those that operate our most vital systems and assets—should be granted special assistance from the U.S. Government and should be expected shoulder additional security and information-sharing requirements befitting their unique status and importance.

If Congress were to create a regime that aligns as closely as possible to the CSC's proposal (i.e., a designation that comes with benefits and burdens), what are the most critical, impactful programs or partnership models that Congress should consider for purposes of mandating participation from designates entities? What types of information should be shared?

Question 3b. Are there authorities CISA currently lacks that it would need if Congress were to decide to mandate such participation, collaboration, or sharing?

Question 3c. Assuming there are no changes to CISA's current funding levels, does CISA have the resources, personnel, and overall capacity to scale up these services beyond what is being offered now—and at what point would additional resources be required to meet heightened demand?

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

Question 4. If Congress were to codify the concept of SICI/SIEs without adding any additional requirements on designated entities, how would that list be different from the Section 9 program?

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

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE FOR ROBERT K. KNAKE

Question 1. In response to Member questions, you observed that many entities that would be classified as SICI/SIEs are very well-resourced organizations, with their own red teaming and threat-hunting capabilities. However, a major roadblock for these entities is that they cannot collect intelligence in the way the U.S. intelligence community can.

What is the ONCD's stance on the creation of a Joint Collaborative Environment, which would allow for these entities to participate in a collaborative environment where it can be trusted that the information being shared there between the public and private sectors can be secured?

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

Question 2. How is ONCD working with CISA to develop a greater understanding of potential additional authorities that could help CISA conduct its SIE process and its collaboration with key sector partners?

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

Question 3. In light of the March 21 announcement by the President on the evolving intelligence concerning a potential cyber threat from Russia, and the accompanying White House fact sheet encouraging U.S. critical infrastructure entities, technology, and software companies to increasingly incorporate security by design, automation, a Software Bill of Materials and undertake other efforts to improve security of software development, what role do you see for CISA and/or ONCD in ensuring Infrastructure Investment & Jobs Act funding is implemented with the greatest attention paid to the cybersecurity standards and requirements built into it?

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

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR ROBERT K. KNAKE

Question 1. In your testimony you speak about how Russia's unprovoked aggression against Ukraine is causing heightened threats against U.S. cyber interest.

Has this link between the desire by a Nation that they may anticipate will be opposed by the United States resulted in cyber attack in the past?

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

Question 2a. Russia interfered in the U.S. Presidential elections in 2016 and again in 2020. A Russia hacker group is said to have attacked Colonial Pipeline.

Are we seeing official and unofficial Russia-based attacks without seeing a link between the two types of threats?

Question 2b. Is it true that the coding style used to construct cyber attacks can indicate their source?

Question 2c. How reliably can we track and assign attribution for attacks?

Question 2d. Have we been doing enough to raise the cost of attacks to make the ransomware less attractive as a tool for theft?

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

Question 3a. On page 6 you stated in your testimony: "Recognizing the unique risks presented in cyber space for the conflict to spill out of Ukraine and onto our shores, the Federal Government has also partnered with industry on tabletop exercises, bringing important critical infrastructure stakeholders".

Are we at risk of being pulled into a virtual conflict over Russia's brutal war against Ukraine and if yes, what would that look like?

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

QUESTION FROM HONORABLE JAMES R. LANGEVIN FOR ROBERT K. KNAKE

Question. Based on the testimony we heard, it's clear that the CISA's Systemically Important Entities effort is engaged in a rigorous identification process. But the next steps of what to do with its list appear less clear to me than the Solarium Commission's vision for SICI, which calls for specific benefits and obligations to SICI entities. While an accurate identification process is important, we must also have a clear picture of the policies and strategies that will govern and strengthen the partnership between the Federal Government and our most critical of critical infrastructure entities.

If CISA develops a list of systemically important entities, what does the administration plan to do with it? How would factors like cyber maturity, as we discussed, play a role in where and how the Government would prioritize its efforts to partner with critical infrastructure owners and operators?

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

QUESTION FROM RANKING MEMBER JOHN KATKO FOR ROBERT K. KNAKE

Question. In light of the March 21 announcement by the President on the evolving intelligence concerning a potential cyber threat from Russia, and the accompanying White House fact sheet encouraging U.S. critical infrastructure entities, technology, and software companies to increasingly incorporate security by design, automation, a Software Bill of Materials and undertake other efforts to improve security of software development, what role do you see for CISA and/or ONCD in ensuring Infrastructure Investment & Jobs Act funding is implemented with the greatest attention paid to the cybersecurity standards and requirements built into it?

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

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE FOR TINA WON SHERMAN

Question 1. The National Infrastructure Protection Plan was last updated in 2013. This hold-up has led to SRMAs not updating their Sector-Specific Plans until the National Infrastructure Protection Plan update occurs.

Dr. Sherman, how has this delay in updating the National Infrastructure Protection Plan hindered SRMA efforts to protect the critical infrastructure sectors they work with? What has the impact been on CISA's ability to protect U.S. critical infrastructure?

Answer. The 2013 National Infrastructure Protection Plan's lack of a recent update has led to limitations for Sector Risk Management Agencies (SRMAs)—the Federal departments charged with providing critical infrastructure sector owner/operators with specialized expertise—in two ways.

First, SRMAs and CISA have no updated guidance for how best to modify their activities, if needed, in response to requirements for SRMAs in the National Defense Authorization Act for Fiscal Year 2021, such as supporting National risk assessment efforts and contributing to critical infrastructure owner/operator emergency preparedness.[1] As part of GAO's on-going review evaluating SRMA responsibilities, GAO is examining whether SRMA's have sufficient guidance from the Department of Homeland Security on approaches for addressing such responsibilities.

Second, the 2013 National Infrastructure Protection Plan calls for SRMAs to update their sector-specific plans on a regular basis. However, SRMAs were without a recent update of the 2013 plan to help guide sector-specific plan revisions. CISA reported in November 2021 that most SRMAs updated their respective sector-specific plans following the publication of the 2013 National Plan and those sector-specific plans currently serve as the strategic guidance for the sectors. However, given the passage of time since these plans were published, they may not reflect the current threat environment. For example, as GAO reported in November 2021, CISA had not updated the 2015 Communications Sector-Specific Plan.[2] As a result, the 2015 plan lacked information on new and emerging threats to the Communications Sector, such as security threats to the communications technology supply chain, and disruptions to position, navigation, and timing services.

Question 2. Dr. Sherman, we know that CISA currently maintains a National Asset Database. You noted in your testimony that through your research, you found that no more than 14 States ever provided input to CISA related to the National Asset Database.

Why have so few States provided input to CISA regarding this database?

Answer. CISA data showed that from fiscal years 2017 through 2021, no more than 14 States (of 56 States and territories) provided new nominations or updates to the National Critical Infrastructure Prioritization Program in any given fiscal year.[3] State officials GAO interviewed questioned the program's usefulness, which may lead to less State participation. Of the 6 State homeland security agencies GAO contacted, only one reported regularly using the program list. Officials from these 6 State agencies also questioned the list's accuracy, and most said that they did not use the list to inform risk communication or influence decisions. Officials from 3 of 6 State agencies said that there were assets on the list that were not critical to their States. Some of the State officials also said that the infrastructure on the list

---

[1] See 6 U.S.C. § 665d.

[2] GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector,* GAO–22–104462 (Washington, DC: Nov. 23, 2021).

[3] The Implementing Recommendations of the 9/11 Commission Act required the Secretary of Homeland Security to establish and maintain a single prioritized list of systems and assets in a National database that the Secretary determines would, if destroyed or disrupted, cause National or regional catastrophic effects. See 6 U.S.C. § 664. Consistent with this requirement, DHS developed the National Critical Infrastructure Prioritization Program.

seemed inconsistent from State to State and that the criteria for adding assets were highly subjective, making the list generally unreliable, in their view.[4]

In addition, critical infrastructure officials, including State officials, GAO interviewed questioned the present-day relevance of the criteria for adding infrastructure to the program list, another reason for limited State participation. Specifically, to be included on the program's Level 1 list (its highest consequence list), an asset's destruction or disruption must meet minimum specified consequence thresholds for at least 2 of the following 4 categories: Economic loss, fatalities, mass evacuation length, and degradation of National security. Senior officials with CISA, as well as other Federal, State, and private-sector officials GAO spoke with, said that the consequence thresholds for these criteria did not reflect the threat environment today, which focuses more on cyber attacks and extreme weather events. The current day threat environment also focuses on vulnerabilities or attacks that can affect multiple entities within a short period. In this scenario, the consequences related to a single asset, entity, system, or cluster may not reach program thresholds, but the aggregate impacts may be nationally significant, according to CISA officials.

QUESTIONS FROM HONORABLE SHEILA JACKSON LEE FOR TINA WON SHERMAN

Question 1. You begin your testimony with the statement: "To improve critical infrastructure security, key actions Department of Homeland Security (DHS) needs to take include: (1) Strengthening the Federal role in protecting the cybersecurity of critical infrastructure and (2) improving priority-setting efforts." Excerpt from your testimony: "Strengthen the Federal role in protecting the cybersecurity of critical infrastructure. Pursuant to legislation enacted in 2018, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS was charged with responsibility for enhancing the security of the Nation's critical infrastructure in the face of both physical and cyber threats. In March 2021, GAO reported that DHS needed to complete key activities related to the transformation of CISA. This includes finalizing the agency's mission-essential functions and completing workforce planning activities. GAO also reported that DHS needed to address challenges identified by selected critical infrastructure stakeholders, including having consistent stakeholder involvement in the development of related guidance. Accordingly, GAO made 11 recommendations to DHS, which the Department intends to implement by end of 2022. Improve priority setting efforts. Through the National Critical Infrastructure Prioritization Program, CISA is to identify a list of systems and assets that, if destroyed or disrupted, would cause National or regional catastrophic effects. Consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007, CISA annually updates and prioritizes the list. The program's list is used to inform the awarding of preparedness grants to States. However, in March 2022, GAO reported that 9 of 12 CISA officials and all 10 of the infrastructure stakeholders GAO interviewed questioned the relevance and usefulness of the program. For example, stakeholders questioned the current relevance of the criteria used to add critical infrastructure to the Prioritization Program list. In 2019, CISA published a set of 55 National critical functions of the Government and private sector considered vital to the security, economy, and public health and safety of the Nation (see figure). However, most of the Federal and non-Federal critical infrastructure stakeholders that GAO interviewed reported being generally uninvolved with, unaware of, or without an understanding of the goals of the framework for its critical functions. GAO made recommendations to DHS in its March 2022 report to address these concerns, such as ensuring stakeholders are fully engaged in the framework's implementation, and DHS agreed with the recommendations."

I have stressed the need for hyper focus on protecting the Nation's critical infrastructure for well over a decade.

Today, as we watch Russia's total disregard for human life—men, women, children, and the elderly are being slaughtered before our eyes. It is clear that there are no rules of engagement, no Geneva Convention fears that will save any of us should Russia engage in a full onslaught against domestic critical infrastructure.

Are we at a point where everyone, private sector, public sector, National security, and law enforcement are on the same page when we talk about the importance of critical infrastructure cyber defense?

Answer. The John S. McCain National Defense Authorization Act for Fiscal Year 2019 created the Cyberspace Solarium Commission to develop consensus on a strategic approach to defending the United States against cyber attacks of significant

[4] GAO, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing*, GAO–22–104279, (Washington, DC: Mar. 1, 2022).

consequences.[5] The commission's March 2020 report was based on collaboration with a wide range of critical infrastructure stakeholders, including private sector, public sector, National security, and law enforcement officials. The report highlighted the importance of critical infrastructure cyber defense and identified approaches for improving the Federal role in leading collaborative cybersecurity efforts.

In addition, a recent Executive Order and GAO's work on high-risk issues facing the Federal Government have identified cybersecurity as a National priority. The May 2021 Executive Order on Improving the Nation's Cybersecurity recognized that persistent and increasingly sophisticated malicious cyber campaigns threaten the public sector, the private sector, and ultimately the American people's security and privacy.[6] The Executive Order called for improvements in the Federal Government's efforts to identify, deter, protect against, detect, and respond to these actions and actors. In its March 2021 High-Risk report, GAO also identified the importance of addressing 4 major cybersecurity challenges and 10 associated critical actions, shown in the figure below.[7] Although the Federal Government has made selected improvements, it needs to move with a greater sense of urgency commensurate with the rapidly-evolving and grave threats to the country.

Four Major Cybersecurity Challenges and 10 Associated Critical Actions Cited in GAO's March 2021 High Risk Report

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government- wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis. | GAO-21-288

In recent years, GAO has also identified several specific areas of stakeholder cybersecurity engagement in need of improvement:

- *National Critical Infrastructure Prioritization Program*.—Through the National Critical Infrastructure Prioritization Program, the Cybersecurity and Infrastructure Security Agency (CISA) is to identify a list of systems and assets that, if destroyed or disrupted, would cause National or regional catastrophic effects. State officials nominate systems and assets for inclusion on this list. GAO's March 2022 report found that CISA and other stakeholders questioned the present-day relevance of NCIPP criteria for adding infrastructure to the list.[8] For example, senior officials with CISA, as well as other Federal, State, and private-sector officials GAO spoke with, said that the consequence thresholds for

[5] Pub. L. No. 115–232, § 1652, 132 Stat. 1636, 2140 (2018).
[6] Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021).
[7] GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO–21–288 (Washington, DC: Mar. 24, 2021).
[8] GAO–22–104279.

the criteria did not reflect the threat environment today, which focuses more on cyber attacks and extreme weather events.

- *Pipeline security*.—DHS oversees pipeline security for the Federal Government, providing both voluntary guidance and required cybersecurity measures for pipeline owner/operators. DHS prioritizes its outreach to pipeline owner/operators based on a risk assessment. GAO reported in December 2018 that DHS's pipeline risk assessments were missing key inputs, including a measure of cybersecurity vulnerabilities.[9] Pipeline owner/operators will likely receive more targeted guidance if DHS collected more information from owner/operators on cybersecurity vulnerabilities as part of its risk-ranking effort.
- *Chemical security*.—The Department of Homeland Security's Chemical Facility Anti-Terrorism Standards program reviews high-risk chemical facilities for adherence to security standards, including cybersecurity performance standards. GAO reported in May 2020 that the program had yet to incorporate identified cybersecurity knowledge, skills, and abilities for inspectors in its workforce planning processes or track data related to covered facilities' reliance on information systems when assessing its workforce needs.[10] Chemical facility owner/operators will likely receive higher-quality inspections if planning for DHS's inspector workforce includes attention to cybersecurity competencies.

Question 2. Is the GAO tracking how collaborations on the issue of cybersecurity of critical infrastructure is being translated into concrete improvements?

Answer. Since 2010, GAO has made about 80 recommendations for various agencies to enhance infrastructure cybersecurity.[11] For example, in February 2020, GAO recommended that agencies better measure the adoption of the National Institute of Standards and Technology framework of voluntary cyber standards and correct sector-specific weaknesses. Specifically, GAO reported that most Sector Risk Management Agencies were not collecting and reporting on improvements in the protection of critical infrastructure as a result of using the framework across the sectors.[12] Therefore, GAO made 10 recommendations—one to the National Institute of Standards and Technology on establishing time frames for completing selected programs—and 9 to the lead agencies, to collect and report on improvements gained from using the framework. Eight of these agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. However, as of November 2021, none of the recommendations had been implemented. Until the lead agencies collect and report on improvements gained from adopting the framework, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructure from threats will be largely unknown. GAO reiterated these recommendations in February 2022.[13]

GAO has also reported on the need for lead agencies to enhance the cybersecurity of their critical infrastructure sectors and subsectors—such as communications, energy, education, financial services, and transportation systems.[14]

Question 3. The GAO is well-suited to collecting data and reporting on the progress of regulatory and legislative intent for a broad range of policy issues. Does GAO have the resources needed to keep pace with the DHS's expanded focus on cybersecurity and cyber defense?

In March 2022, GAO released its strategic plan for fiscal years 2022 through 2027 along with reports on the key efforts GAO expects to cover during this period, as well as current trends affecting Government and society.[15] One of GAO's key goals is to help Congress respond to changing security threats and the challenges of global interdependence. Among other things, key efforts related to this goal focus on assessing cyber risks to the security and resilience of the Nation's critical infrastruc-

---

[9] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO–19–48 (Washington, DC: Dec. 18, 2018).

[10] GAO, *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities*, GAO–20–453 (Washington, DC: May 14, 2020).

[11] GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO–21–288 (Washington, DC: Mar. 24, 2021).

[12] GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements,* GAO–20–299 (Washington, DC: Apr. 9, 2020).

[13] GAO, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance,* GAO–22–105103 (Washington, DC: Feb. 9, 2022).

[14] See, for example, GAO, *Cybersecurity: Federal Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure,* GAO–22–105530 (Washington, DC: Dec. 2, 2021).

[15] GAO, *Strategic Plan 2022–2027,* GAO–22–1SP (Washington, DC: Mar. 15, 2022); GAO, *Key Efforts 2022–2027,* GAO–22–2SP (Washington, DC: Mar. 15, 2022); and GAO, *Trends Affecting Government and Society,* GAO–22–3SP (Washington, DC: Mar. 15, 2022).

ture and assessing DHS's efforts to manage risks and share information with public and private-sector partners to protect the Nation's critical infrastructure.

In April 2022, the Comptroller General of the United States testified on the subject of GAO's budget request of $810.3 million for fiscal year 2023.[16] This budget request will enable GAO to increase capabilities associated with growing cybersecurity developments and complex National security issues, among other topics. Given the critical importance of these topics, GAO is continuing to grow its workforce for cybersecurity and National security. For example, on April 20, 2022, GAO posted an announcement for multiple senior analyst positions focusing on National security. Further, GAO's growing cyber expertise includes its Center for Enhanced Cybersecurity, a dedicated group of cyber professionals that could delve into the technical details of agency systems and networks and identify underlying persistent cybersecurity weaknesses. As networks and information systems have become more elaborate, diverse, and interconnected, GAO has recognized the need to cultivate a center of excellence to conduct in-depth technical audits.

Finally, GAO has reported that key actions DHS needs to take include strengthening the Federal role in protecting the cybersecurity of critical infrastructure and improving priority-setting efforts.[17]

[16] *GAO Budget, Before House Appropriations Committee, Subcommittee on Legislative Branch,* 117th Cong. (2022) (Statement of Comptroller Gen. of the United States Gene L. Dodaro). Accessed April 28, 2022, *https://plus.cq.com/doc/testimony-6503637?2.*

[17] GAO, *Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure,* GAO–22–105973 (Washington, DC: Apr. 6, 2022).