

**CISA 2025: THE STATE OF AMERICAN
CYBERSECURITY FROM CISA'S PERSPECTIVE**

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

APRIL 27, 2023

Serial No. 118–9

Printed for the use of the Committee on Homeland Security



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

U.S. GOVERNMENT PUBLISHING OFFICE

52–983 PDF

WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

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

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

STEPHEN SIAO, *Staff Director*

HOPE GOINS, *Minority Staff Director*

NATALIE NIXON, *Chief Clerk*

SEAN JONES, *Legislative Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

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

CARA MUMFORD, *Subcommittee Staff Director*

MOIRA BERGIN, *Minority Subcommittee Staff Director*

ALICE HAYES, *Subcommittee Clerk*

CONTENTS

	Page
STATEMENTS	
The Honorable Andrew R. Garbarino, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	1
Prepared Statement	2
The Honorable Eric M. Swalwell, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	3
Prepared Statement	4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement	6
WITNESS	
Ms. Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA):	
Oral Statement	7
Prepared Statement	9
APPENDIX	
Questions for Jen Easterly From Chairman Andrew R. Garbarino	41
Questions for Jen Easterly From Ranking Member Eric Swalwell	43
Questions for Jen Easterly From Honorable Robert Menendez	44

CISA 2025: THE STATE OF AMERICAN CYBERSECURITY FROM CISA'S PERSPECTIVE

Thursday, April 27, 2023

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

The subcommittee met, pursuant to notice, at 2:03 p.m., in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

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

Also present: Representative Clarke.

Mr. GARBARINO. The Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection, will come to order.

The purpose of this hearing is to receive testimony from Jen Easterly, director of Cybersecurity and Infrastructure Security Agency, or CISA.

I now recognize Ranking Member Swalwell for the purposes of seeking unanimous consent.

Mr. SWALWELL. Thank you, Chairman.

I ask unanimous consent that the gentlelady from New York, Ms. Clarke, be permitted to participate in today's hearing.

Mr. GARBARINO. Without objection, so ordered.

I now recognize myself for an opening statement.

Welcome back for our second subcommittee hearing of the Congress. Last month, we hosted industry leaders to give their perspective on the state of American cybersecurity and particularly how the Cybersecurity Infrastructure Security Agency, or CISA, has developed since its creation 5 years ago. I'm glad that we will hear directly from CISA director Jen Easterly on her views on CISA's evolution and where it needs to grow and mature by 2025.

Director Easterly and I have had a fantastic working relationship since I started as Ranking Member of the subcommittee last Congress. I look forward to continuing our strong bipartisan relationship this Congress.

In our last hearing, there were some common themes from our witnesses that I hope to further explore with Director Easterly this afternoon.

First, we learned that CISA must work with the industry and interagency partners to ease compliance, the compliance burden that industry faces from duplicative regulation. It's clear that our

Nation must increase resilience to cyber risk across the board, particularly within our critical infrastructure sectors, but we must find the right balance between regulatory burden and improving security outcomes.

We also heard a lot about one of CISA's newest initiatives, the Joint Cyber Defense Collaborative, or JCDC. We heard that JCDC has the potential to be a value-add to the private sector, but additional transparency around its mission and processes would benefit both the JCDC and industry.

Finally, and perhaps most foundationally, we heard about the need for robust cybersecurity work force. We need not only enough people but the right people with the right skills and the right jobs. This is one of my top priorities this Congress, and I'm looking forward to hearing Director Easterly's perspective on how CISA can best contribute to the development of our national cyber work force.

This hearing is timely. It comes as we are evaluating the President's fiscal year 2024 budget request. CISA is requesting \$3.1 billion, \$145 million increase over fiscal year 2023 enacted—fiscal 2023 enacted funding level. The dialog we have during this hearing will help inform our committee's review of the budget, particularly the new program CISA proposes within, including the evolution of the National Cybersecurity Protection System.

I think I speak for all Members on this dais when I say that we want CISA to succeed. Its mission is too important to fail. It is our responsibility to ask pointed but productive questions about CISA's stewardship of the resources and authorities Congress has given it. As I said in our last hearing, Congress intends to be a partner to CISA to ensure the agency meets its full potential.

Director Easterly, I look forward to your testimony today, and I thank you for being here.

[The statement of Chairman Garbarino follows:]

PREPARED STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

Welcome back for our second subcommittee hearing of the Congress. Last month, we hosted industry leaders to give their perspective on the state of American cybersecurity and particularly how the Cybersecurity and Infrastructure Security Agency, or CISA, has developed since its creation 5 years ago. I am glad that we will hear directly from CISA Director Jen Easterly on her views on CISA's evolution and where it needs to grow and mature by 2025. Director Easterly and I have had a fantastic working relationship since I started as Ranking Member of this subcommittee last Congress—I look forward to continuing our strong bipartisan relationship this Congress.

In our last hearing, there were some common themes from our witnesses that I hope to further explore with Director Easterly this afternoon.

First, we learned that CISA must work with industry and interagency partners to ease the compliance burden that industry faces from duplicative regulation. It's clear that our Nation must increase resilience to cyber risk across the board, particularly within our critical infrastructure sectors. But, we must find the right balance between regulatory burden and improving security outcomes.

We also heard a lot about one of CISA's newest initiatives: the Joint Cyber Defense Collaborative, or JCDC. We heard that JCDC has the potential to be a value-add to the private sector but additional transparency around its mission and processes would benefit both JCDC and industry.

Finally, and perhaps most foundationally, we heard about the need for a robust cybersecurity workforce. We need not only enough people but the right people with the right skills, in the right jobs. This is one of my top priorities this Congress and I am looking forward to hearing Director Easterly's perspective on how CISA can best contribute to the development of our national cyber workforce.

This hearing is timely. It comes as we are evaluating the President's fiscal year 2024 budget request. CISA is requesting \$3.1 billion, a \$145 million increase over the fiscal year 2023 enacted funding level. The dialog we have during this hearing will help inform our committee's review of the budget, particularly the new programs CISA proposes within, including the evolution of the National Cybersecurity Protection System.

I think I speak for all the Members on this dais when I say that we want CISA to succeed. Its mission is too important to fail. It's our responsibility to ask pointed but productive questions about CISA's stewardship of the resources and authorities Congress has given it. As I said in our last hearing, Congress intends to be a partner to CISA to ensure the agency meets its full potential. Director Easterly, I look forward to your testimony today and thank you for being here.

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

Mr. SWALWELL. Thank you, Chairman.

Welcome, Director. It was just 12 hours ago that the Chairman and I were here early in the morning with our colleagues voting. I don't think we voted the same way on many of the amendments yesterday, but on this issue and your success, there is no daylight between the Chairman and I and my colleagues. Your success is America's success in this space, and that is something we are rooting for and want to enable.

I also represent an East Bay California district that is home to tech giants like TriNet and Workday, but also an emerging cybersecurity insurance company called Cowbell Cyber, and have worked with all of them to protect, not just large companies, but small- and medium-size companies from emerging threats.

As the Chairman said, CISA is at an inflection point, and Congress made CISA an operational component of DHS 5 years ago. Since then, its budget has nearly doubled, and Congress has provided it with a range of new authorities, from mandatory cyber incident reporting to persistent threat hunting on Federal networks to Cyber Century. CISA has ambitiously taken on new responsibilities to meet the demands of an evolving threat landscape, building trusted relationships with new stakeholders in the process.

For that, I and our team commend CISA for its proven ability to dynamically respond to evolving threats ranging from election security, to open-source software vulnerabilities, to the Shields Up campaign. As it relates to election security, I hope to hear an update from CISA on some recent successes; this launch promising new initiatives, including the National Risk Management Center and the Joint Cyber Defense Collaborative, a collaboration that so many outside organizations, private-sector folks, are asking how do we get in, how do we participate, which to me means you are a victim of your own success in that regard in that there's high interest in growing and expanding the ability to share information and collaborate to take on our threats. All of these are worthy efforts. I support them and am committed to their success.

Today I look forward to hearing how CISA will continue to deliberate in the new work it takes on and the commitments it makes to our partners. As more stakeholders become aware of CISA and its capacity, they have placed more and more demands on its resources. CISA cannot be, as you know, everything to everyone, and it certainly does not have the resources to boil the ocean.

Becoming the powerhouse cybersecurity and critical infrastructure defense agency, CISA has the potential to be—requires—what

CISA has the potential to be requires clear strategic direction and determined leadership. I have every confidence that Director Easterly has both, and I will be interested in learning more about your vision for CISA moving forward.

I'm also interested, as I referenced, in the future of JCDC. Stakeholders have applauded JCDC as an innovative, flexible tool for CISA to gather and fuse threat information, foster real-time collaboration, and push out security practices through initiatives like its Shields Up campaign.

Over the past year-and-a-half, CISA has expanded JCDC's focus to include open-source software security and protecting high-risk communities by journalistic or civil society organizations. Although these are worthwhile efforts, it's unclear what criteria JCDC is using to select which areas to focus on, which organizations to partner with, and not how these activities are tied to the JCPOs original purpose of streamlining, cyber planning, and operational collaboration.

I look forward to candid conversations about defining JCDC's core functions, how to ensure JCDC partners are involved in decisions about its future, and how it can bring a more proactive posture to CISA's defense activities. Formalizing the answers to these questions through authorization will ensure JCDC has enduring value for years to come.

On a related note, I understand that CISA is in the process of revamping the National Risk Management Center, and look forward to learning more about plans to make CISA's—to make it CISA's analytical hub.

Finally, it's critically important that CISA do more to secure industrial control systems and other operational technology. I appreciate CISA's support for my legislation that we passed into law last year, the Industrial Control Systems Cybersecurity Training Act, which will solidify the existence of meaningful training courses to ensure OT remains at the forefront of our security focus.

As I am sure you'll agree, CISA must develop that work force now, not 5 years from now, while also doing more to promote threats—to understand threats to OC systems, push out its cyber performance goals, and grow programs like Cyber Century that monitor our OT threats.

Thank you again to the Chairman for convening us here today.

Thank you, Director Easterly, and your team who's worked with us, for your testimony, and I look forward to a robust conversation about attacking the threats that we face.

I yield back.

[The statement of Ranking Member Swalwell follows:]

PREPARED STATEMENT OF RANKING MEMBER ERIC M. SWALWELL

APRIL 27, 2023

Good afternoon. I want to thank my friend, Chairman Garbarino, for holding today's hearing on the future of the Cybersecurity and Infrastructure Security Agency, and echo his appreciation to Director Easterly for her participation today.

CISA is at an inflection point.

Congress made CISA an operational component of DHS nearly 5 years ago.

Since then, its budget has nearly doubled and Congress has provided it a range of new authorities—from mandatory cyber incident reporting, to persistent threat hunting on Federal networks, to CyberSentry.

And CISA has ambitiously taken on new responsibilities to meet the demands of the evolving threat landscape, building trusted relationships with new stakeholders in the process.

I commend CISA for its proven ability to dynamically respond to evolving threats, ranging from election security to open source software vulnerabilities to the Shields Up campaign.

It has launched promising new initiatives, including the National Risk Management Center and the Joint Cyber Defense Collaborative, aimed at maturing how the Government understands systemic risk and operationalizes partnerships across agencies and with the private sector.

All of these are worthy efforts. I support them, and I am committed to their success.

At the same time, at this critical juncture, CISA must be deliberate in the new work it takes on and the commitments it makes to its partners.

As more stakeholders have become aware of CISA and its capacity, they have placed more and more demands on its resources.

CISA cannot be everything to everyone, and it cannot boil the ocean.

Becoming the powerhouse cybersecurity and critical infrastructure defense agency CISA has the potential to be requires clear strategic direction and determined leadership.

I have every confidence that Director Easterly has both, and I will be interested in learning more about her vision for CISA moving forward.

I am also interested in discussing the future of JCDC.

Stakeholders have applauded JCDC as an innovative, flexible tool for CISA to gather and fuse threat information, foster real-time collaboration, and push out security practices through initiatives like its “Shields Up” campaign.

Over the past year-and-a-half, however, CISA has expanded JCDC’s focus to include, open-source software security or protecting high-risk communities like journalistic or civil society organizations.

Although these are worthwhile efforts, it is unclear what criteria JCDC is using to select which areas to focus on, which organizations to partner with (and for what reason), and how these activities are tied to the JCPO’s original purpose of streamlining cyber planning and operational collaboration.

I look forward to candid conversations about defining JCDC’s core functions, how to ensure JCDC partners are involved in decisions about its future, and how it can bring a more proactive posture to CISA’s defensive activities.

Formalizing the answers to these questions through authorization will ensure JCDC has enduring value for years to come.

On a related note, I understand that CISA is in the process of revamping the National Risk Management Center, and I look forward to learning more about plans to make it CISA’s analytical hub.

Like JCDC, I believe NRMCM would benefit from authorization and hope to work with you on that effort as you finalize the restructuring process.

Finally, it is critically important that CISA do more to secure industrial control systems (ICS) and other operational technology (OT).

These systems deliver indispensable services—the water we drink, the energy that powers our home, the gas we put in our cars, the goods we manufacture, and countless others.

They are also increasingly connected to the internet, uniquely vulnerable, and require specialized expertise to secure—and we don’t have nearly enough OT security professionals in the workforce today.

CISA needs to be developing that workforce now, not 5 years from now—while also doing to more to understand threats to OT systems, push out its Cyber Performance Goals, and grow programs like Cyber Sentry that help to monitor OT threats.

Thank you, again, Director Easterly, for your testimony.

I yield back.

Mr. GARBARINO. Thank you, Ranking Member Swalwell.

I do not see the Chairman or the Ranking Member of the full committee. So other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

APRIL 27, 2023

Good afternoon. I want to thank Chairman Garbarino and Ranking Member Swalwell for organizing this important hearing and Director Easterly for coming to testify before the subcommittee today.

The subject of today's hearing is of particular importance to me, since I was one of a small group of legislators who spent years working on legislation to remake CISA's predecessor agency—a small, under-resourced headquarters component known as the National Protection and Programs Directorate—into the operational cyber powerhouse we know today.

Since Congress established CISA 4½ years ago, the agency has developed a broad range of capabilities to defend critical infrastructure from cyber and physical threats.

I am proud of the Homeland Security Committee's bipartisan work to ensure CISA has the authorities and resources necessary to fulfill its broad and incredibly important mission, and I have been impressed with how Director Easterly has utilized these authorities to build out CISA's capabilities and visibility.

As CISA continues to mature as an agency, it is essential that it maintain a clear vision of the agency's role.

In particular, as the agency determines its priorities, CISA must ensure that both cyber and physical threats continue to receive the necessary attention.

I was concerned that the President's budget request included proposed cuts to vital programs within the Infrastructure Security Division.

The distinction between cyber and physical threats is not always as clear as it may seem, and CISA's ability to coordinate security efforts against all threats is part of what gives it a unique role in defending critical infrastructure.

Continuing to balance investments across all divisions will produce the most security benefits.

To that end, I am also interested to hear more about CISA's plans for the National Risk Management Center, which if utilized properly, has the potential to become a vital center for risk analysis, serving CISA, other Federal agencies, and critical infrastructure more broadly.

The Biden administration's new National Cybersecurity Strategy, released earlier this year, lays out ambitious goals for improving the state of our Nation's cybersecurity.

The Strategy provides clear objectives for Federal agencies to implement as they carry out their cybersecurity mission.

CISA's role as the national coordinator for critical infrastructure security and resilience will make it a central player in bringing together the Federal Government, State and local governments, and the private sector in carrying out the Strategy.

But, considering the broad range of stakeholders that CISA serves, it risks being pulled in too many directions.

I look forward to hearing more about how CISA plans to contribute to the Strategy's implementation as the administration develops more detailed plans for implementing its strategic objectives, and how CISA will prioritize its own goals.

As CISA continues to grow as an agency, I appreciate that it is working hard to fill the many vacancies in its ranks.

I urge CISA to use the significant hiring it plans to undertake in the coming year to improve the diversity of its own workforce, just as it must prioritize efforts to educate and train a more diverse cyber workforce nationally.

Additionally, expanding the number and diversity of voices CISA hears from as it consults with outside stakeholders, both formally and informally, will make CISA better able to address the broad range of threats our Nation faces.

I hope as the Cybersecurity Advisory Committee continues its work going forward that its makeup will be more inclusive of the number of women and people of color with cybersecurity expertise whose perspective CISA would benefit from hearing.

Thank you again to the Chair and Ranking Member for their on-going work to strengthen our Nation's cybersecurity and to Director Easterly for her tireless work at CISA.

I yield back.

Mr. GARBARINO. I am pleased to have Director Easterly before us today to discuss this very important topic. I ask that our witness please rise and raise their right hand.

[Witness sworn.]

Mr. GARBARINO. Let the record reflect that the witness has answered in the affirmative.

Thank you. Please be seated.

I would now like to formally introduce our witness, Jen Easterly. She's the director of the Cybersecurity and Infrastructure Security Agency at DHS. She was nominated by President Biden April 2021, and unanimously confirmed by the Senate on July 12, 2021. That's no easy feat.

As director, Director Easterly leads CISA's effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day.

Before serving in her current role, she was the head of Firm Resilience at Morgan Stanley, responsible for ensuring preparedness in response to business-disrupting operational incidents and risks. Director Easterly also has a long tenure in public service, to include two tours at the White House.

Director, thank you for being here today. I now recognize you for 5 minutes to summarize your opening statement.

STATEMENT OF JEN EASTERLY, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

Ms. EASTERLY. Thank you so much, Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, for the opportunity to appear before you today. I'm really excited to share what we're doing to ensure that the CISA of today and of tomorrow is the agency that our Nation deserves.

As America's cyber defense agency, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every day. Since CISA was established in 2018, the threats we face have become more complex, more geographically dispersed, and they affect the entire cyber ecosystem, from Federal civilian government agencies, to businesses large and small, to State and local governments and, ultimately, the American people.

CISA's mission has never been more urgent, and it's a sense of urgency that each of us at CISA feels every day to ensure that we are making the best use of the resources and authorities that Congress has generously provided to us over the past several years in demonstrating a clear return on investment to both you and to the American people.

As you're well aware, the past 2 years have been pretty intense, from the Solar Wind supply chain compromise to the ransomware attack on Colonial Pipeline, from vulnerabilities exploited in Microsoft Exchange servers to vulnerabilities mitigated in Log4j software, from our Shields Up campaign to safeguard critical infrastructure from Russian malicious cyber activity, to efforts across the Nation to help State and local election officials secure election infrastructure during the 2022 midterms.

CISA, along with our partners, has been front and center in each. We've aggressively leveraged all of the authorities that we've been granted to enhance our operational visibility into Federal civilian networks through persistent hunting to conduct planning and operations with our industry partners, including our operational technology and industrial control system partners through

the Joint Cyber Defense Collaborative; to identify vulnerable systems through our admin subpoena process and notify our partners to prevent them from being exploited; to serve as both a sector risk management agency for eight sectors and one subsector; and, more broadly, as the national coordinator for critical infrastructure security and resilience, working with our sister SRMAs to reduce cross-sector risk.

Even as we've maintained the highest operational tempo in an increasingly complex and demanding threat environment, we've been growing and maturing as a new agency, co-creating a culture of collaboration to enable us to attract and retain the best talent in the Nation and, indeed, growing that talented work force by nearly 1,000 new teammates in the last couple of years; meticulously executing our rapidly-expanding budget to ensure we remain responsible stewards of taxpayer dollars.

Last September, we published our first-ever strategic plan, which outlines our ambitious goals through 2025 across four key pillars: Cyber defense, risk reduction and resilience, operational collaboration, and agency unification.

I greatly appreciate this committee's steadfast work to help CISA achieve these goals. I also appreciate that the tenets outlined in the CISA 2025 plan, from optimizing the organization, growing an expert cyber work force, enhancing operational visibility, advancing our capabilities, harnessing partnerships, and measuring outcomes to determine progress are all well-aligned. So our efforts together can advance a shared vision for cybersecurity in America.

We're aggressively executing this plan, working with our trusted partners, to enable a collective defense of our critical infrastructure, to include working with those target-rich, cyber-poor entities like small businesses and school districts and water facilities and hospitals and local election offices, to ensure that they have the resources and tools they need to improve their cybersecurity and build resilience.

Needless to say, there is much, much more to be done to protect and defend our Nation's critical infrastructure, from driving adoption of secure-by-design principles in our technology products, to championing corporate cyber responsibility in every board room, to implementing a groundbreaking cyber incident reporting regime, and much more to be done to mature our great team and optimize our value to our partners, with perhaps no partner more fundamental to our success than you all.

We would not be here today without tremendous bipartisan Congressional support, especially from this committee and this subcommittee. We are very grateful for your commitment to ensuring that CISA is armed with the talent, the resources, and the authorities necessary to meet our mission of reducing risk to the critical infrastructure Americans rely on every day. This is truly a no-fail mission. Thanks to your support, we are thriving.

While we're proud of what we've accomplished to date, we recognize the criticality of continued support in terms of authorities and budget to ensure that we sustain this progress. We must and we will continue pushing hard, under your oversight and with your support, to strengthen this agency and, by extension, the security and resilience of our Nation.

Thank you for the opportunity to appear before you today. I look forward to your questions.

[The prepared statement of Ms. Easterly follows:]

PREPARED STATEMENT OF JEN EASTERLY

APRIL 27, 2023

Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you for the opportunity to testify regarding the priorities of the Cybersecurity and Infrastructure Security Agency (CISA) in the coming year.

In today's interconnected society, our Nation faces a wide array of serious risks from many threats, all with the potential for significant consequences that can impact our critical national functions. These functions are built as "systems of systems" with complex designs, numerous interdependencies, and inherent risks. While this structure allows for significant gains in efficiency and productivity, it also allows opportunities for nation-state actors and criminals, foreign and domestic, to undermine our national security, economic prosperity, and public health and safety, creating cascading effects across our Nation.

As the Nation's cyber defense agency, CISA is charged with leading the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Securing our Nation's critical infrastructure is a shared responsibility requiring not just a whole-of-Government, but a whole-of-Nation approach. CISA is only able to accomplish our mission by building collaborative, trusted partnerships across all levels and branches of government, the private sector, academia, and the international community. CISA's Joint Cyber Defense Collaborative (JCDC), for the first time, enables the Government, the private sector, and U.S. international partners to come together to develop joint cyber defense plans and enable real-time information sharing.

As part of this mission, CISA plays two key operational roles. First, we are the operational lead for Federal cybersecurity, charged with protecting and defending Federal Civilian Executive branch (FCEB) networks (e.g., the ".gov"), in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and agency chief information officers and chief information security officers. Second, we serve as the coordinator of a national effort for critical infrastructure security and resilience, working with partners across Government and industry to protect and defend the Nation's critical infrastructure. In both roles, CISA leads incident response to significant cyber incidents in partnership with the Federal Bureau of Investigation (FBI) and the intelligence community.

I am truly honored to appear before this committee today to discuss CISA's critical mission and our exceptional workforce that works tirelessly every day to fulfill it. Since being sworn in as director, I continue to be impressed with the talent, creativity, and enthusiasm of the dedicated CISA employees I am entrusted to lead. I have the best job in Government.

CISA 2023 AND 2024 PRIORITIES

Looking forward into the coming year, CISA will remain focused on strengthening our Nation's cyber and physical defenses. We will work closely with our partners across every level of government, in the private sector, and with local communities to protect our country's networks and critical infrastructure from malicious activity and will continue to share timely and actionable information, intelligence, and guidance with our partners and the public to ensure they have the tools they need to keep our communities safe and secure and increase nationwide cybersecurity preparedness.

Overall, we continue to make critical investments in our mission-enabling activities and functions that will mature the agency and better support the execution of our operational capabilities. CISA's Mission Support program provides enterprise leadership, management, and business administrative services that sustain day-to-day management operations for the agency. This is essential to ensure we can hire a diverse and talented workforce and execute our missions with the technology and speed that keep us ahead of our adversaries.

CISA is also focused on the work we must do to implement the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CISA must ensure that it has the staffing, processes, and technology capabilities in place to successfully implement and utilize information provided through CIRCIA. We must engage in additional outreach efforts regarding the notice of public rulemaking and the planning efforts required to educate covered entities and CISA stakeholders on the cyber inci-

dent reporting requirements, reporting protocols, and reporting methods, as well as voluntary reporting options. In addition to the rulemaking process, CISA must ensure we can receive, manage, analyze, secure, and report on incidents reported under CIRCIA, maturing our current ability to receive and analyze incident reports, manage incidents, coordinate with and notify the interagency, and implement incident data protection functions required by CIRCIA.

CYBERSECURITY

The Cybersecurity Division (CSD) spearheads the national effort to ensure the defense and resilience of cyber space. CSD will continue to build the national capacity to detect, defend against, and recover from cyber attacks. CSD will continue working with Federal partners to bolster their cybersecurity and incident response postures and safeguard FCEB networks that support our Nation's essential operations. CSD will also continue our critical work partnering with the private sector and State, local, territorial, and Tribal (SLTT) governments to detect and mitigate cyber threats and vulnerabilities before they become incidents.

New efforts at CSD will include initiating the Joint Collaborative Environment (JCE), which will enable CSD to develop an internal analytic environment that provides more efficient analysis of mission-relevant classified and unclassified data through automation and correlation to identify previously-unidentified cybersecurity risks. The JCE enables CSD to fulfill its mission and better integrate cyber threat and vulnerability data that CISA receives from our Federal, SLTT, and private-sector stakeholders, and rapidly work with those stakeholders to reduce associated risk. To effectively execute our role as the operational lead for Federal civilian cybersecurity, CSD must maintain and advance our ability to actively detect threats targeting Federal agencies and gain granular visibility into the security state of Federal infrastructure. To effectuate these goals, CSD continues to mature the National Cybersecurity Protection System (NCPS) and Cyber Analytics Data System (CADS).

In the coming year, portions of the NCPS will transition to the new CADS program with intrusion detection and intrusion prevention capabilities remaining under the legacy program. CADS will provide a robust and scalable analytic environment capable of integrating mission visibility data sets, visualization tools, and advanced analytic capabilities to cyber operators. CADS tools and capabilities will facilitate the ingestion and integration of data as well as orchestrate and automate analysis that supports the rapid identification, detection, mitigation, and prevention of malicious cyber activity.

Together with the Continuous Diagnostics and Mitigation (CDM) program, these programs provide the technological foundation to secure and defend FCEB departments and agencies against advanced cyber threats. CDM enhances the overall security posture of FCEB networks by providing FCEB agencies and CISA's operators with the capability to identify, prioritize, and address cybersecurity threats and vulnerabilities, including through the deployment of Endpoint Detection and Response (EDR), cloud security capabilities, and network security controls.

CSD will continue to advance the CyberSentry program, which is a voluntary partnership with private-sector critical infrastructure operators designed to detect malicious activity on the Nation's highest-risk critical infrastructure networks. CyberSentry provides best-in-class commercial technologies that allow both CSD analysts and each partner organization to rapidly detect threats that attempt to move from an organization's business network to impact industrial control systems. While CyberSentry is intended only for the most at-risk or targeted critical infrastructure entities, CSD intends to deploy capabilities to additional critical infrastructure partners to meet significant demand for the program based upon operational successes achieved to date.

INTEGRATED OPERATIONS

The Integrated Operations Division (IOD) coordinates CISA operations at the regional level and delivers CISA capabilities and services to support stakeholders in preparing for, mitigating, responding to, and recovering from incidents that impact critical infrastructure. Additionally, IOD monitors and disseminates cyber and physical risk and threat information; provides intelligence context to support decision making; and performs agency-designated Emergency Support Functions. IOD will continue to enable seamless and timely support to CISA stakeholders across the Nation, meeting our partners where they are in communities in every State.

INFRASTRUCTURE SECURITY

CISA's Infrastructure Security Division (ISD) leads and coordinates national programs and policies on critical infrastructure security, including conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance. ISD's mission focuses on efforts such as reducing the risk of targeted violence directed at our Nation's schools, communities, houses of worship, and other public gathering locations. In addition, ISD leads programmatic efforts to secure our Nation's chemical infrastructure through implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) regulation, authority for which is expiring on July 27, 2023.

EMERGENCY COMMUNICATIONS

CISA's Emergency Communications Division (ECD) enhances public safety communications at all levels of government across the country through training, coordination, tools, and guidance. ECD leads the development of the National Emergency Communications Plan (NECP) and 56 State-wide Communications Interoperability Plans to maximize the use of all communications capabilities—voice, video, and data—available to emergency responders and to ensure the security of data exchange. ECD also assists local emergency responders to communicate over commercial networks during natural disasters, acts of terrorism, and other significant disruptive events. The Emergency Communications program supports Nation-wide sharing of best practices and lessons learned through facilitation of SAFECOM and Emergency Communications Preparedness Center governance bodies.

STAKEHOLDER ENGAGEMENT

The Stakeholder Engagement Division's (SED) activities focus on fostering collaboration, coordination, and a culture of shared responsibility for national critical infrastructure risk management with Federal, SLTT, and private-sector partners in the United States, as well as international partners. SED also executes CISA's roles and functions as the Sector Risk Management Agency (SRMA) for 8 of the Nation's 16 critical infrastructure sectors and will lead coordination with SRMAs, the broader national voluntary critical infrastructure partnership community, and across all sectors to ensure the timely exchange of information and best practices. In partnership with the Federal Emergency Management Agency (FEMA), SED will continue implementing the State and Local Cybersecurity Grant Program, to include providing subject-matter expertise and leading program evaluation efforts to ensure State and local entities can access grant resources to enhance cybersecurity resiliency and reduce cybersecurity risk.

NATIONAL RISK MANAGEMENT CENTER

The National Risk Management Center (NRMC) develops analytic insights to identify and advance risk mitigation opportunities that improve national security and resiliency across critical infrastructure sectors. These analytic products support investment and operational decision making throughout the public and private sectors. The NRMC will continue two critical efforts related to SRMAs and National Critical Function (NCF) Analytics in the coming year.

First, the NRMC will continue to expand risk analysis and risk management across high-priority critical infrastructure sectors. This risk analysis provides insight into cross-sectoral risk and significant sector-specific risks to support all of CISA in routinely identifying and prioritizing focused risk-management opportunities to create tangible risk reduction outcomes. Second, the NRMC will continue our NCF efforts to enhance analytic capabilities, including methodology and framework development to identify and characterize critical infrastructure interdependencies within and across NCFs. This includes applied analysis to meet specific analytic requirements in the infrastructure community to enable CISA to understand consequences that extend beyond a single sector.

CONCLUSION

I am honored to represent my dedicated teammates at CISA who work indefatigably in support of our mission to understand, manage, and reduce risk to our cyber and physical infrastructure. The risks we face are complex, geographically-dispersed, and affect a diverse array of our stakeholders, including Federal civilian government agencies, private-sector companies, SLTT governments, and ultimately the American people. However, CISA stands ready to carry out these critical mission imperatives.

Before I close, I would like to take a moment to recognize the Homeland Security Committee's and this subcommittee's strong support for CISA. For myself, and on behalf of our CISA workforce, thank you for your support. As one team unified behind our shared mission, we will continue to operate in an efficient and cost-effective manner. There is much work to be done and I look forward to working with you during the 118th Congress to continue strengthening this agency, and by extension, the security and resilience of our Nation's networks and critical infrastructure.

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

Mr. GARBARINO. Thank you, Director Easterly.

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

I'm not going to call myself first because my Vice Chair has another hearing she has to go to and I know she's got some very interesting questions, so I would like to yield.

I recognize Ms. Lee from Florida for 5 minutes.

Ms. LEE. Thank you, Mr. Chairman. Thank you, Director Easterly, for being here today.

In my former role as Florida's secretary of state, I had the opportunity, of course, to work with you; your predecessor, Director Krebs; your team over at CISA, in working to secure election infrastructure. So I'd like to begin there with a couple of questions about that sector and the work of CISA in the elections arena.

Starting out, would you please describe for the committee what CISA does in collaboration with State and local election officials as it relates to cyber-specific risk assessments, and then also, where appropriate, the deployment of hunt and incident response teams to State and local elections offices? Would you please describe those services, when they are utilized, and whether you see the need for them increasing or decreasing?

Ms. EASTERLY. Yes. Thanks so much. Thank you for your partnership and your leadership on this issue in particular.

So as you know, we've been in this role now since 2017, and we have been learning constantly about the demands of election security—election infrastructure security. Really, I would say refining our relationships with State and local officials to ensure that we are meeting their demands. As I think you know, from 2017 to 2020, our focus was very much on those cyber services, from vulnerability scanning to remote vulnerability assessments, to penetration testing, to helping with incident response. I think actually we are in a much better place in terms of cyber hygiene and cybersecurity with our election infrastructure.

One thing that we found, however, going through 2022 was that the threats were very different now. Not only was there cyber, but there was also physical security issues, there were insider issues, and there were issues of concern around foreign influence and disinformation. So while we continue to provide those cybersecurity services, we are actually expanding our full range of services based on the demands that we're getting from State and local officials.

So one of the things that we did earlier this year was set up a full road map along five lines of effort, and we provided it to our State and local election officials. A full range of those cybersecurity services that you mentioned, Congresswoman, but also physical security, insider security. Then we're really pushing hard to get be-

yond the State and the State election directors, so we can get down to communities and counties and parishes and towns, because we see those are the entities that are truly rich as a target but cyber poor.

So the other thing we did is we put together a place mat of services so that there was no mystery in terms of what we offer. We made that available to all of our constituents using our field forces that we've grown almost double over the past several years.

Ms. LEE. On that subject, I know one of the challenges that faces CISA and many other partners across sectors as it relates to technology and cyber is recruitment and retention of appropriate talented, trained people. I know CISA launched the Cyber Talent Management System back in 2021, with the effort, the intention to be to recruit and retain the appropriate professionals you need for your work force.

How has CTMS been working? You mentioned the expansion of your team. Have you been able to effectively and efficiently recruit? How does your fiscal year 2024 request support the use of that operation and recruitment?

Ms. EASTERLY. Yes. Thank you for asking the question. That was, as you probably know, about 7 years in the making. So actually implementing it has been something that's been a real project that we've continuously had to look at how it's working and ensure it truly streamlines our ability to bring on more talent.

I think we're at about 80 people with the Cyber Talent Management System and some really extraordinary talent. At this point in time, we continue to use our Title V authorities, our normal authorities to bring on talent. We are hoping to use CTMS more aggressively this year. But I will tell you, I think the recruiting that we've done to date is a real success story: 516 people last year, we're on pace to exceed that, our retention level is between 7 and 8 percent. It's not just quantity. We are bringing in some of the best talent across the country.

While our work force has grown every year, the request that we put into the budget only adds very small increment, I think maybe 10 people. So what we're doing now is trying to get down to about 90 percent total, and then, of course, we'll focus on retention. But to be frank, I am OK if somebody comes to work at CISA for 3 to 5 years and then goes off to a hospital or a power company or a bank to help them with their critical infrastructure security, because at the end of the day, this is really about collective cyber defense, and we need to work together hand-in-hand.

Ms. LEE. Mr. Chairman, my time has expired. I yield back.

Mr. GARBARINO. The gentlelady yields back.

I now recognize the gentleman from Louisiana, Mr. Carter, for 5 minutes.

Mr. CARTER. Mr. Chairman, thank you very much.

Director Easterly, thank you very much for being here. Thank you for the incredible work that you do.

In my home State of Louisiana and around the Nation, far too many higher education institutions are experiencing data breaches. What steps is CISA taking to protect the privacy and integrity of our institutions and combat critical infrastructure cybersecurity issues?

Ms. EASTERLY. It's a real—it's a real scourge across the country. One of the focus areas that we did, actually, based on being asked by the Congress to take a look at the K-12 Cybersecurity Act, was we spent a lot of time putting together a guide for K-12 schools and school districts across the country. We worked with a lot of experts to ensure that it was a guide that schools which were part of those target-rich, resource-poor entities could actually take advantage of. So we created this guide, very simple steps about things that can be done to prevent data breaches and ransomware attacks. We've seen a lot of that.

Then what we're doing is working with our field forces to actually do outreach across the country to schools and school districts to ensure that they understand the resources, the free resources that we provide, and they can take advantage of them so they can drive down risk. So we've aggressively started that outreach at the beginning of fiscal year 2023, so that at the end of the day, we can measure success by seeing whether we were able to drive down some of these events that unfortunately—

Mr. CARTER. How does that success measure?

Ms. EASTERLY. So what we want to do—

Mr. CARTER. Are you seeing success marginally?

Ms. EASTERLY. So we see success based on the feedback we're getting. The problem is, is we don't know the universe of these threats at this point in time. This is why the CIRCIA, the Cyber Incident Reporting for Critical Infrastructure Act, is so fundamentally important, because we'll finally get an idea of the universe of ransomware incidents. For right now, it is a lot of the feedback that we get directly saying, because you came and spent time with us, we implemented these things and it's helped us improve our cybersecurity.

Mr. CARTER. Tell me about HBCUs. We know that HBCUs have come under attack. I'm an alumnus of Xavier University. Xavier University was hit with a substantial cyber attack that crippled the university and its system for some time. I know that Howard University and many others, likewise, in almost sequence, at one point there were like eight HBCUs, I think, that were hit in succession.

Can you share with us any plans or actions that you've taken since that to protect or encourage or enhance the ability to make those institutions safe going forward, or safer?

Ms. EASTERLY. Yes. Thanks for asking the question. So we've actually done a lot of work with HBCUs. Unfortunately, much of that work is about the bomb threats that they have received, to ensure that their physical security and that they were prepared for that. At the same time, however, we have been working as part of our outreach to target-rich, resource-poor entities to help them understand those steps that they can take to increase their baseline.

I don't have the information specifically on our outreach with respect to cyber for HBCUs, Congressman, but I'm happy to get back to you on that.

Mr. CARTER. OK.

Ms. EASTERLY. The one point I would make is, a recent program that we just implemented had some real stunning near-term success, and some of it is with institutions of higher learning, and that's the Pre-Ransomware Notification Initiative. We'll get tips

from security researchers and from industry about ransomware getting put down on a system. Before it actually gets activated, we can actually notify that entity and they can do something about it before they have a really bad day. Many of the targets that we've been notifying are K-12 and institutions of higher education. So I'm happy to get you more details.

Mr. CARTER. With the minute, 36 seconds left, I want to ask you quickly about drones. We know that we see the increased use of drones. We visited the Southern Border this past weekend. We know that drone traffic is incredible and a real impediment to protecting the Southern Border. We also know that critical infrastructure, pipelines, utility companies, are crime scenes, and drug trade. Because my understanding is now that the drones are bigger, they're fuel-operated, so they can go longer, faster, and they have the capacity to carry up to 50, 60 pounds, which makes them very, very dangerous.

Can you share with us what you can about what you guys are doing relative to critical infrastructure in the drone usage?

Ms. EASTERLY. It's a real concern of ours as well. We have a section that's part of our infrastructure security that focuses on physical security that is taking a hard look at this issue. We've done a few assessments to date, and we're looking to update them, working with our partners. But I've spent time, in particular up in New York, where there's a real concern from our folks on the ground of nefarious use of some of these capabilities.

So I'd be happy to follow up with you and get more information on the kind of things we're doing and get your feedback on what might be more helpful to your constituents.

Mr. CARTER. If there's anything that you can share that we can share with them in the way of grants, in the way of resources, in the way of things that they could be doing to better protect or arm you with facts that are going on, whether it's at the university level, at the plants or crime scenes or other critical infrastructures, that there may be resources that they may not be available or aware of that we could make available to them would be very—

Ms. EASTERLY. Yes. I'd love to follow up on that conversation in particular.

Mr. CARTER. Thank you very much. Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize myself for 5 minutes of questioning.

Director Easterly, I'd like to start my questions today by asking you about a fundamental issue: Our cyber work force challenge. CISA is obviously not the only place where the work force gap is an issue, and there are many agencies in the Federal Government and companies across the private sector that are working to improve the national cyber work force. You know, we've talked about, and you just said in your answers to Ms. Lee, how you have been able to make some hires recently. That's very exciting news.

But I want to know, what do you see as CISA's role in developing the national cyber work force both public and private?

Ms. EASTERLY. Yes. Thanks for the question, Chairman. So I look at this as, first of all, we've got to make sure CISA has what we need. Then there's, of course, the Federal work force, I think probably some 35,000, focus there. In the country itself 700,000. Cyber

is a borderless space, if you look at the big number around the world with our allies, 3.5 million.

So I'd say a couple of things. First of all, with respect to the country, I do—just because we serve as America's cyber defense agency, I do think we play an important role in helping to build that pipeline, because at the end of the day, I want to make sure CISA is successful in the next 25, 50, 100-plus years. That, frankly, has to start from the youngest of ages.

So one of the things that we've done based on a grant that we received, the Cyber Education Training and Assistance Program, we've given that grant to the Cyber Innovation Center, and they make curriculum available to K-12. So that if you are giving this curriculum to help some of our more younger members understand that, hey, this cyber thing is not that scary, it is really interesting, I want to be a part of it, that can actually start that pipeline. So I think that's one really important aspect of it.

We also do training, retraining for the Federal work force, for those who might want to get into cyber. Then we give grants to organizations, like the NPower and the Cyber Warrior Foundation, and those are underserved communities. So we're looking using a myriad of tools. We're also working, of course, across the Federal Government with NIST, with the Office of the National Cyber Director that's working on the more fulsome cyber work force strategy.

Mr. GARBARINO. I appreciate that and all the hard work that CISA's doing. It's definitely—as you said, it's borderless. I called it the third border the other day, but I got yelled at by my staff for saying that, so I think I'm not allowed to say it anymore.

So I do actually want to focus on something that was brought up by one of our witnesses from—she was from the Bank Policy Institute. She testified that, Financial Services Sector, the cyber work force is spending 30 to 40 percent of their time on regulatory compliance. The SEC—and I just met with a major bank CISA last week who said by the end of this year when some other regulations come out it is probably going to be closer to 50 percent.

The SEC proposed a rule that seems to conflict with the requirements and the Congressionally-mandated Cyber Incident Reporting for Critical Infrastructure Act. So I'm wondering—we had Chairman Gensler in front of the Financial Services Committee last—2 weeks ago. What steps did you and Chairman Gensler take to harmonize the proposed SEC rule at the Cyber Incident Reporting for Critical Infrastructure Act rule making?

Ms. EASTERLY. Yes. Thank you for the question. Having spent 4.5 years at Morgan Stanley, and I know Heather and very sympathetic to those views, we don't want to create burden or chaos. What we want to do is ensure that we get the information in a streamlined way.

So, of course, we've had discussions across the Government. As you know, Chairman, one of the things in CIRCIA was, of course, the Cyber Incident Reporting Council, which is working to figure out how to best harmonize among the various asks that we have from the private sector.

I think the good news is, in the legislation that you all gave us, it very specifically accounts for any crossover. So very specifically,

legislation says that if there's a requirement to report to another agency and they have a reporting time line that's similar to ours, if they have substantially similar information, then you can sign a memorandum of agreement so you don't have to report twice. We are working to ensure that that is a streamline process. I think that is really important, again, from a harmonization perspective.

Mr. GARBARINO. I appreciate that. I know the Council's supposed to be giving us a report and we are waiting for that.

I did want to follow up. Have you spoken to Chairman Gensler? From his testimony, it made it sound like you two speak quite often.

Ms. EASTERLY. We absolutely have spoken. I think we are both trying to accomplish the goal of ensuring that we get the information that we need. His role is different than mine, of course. The reason why we need the information is so we can render assistance, and also we can use that to help protect the wider ecosystem. So I'm sure we'll end up in a—I hope we'll end up in a good place.

Mr. GARBARINO. I hope so too. I'll just say, 50 percent of your time on having somebody spend 50 percent of their time on compliance, you know, that means 50 percent of the time they're not on defense—

Ms. EASTERLY. One hundred percent.

Mr. GARBARINO. So I appreciate that. I yield back.

I recognize the gentlelady and former Chairwoman of this committee, Ms. Clarke from New York.

Ms. CLARKE. Good afternoon. Let me begin by first thanking our Chairman Garbarino and Ranking Member Swalwell for permitting me to waive on to the subcommittee for holding this very important hearing on the state of our Nation's cybersecurity posture and CISA's role and perspective. Thank you, gentlemen.

Let me also thank Director Easterly for your leadership and service and for joining us today.

When I chaired this subcommittee last Congress, I often remarked that there is a disconnect, an imbalance, if you will, between the scope of CISA's mission versus its authorities. Congress expects CISA to carry out one of the broadest, most ambitious missions in the Federal cyber space. But its authorities pale in comparison to many of its components and counterparts.

At least until recently, in the 117th Congress, we worked across the aisle to pass legislation to empower CISA within the inter-agency, grow its visibility into cyber threats, and make sure CISA can require, not just request, that companies report cyber incidents to CISA for the benefit of the broader ecosystem. So I for one am ready to start seeing these results.

So, Director Easterly, my first question is about CIRCIA. First, is CISA on track to meet the rulemaking deadline and statute? What would it take for CISA to move faster?

Ms. EASTERLY. Thank you very much. Great to see you again, Congresswoman.

I think few people in this country want me to move faster than me. You know, and we did want an accelerated process, but we were told to go through the full rulemaking process, and we are.

You know, you point out an authorities perspective. We don't do law enforcement, we don't do intel, we are not a military agency.

We're a voluntary agency at the end of the day. So we felt that the consultative process was really important, particularly given some of the concerns that the Chairman articulated, so we did 27 listening sessions, 17 of those were virtual. We did a request for information. We received 130 comments.

We used all of that to help create the rule, which actually now exists in draft, and we are going to have to go through the process. But that rule should go out, the notice of proposed rulemaking should go out on time in March 2024. Then the final rule is on schedule 18 months later, September 2025.

Please trust me, I'm trying to do everything I can to accelerate that process, but we want to get it right because it is so important and so groundbreaking.

Ms. CLARKE. Yikes. My next question is, what is CISA doing in the mechanism to make sure that it can hit the ground running when these rules go into effect?

Ms. EASTERLY. So it's a really important question, and some of this was reflected in our budget, because this is not a trivial task. We need to make sure that we have the people and the technical infrastructure in place to be able to take these huge amounts of reports that we're going to get, to ingest them, to triage them, to analyze them, to respond to them, and then to use them in an anonymized way to enable us to actually get that information out to protect the larger sector. So that is a huge amount of work, not only just the administrative aspects of the rule making, but actually all of the technical infrastructure in place across the agency. So we are in the process of leveraging the funds that we've received and will hopefully receive to be able to create that.

Ms. CLARKE. So I want to thank you, because in responding to Chairman Garbarino, you spoke about the regulatory harmonization. That's a really key component. That's the only way we are going to keep our private-sector partners engaged and on-board and really feeling as though they're being heard.

Ms. EASTERLY. Yes, ma'am.

Ms. CLARKE. My next question to you is whether CISA has an approach for Federal regulators, like the SEC or FCC, about entering into MOUs to share incident reports.

Ms. EASTERLY. Yes, 100 percent, and that's what I mentioned. But I think this is a really good part of the legislation. I mean, specifically it exempts the statute-exempt companies from reporting to CISA if three conditions are met: If it's similar information, similar time frame, and if the other agency agrees to put an MOU in place. So we are very happy to do that. We just need to negotiate each of those MOUs, and our intent is to do that between the notice of public rulemaking and the final rule.

Ms. CLARKE. Very well. Well, before I close, I just want to reiterate how important it is that CISA continue to engage with stakeholders and hear outside perspectives about how to make the rules as smart, effective, and tailored as possible to the goals of CIRCIA. So thank you very much.

Mr. Chairman, I yield back.

Ms. EASTERLY. Thank you, ma'am.

Mr. GARBARINO. The gentlelady yields back. Thank you for coming. We love having you back here.

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

Mr. EZELL. Thank you, Mr. Chairman. Good seeing you this morning—this afternoon, Ms. Clarke and other Members.

Director Easterly, thank you for being here to participate today in this very important hearing. I'd like to talk about CISA's partnership with the FBI, especially considering the Joint Ransomware Task Force recent work to take down these bad actors.

I understand that JCDC is working to update the National Cyber Incident Response Plan, which will also address this partnership. This updated plan, how do you think CISA and the FBI will work together to address incident responses?

Ms. EASTERLY. Thank you for the question. I have to say that, you know, in my almost 30 years in Government, I have never seen such a great partnership. I say that really sincerely. Some of that was owing to personalities, but I think it is very much a result of the mission, it's a function of the mission.

So we partner very closely with FBI. In fact, the legislation, the Joint Ransomware Task Force was actually—said CISA will lead. We made the decision, we said that doesn't really make a lot of sense. We need to make sure that FBI is with us, linked arms, and so we made them a co-lead, because it's really important. As you know, we have the asset response—responsibilities and FBI has the threat response. So we work together very symbiotically in everything we do to ensure that, when there's an incident, we can be there to help respond and FBI can be there to render assistance but to also investigate.

So I'm incredibly pleased at the quality of that relationship, both at the Federal level, sir, but also with local law enforcement. That's something that our field forces on the ground have developed really close working relationships over the past couple years.

Mr. EZELL. Thank you for that. That is just so important working with, not only the FBI but with our local law enforcement, which is my background.

So CISA is requesting \$98 million for requirements with a cyber incident reporting for critical infrastructure. Can you talk just a little bit about how the agency plans to spend this money?

Ms. EASTERLY. Yes, absolutely. Thank you for that. So as I was saying, this is one of the most important groundbreaking things that I think the Congress has done for cybersecurity, because for the first time, we will understand much more about the universe of incidents and attacks; and we really don't. Anybody that says it's going up, it's going down, is completely anecdotal. So for the first time, we'll have a better picture of that.

But it is not a trivial endeavor to set up the infrastructure to enable us to ingest those reports, to triage them, to analyze them, to enable a response, and then to use them in an anonymized way that protects the victim but be able to provide that as warning to the rest of the sector in the ecosystem to help them drive down risks.

So that \$98 million is both people, but it's also technical infrastructure that will enable us to do all of those things, from case management to stakeholder relationship management to a threat intel platform to an analysis capability. That's what we are putting

in place now, sir, and hope that we get the additional funding to allow us to do this the right way. It's important for the Nation.

Mr. EZELL. Thank you. Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize Mr. Menendez from New Jersey for 5 minutes of questioning.

Mr. MENENDEZ. Thank you, Mr. Chairman and Mr. Ranking Member. Thank you for bringing us together here, second time in this room in less than a couple of hours. So it's just good to see you all in such a good mood.

Director Easterly, thank you for joining us today. You know, I'm really thankful to be on this subcommittee. I think about cybersecurity as often as I can. I'm also on the Transportation and Infrastructure Committee here, and serve for the Eighth Congressional District in New Jersey, which is home to what security experts call the most dangerous 2 miles in the country, and that was really because of the physical assets and from a physical security perspective. But increasingly, I think about all of the challenges from a cybersecurity one. So I'm fortunate to have you here today and thankful for the work that you do.

I guess starting off, you know, I think about it a lot but you deal in it every day. Probably the most significant position that we have in our country.

How do you feel about America's preparedness from a cybersecurity perspective addressing, guarding against cyber attacks today in 2023, on a scale of 1 to 10, let's say?

Ms. EASTERLY. I think we have made vast strides, even just over the last couple of years. I think there is much work to be done, to be very frank. In particular, my big concern is nation-state adversaries, in particular China.

Mr. MENENDEZ. Yep.

Ms. EASTERLY. If you read the—which I'm sure you did—the intelligence community annual assessment that specifically talks about actions that China may take to disrupt our critical infrastructure in the event of a conflict, I am motivated every day on the urgency of ensuring that the country is as prepared as possible to withstand but really to be resilient too. At the end of the day, I think our ability to prevent is very, very difficult. We have to be able to mitigate and to recover and to have the resilience to get our Nation back up and running if there is a major attack.

Mr. MENENDEZ. I appreciate that. When you engage with different stakeholders from industry, you know, government actors, what is their perception of the risk that cybersecurity or cyber threat poses to all of us, either from municipalities who may see their tax department hacked, to infrastructure or operators of various infrastructure systems, transportation systems? Where do you see across the board in a blended sort-of average on a scale of 1 to 10?

I'll let you off, because I'm thankful to have you here, and I won't make you share with us a specific number. But, you know, I'm just trying to gauge what the perception is out there of this threat and how serious people are taking it, because we need to take it. This is, in my opinion, one of the most critical threats to the well-being of our Nation.

Ms. EASTERLY. Yes. I agree with you, and I think it's improving. It's improving because of Colonial Pipeline.

Mr. MENENDEZ. Yep.

Ms. EASTERLY. It's improving because of the scourge of ransomware. You know, ransomware has become, sadly, a kitchen-table issue and, therefore, we are making cybersecurity and cyber hygiene a kitchen-table issue. It's not where it needs to be, but it's much better because of those things. So we are working now with our field force day in/day out with businesses large and small with some of these entities that weren't really thinking about their cybersecurity, and telling them, these are the basics that you need to do. Because it's not—when you're doing the basics, you can actually deal with the vast majority of the kind of threats that you would get from a cyber criminal organization.

Mr. MENENDEZ. You know, definitely let us now how we can help amplify that message, right? You know, when we do small business tours, right, we are generally talking about, you know, tax credits to small businesses, right. But, like, we should be talking about cybersecurity as well when we're visiting, you know, all these different institutions, small- and medium-sized businesses, companies in our districts.

But you're sort-of alluding to the challenge that I'm sure gives you a lot of concern, that gives me a lot of concern, is that we're admittedly not where we need to be. The way I see this threat, especially when you talk about nation-state adversaries, right, because it's not just China; it's Russia, it's Iran. They are serious about having this ability to target our various on-line components, especially our infrastructure, which concerns me.

But the thing that keeps me up sometimes at night, because a lot of things on this job keep me up at night, not my friends here, this cybersecurity subcommittee is great. But the reality is that the speed of a threat and the way in which it can develop is exceedingly fast. As we do in this country, we're thoughtful, but that means that we're not as quick as our adversaries may be.

What can we do here to enable you, to enable your partners and various stakeholders to not just be constantly playing catch-up, which is going to be harder and harder to do the more compounding that this challenge becomes, but what can we do to potentially get ahead in the not too distant future?

Ms. EASTERLY. Yes. Thank you for asking the question. It's a really, really important one.

First, in terms of how you can help, to help amplify our message, I think, Chairman, you've done that before in terms of, you know, I'm a big fan of multifactor authentication. So I think, Congresswoman, you have as well. So I would welcome all of you to help us get that message out. That's one thing.

The other thing is, we have done cybersecurity roundtables in some of your districts, and we would love to do more. So if that's something we can do to sit down with your constituents, please let us know. We've got field forces.

Now, to your larger question, I think it's exactly the right one, at the end of the day what we are doing as a status quo can help make us more resilient, but I do not think it's sufficient or sustain-

able. I think we need to take a different approach, and this is one of the things we've been doing a lot of work on.

First and foremost, we need to ensure that the technology that underpins the critical services and functions that Americans rely on every day is built secure, secure by design with a limited number of vulnerabilities, and secure by default with things like multi-factor authentication, built in from the start. We have, because of misaligned incentives, basically allowed innovation—and we love innovation—but innovation should not trump safety and security in a world where we all rely on tech. So that's a really important message, and I'd love to talk more about it at a separate time.

The second thing is we need to make sure that every leader, every CEO, every board room is embracing corporate cyber responsibility as a matter of good governance. Incredibly important that that not get delegated to the IT people at a CISO, but that CEOs see it as their responsibility.

Then, finally, we need to continue pushing hard on persistent operational collaboration, the kind of things that we're building with the Joint Cyber Defense Collaborative. That's about a default to share on malicious activity, knowing that a threat to one is a threat to all. It's about a coequal partnership between Government and industry, with reciprocal expectation of value-add and transparency where the private sector doesn't have to worry about punitive sanction because they share information. Then getting rid of the friction. It has to be a frictionless experience. We have to have shared analytics, shared platforms. That's what we are building with our joint collaborative environment and our cyber analytic data services.

So those three things are different in kind. I believe it's those kind of things that will really enable us to get ahead of this very difficult threat.

Mr. MENENDEZ. Chair, I appreciate your generosity on time. I yield back.

Mr. GARBARINO. I thought it was a very important question. I really wanted that on the record. So the gentleman yields back.

I now recognize my colleague from Texas, Mr. Luttrell, for 5 minutes of questioning.

Mr. LUTTRELL. It's what's the best part about going last. Everybody asked the questions that I was going to ask.

Thank you, Mr. Menendez, that was mine. I've been prepping that for 2 weeks.

Mr. MENENDEZ. I had been prepping it for 3 weeks.

Mr. LUTTRELL. All right. Always an overachiever.

Mr. MENENDEZ. Don't worry, you're not last.

Mr. LUTTRELL. I mimic my colleague from California, Mr. Swalwell's statement. You are the leading edge. You're the next phase of combative frontier in the protection of our countries, the cyber space. We'll no longer fight wars the way that my colleagues and I did in the military with bombs, planes, and guns. It's you. So thank you for taking and shouldering that weight.

To drive a point home real quick, as far as when Mr. Menendez asked what we can do, I think we just need to stay out your way and give you the autonomy that you need. Understanding that in

the cyber space, when it comes to threat and risk, we are so siloed, and that is an issue.

Are you having success in breaking down those silos when it comes to multidepartment coordination?

Ms. EASTERLY. Yes, it's a great question. I think one of the things that the Joint Cyber Defense Collaborative gave us was the legislation. You know, it's in statute. It's the only cyber entity in statute that says we bring together the Federal cyber ecosystem. So not just CISA, but FBI and NSA and CYBERCOM and other agencies. That's why, you know, it was built to actually break down those silos, and we've been doing that over a short period of time, not just bringing in industry, but bringing in State and local colleagues, bringing in international partners, and then by design, bringing in the Federal Government. That is not an easy thing to do, sir.

Mr. LUTTRELL. I wouldn't think so.

Ms. EASTERLY. But we are trying really hard. I have to say, you know, I joined this—I joined this job from the private sector, and I thought there were a lot of issues with silos and a lack of cohesion. So we know what the problem is and we are working hard to enable us to fix it.

Mr. LUTTRELL. That's great to hear. I'm sure just the sheer scalability is pretty arduous.

But as far as operating across multiple cloud services, you know, with our threat-hunting teams, are we having success in that? Because everyone's different. I mean, the communication between the two are just completely—they are just Army-Navy to each other. That's an analogy. I'm sorry.

Ms. EASTERLY. Be Navy.

Mr. LUTTRELL. I was waiting on that one, right.

To my point, if we do have a threat or an active attack in a certain corporation, a department, whatever, do we have success if it can move across multiple domains, with its ability to track that, but also notify and prevent?

Ms. EASTERLY. Yes. I mean, it's another really, really important question. Let me hit first from the Federal civilian dot-gov, because we've been looking to make a lot of improvements there. So we are now—we have radically improved visibility that we really didn't have in Solar Winds. So because of the authorities that we have to put endpoint detection and response capabilities at departments and agencies, we can do that persistent hunting so we can have that visibility. We also now have something that gives us a dashboard level view to say what's going on at those systems. So that visibility is improving.

On cloud providers in particular, you know, there's something called the shared responsibility model. I'm thinking, you know, as a military guy, you know, if no one's in charge, like, no one's in charge.

Mr. LUTTRELL. Right.

Ms. EASTERLY. If everyone's in charge, no one's in charge. So I have a little bit of concern with the shared responsibility model, particularly if it's putting the burden of responsibility on businesses that just don't have the resources to bear it. So I think at the end of the day, cloud providers need to bear the bulk of the se-

curity burden, and the visibility should come back to the entity that is contracted with those cloud service providers.

So very important that things like logging, for example. Security logs help us understand the nature of a threat and malicious activity. But oftentimes if a cloud service provider is charging you extra for that security feature, then the customer will lack visibility. So there are things that we need to do to work with cloud providers to ensure that the shared responsibility model is not misplacing the burden on those who can't bear it.

Mr. LUTTRELL. OK. I really would like to see that, not that it's not doing this, but translate down into my rural district in Polk County. You know, that's just something that hasn't come to fruition yet. So I'm hoping this system will continue to push the envelope and make sure that the—it's the American public, at the end of the day, that needs protecting, not our—everyone.

Ms. EASTERLY. One hundred percent. Yes.

Mr. LUTTRELL. I thank you so much. I yield back, Mr. Chairman.

Ms. EASTERLY. I'd love to come out to your district and—

Mr. LUTTRELL. Come on.

Ms. EASTERLY [continuing]. Have a discussion.

Mr. LUTTRELL. You bet.

Mr. GARBARINO. The gentleman yields back.

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

Mr. SWALWELL. Thank you, Chairman.

Director, as you've laid out your mission and your accomplishments and your challenges, I see it that one of your greatest challenges is to figure out what are your core competencies and what you can do well to have the greatest impact and then what are the gaps that CISA can fill. Also, what are the most important functions that need to be carried out, even when doing so is controversial or risks picking a fight? So I was hoping you could speak to that.

Ms. EASTERLY. Yes. Thank you for—thank you for asking the question.

You know, when I came into this job, my predecessor is a great friend of mine, did a strategic intent document. That laid out some great priorities for what we do operationally, but, you know, frankly, we needed a road map. So we spent about a year actually developing that strategic plan. If you take a look at that, and I'm sure you've seen it, but it's organized not by our divisions or our mission-enabling offices. It's organized by four key principles: Cyber defense, infrastructure risk and resilience, operational collaboration, and agency unification. Because I'm a firm believer that if everything is a priority, nothing's a priority. So we basically laid out, these are the things that everybody in the agency needs to do, and we laid out representative outcomes, as well as a measurement approach.

Now, based on that, every entity, every division, every mission-enabling office did an annual operating plan that lays out at a more granular level the measures of effectiveness and measures of performance that they are responsible for, and I track them on a quarterly basis. So we are really looking at being much more rigorous in how we allocate our resources and how we allocate our

time to ensure that we are being good stewards of the taxpayer dollars.

Mr. SWALWELL. Thank you, Director. With respect to JCDC, I have a similar question. CISA needs to decide, you know, what are the core capabilities JCDC will focus on where it also can be most effective and put structure and processes in place to formalize those functions. So can you help me understand how you're thinking about some of those questions as it relates to JCDC's scope and mission moving forward?

Ms. EASTERLY. Yes, absolutely. I think I just gave them a copy, you and the Chairman. I'm happy—would love to have a team come in and brief anybody who's interested, because I really think this is one of the most important groundbreaking things that the Congress has given us. So we have the strategy for the JCDC that we just finished up serendipitously in time for this hearing.

So the focus is about two fundamental things. One is about planning and ensuring that we can plan against the most serious threats to the Nation. The second is collaborative fusion to help us understand the threat and then to drive down risk to the Nation.

Now, given the myriad of threats that we face, there are a lot of demands that we have to enable us to be able to respond and be proactively prepared for various threats. So we've operationalized it against a significant vulnerability, Log4j, with the Shields Up campaign with the elections. But we are being very deliberate about what efforts we take on, and that is based on the threat and based on the feedback that we get from our partners.

So if you look at the planning agenda, it's water, it's energy, it's open-source software to reduce risk to industrial control systems. So it's things that our partners asked us to focus on that we, based on the threat and the risk, we decide to focus on. But every one of those efforts has outcomes that are measurable, and then we get feedback from our partners.

Mr. SWALWELL. Earlier this week, DHS released its proposal to authorize the Cyber Safety Review Board, CSRB, a public-private panel established by Executive Order in 2021 to investigate significant cyber incidents, as you alluded to earlier, similar to NTSB.

What would the relationship be between the CSRB and CISA? How would it interact with CISA's new cyber incident reporting authorities, specifically, as you referenced in your opening statement, the subpoena authority? Do you see CSRB as sufficiently separate from CISA to preserve its voluntary partnerships with the private sector?

Ms. EASTERLY. Yes, absolutely. I mean, the CSRB—so I appoint the members and we actually manage the infrastructure and the contract for that, but they have a distance from me, so I'm not part of that decision making, to keep some important, sort-of, cushion there.

With respect to the admin subpoena, you know, the Congress very helpfully gave us admin subpoena separate, which allows us to actually do scanning of infrastructure, and then if we see a vulnerability, we can do a subpoena to find out who that victim is so we can tell them.

You know, there is admin subpoena authority that comes with the CIRCIA as well.

So I think it's probably a helpful thing, for the CSRB to have it. I don't think that there are any issues with their admin subpoena power as it relates to CISA's secret sauce, frankly, which is being seen as a trusted partner, not a regulator or not anybody who's going to issue punitive sanction.

Mr. SWALWELL. Great. Thank you.

I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize my friend from Florida and the Chair of the Transportation and Maritime Security Subcommittee, Mr. Gimenez.

Mr. GIMENEZ. Thank you very much, Mr. Chairman.

Thank you to the Ranking Member.

Ms. Easterly, two separate subjects I want to talk about. One of them is, when I was mayor of Miami-Dade, I was approached and said that there may be some issues with the cranes at our port, where, I think, out of 13 cranes, 10 of them were made in China, and now—and then later found out maybe about 70—maybe 70—70 to 80 percent of the cranes in the United States are actually made in China.

Now, some of those cranes have—all of those that are made in China have the skin, the bones, OK, are made in China, but in some the internal workings, the guts, some of the computer systems and the operating systems, may be made in Germany or some other place. But in some it's all Chinese-made. I was made aware that there may be some threats with this.

I have two things I'm concerned about. No. 1, if the CCP decides not to replace with replacement parts or spare parts when they break down, it could hurt our ability to provide commerce, since most of the stuff that we move moves through these cranes; or, No. 2, if it's actually Chinese software reporting back to the CCP so they can track everything that we do—what cargo is flowing through, to where, et cetera, et cetera.

Have you assessed that situation in the United States?

Ms. EASTERLY. Yes, it is a real concern of ours. I think my head of cyber is going to appear before your committee on the 10th of May.

You know, I think you're referring to Zhenhua, the port machinery company—70, 80 percent, 23 seaports. We have significant concerns about supply chain disruption as well as surveillance. We are working with our partners across the Government to help with analysis and what we can do about it—difficult, given the market-share piece of this. But I do think it is a significant problem that we need to turn our attention to.

I also would just say, Congressman, that this is a piece of the larger issue of Chinese technology encroaching into our national security. I worry about that from a very strategic perspective.

We're actually setting up a counter-PRC cyber effort that will be led by a very talented person that we're bringing on through cyber talent management system authorities.

But these are things that we absolutely have to get ahead of.

Mr. GIMENEZ. Fair enough. I don't want to give too much away, because, you know, it's his committee, not my committee. So I'll bring it to mind.

The other thing I want to talk about is completely different, and it just came to me: That 80 percent of the drones that are used in the United States are actually manufactured in China too. It's come to my attention that, on occasion, with these drones, you hook it up to try to get a software update, OK? I was wondering if, when you're doing these software updates, you're also downloading information the other way.

So can you imagine—can you imagine if the CCP, the PRC had all the information gathered, all the images gathered by 80 percent of the drones flying around? That's an incredible amount of data.

So is that download two-way, or is it one-way? Have we ever checked out to see if there's information going the other way? Or is something—I just thought of something nobody thought of?

Ms. EASTERLY. Yes. No, when you think about the number of Chinese drones, it makes you worry less about the high-altitude balloon, in some ways, when you consider that. But, you know, all of these are significant threats that we need to take seriously.

I don't know the specifics. What I would tell you from a technical perspective that I worry more about is not something being uploaded but if they're saying, download this software, provide this update, they could be putting something malicious in that update. That was sort-of what happened with SolarWinds and the Russians; there was something malicious in that software update.

So I do think that there are significant concerns, again, given any sort of oversight or surveillance of a foreign adversary who's clearly the preeminent threat to this Nation.

Mr. GIMENEZ. But do you know for sure they're not uploading information back to the host?

Ms. EASTERLY. I do not know that. Happy to check it out—

Mr. GIMENEZ. Yes.

Ms. EASTERLY [continuing]. Or get you some information on it.

But, you know, there's Chinese capabilities that are getting—TikTok, for example. There's a ton of data from the 130 million Americans that use that that is very likely going back to the PRC.

Mr. GIMENEZ. What's your agency doing about Trojan horses? When I say "Trojan horse," it's some kind of malware that's stuck in a program that just sits dormant until they decide to unleash it.

Ms. EASTERLY. Yes.

Mr. GIMENEZ. That worries me too, that there may be it Trojan horses all over the place we know nothing about—

Ms. EASTERLY. Yes.

Mr. GIMENEZ [continuing]. And then, all of a sudden, you know, "OK, unleash havoc on the United States."

Are we taking steps to try to avert that too?

Ms. EASTERLY. Well, that sort-of goes to the entire heart of our mission, sir, really, I mean, because our job is to protect and defend critical infrastructure. It's our work with partners across the country to ensure that they're aware of those types of capabilities that can be used not just for espionage but also for destruction or disruptive purposes.

So a lot of this comes down to education. But, also, it comes down to my earlier point. The technology that we rely on every day was not created with security and safety in mind. I think it's incredibly

important that those technology products are tested and developed specifically before it comes to the consumer to look for potential vulnerabilities like that.

Mr. GIMENEZ. Thank you, ma'am. My time is up.

Ms. EASTERLY. Thank you, sir.

Mr. GARBARINO. The gentleman yields back.

We've finished the first round of questions. I think there are couple who want to ask a second round.

So don't worry, your doughnut is safe in the back. We still have it for you.

So we're going to start the second round. I'm going to recognize the gentleman from Louisiana, Mr. Carter, for a second round of questions.

Mr. CARTER. Thank you, Mr. Chairman.

Director Easterly, as we see technology move as fast as it does, we know that every day there's some new mode or method to infiltrate, to damage, to destroy.

On a scale of 1 to 10, what would you say your agency feels about your ability and capability to remain competitive and equal to, hopefully a step ahead of, the bad guys?

Ms. EASTERLY. It's hard to give you a 1 to 10. I would want to say we're—

Mr. CARTER. You can give me a 4 to 6, if you want.

Ms. EASTERLY [continuing]. At a 7. But, you know, it's an anecdotal thing. Every day, we work to stay ahead of an adversary.

I think, to be very frank with you, Congressman, I don't worry about capability. I think the United States of America has the most capable cyber forces in the world. I worry about the asymmetry of values. Because our adversaries—the Chinese, the Russians, the North Koreans, the Iranians, cyber criminals—will do things with impunity that we, frankly, wouldn't do, as a values-based democracy. That's where I think we have to be concerned.

That's why this idea of the status quo being unacceptable—we have to ensure that everybody in this Nation, from K through gray, is aware of what they need to do to stay safe on-line, that CEOs are taking responsibility, that software companies are building safe products, and that we are all working closely together for the good of the Nation.

Mr. CARTER. Along that line, the Biden administration's National Cybersecurity Strategy attempts to shift the emphasis away from consumers to the provider. This is a big idea that could substantially impact the price of software, its utility, cost, and competitiveness for the U.S. software industry and international markets.

Understanding that much of our economic prosperity for the past several decades is based on innovation in computer software, what microeconomic model is DHS proposing to deal with this?

When we shift the responsibility, there's a lot of risk that comes with that and a lot of challenge.

Ms. EASTERLY. Yes. I can't speak to the microeconomic model. I'm happy to follow up on that. I think—

Mr. CARTER. OK. Now, that's No. 3 that you couldn't speak to today for me. Just keep—just keep a record.

Ms. EASTERLY. You know, I'm a macroeconomic person. But, you know, happy to follow up.

Mr. CARTER. Fair enough.

Ms. EASTERLY. But, look, at the end of the day, this is a big concept, shifting the burden.

Just to kind-of talk about this at a strategic level, it's been 40 years since the internet came into being, right, with TCP/IP. You think back to 1983. Nobody thought about security when creating an internet. Nobody thought about safety security when creating software. Nobody thought about that when we were moving fast and breaking things with social media. Here we are in AI, and we're hurdling into a space that, frankly, we don't know what the outcomes will be.

So I am a huge fan of innovation. It's one of our core values. But what I'm saying, Congressman, is, we cannot let innovation be the most important thing that we look at when we're thinking about creating products that Americans rely on every single day.

I want to live in a world where I do not have to teach my 90-year-old mom how to enable multifactor authentication on her phone. I want to live in a world where I don't have to check the box that I agree to the 17,000-word contract to turn my phone on that basically says, "You're liable for everything bad that happens here."

Mr. CARTER. Aren't we there? Aren't we there?

Ms. EASTERLY. Aren't we there in terms of—

Mr. CARTER. All of the things that you just mentioned.

Ms. EASTERLY. No, not at all. None of these things are baked in. That's the world that we need to live in, where security and safety is baked in, just as your seatbelt, your airbags are baked in and come with your car.

Mr. CARTER. I find that the more technology moves, the more sophisticated the basic functions are. You mentioned the telephone; you mentioned checking the box. That stuff does exist now, and it's getting more and more complicated for the average person to use any level of electronics.

I understand the importance of technology moving. Are we moving in a direction that we're able to combat the threat of the—the infrastructure threat of ransomware, cyber attacks that cripple networks?

Ms. EASTERLY. Yes, I think we are indeed getting more capable as a Nation. A lot of that is the growth in this agency that the Congress has generously helped us with.

But, you know, at the end of the—I think we're sort-of saying the same thing here, Congressman. The complexity—we should not be putting the complexity on the consumer. The complexity needs to be put on the provider so everything is almost seamless and easy for the consumer. The consumer shouldn't have to figure out how to implement all those security controls. They need to come baked in.

Mr. CARTER. With that, are you concerned about what it does to the economics of it? I don't want to go deep into the macroeconomics of it, but the costs associated, what does that mean to the consumer?

As we shift more responsibility to the provider, it's safe to assume that we're going to also see some pushback on what it costs—

Ms. EASTERLY. Yes.

Mr. CARTER [continuing]. The individual.

Ms. EASTERLY. I would much rather live in a world where I have much safer products. In a world that everything is digitized and connected and we are increasingly vulnerable as we leap into this space where everything is going to be smart and IoT, I would much rather pay it at the front end and know that I have a safe product, rather than knowing I'm going to get attacked with ransomware. Any of that—

Mr. CARTER. I could not agree with you more, except we have to—

Mr. GARBARINO. The gentleman's time has—

Mr. CARTER. May I just kind-of finish real fast?

But we have to take into consideration that we have a lot of poor people. There are a lot of people who—that extra fee that we're talking about that's tacked on to the consumer makes a big difference to a person that's on a fixed income, that's unemployed or underemployed.

So I would just ask that as we move forward that we're considerate of the fact that, while we want to make sure that the provider does this and there may be an extra cost associated, let's just be mindful that that extra cost, to many Americans, can be deal-breakers.

Ms. EASTERLY. Hundred percent.

Mr. CARTER. Thank you.

I yield back, sir.

Mr. GARBARINO. Thank you.

I now recognize Mr. Ezell from Mississippi for 5 minutes.

Mr. EZELL. Thank you, Mr. Chairman.

Thank you, Director, again, for being here this afternoon. It's good to see you and hear all this stuff that is very complicated.

I live in basically a pretty rural district. How is the CISA addressing some of the challenges with cybersecurity in the rural areas, especially with the cyber work force?

You know, we've kind-of talked about that some, but, you know, out in the rural areas, you know, we need a little help.

Ms. EASTERLY. Yes. One of the things I'm most excited about, sir, is the cybersecurity grants for State and local.

Mr. EZELL. Yes.

Ms. EASTERLY. I think this is a really groundbreaking program. You know, a billion dollars is not a lot, but I think if we can prove out the model, we can actually make a real difference to those entities that, frankly, are not well-resourced at all.

So I think, as you know, 80 percent of the money goes out to local, and 25 percent of that goes to rural. So it is very specifically focused on how to improve cybersecurity in places that typically don't have resources.

So what we've seen to date is, we've seen requests for training to improve that cyber work force; we've seen requests for equipment; and requests for assessment. I think we've got 15 plans in. We have approved all but, I want to say, two of them. Then seven, I think, have already—the money has already gone forward.

I think Mississippi actually may be one of them. So I will check on that. But that money, I think, has already been disbursed.

So we're working very hard to get that out the door.

Mr. EZELL. Thank you very much.

We plan on having a cybersecurity roundtable in August, and hopefully we could reach out and maybe you could come out and help us a little bit.

Ms. EASTERLY. I would love that.

Mr. EZELL. Very good. Would think you could get some good seafood down on the Gulf Coast.

You know, we've talked a lot about some of the threats, but, in your view, what is the greatest cybersecurity threat that the Congress should be paying attention to right now?

Ms. EASTERLY. Yes, I think there are two epoch-defining threats and challenges. One is China, and the other, I think, is artificial intelligence.

There are some incredible things that AI will do, but we need to ensure that, just as we're talking about technology being built with security in mind, we need to ensure that these fantastic capabilities have the right controls and guardrails to keep us safe and secure.

So I think those two challenges are things that we're going to be concerned about over the next 10, 20 years and more.

Mr. EZELL. Thank you very much.

Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize my colleague from New Jersey, Mr. Menendez, for a second round.

Mr. MENENDEZ. Thank you, Chairman. I again just want to express my appreciation for you holding this hearing today.

My colleague from Florida, we have ports in my district. I was the commissioner of the Port Authority of New York and New Jersey and seeing our cybersecurity spending go up and up each and every year because of the importance of our infrastructure and being very sensitive to how much of our technology is produced in China.

The other reason I like being here is because: My grandmother lived to be 98. She only had a high school education, but into the last years of her life she loved learning about the new technology and watching it develop. You can imagine someone who was 98, the technology and the advances in technology.

She said she loved learning about it and it didn't scare her at all, but what scared her is how quickly it was changing and that we weren't giving ourselves the opportunity to think about what it means for us. So your point about innovation just brought me back to those conversations, and they're important ones.

But you also brought up so many good points, so thank you for your testimony. Thank you for what you're doing in your role as director.

You know, but going back to the secure-by-design, secure-by-default, I mean, there seems to be sort-of a challenge there because of, as my colleague was alluding to, how much of our technology is produced in China, which you've made several references to in your testimony. Secure-by-design, secure-by-default, makes complete sense. But if we're not developing it, then how do we make

sure and hold accountable, you know, foreign potential adversaries who are developing critical technology for us?

You also said how much we rely on technology, which we are, right? So it's becoming a compounding problem, where we are almost losing the ability to live without this technology and yet we're not developing it ourselves.

So how, in this sort-of manufacturing, R&D sort-of space and time that we live in, with the reliance on countries like China, can we get to a secure-by-design, secure-by-default future?

Ms. EASTERLY. Yes. So we are actually very actively ensuring that, if there is Chinese technology or products within our supply chain, certainly for the Federal Government but also in terms of our ability to use a platform for informing critical infrastructure owners or operators about the dangers of Chinese technology, we would recommend that that be replaced or not used, frankly, which—

Mr. MENENDEZ. That's a challenging thing.

Ms. EASTERLY [continuing]. Which is very—I agree with you, Congressman.

Mr. MENENDEZ. When you say supply chain and making sure you go through all the levels of the supply chain to make sure all the different component pieces are secure-by-design, secure-by-default—

Ms. EASTERLY. It is very challenging. You know, as my friend Kemba Walden likes to say, the word “easy” does not appear in the National Cybersecurity Strategy.

But it's one of the reasons, to be frank, we are pushing so hard on the instantiation of software bill of materials. You know, we have to understand what is in our supply chain.

Mr. MENENDEZ. I understand.

Ms. EASTERLY. Incredible complexity. But, you know, we can't say that, because I didn't know, I was able to—you know, our foreign adversaries did these implants and now our infrastructure has been compromised and disrupted or ultimately destroyed in the event of a conflict.

So these are all very difficult things, but, you know, frankly, that's why this subcommittee and this partnership is so important to the security of the Nation.

Mr. MENENDEZ. Absolutely. And please—and I'm sure you know this, but please do consider us a partner, and these are things that we want to work on.

But, you know, if there is a way or almost thinking about it sort-of as like a way to, as we sort-of onboard technology or bring it through, just—because I think the going through the supply chain—because you just see it on the sanctions front, right, and all the workarounds that there are, from, you know, different state actors, NDIs that appear on our sanctions list. That alone is really challenging to track, and then when you get to technology and being able to do that cross-border, I feel like that's going to be a challenge.

But this was all really helpful. I went over on my last time, so I'm going to be mindful this time. My colleague from Texas just arrived, so I want to make sure she gets to her questions sooner.

Thank you again so much, and I really look forward to continuing this conversation with you and your staff.

I yield back.

Mr. GARBARINO. Thank you.

The gentleman yields back.

I now recognize Mr. Gimenez from Florida for his second round.

Mr. GIMENEZ. Thank you, Mr. Chairman.

You know, as we talk about the big threat—and you said the two big threats are the CCP and AI. We also talked here about how we need to start to decouple. But if I were to tell you that I just heard of a major purchase of Chinese computers from one of our major departments, like, half a billion dollars' worth, all right, it kind-of makes you start—you know, are they listening to us? Or are they—who are they listening to, that they would go and buy half a billion dollars in computers, computers made in China or by a Chinese company? So I think we need to get that word out.

I think there's—you know, since I serve on the Select Committee on China, you know, it's one of the areas that I find where we have bipartisan support and we kind-of think the same way. We may not have the same solutions or maybe an iteration of solutions, but we're on the same path, you know? It's good to see that America has finally woken up and, collectively, we're working to address this threat.

I want to go to AI. You know, people are trying to make—trying to say, “Hey, we need to slow down AI.” Frankly, we cannot slow down AI, because our adversaries are not going to slow down where they are, and they understand the potential of artificial intelligence and all sorts of things. But in military hardware, AI, if they get that advantage on us, it's huge. Huge. So we can't. We have to keep going.

But, with that being said, AI has the potential to do incredible good. Unbelievable good. Mankind, womankind, you know, the human race can just explode, all right, with new findings, new knowledge, new abilities through the use of this technology.

But, then, AI can also be incredibly destructive. So the only defense that we're going to have against AI is AI. So are we developing that capability too? You have—AI can do good, but then you also know that AI can do bad, so you have to have the defensive AI to fight the bad AI.

Are we working on that too?

Ms. EASTERLY. Yes, I mean, I am not an AI technical expert. I know that there is a lot of work being done both on the defensive side and on the offensive side.

I agree with you, Congressman, that there are some amazing things that can be done with this capability. But I've also, probably much like you, seen a dark side when I was in the Army, when I was deployed many times, and when I was the head of counterterrorism at the White House.

What I worry about are our adversaries, whether it's a nation-state like China or a terrorist or a criminal, using these to create malware, cyber weapons, to create bio-weapons, to do genetic engineering, to do things that, frankly, we may not do, as a values-based democracy.

I think we need to have those really difficult and important conversations, because I really do believe in the power of good for technology, but AI will also be the most powerful weapons of this century. The most powerful weapons of the last century, nuclear weapons, were built and maintained by governments who were disincentivized to use them. This technology is built by companies, whose job it is to maximize profits for their shareholders. So it's a different conversation.

I applaud the efforts to try and get ahead of it, both by the Congress as well as many across the Federal Government. I think it's incredibly important.

Mr. GIMENEZ. Thank you very much.

I yield back.

Ms. EASTERLY. Thank you, sir.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Let me thank you for the courtesies extended and thank the Ranking Member for the courtesies extended. Appreciate being delayed for other meetings.

But let me welcome you, Director Easterly. I'm hoping to get some real quick questions in.

I invited you last year—it starts out with an invitation—to the Energy Braintrust that I host, the Congressional Black Caucus Foundation. You were kind enough to send someone. But I am now inviting you for 2023. This Braintrust has been around now for more than 30 years, and we have enjoyed the participation of many in the administration.

So someone is taking notes, and I appreciate it very much that you're doing so.

I want to just continue in the line of questioning. I find the production domestically of chips—and I wanted to raise some quick questions.

How important is the manufacturing of chips in the United States to cybersecurity, the security of our cyber system, doing our chips—having that manufacturing capacity right here in the United States?

Ms. EASTERLY. I think it's hugely important for the United States to have that chip manufacturing capacity. From a technology perspective, I mean, certainly in terms of cybersecurity systems, chips are not a huge piece of the actual process—

Ms. JACKSON LEE. Right.

Ms. EASTERLY [continuing]. But they're part of the technology, absolutely.

Ms. JACKSON LEE. We remember that during the pandemic, when phones, cars, and others were not able to be manufactured because of the supply chain.

Let me quickly move to Houston. The list of critical infrastructure includes petrochemical companies. In fact, in years past, when we think about cyber or think about infrastructure, it was listing these fixed entities, and we heavily—which heavily rely on automation.

Have petrochemical companies engaged with CISA in order to develop a good working relationship to deal with their critical infrastructure problems?

I have another quick question, but go ahead.

Ms. EASTERLY. Yes, ma'am, absolutely. We service the sector risk management agency for the chemical sector and have great relationships with those industries.

Ms. JACKSON LEE. One of the gaps in CISA, in terms of across the Nation, are NGO's, faith organizations, neighborhood organizations, small businesses, maybe even small colleges. So I'd be interested in working with the agency for a roundtable and laying the groundwork of informing that kind of level in the United States that are not necessarily informed.

Is that a good idea, to make sure that we can have CISA in our communities talking to that level and to be able to raise up their understanding of the importance of cybersecurity?

Ms. EASTERLY. Love it.

Ms. JACKSON LEE. We all have had the horrors of ransomware. We are facing it, the threats over the years, the stories, the tall tales, if you will. Russia continues to harbor large numbers of ransomware gangs.

We know this threat will remain forward, but I've been impressed about what you've done. Do you want to expand a little bit on how you've gotten your hands around ransomware?

I'm looking at my time, so let me put the second question in.

AI is here. I was just talking to my seatmate here, and I was saying it was coming, and he made it very clear that we both agree it is here.

I'm concerned about large populations—low-income, minorities, rural persons—out of the circle of even understanding AI and its good and its dangers. Maybe you could comment on that as it relates to cybersecurity and maybe the gaps of knowledge.

So, first, Russia and the ransomware and then, second, the AI and its accessibility to those low-income communities.

Thank you so much.

Ms. EASTERLY. Thank you so much, Congresswoman.

On ransomware, we have done so much since the summer of 2022—2021, actually, following the Colonial Pipeline attack.

Specifically, we stood up stopransomware.gov, which is a one-stop-shop website that brings together all of the Federal resources of the Government to explain what ransomware is, what to do if you get hit with ransomware, and, more importantly, how to build resilience to ransomware.

We also stood up the Joint Ransomware Task Force recently, and we're very focused on target-rich, resource-poor, those communities that, frankly, like schools and hospitals and water facilities, local election offices, that don't have those resources. So we are very focused on providing things like ransomware assessments and best practices that they can use to deal with the scourge of ransomware.

The other thing that we just launched is our Ransomware Vulnerability Warning Pilot, where entities, no matter what your size is, can sign up for vulnerability scanning and then get a prioritized list of where they might have vulnerabilities, where ransomware

actors, like Russian-sponsored ransomware actors, have specifically leveraged ransomware, so that allows them to patch those.

Then, finally, our pre-ransomware initiative, where we are getting tips from industry, from researchers, from threat intel, that tell us that malware has been deployed but not yet activated. It's usually hours to days before malware is used to encrypt. Then we reach out in our field force—we've done it with K-12 schools, with local towns—to help them prevent, you know, a really bad day. That is the virtue of the model we've built with trust with industry.

So those are some of the things that we're doing, and we're going to continue to drive that forward.

On artificial intelligence, again, there are great capabilities. I think we need a really hard look at who these capabilities—who they're being used by, who they can be made available to, but also the guardrails for safety and security that are being put in place even as we innovate in this space.

So I think it's a longer, much—you know, a hugely important conversation, so I appreciate the question, Congresswoman.

Ms. JACKSON LEE. I look forward engaging through this committee or otherwise. I think it's an important discussion for Members of Congress.

Ms. EASTERLY. Thank you, ma'am.

Ms. JACKSON LEE. I thank you so very much.

Thank you for the time.

Mr. GARBARINO. Absolutely.

Ms. JACKSON LEE. I yield back.

Let's do it. Thank you.

Mr. GARBARINO. The gentlelady yields back.

The end is almost near, Director. I think, though, the fact that everybody has been here today for a second round of questions—I mean, we've never had attendance like this, but that just shows how much everybody respects your opinion and how important of an issue this is.

So I'm going to recognize myself for my second round of questions.

I had a couple on secure by design and default, but I really enjoyed the questions before. I thought that was a great conversation. So I'm going to move ahead to—my staff actually prepared enough questions if we had eight rounds of questions, so I'll probably submit a couple and have you respond in writing.

But I did want to get to on the—we talked a lot about the JCDC in our last hearing, and we talked a little bit about it today as well. I have spoken to a couple people that are on—or companies that are on the JCDC. We've heard that some of the companies are frustrated that information coming out of the JCDC is frequently already publicly available and isn't as timely as it could be.

What information do organizations get through the JCDC that goes beyond what DHS already publishes through other channels that many JCDC members already participate in or already have access to?

Let me—I just wanted to add, they all loved the idea—nobody—they all loved the idea of the JCDC, but they did have this complaint about it.

So, if you could answer, that'd be great.

Ms. EASTERLY. Yes. You know, one of our operating principles at CISA is to treat feedback as a gift, and we are constantly talking to our partners so that we can improve. Because, at the end of the day, the model has to be, we're transparent, we're responsive, and we're adding value. If we're not adding value to the job of the cyber defender, we should go away. I know how hard that job is, and we're just trying to help them.

You know, anecdotally, I think we've heard various flavors of, you know, "these products are fantastic" and "these products are things that we've already seen." So I don't want to put too much into the fact that these are all—that you might hear one or two things. I would like to actually come back to you maybe with a more fulsome presentation based on recent feedback. We did two roundtables out at RSA.

I mean, I will tell you, what's substantially different in the products and the advisories that we've put out over the past year is, first of all, they're all multisealed. That makes a difference, to have CISA and FBI and NSA and, by the way, our international partners on there as well. It's sending, finally, a coherent signal to industry that this is the voice of the U.S. Government collaboratively providing you feedback.

Frankly, we have those enriched buyer industry partners who are giving us information that helps to make those products better.

So, again, I'll go back and get you more specifics on that.

But I think we've really evolved that into a better place, to be honest with you.

Mr. GARBARINO. Great. And, look, everybody that I've spoken to, they said, CISA, when they provide information, has been responsive, much more than other agencies that are involved. So that's great on your part, so we do appreciate that.

We've also—so how does—there was also some comments about how membership decisions are made. I know we can—maybe we can work that into the presentation. But could you talk about how CISA balances the benefits of having a wider range of partners at the table with the risk that too large of a JCDC could reduce the efficiency—

Ms. EASTERLY. Yes.

Mr. GARBARINO [continuing]. Of operational collaboration and decrease trust between the members?

Ms. EASTERLY. Yes. Thanks for asking that question.

You just said it: trust. Right? We have a lot of people—Ranking Member Swalwell mentioned, a lot of people want to join the JCDC. We want to benefit from their expertise and their vulnerability and their capabilities, but we also want to make sure that we have trust groups.

So we started out, when we set this thing up in August 2021, we started out with the Big Tech companies. Why? Because they have the most global visibility. If you're an infrastructure provider, a cybersecurity vendor, a software vendor, they have global reach. We wanted to solve—help solve that visibility problem that was illuminated in SolarWinds, where we lacked visibility.

So we started out with a small group, but since that period of time, we have been adding on hundreds of partners. We're at 231. But the projects that we work on are basically 20 of these entities.

So we are keeping the trust groups small. We're focused on efforts that address the biggest risks to the Nation. We are constantly doing after-action reviews to ensure that we can actually take great advantage of, you know, the talents, the authorities, the capabilities.

But one other thing I'd say, Chairman, is, we talk a lot about industry, but the JCDC is actually industry, international partners, Federal partners, and State and local partners. So when you think about the tapestry of visibility that comes together based on the inputs of all of those partners, I would challenge some of the comments about the lack of value. I think, as we've evolved, I think we're getting into a place where that information is enriched and full of a lot more value than anything we've provided before from the Federal Government.

Mr. GARBARINO. Director, I appreciate that.

Like I said, I have a couple more, but I'm going to let you off the hook. I'll send them and have you respond in writing. I appreciate it.

I now yield to the Ranking Member, my colleague from California, Mr. Swalwell, for his second round.

Mr. SWALWELL. Great. Thank you, Chairman.

Just following up on my colleague from the Miami area, he talked about, you know, the concern about Chinese drones and Chinese technologies in our infrastructure.

I privately mentioned to him but I'll mention to my other colleagues that John Garamendi and I introduced legislation this week called the Airport Infrastructure Vehicle Security Act, which would prohibit Federal funds from being spent on Chinese buses.

They are flooding our communities with cheap passenger buses. It's not just that, you know, this hurts the ability to "make it in America," but, you know, they're wiring these buses up with WiFi and other abilities to connect to the network.

So we'll send that around to everyone.

On AI, to kind-of take this to the worst-case scenario, I understand that a zero-click attack is where I could receive a text message or an email, and even with the best cyber hygiene, because it was sent to me, that's it, they're in.

I also understand that, right now, to conduct those zero-click attacks, they're very resource-intensive, they're very expensive. So adversaries have to really want to get into someone's system or device.

Does AI put us at risk of significantly reducing the cost for the adversary to carry out a zero-click attack?

Ms. EASTERLY. I mean, I don't have a technical study on that, but I would assume so. I think, as much as AI can be used for amazing things, I think it can be used by our adversary to cause great damage.

You know the saying, Ranking Member, is, you know, you only have to be right once, as an adversary; as a defender, you've got to be right all the time. Think about that in terms of the offense-defense overmatch of an adversary.

Mr. SWALWELL. Yes.

Ms. EASTERLY. So it makes our job even more difficult.

Now, the optimist—and I used to be a big tech optimist, and now I’m a tech realist—will say, “Well, we can also create these incredible defensive AI capabilities.” And that’s probably true.

Mr. SWALWELL. Sure.

Ms. EASTERLY. But the thing that I worry about is, we are hurtling into this space driven by competition in business, not necessarily driven by safety or security concerns.

While I am—to Congressman Menendez’s point earlier, I am concerned about China, but look at the difference. China is focused on implementing AI with a huge amount of regulation, right? So that’s the difference. They are actually being very purposeful about how they’re controlling and evolving that capability. We are not.

So I think we need to just think about what AI looks like in China and what AI looks like here and how it could be used for nefarious purposes.

Mr. SWALWELL. Shifting to insurance, you know, there’s not a lot of insurers in the cyber market. One insurer told me that the most successful insurer is not the person who has the most policies, because you would not be able to cover the risk if there was a significant, wide-spread attack.

I know in the cybersecurity strategy that you put out, you do conceive or at least contemplate, you know, a TRIA-like system. I just wanted to know if you could just speak more to cyber insurance.

Particularly, I’m thinking of, you know, the giants. They’re going to figure it out, and they’re going to have, sort-of, the best left-of-boom defenses. I really do worry, though, about the SMEs, you know, the small and medium-size businesses, who you have described as target-rich, cyber-poor.

So could you just wrap up here, with my final minute, and just to speak to cyber insurance?

Ms. EASTERLY. Yes, absolutely. You know, we are doing this study based on the National Cybersecurity Strategy.

I think it’s—the difficulty kind-of goes back to the fact that we do not have a comprehensive view of the landscape because, heretofore, we don’t have that legislation—or, we don’t have that implementation on CIRCIA. I think that hinders cyber insurance companies from being able to price insurance policies, if you don’t understand what your baseline is for cyber incidents and attacks.

That’s also, you know, some of the discussion on—I think Lloyd’s made the decision that they exclude state actors—

Mr. SWALWELL. War exceptions.

Ms. EASTERLY [continuing]. Policies from state actors, the war exception, which would make it difficult if you connect, like, NotPetya and state-sponsored criminals.

So it’s a space that I think will benefit from a better understanding of the ecosystem and, I think, a robust sort of TRIA-like study. I welcome that work to come. But it’s also something I’d love to dig more deeply into—

Mr. SWALWELL. Great.

Ms. EASTERLY [continuing]. Especially because you’ve got Cowbell in your district—

Mr. SWALWELL. Yes.

Ms. EASTERLY [continuing]. And we have talked to them before.

Mr. SWALWELL. Great. Thank you.

I yield back.

Mr. GARBARINO. Thank you.

The gentleman yields back.

I almost made a “cowbell” question—or, joke, but I didn’t.

I love the idea on cyber insurance. I think, even though we don’t have direct oversight here, I do see it also on the Financial Services Committee, the Insurance Subcommittee. So, if we could somehow work out a hearing on that, I think it’d be great.

But I want to thank Director Easterly for the valuable testimony and the Members for their great questions today.

The Members of the subcommittee may have some additional questions—I know I do—for you. We would ask the witness to please respond to these in writing.

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

Without objection, the subcommittee stands adjourned.

Ms. EASTERLY. Thank you, sir.

[Whereupon, at 3:47 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FOR JEN EASTERLY FROM CHAIRMAN ANDREW R. GARBARINO

Question 1. In our last hearing, I asked Ms. Tina Won Sherman from GAO whether CISA's ability to support the Sector Risk Management Agencies (SRMA) had grown commensurate with its budget. She answered that we really can't tell.

What metrics do you all use to measure and evaluate CISA's support to the SRMAs?

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

Question 2a. The administration is re-writing Presidential Policy Directive-21, which sets Executive branch policy when it comes to Sector Risk Management Agencies.

Where do you think CISA's role starts and stops when it comes to supporting the SRMAs?

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

Question 2b. What are you doing in the mean time to support the SRMAs as you prepare to re-write the National Infrastructure Protection Plan and they prepare to re-write their sector-specific plans?

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

Question 3a. CISA's foundational mission is to administer Federal civilian Executive branch (FCEB) cybersecurity requirements, a daunting but hugely important task. It's my sense that your agency struggles in part with how other departments and agencies in the Government perceive it.

How do you view CISA's role in the FCEB? Do you think CISA should be a Service provider? Operational partner? Advisor? Something else?

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

Question 3b. What can Congress do to support and develop CISA's position in the interagency?

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

Question 4a. We have been talking about revamping one of CISA's flagship Federal cybersecurity programs, the National Cybersecurity Protection System, which includes EINSTEIN, for a long time. It's an outdated program that has faced problems, including struggles to fully implement the requirements.

How does CISA plan to overcome the issues that have plagued previous iterations of NCPS?

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

Question 4b. As you build this new program, how do you envision it fitting into a very dynamic environment as agencies implement requirements from the May 2021 Cyber Executive Order, including the Zero Trust Strategy, and other specific capability requirements? How are you ensuring it isn't duplicating those efforts?

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

Question 5. Director Easterly, as you know, Executive Order 14028 from May 2021 required all Federal agencies to adopt endpoint detection and response or EDR technologies, with CISA charged with that deployment.

Can you provide us with an update on the status of deployment across the FCEB? How many agencies has it been deployed on? Who has not deployed it yet?

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

Question 6. The committee is aware that CISA is currently paying for the first 2 years of certain Continuous Diagnostics and Mitigation (CDM) shared services for agencies, after which the agencies must pay.

Is that accurate? Please explain how this process is working and if there are any agencies who are not planning to pay for those services in year 3.

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

Question 7. We have heard that CISA has narrowly defined what it considers as an endpoint to only workstations or desktops and has left out others like mobile devices and cloud environments.

Is CISA going to add mobile and cloud to the program? If not, why not?

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

Question 8. Director Easterly, has CISA considered operating EDR as a shared service? If not, why?

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

Question 9. As you know, DHS has provided CDM services to agencies for several years now. So far, CDM's attention has been primarily on larger agencies.

What is your perspective on how the CDM program might evolve to provide the same level of attention to smaller and independent agencies?

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

Question 10. According to BlackBerry's just-released quarterly Global Threat Intelligence Report, governments face an ever-growing number of cyber threats that are increasing in sophistication. Earlier this month, you observed that terrorists, cyber criminals, and adversary nation-states could make use of advancements in artificial intelligence (AI) technologies to weaponize cybersecurity.

In the face of this threat, are Federal civilian Executive branch agencies adequately leveraging advanced AI-enabled cybersecurity tools to enhance the defense of Federal networks, especially against AI-capable adversaries? If not, why not?

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

Question 11. According to BlackBerry's just-released quarterly Global Threat Intelligence Report, the Russia-linked malware PIPEDREAM recently attempted to compromise industrial control systems in U.S. energy and gas infrastructure.

How concerned are you about the recurrence of such threats within the energy sector, and across other critical infrastructure sectors—and what can industry do to better prepare itself for such incidents?

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

Question 12. It is vital to increase cybersecurity across all sectors in the United States, but how are you currently supporting more mature sectors, such as the financial services industry?

How will CISA support cross-sector risk identification and mitigation planning for more cyber-mature sectors?

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

Question 13. Based on a report issued by Expert Insights in March of this year, 71 percent of ransomware attacks are targeted at small businesses, companies that are in your own words, "Target-Rich and Resource-Poor."

Besides issuing guidelines, what else can CISA be doing to help small businesses respond to these attacks?

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

Question 14. Watching the various cyber activities leading up to and during Russia's war on Ukraine, what do you see as cyber-based indicators that countries like China may exhibit before an invasion of a sovereign country like Taiwan?

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

Question 15. The FBI, DHS, and CISA as well as other Government agencies are charged with protecting the American public from cyber attacks and tracking down cyber perpetrators. But to do that, data is key.

Where do you see reconciliation between their duties to identify, defend, and prosecute cyber criminals and the data/tools needed to do so, and privacy of citizens?

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

Question 16a. CISA has been working on a set of cybersecurity performance goals (CPG). There is concern in the private sector that these voluntary performance goals will wind up being treated like the presumably voluntary NIST CSF—as a de facto template for mandatory requirements.

Can you tell us how these CPGs fit into this construction that liability should be on the provider?

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

Question 16b. Can you describe how CISA engaged the private sector, including the operational technology community, and other stakeholders to gain feedback and make changes?

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

Question 16c. If an entity wants CISA to consider changes to the CPGs, what systems exist to provide input to CISA?

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

Question 16d. With what periodicity does CISA plan to update the CPGs?

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

Question 16e. How will CISA measure and evaluate the effectiveness and impact of the CPGs on reducing cyber risk and enhancing resilience, and how will those measurements guide future CPG updates?

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

Question 17. CISA is leading in the Federal space in providing support to educators on school security and safety. Given the differing needs of schools throughout the Nation, how does CISA's school safety teamwork with regional or local institutions like the New York State Center for School Safety to "train the trainer" and disseminate Federal resources?

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

Question 18. In the Cybersecurity Best Practices for Smart Cities document released by the "Five Eye Nations" on April 19, 2023, the guidance suggests that "Organizations should use only trusted information and communications technology (ICT) vendors and components."

How does a business become a trusted ICT vendor and what is CISA doing to expand partnership opportunities with businesses and organizations?

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

Question 19. Last November, you announced that CISA plans to expand the Cybersecurity Education and Training Assistance Program (CETAP) Nation-wide after a successful program in the State of Louisiana training educators for K–12 cybersecurity education. Congress believes strongly in this program—having codified it into law and appropriating resources despite successive budget requests that have zeroed out the funds.

What is CISA's plan to scale CETAP to get more teachers trained so these teachers can help train the next generation of the cyber workforce and the entire citizenry to be more cyber aware?

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

Question 20a. In February 2020, Executive Order No. 13905 was issued by the Executive Office of the President. This Executive Order required that the Secretary of Homeland Security support resilient positioning, navigation, and timing (PNT) solutions by working with sector-specific agencies to develop contractual language for Federal contracts for products, systems, and services that support or utilize PNT services.

Critical infrastructure resilience is a top priority for this committee as it works to help support DHS and CISA's goals for improving our Nation's cyber posture. Can you provide an update on the state of PNT implementation?

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

Question 20b. We understand that PNT profiles were established in accordance with the Executive Order. What is the next step for DHS in relation to EO13905 implementation, and are there significant barriers to completing the requirements of EO13905?

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

Question 20c. The EO requires the development of "contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services." In the development of such contractual language, how will CISA tailor sector specific requirements to encourage private-sector use in a manner that does not encourage any single solution?

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

Question 20d. We also understand that the National Risk Management Center (NRMC) is taking the lead on this effort. Does the CISA budget request provide the agency with enough discretionary support to fulfill the requirements of EO13905? If not, what further resources or information would be required by NRMC to make progress on working with sector-specific agencies to develop contractual language?

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

QUESTIONS FOR JEN EASTERLY FROM RANKING MEMBER ERIC SWALWELL

Question 1a. CISA recently announced a plan to establish a Systemically Important Entities Office, with the goal of identifying "target rich, cyber poor" entities, targeting K–12 schools, hospitals, and water and wastewater sectors. CISA also plans to establish an "enhanced engagement" program with these sectors. This is an extension of an effort DHS has been trying to accomplish for nearly two decades, through efforts like the Section 9 list and the National Asset Database—but has been unsuccessful.

Please describe the remit of the Systemically Important Entities (SIE) Office and where it will fit into CISA's organizational structure.

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

Question 1b. How will this SIE effort, and the program office, differ from previous efforts to identify the critical of the critical, such as the Section 9 list and the National Asset Database?

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

Question 1c. More specifically, what is the relationship between SIEs and entities on the Section 9 list? What do you see as the difference in the scope of these two designations?

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

QUESTIONS FOR JEN EASTERLY FROM HONORABLE ROBERT MENENDEZ

Question 1a. CISA has previously touted efforts with private entities like CYBER.org, the Girl Scouts of America, and Girls Who Code as examples of partnerships that can help amplify educational opportunities and grow the pipeline of cybersecurity workers.

Has CISA experienced any successes or challenges in public-private partnerships for cybersecurity workforce development? Please describe the successes and challenges and detail how the agency overcame any challenges.

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

Question 1b. Please provide a list of private-sector entities, including academic and non-profit organizations, with which CISA partners to strengthen the cybersecurity workforce. Please describe the nature of the partnership, the activities jointly engaged in, and the demographic groups each of these partnerships seeks to reach.

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

Question 1c. If the agency requires additional resources such as funding or authorities to better engage non-governmental entities for cybersecurity workforce development, please describe what those may be.

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

Question 2a. As you know, CISA issued \$2 million in grants to NPower and the CyberWarrior Foundation as part of a 3-year pilot program announced in October 2021.

Please provide an update on these activities. How have NPower and CyberWarrior started executing their grants? What plans do they have to continue spending their award over the 3-year period? How will CISA track and monitor their performance?

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

Question 2b. How will CISA measure success for these grant awards, and what criteria will be used to determine success or failure? Does CISA have a process in place to incorporate any lessons learned into future grant-making activities?

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

