EVOLVING THE U.S. APPROACH TO CYBERSECURITY: RAISING THE BAR TODAY TO MEET THE THREATS OF TOMORROW

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 3, 2021

Serial No. 117–36

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
47–035 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Donald M. Payne, Jr., New Jersey
J. Luis Correa, California
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Eric Swalwell, California
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
Val Butler Demings, Florida
Nanette Diaz Barragán, California
Josh Gottheimer, New Jersey
Elaine G. Luria, Virginia
Tom Malinowski, New Jersey
Ritchie Torres, New York

John Katko, New York
Michael T. McCaul, Texas
Clay Higgins, Louisiana
Michael Guest, Mississippi
Dan Bishop, North Carolina
Jefferson Van Drew, New Jersey
Ralph Norman, South Carolina
Mariannette Miller-Meeks, Iowa
Diana Harshbarger, Tennessee
Andrew S. Clyde, Georgia
Carlos A. Gimenez, Florida
Jake LaTurner, Kansas
Peter Meijer, Michigan
Kat Cammack, Florida
August Pfluger, Texas
Andrew R. Garbarino, New York

Hope Goins, *Staff Director*
Daniel Kroese, *Minority Staff Director*
Natalie Nixon, *Clerk*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

EVOLVING THE U.S. APPROACH TO CYBERSECURITY: RAISING THE BAR TODAY TO MEET THE THREATS OF TOMORROW

Wednesday, November 3, 2021

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:03 a.m., via Webex, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Payne, Slotkin, Cleaver, Green, Clarke, Titus, Watson Coleman, Torres, Katko, Higgins, Guest, Van Drew, Norman, Miller-Meeks, Clyde, Gimenez, LaTurner, Meijer, Cammack, Pfluger, and Garbarino.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

I would like to thank National Cyber Director Inglis and CISA Director Easterly for participating in today's hearing on how the Federal Government is maturing its approach to securing Federal networks and critical infrastructure. At the outset, I would like to commend the administration for its steadfast commitment to confronting the cybersecurity challenges facing the Nation, and I would like to thank both of you for the important role you play. This committee has a long history of bipartisan collaboration in support of advancing strong, sound cybersecurity policy, and we look forward to working with both of you in your respective roles.

Last Congress, Members of the committee worked together to raise CISA's funding, expand CISA's authorities, and authorize the National cyber director. With the support of this committee, CISA worked tirelessly with State and local election officials to ensure the most secure election in history—during a global pandemic no less. But late last year, we learned that the Russian government conducted a sophisticated supply chain attack and gained access to our Government and private-sector networks. Only months later, Microsoft disclosed that Chinese hackers exploited multiple zero-day vulnerabilities in Microsoft Exchange Servers to gain access to emails and maintain persistent access to the networks. A series of high-profile ransomware attacks threatening the fuel and food supply followed. Just yesterday, voters went to the polls to cast their ballots even as efforts to push the big lie and erode public confidence in democratic institutions persist.

These events forced three important conversations: How do we activate resources and authorities quickly to modernize Federal network security programs? Does the Federal approach to securing critical infrastructure, which relies heavily on voluntary frameworks, serve the National security interests of the American people? How do we protect public confidence in our democratic institutions, particularly our elections?

To its credit, the administration has confronted these challenges head-on, laid out a bold agenda, and put its money where its mouth is. From the ambitious Executive Order on Improving the Nation's Cybersecurity, to the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, to the pipeline security directives, the administration is aggressively leveraging existing authorities to raise the Nation's cybersecurity posture. Last week, the White House asked Congress to expand the Environmental Protection Agency's ability to regulate cybersecurity for the water sector.

Moving forward, I will be interested to know whether you expect the administration to leverage or seek similar authorities to impose mandatory cyber standards on other sectors, and if so, what you expect the role of your organizations to be in that process.

Given my role on both this committee and the January 6th Select Committee, I am disturbed by how disinformation fosters conspiracy theories, divides us, and makes us doubt our democratic institutions. I will be interested to understand how CISA's maturing its election security activities, related to both the security of election infrastructure and its rumored control efforts.

While I appreciate the administration doing what it can by leveraging the authorities it has, this committee is working hard to provide many of the additional authorities necessary for CISA to take on the challenges ahead. For example, bipartisan members of the committee offered amendments to the NDAA that would establish a mandatory cyber incident reporting framework, authorize the CyberSentry program, and establish the Joint Collaboration Environment. I am hopeful that today we can discuss how you will implement those measures when they are enacted into law, as I expect them to be.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

NOVEMBER 3, 2021

Good morning. I would like to thank National Cyber Director Inglis and CISA Director Easterly for participating in today's hearing on how the Federal Government is maturing its approach to securing Federal networks and critical infrastructure.

At the outset, I would like to commend the administration for its steadfast commitment to confronting the cybersecurity challenges facing the Nation, and I would like to thank both of you for the important role you play.

This committee has a long history of bipartisan collaboration in support of advancing strong, sound cybersecurity policy, and we look forward to working with both of you in your respective roles.

Last Congress, Members of the committee worked together to raise CISA's funding, expand CISA's authorities, and authorize the National cyber director.

With the support of this committee, CISA worked tirelessly with State and local election officials to ensure the most secure election in history—during a global pandemic no less.

But late last year, we learned that the Russian government conducted a sophisticated supply chain attack and gained access to our Government and private-sector networks.

Only months later, Microsoft disclosed that Chinese hackers exploited multiple zero-day vulnerabilities in Microsoft Exchange Servers to gain access to emails and maintain persistent access to the networks.

A series of high-profile ransomware attacks threatening the fuel and food supply followed.

And just yesterday, voters went to the polls to cast their ballots even as efforts to push the Big Lie and erode public confidence in democratic institutions persist.

These events forced three important conversations.

- How do we activate resources and authorities quickly to modernize Federal network security programs?
- Does the Federal approach to securing critical infrastructure—which relies heavily on voluntary frameworks—serve the National security interests of the American people?;
- How do we protect public confidence in our democratic institutions, particularly our elections?

To its credit, the administration has confronted these challenges head-on, laid out a bold agenda, and put its money where its mouth is.

From the ambitious Executive Order on Improving the Nation's Cybersecurity, to the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, to the pipeline security directives, the administration is aggressively leveraging existing authorities to raise the Nation's cybersecurity posture.

Last week, the White House asked Congress to expand the Environmental Protection Agency's ability to regulate cybersecurity for the water sector.

Moving forward, I will be interested to know whether you expect the administration to leverage or seek similar authorities to impose mandatory cyber standards on other sectors, and if so, what you expect the role of your organizations to be in that process.

Given my role on both this committee and the January 6th Select Committee, I am disturbed by how disinformation fosters conspiracy theories, divides us, and makes us doubt our democratic institutions.

I will be interested to understand how CISA's maturing its election security activities, related to both the security of election infrastructure and its rumor control efforts.

While I appreciate the administration doing what it can by leveraging the authorities it has, this committee is working hard to provide many of the additional authorities necessary for CISA to take on the challenges ahead.

For example, bipartisan Members of the committee offered amendments to the NDAA that would establish a mandatory cyber incident reporting framework, authorize the CyberSentry program, and establish the Joint Collaboration Environment.

I am hopeful that today we can discuss how you will implement those measures when they are enacted into law, as I expect them to be.

With that, I look forward to the testimony from the witnesses and I yield back.

Chairman THOMPSON. With that, I look forward to the testimony from the witnesses and I yield to the Ranking Member of the full committee, the gentleman from New York, Mr. Katko.

Mr. KATKO. Thank you, Chairman Thompson, for hosting this most important hearing today. Welcome to the witnesses, Director Inglis and Director Easterly. I am pleased to have both of you here.

I am going to echo the Chairman's sentiments. This isn't partisan at all, these are damned good appointments to really important positions within the cybersecurity realm. I applaud the administration for doing that.

I appreciate you all being here today to provide testimony on your strategic goals and discuss how Congress can work with the administration to secure the cyber threats of tomorrow.

We started off 2021 by uncovering the impact of the devastating Solar Winds cyber espionage campaign. But, as we all know, the attacks did not stop there. While they may seem distant, the Microsoft exchange vulnerability, Pulse Connect, and other significant ransomware attacks, including the attacks on Colonial Pipeline, Kaseya, and JBS, happened this year alone. As a result, CISA has issued an unprecedented number of emergency directives, alerts, and advisories regarding serious vulnerabilities and cyber threats. Just this week, CISA announced it was issuing a binding operational directive to quickly remediate known vulnerabilities across the Federal enterprise, and I applaud that.

The volume of our alerts, advisories, and directives goes to show the pervasiveness of vulnerabilities affecting owners and operators of critical infrastructure and Federal networks.

CISA has performed commendable work given the daunting task it has faced over the past 20 years. This in part has been due to additional authorities from the Fiscal Year 2021 National Defense Authorization Act. This includes significant authorities, such as the ability to issue administrative subpoenas to notify critical infrastructure entities of vulnerable devices, as well as the authority to conduct threat hunting on Federal agency networks without advance notice.

While new authorities are an important piece, CISA must also be fully funded. I have been a strong proponent of responsible growth at CISA and I am pleased the House Committee-passed appropriations bill puts the agency on that path.

We must also move past bureaucratic turf battles and remember that cyber incidents are rarely sector-specific. We need to continue building on the resources within CISA as a central agency that can quickly connect the dots when a malicious cyber campaign spans multiple sectors and then share that information across a broader critical infrastructure community.

Director Inglis, this is where I expect you to have an important role. Given your role as a principal advisor for cybersecurity, the "head coach", as I like to call it, or as the overseeing the entire Federal Government's cybersecurity mission, it is important that you are setting the tone that everyone has a role to play and must work together.

I look forward to learning more about the various roles and responsibilities of your position, the National Security Council, and the CISA director.

To ensure CISA can successfully carry out its mission, it needs a higher degree of visibility into cybersecurity threats and incidents impacting private-sector networks. Increased collaboration across governments and private industry is essential. I applaud new initiatives, such as CISA's stand-up of the Joint Cyber Defense Collaborative.

We also need to ensure the information being shared with the private sector is timely, actionable, and meets the needs of a diverse set of cross-sector stakeholders. To be sure, we need to work on that and get better with that.

It is important that there be a high-value proposition for entities to partner with CISA. It can't be a one-way street.

I am pleased to have partnered with Chairman Thompson and Subcommittee Chairwoman Clarke on mandatory cyber incident reporting legislation, as it will be another important tool for CISA to have to protect the critical infrastructure community, but it won't be a silver bullet.

We live in a world of an increasingly interdependent web of hardware, software services, and other connected infrastructure. Single points of failure in layers of systemic importance across this ecosystem leave the potential for cascading impact, which I have been focusing on legislation which would require that CISA designate and prioritize risks to key infrastructure sectors as they work to mitigate cyber risks across the various industry sectors and Government entities facing threats from nefarious cyber actors every day.

As CISA nears its whopping third anniversary in a few weeks, it is incumbent upon Congress to ensure CISA is appropriately prioritizing its mission space and focusing on what it does best within its limited resources to address the most pressing challenges in the evolving threat environment.

Between these two highly-capable witnesses here today, Director Easterly and Director Inglis, I am confident that our Federal Government is poised to tackle the growing litany of cyber threats facing our Nation.

I want to just note from a personal standpoint before I end, this is the way Government is supposed to work. You all are getting along and you are working well together. I dare say you should stand as an example for other agencies to follow, just like I hope Chairman Thompson and I set an example for others in Congress, which we hope they would follow more than they do.

Again, I want to thank you very much for being here today and I look forward to hearing testimony from both of you.

I yield back.

[The statement of Ranking Member Katko follows:]

Statement of Ranking Member John Katko

Thank you, Chairman Thompson, for hosting this hearing today. Thank you to Directors Easterly and Inglis for joining us to provide testimony on your strategic goals and discuss how Congress can work with the administration to secure the cyber threats of tomorrow.

We started off 2021 by uncovering the impact of the devastating SolarWinds cyber espionage campaign, but, as we all know, the attacks did not stop there.

While they may seem distant, the Microsoft Exchange Vulnerability, Pulse Connect, and other several significant ransomware attacks, including the attacks on Colonial Pipeline, Kaseya, and JBS, happened this year alone.

As a result, CISA has issued an unprecedented number of Emergency Directives, Alerts, and Advisories regarding serious vulnerabilities and cyber threats. Just this week, CISA announced it was issuing a Binding Operational Directive to quickly remediate known vulnerabilities across the Federal enterprise.

The volume of alerts, advisories, and directives goes to show the pervasiveness of vulnerabilities affecting owners and operators of critical infrastructure, and Federal networks.

CISA has performed commendable work given the daunting task it has faced over the past few years. This, in part, has been due to additional authorities from the Fiscal Year 2021 National Defense Authorization Act (NDAA).

This includes significant authorities such as the ability to issue administrative subpoenas to notify critical infrastructure entities of vulnerable devices, as well as the authority to conduct threat hunting on Federal agency networks without advanced notice.

While new authorities are an important piece, CISA must also be fully funded. I have been a strong proponent of responsible growth at CISA, and I'm pleased the House Committee-passed Appropriations bill puts the agency on that path.

We must also move past bureaucratic turf battles and remember that cyber incidents are rarely sector-specific. We need to continue building on the resources within CISA as the central agency that can quickly connect the dots when a malicious cyber campaign spans multiple sectors, then share that information across the broader critical infrastructure community.

Director Inglis, this is where I expect you to have an important role. Given your role as the principal advisor for cybersecurity, or as I like to call it, the head coach, the one overseeing the entire Federal Government's cybersecurity mission. It's important that you're setting the tone that everyone has a role to play and must work together. I look forward to learning more about the various roles and responsibilities of the NCD, the National Security Council, and the CISA director.

To ensure CISA can successfully carry out its mission, it needs a high degree of visibility into cybersecurity threats and incidents impacting private-sector networks. Increased collaboration across governments and private industry is essential. I applaud new initiatives such as CISA's stand-up of the Joint Cyber Defense Collaborative (JCDC).

We also need to ensure that information being shared with the private sector is timely, actionable, and meets the needs of a diverse set of cross-sector stakeholders. It's important that there be a high-value proposition for entities to partner with CISA—it can't be a one-way street.

I am pleased to have partnered with Chairman Thompson and Subcommittee Chairwoman Clarke on mandatory cyber incident reporting legislation, as it will be another important tool for CISA to have to protect the critical infrastructure community. But it won't be a silver bullet.

We live in a world of an increasingly interdependent web of hardware, software, services, and other connected infrastructure. Single points of failure and layers of systemic importance across this ecosystem leave the potential for cascading impact.

Which is why I have been focusing on legislation which would require that CISA designate and prioritize risks to key infrastructure sectors as they work to mitigate cyber risks across the various industry sectors and Government entities facing threats from nefarious cyber actors every day.

As CISA nears its third anniversary in a few weeks, it's incumbent on Congress to ensure CISA is appropriately prioritizing its mission space and focusing on what it does best within its limited resources to address the most pressing challenges in the evolving threat environment.

Between the two highly-capable witnesses here today, Director Easterly and Director Inglis, I am confident that our Federal Government is poised to tackle the growing litany of cyber threats facing our Nation.

Again, thank you for being here today, and I look forward to hearing your testimony.

Chairman THOMPSON. The gentleman yields back.

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

I now welcome our panel of witnesses.

Our first witness is National Cyber Director Chris Inglis. Director Inglis has over 40 years of Government service, including 30 years of service in the Air Force. Director Inglis held singular leadership assignments at the Department of Defense and the National Security Agency throughout his career, including deputy director and senior civilian leader.

Our second witness is Cybersecurity Infrastructure Security Agency Director Jen Easterly. Director Easterly also has a strong record of Government service, including two tours of the White House during both the Obama and Bush Two administrations. An Army veteran of 20 years of service, she was responsible for standing up to Army's first cyber battalion and was instrumental in the design and creation of the United States Cyber Command.

Before we begin receiving testimony, I would like to recognize the impressive military service records of both of our witnesses and thank them for all, and all the veterans, for their service in advance of Veterans Day next week.

Thank you for your participation here today. I look forward to your testimony.

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

I now ask each witness to summarize their statement for 5 minutes, or do the best you can, beginning with Director Inglis.

STATEMENT OF J. CHRIS INGLIS, NATIONAL CYBER DIRECTOR, EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

Mr. INGLIS. Chairman Thompson, Ranking Member Katko, distinguished Members of the committee and staff, thank you for the privilege to appear before you today and the honor to appear alongside Director Easterly. I am eager to update you on the Biden/Harris administration's progress in standing up the new Office of the National Cyber Director and to discuss the administration's approach to cybersecurity.

The President's commitment to cybersecurity is a matter of National security and is an issue of concern to all Americans, as evidenced by the positions he created, the appointments he made, as well as by the speed with which the administration continues to modernize defenses and bolster our security.

I am of course appearing before you today as the inaugural National cyber director, a position this Congress created in January, confirmed for me in June after nomination by President Biden. I am grateful for the confidence that the President and the Congress have placed in this role, for the opportunity to bring it to life, and for the cybersecurity and critical infrastructure resilience investments you are endeavoring to make in the proposed infrastructure investment and Jobs Act, and elsewhere. I remain committed to engaging with you as we can on these critical and shared imperatives.

To that end, I am pleased to tell you that the new office is making progress as full-fledged leader in these imperatives. On Thursday, October 28 we publicly released the National cyber director's first strategic intent statement, which outlines the strategic approach and the scope of the work that I intend the office to undertake. At the same time, we announced the designation of Chris DeRusha as the deputy National cyber director for Federal cyber security, a dual-headed title that he will hold along with his current role as the Federal chief information security officer. We will create unity of effort and unity of purpose in our shared mission to ensure the security of Federal networks. Both of these announcements lay the groundwork for the office's approach, but are certainly not the sum total of our intended endeavors. We continue to build out the National cyber director team and, equally important, relationships with key partners inside and outside of the Federal Government and will follow up in the very near future with a more concrete comprehensive description of our priorities and the strategic objectives that will guide our work for years to come.

The Office of the National Cyber Director is of course currently constrained by the lack of an appropriated budget and we continue to work with Congress to secure the resources we need to bring on key staff. Beyond the constraint this places on our ability to hire key staff members, make necessary procurement and acquisitions, and find permanent office space for our future, the lack of appropriations inhibits our ability to plan and delays our ability to quickly and fully make the expected contributions of the National cyber director.

That limitation notwithstanding, I am pleased to inform the committee that we have built a robust pipeline of talent and once appropriations are available expect to reach a total of 25 personnel on board by the end of December and a full complement sometime later in fiscal year 2022.

As I have testified previously to the Senate Homeland Security and Governmental Affairs Committee, the National cyber director looks to four key outcomes as its benchmark of success. Given the foundations that these priorities establish for accountability of the National cyber director, I will comment briefly on them here.

First, the Office will drive coherence across the Federal enterprise, ensuring that we build, operate, and defend digital infrastructure under control of the Federal Government and support the private security with unity, purpose, effort, and messaging.

Second, we will zero in on improving private-public collaboration, supporting and building on the work of CISA and others.

Third, in close collaboration with the Office of Management and Budget, we will ensure that the U.S. Government is aligning its resources to its aspirations and accounting for the execution of cyber resources entrusted to its care.

Finally, the Office will work to increase present and future resilience not only within the Federal Government, but across the American digital ecosystem, in technology, the skills of our people, and in roles and responsibilities. This is, of course, a big task which we have initiated by exercising incident response and planning processes and we will continue to evolve these processes so they are future-proved for tomorrow.

None of this work occurs in a vacuum and much of the credit for progress in developing these themes and in the work of putting them into practice must go to my partners on the National Security Council, my colleague sitting alongside me, Director Easterly, and many others serving in the Federal cyber ecosystems. The challenges we face are daunting and overcoming them will require realizing a digital ecosystem that is resilient by design and robustly defended, a policy and commercial environment that aligns actions to consequences, and ensuring that public and private sectors proactively and decisively collaborate.

Although the Office of the National Cyber Director is a young and still small office, we have made significant progress and are building robust relationship with our inter-agency partners. When funding is in place and with the continued leadership and support of this Congress, the ONCD will be in a strong position to lead in enhancing the security and resilience of our Nation's cyber ecosystem.

I thank you for the opportunity to testify before you today. I look forward to your questions.

[The prepared statement of Mr. Inglis follows:]

PREPARED STATEMENT OF J. CHRIS INGLIS

NOVEMBER 3, 2021

Chairman Thompson, Ranking Member Katko, distinguished Members of the committee, and your staff—thank you for the privilege to appear before you today, and the honor to appear alongside Director Easterly. I am eager to update you on the Biden-Harris administration's progress in standing up the new Office of the National Cyber Director (ONCD) and to discuss the administration's approach to cybersecurity. The President's commitment to cybersecurity as a matter of National security is evident both by the positions he created and appointments he made, as well as the unmatched speed with which the administration continues to act to modernize our defenses and bolster our security in 11 short months.

But first, I wanted to recognize the history of this particular moment. I am appearing before you as the first National cyber director (NCD), a position the Congress created just last year, and then confirmed me for following my nomination by President Biden. I am grateful for the confidence that the President and Congress have placed in me in this role, as well as for the cybersecurity and critical infrastructure resilience investments that you are endeavoring to make in the proposed Infrastructure Investment and Jobs Act and elsewhere. I remain committed to engaging with you as we take on these critical, shared imperatives.

To that end, I am pleased to tell you that our new office is making progress as a full-fledged leader in those imperatives. On Thursday, October 28, I released the NCD's first Strategic Intent Statement, which outlines at a high level the strategic approach and scope of work I expect my office to undertake. At the same time, I announced the designation of Chris DeRusha as a deputy National cyber director for Federal cybersecurity, a dual-hatted title he will hold along with his current role as Federal chief information security officer, creating unity of effort and unity of purpose in our shared mission to ensure the security of Federal networks. Both of these announcements lay the groundwork for the ONCD's approach but are certainly not the sum total of our endeavors. We will continue to build out our leadership team and our strategic intent will soon be followed by a more concrete, comprehensive description of our priorities and strategic objectives that will guide our work for years to come.

While we will continue working with Congress to secure the resources we need to bring on key staff, I am pleased to inform the committee that we have built a robust pipeline of talent and expect to reach a total of 25 personnel on board by the end of December. Additionally, with limited funds from the President's Unanticipated Needs Fund, we have procured an office suite for the Office of the National Cyber Director at the 716 Jackson Place Townhome within the White House complex. I would emphasize, however, that without appropriations, we remain limited in our ability to hire key staff members, make necessary procurement and acquisitions, and find permanent office space for our future, full complement of staff. More fundamentally, the lack of appropriations inhibits our ability to plan and delays our ability to quickly and fully realize the role of the NCD.

As I have testified previously to the Senate Homeland Security and Government Affairs Committee, the ONCD looks to four key outcomes as its benchmark of success. Given the foundations these priorities establish for ONCD accountability, I will comment on them here.

- First, the ONCD will drive coherence across the Federal cyber enterprise—from coordinating with NIST in standards and guideline development, harmonizing our approach to supply chain risk management, supporting the Cybersecurity and Infrastructure Security Agency (CISA) in providing operational support to Federal agencies, and working in partnership with OMB to resource these key cybersecurity initiatives. This means ensuring that the Government is speaking with one voice, moving in the same direction, and, to the greatest extent practicable, sharing common priorities by which we can organize our collective efforts for maximum possible effect. Acting with unity of purpose and effort in the defense of our digital infrastructure is an absolute imperative.
- Second, the ONCD will ensure the continued improvement of public-private collaboration in cybersecurity. We will work closely with Director Easterly, CISA, the National Institute of Standards and Technology (NIST), and Sector Risk Management Agencies and seek to expand engagement and partnership across sectoral lines to new levels—because tackling the cyber challenges we face demands nothing less. The new Joint Cyber Defense Collaborative (JCDC), hosted by CISA and leveraging authorities, capabilities, and talents of the Federal cyber ecosystem in partnership with industry, will play an important role in this effort, and I look forward to working with the JCDC and other associated initiatives to ensure synergy across the Federal Government.
- Third, we will ensure that the U.S. Government is aligning our cyber resources to our aspirations and accounting for the execution of cyber resources entrusted to our care. We are in close discussions with OMB on how best to exercise the National Cyber Director's budget review and recommendations authority to identify investments that warrant an increase and those that may not be having the intended impact or effect. The ONCD intends to work with and through OMB in assessing and evaluating the performance of these investments and advising departments and agencies on recommended changes and updates in alignment with administration priorities.

- Finally, the Office will work to increase present and future resilience of technology, people, and doctrine, not only within the Federal Government, but also across the American digital ecosystem. We expect to do this by identifying common, emerging priorities in partnership with relevant departments and agencies and planning strategic, Government-wide initiatives to address them. That is a big task for which we will start by exercising our incident response and planning processes, and we hope to soon be working to ensure our workforce, technologies, and our structures and organizations are not only fit for purpose today, but are prepared for the challenges of tomorrow.

None of this work occurs in a vacuum, and much of the credit for progress in developing these themes and in the work of putting them into practice must go to my partners at the National Security Council, my colleague sitting alongside me—Director Easterly—and many others serving in the Federal cyber ecosystem.

Attempting to subvert this cyber ecosystem is attractive to our adversaries and frustrating to our allies because of how difficult it is for any one country or entity to have the benefit of a complete picture of actions and actors across its shared spaces. Cyber space allows a reach and efficiency of scale unrivaled in any other domain, meaning that our geopolitical competitors can have global reach and strategic effect; criminals and malicious actors can wield an unprecedented level of influence, impact, and coercion.

The general strategic imperatives emerging in response to these threats includes ensuring our digital infrastructure is resilient by design, proactively defended by collaborative coalitions, and backstopped by a doctrine that delivers benefits for good behavior and costs for bad. For the committee's consideration, I submit there are three categories of threat that are systemic, enduring, and globally diffuse in nature and warrant continued effort and attention.

- First is the vulnerability of our software supply chains. As we saw with the SolarWinds intrusion, sophisticated malicious actors are exploiting security and quality control seams among software service providers and software development pipelines, affording those actors the ability to rapidly "scale up" the reach and depth of their malicious activities across our digital ecosystem.
- Second is the pervasive vulnerability of the products and devices that enable opportunistic cyber attacks typified by ransomware actors and more sophisticated actors alike. Poor security practices, insecure design, short-sighted approaches to doctrine, and a lack of cyber talent among the workforce remain wide-spread, even in the face of known flaws, shortcomings, and vulnerabilities. Propagating best practices—including enforcing accountability for those who do not adhere to those practices—will be critical to righting the ship.
- Finally, we must remain laser-focused on maintaining the integrity of our information and telecommunications infrastructure against high-risk actors. Large portions of the hardware supply chain underpinning our most critical such technologies are located in countries that could leverage it for intelligence gathering or disruption at global scale.

These threats are serious and are receiving urgent and aggressive attention from the Biden-Harris administration. The administration is also, however, looking beyond these immediate threats and toward how to shape the future of cyber space so that such threats are systemically blunted or mitigated. This requires not only a thorough understanding of the nature of the threats, but also a clear vision for our digital ecosystem and what we want that ecosystem to achieve. With such a vision, we can pursue the fundamental, systemic changes necessary to realize the digital future in which we want to live. Such changes require clarity of accountability and depth of collaboration.

Accountability must flow in both positive and negative directions. It is rarely clear what it means to "do the right thing" when preparing or responding to a cyber incident, and harder yet to celebrate the benefits of an attack avoided. Conversely, the consequences for failing to take appropriate security steps are not always clear, even for those who knew (or should have known) how to secure their systems and who had the resources to do so, yet still chose not to do it. A key priority for the ONCD will be examining roles and responsibilities between the public and private sectors so as to make the required clarity of responsibility more actionable. It is an oft-cited statistic that 85 percent of our critical infrastructure is owned and operated by the private sector, and that privately-owned critical infrastructure is increasingly core to the Government's imperative to protect and provide for National security. Shared defense is not a choice, but an imperative.

Incorporating these lessons into a modern social contract will also require us to consider which stakeholders in the digital ecosystem should be held accountable for what magnitude of responsibilities. As I articulated in our office's first Strategic Intent Statement, the complexity of our challenges in cyber space has too often resulted in responsibility for systemic cyber risk being devolved onto the smallest, least-sophisticated actors: Individuals, small businesses, and local governments. The potential consequences of one key individual's password being compromised are simply too grave; tools like multi-factor authentication are a critical means to staunch the bleeding, but are not in and of themselves a systemic remedy. It is unreasonable to ask everyday Americans to maintain constant digital vigilance without also looking to key stakeholders to shoulder a greater share of this ecosystem-wide burden, especially those firms charged with operating and securing our information and communications systems and networks. How and where this burden reallocation should happen will be one of our preeminent objectives.

To achieve these and other objectives, it is clear that more routine and explicit statements of priorities and guidance on a year-to-year basis will support Departments and agencies in their efforts to set their own planning and operational priorities. The Federal Government undertakes a vast array of actions and programs to support and defend the private sector in cyber space; ensuring coherence across these lines of effort will be key in ensuring these initiatives are always mutually supporting and never redundant. Realizing this unity of effort and unity of purpose will continue to be a core guiding principle in all that we do. We have the good fortune of having a number of capable agencies at the forefront of securing and defending cyber space—CISA, FBI, Department of Defense, the National Security Agency, Department of Energy, and NIST, among others—whose roles complement one another and who, working together, strengthen our defense of cyber space in ways that could not happen if they were in competition or isolation. The more we can support these agencies' synchronized efforts and partnerships, with each other and the private sector, the greater the return on our investment will be for the American people.

The Biden-Harris administration has already made progress in addressing these issues and countering the threats we face in cyber space—most recently during last month's 30-nation summit on ransomware. On May 12, 2021, President Biden issued Executive Order 14028, Improving the Nation's Cybersecurity, taking bold, aggressive action to transform Federal Government cybersecurity for the better, and through that, to improve the security of critical infrastructure for all Americans. Since the President signed the Order, OMB, CISA, NIST, and others in the interagency have worked tirelessly to ensure its successful implementation. This includes developing contracting requirements, implementation guidance, cybersecurity expectations, information-sharing improvements, and incident notification requirements. Our expectation is that the Federal Government's purchasing power is great enough that the requirements in the Executive Order will drive improvements throughout industry, even outside of direct contractual relationships with the Government.

The President has also taken aggressive action to secure the Nation's critical infrastructure. His Industrial Control Systems Cybersecurity Initiative has already driven improvements in the electricity and pipeline subsectors and will soon expand to other areas. On July 28, he signed a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, which among other things directed CISA and NIST to develop performance goals for critical infrastructure cybersecurity. Director Easterly can give you more details about the terrific progress CISA and NIST have made in this area.

Steps like these are critical to ensuring that critical infrastructure owners, whether public or private sector, implement necessary security measures and become more accountable for their responsibility to the broader economic and digital ecosystem in which they reside. The importance of this dynamic has been reinforced by recent ransomware attacks against critical infrastructure entities. The Colonial Pipeline attack was a stark illustration of how the increasingly digitized nature of every part of our commercial ecosystem can create cascading, physical consequences. We hope that this real-world example will catalyze stakeholders across the public and private sectors to implement security controls commensurate with the importance of their operations.

These are daunting undertakings, and overcoming them will require realizing a digital ecosystem that is resilient by design, a policy and commercial environment that aligns actions to consequences, and ensuring public and private sectors are postured to proactively, decisively collaborate. Although the Office of the National Cyber Director is a young and still small office, we have made significant progress, and are building robust relationships with our interagency partners. When funding is in place, and with the continued confidence and support of this Congress, ONCD will be in a strong position to lead in enhancing the security and resilience of our Nation's cyber ecosystem. Thank you for the opportunity to testify before you today, and I look forward to your questions.

Chairman THOMPSON. Thank you.

Director Easterly.

STATEMENT OF JEN EASTERLY, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. EASTERLY. Great. Thank you.

Chairman Thompson, Ranking Member Katko, Members of the committee, thanks very much for the opportunity to testify today.

I am really thrilled to be here as your partner in protecting the American people from cybersecurity threats. We know that cybersecurity is a team sport, so I am also honored to testify before our Nation's first cyber director, my teammate and friend, Chris Inglis.

I want to start by also thanking this committee for your steadfast support in ensuring that CISA has the resources and authorities need to carry out the critical and substantial mission of the agency.

As you know, CISA serves both as the operational lead for Federal cybersecurity and as the National coordinator for critical infrastructure security and resilience. Our goal is to lead the National effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. The mission is challenging to execute and the stakes couldn't be higher if we fail.

Our mission can only be accomplished through strong collaborative partnerships and collaboration is built into our DNA at CISA. Partnerships are our strength, our ability to share information broadly about threats and vulnerabilities to enable early warning and prevent other victims from getting attacked. This is what I consider one of CISA's most important superpowers, our authorities to share information broadly with a variety of key stakeholders.

Now, as we evolve our approach to cybersecurity, my goal as director is to fundamentally shift the paradigm from public-private partnership into public-private operational collaboration. From information sharing into information enabling. Timely, relevant, and most importantly, actionable data that network defenders can use to increase the security and resilience of their networks.

Powering this shift is the new Joint Cyber Defense Collaborative, or JCDC, build off the concept of the Joint Cyber Planning Office. Authorized and resourced by Congress, the JCDC is driving two key changes. First, it is the only Federal cyber entity that by statute is required to bring together the capabilities across the Federal Government, State and local partners, and our Nation's critical infrastructure owners and operators. We are working closely with the largest cloud providers, internet providers, cybersecurity companies, and Federal partners, like FBI, NSA, and the National Cyber Director, to take collective action against urgent cyber risks.

Second, it is the first effort to focus on creating, exercising, and executing cyber defense plans that proactively address risk before an incident occurs. This effort is a major step forward, leveraging unique capabilities of Government and the private sector to drive risk reduction at scale.

We are already yielding positive results. We are validating and sharing information across broad swaths of partners in multiple sectors and producing measurable mission impact. Last month we utilized JCDC partner information with FBI and NSA to develop and issue joint guidance against BlackMatter ransomware that critical infrastructure entities are actively using to protect themselves.

Going forward we are going to focus on defining a robust planning agenda and producing plans to adjust ransomware risks and threats to cloud infrastructure.

We are also taking urgent steps to reduce National cybersecurity risks. This morning we issued a new Binding Operational Directive that fundamentally changes how the Federal civilian Government addresses vulnerabilities being actively exploited by our adversaries. Under this directive Federal agencies must now fix vulnerabilities identified by CISA within specified time frames and update their security programs to effectively account for these requirements. This directive will significantly improve the Federal Government's vulnerability management practices and degrade our adversaries' ability to exploit known vulnerability. While the BOD only covers Federal civilian agencies, we strongly recommend that every network defender review the known vulnerabilities posted publicly at CISA.gov and prioritize urgent remediation.

I was gratified to see significant reports for this directive, to include from this committee.

I also consider our partnership with Congress, and specifically this committee, as absolutely essential to CISA's mission success. Last year's NDAA included significant new authorities for CISA, to include the administrative subpoena. We have issued over 30 of these that have directly resulted in mitigation of numerous vulnerable devices. We are also positioning CISA to conduct persistent hunt across Federal civilian networks through deployment of endpoint detection and response tools.

Another factor critical is our people. I want to make CISA the place where the Nation's best cyber defenders and security professionals want to work. We are making positive strides on this front. Just last week we announced that Washington Secretary of State Kim Wyman will be joining CISA to lead our election security efforts. I am thrilled about welcoming her to the team at the end of this month.

I am also pleased to finally leverage the Cyber Talent Management System later this month. CTMS will help CISA cut time to hire, reduce bias, and ensure that we are assessing the right skills while enhancing work force diversity. There are a number of areas where we must continue strengthening CISA and I am grateful for the committee's work to advance key legislative priorities, including cyber incident reporting, new State and local government cybersecurity grant opportunities, and codifying key CISA ICS authorities, like the CyberSentry Program.

You have my commitment to continue working together as partners to advance these and other crucial legislative priorities.

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

[The prepared statement of Ms. Easterly follows:]

Prepared Statement of Jen Easterly

November 3, 2021

Chairman Thompson, Ranking Member Katko, and Members of the committee, thank you for the opportunity to testify on how the Cybersecurity and Infrastructure Security Agency (CISA) is positioned to enhance the security and resilience of our Nation's Federal networks and critical infrastructure.

I am truly honored to appear before this committee today to share my vision for CISA. Since being sworn in as director in July, I continue to be impressed with the talent, creativity, and enthusiasm of the dedicated CISA employees I am entrusted to lead. As I have shared with my team every day, I have the best job in Government.

At CISA, our mission is to lead the National effort to understand, manage, and reduce cyber and physical risk to our critical infrastructure. Our vision is a secure and resilient critical infrastructure for the American people. At the heart of this mission is partnership and collaboration. Securing our Nation's cyber and critical infrastructure is a shared responsibility, and has never been more important than it is today. At CISA, we are challenging traditional ways of doing business and are actively working with our Government, industry, academic, and international partners to move from traditional public-private partnerships to public-private operational collaboration.

WHO WE ARE

Established by the CISA Act of 2018, CISA is the Nation's Cybersecurity and Infrastructure Security Agency.

While our programmatic mission areas deal in cyber defense, infrastructure security, and secure and interoperable communications, holistically, as one CISA, the organization is comprised of teams of individuals with expertise across a wide spectrum of professional backgrounds and disciplines. Each and every one of them rely on each other to achieve our shared objectives. We recognize the connective tissue that binds us together and ensures we are able to be successful in our mission to lead the National effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Our core values represent the fundamental tenets of our CISA organization: Collaboration, innovation, service, and accountability. Living these core values every day with a growth mindset are the pathways to our mission success.

To achieve success in our cybersecurity mission, we build the National capacity to defend against cyber attacks and work with our Federal partners and provide them with cybersecurity tools, incident response services, and assessment capabilities to safeguard the Federal civilian Executive branch networks that support our Nation's essential operations. We strengthen our Nation's cyber defense by leading asset response for significant cyber incidents and ensuring that timely and actionable information about known cyber threats and incidents is shared with Federal and State, local, territorial, and Tribal (SLTT) officials, as well as our international and private-sector partners, to ensure the security and resilience of our critical infrastructure.

Within our infrastructure security mission, we enhance the protection of critical infrastructure from physical threats through enabling risk-informed decision making by owners and operators of critical infrastructure. Our activities include conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance Nation-wide. Our infrastructure security program leads and coordinates National efforts on critical infrastructure security. This includes reducing the risk of successful attacks against soft targets and crowded places, such as in our schools, and from emerging threats. CISA also leads efforts to secure our Nation's chemical sector infrastructure, enhancing security and resilience across the chemical industry to reduce the risk of hazardous chemicals being weaponized. To this end, CISA has developed voluntary and regulatory programs and resources to help stakeholders—private industry, public sector, and law enforcement—secure chemical facilities from many threats: Malicious cyber activity, biohazards, insider threats, and theft and diversion.

Key to success in our cybersecurity and infrastructure security mission is identifying and understanding risk, especially risk that is systemic to our Nation's critical networks and infrastructure. CISA's National Risk Management Center leverages sector and stakeholder expertise to identify the most significant risks to the Nation, and to coordinate risk reduction activities to ensure critical infrastructure is secure and resilient both now and into the future. The goal of the NRMC is to create an environment where Government and industry can collaborate and share expertise to enhance critical infrastructure resilience by focusing on collective risk to National Critical Functions including through key initiatives such as election security, Fifth Generation Network technology, supply chain risk mitigation, and more.

Our emergency communications mission works to ensure reliable and resilient, real-time information sharing among first responders during all threats and hazards. CISA enhances National security and public safety interoperable communications at all levels of government across the country through training, coordination, tools, and guidance. We lead the development and implementation of the National Emergency Communications Plan to maximize the use of all communications capabilities available to emergency responders—voice, video, and data—and ensure the security of data and information exchange. CISA assists emergency responders and relevant Government officials with communicating over commercial networks, using priority telecommunications services during natural disasters, acts of terrorism, and other man-made disasters.

Underpinning our mission is CISA's commitment to preserving individual privacy, civil rights, and civil liberties protections in our operations and our engagements. We recognize that when Congress statutorily required CISA to have a privacy officer for the agency that we needed to—by default—fully integrate privacy, civil rights, and civil liberties protections into everything we do. We are proud of the fact that a number of our activities have the added benefit of enhancing privacy, civil rights, and civil liberties.

THREAT LANDSCAPE

In our globally interconnected world, our critical infrastructure and American way of life face a wide array of serious risks with significant real-world consequences. Today, the critical functions within our society are built as "systems of systems," complex designs with numerous interdependencies and systemic risks that can have cascading effects. This is something we have known for years as nation-state actors and criminals increasingly leverage both cyber space and traditional physical means in their attempts to subvert American power, American security, and the American way of life. Many of these challenges are exacerbated by the COVID–19 pandemic, which has led to an unprecedented number of Americans working from home, meaning the potential for malicious actors to exploit vulnerabilities has expanded exponentially. Additionally, we are realizing the impact of climate change on our National security and economic prosperity interests, and must work with the infrastructure security and resilience community to mitigate them—through planning efforts that include community resilience, and a whole-of-Government guidance and information-sharing effort.

At the same time, ransomware has become a scourge on nearly every facet of our lives, and it's a prime example of the vulnerabilities that are emerging as our digital and our physical infrastructure increasingly converge. Earlier this year, we saw the Colonial Pipeline attack shutter gas stations along the East Coast and the JBS attack cause certain food prices to rise. We have also seen ransomware attacks on schools, police departments, hospitals, and small businesses around the country, and they are growing in number, scale, and sophistication. Disrupting this scourge requires a whole-of-Nation effort, and the Department of Homeland Security (DHS) helps lead that effort, and led the development of a whole-of-Government website, stopransomware.gov, which provides users with a central, authoritative source for guidance, toolkits, and other resources from across the Federal Government. CISA's mission focuses on raising awareness before disaster strikes, and supporting victims when it does. We help potential victims understand their risk, reduce vulnerabilities, and mitigate the impact if they are attacked. When attacks threaten our critical infrastructure or National critical functions, we offer on-site assistance to help victims get back on their feet and share operationally relevant information with our partners and the public to prevent the spread to other potential victims and sectors. Our partners can use these resources to reduce the risk and impact of ransomware attacks.

While cyber intrusions and ransomware dominate the recent headlines, physical threats to our people and our critical infrastructure remain a top concern. Terrorism, mass shootings, and other forms of targeted violence continue to threaten our schools, places of business, houses of worship, and other soft targets and crowded places. In 2020 alone, there were more than 12,000 explosive-related incidents and more than a 70 percent increase in domestic bombings, according to the Department of Justice's U.S. Bomb Data Center. These types of physical threats can cause mass casualties, lead to hundreds of millions of dollars in damage, and cause cascading damage across vital physical and cyber infrastructure. From a broader perspective, as modern threats become more sophisticated, it is important to stay vigilant and take proactive measures to enhance the security and resilience of our communities and critical infrastructure.

The risks we face today are complex. They are dispersed both geographically and across a variety of stakeholders. They are challenging to understand, and even more difficult to address. But here at CISA we have an incredible team ready to execute our mission in collaboration with a diverse group of partners across all sectors. CISA will continue to support and empower our partners to secure and defend America's cyber ecosystem and critical infrastructure. While we face an array of cyber and physical threats, our adversaries continue to push mis- and disinformation in an attempt to divide Americans and cast doubts about the legitimacy of our elections and our democratic processes, among other issues. These are just a few of the threats we face, and tackling them is no easy feat. It will take teamwork and a relentless dedication to our mission. Fortunately, in my first 100+ days at CISA, it's become clear that we are up to the challenge.

PRIORITIES

For me, it was clear from my first days as director that people are CISA's No. 1 asset. My goal is for CISA to be the place where our Nation's best cyber defenders and security professionals want to work. I am intently focused on building a culture of excellence that prizes teamwork and collaboration, innovation and inclusion, ownership and empowerment, transparency and trust. To that end, we are committed to attracting and retaining world-class talent by implementing a vibrant, and providing an end-to-end talent management ecosystem that spans from recruiting and hiring, to on-boarding and integration, mentorship and coaching, certification and training, recognition and promotion, and succession planning and retention.

Even as we focus on cultivating our workforce of today, it is important to recognize that our efforts also play an important role in helping build the cyber workforce of tomorrow. On November 15, 2021, the Department will launch the Cybersecurity Talent Management System (CTMS) and begin hiring employees in the DHS Cybersecurity Service (DHS–CS). DHS, including CISA, will use this system to grow the future cybersecurity workforce with greater flexibility to attract and retain the best cyber talent.

As one of the early women graduates of West Point, I have a deep appreciation for the importance of having diversity of background and experiences represented in the room when key decisions are made. That is why I am focused on keeping hiring centered around diversity by hosting specialized events, applying innovative sourcing techniques, and implementing branding campaigns as a means of attracting top talent. I will continue working to employ new and innovative recruitment and hiring strategies that cut the time to fill positions, reduce bias, and decrease unnecessary assessment while enhancing the diversity of our workforce. My vision is to make CISA a leader in diversity among both the Federal Government and the broader tech workforce.

Collaboration to achieve these workforce and diversity goals is fundamental. So are our efforts to build relationships, trust, and connectivity with State and local officials, private sector, and our interagency partners. CISA is meant to be an agency that is agile, flexible, and able to respond quickly to changing threats through collaboration with both the public and private sectors. And, to this end, we sustain our trusted and effective partnerships between Government and the private sector, which are the foundation of our collective effort to protect the Nation's critical infrastructure. With large portions of critical infrastructure in our country owned and operated by the private sector and municipalities, those partnerships are vital to ensuring a safe and secure America. Our partners bring expertise and a unique ability to drive climate change impact and cyber defense activities in their jurisdictions, and it is precisely this assembly of knowledge that will allow us to be better prepared to achieve deep operational collaboration that ultimately reduces the greatest risks to our Nation.

UPDATES AND ACCOMPLISHMENTS

There is a lot of good work being done at CISA. I am particularly proud of the agency's efforts to stand up a new initiative called the Joint Cyber Defense Collaborative or JCDC, meet important deadlines from President Biden's Executive Order on Improving the Nation's Cybersecurity, and expand and strengthen key partnerships during my first 100 days. Allow me to elaborate on each of these accomplishments.

In August, CISA launched the JCDC, which unifies cyber defense capabilities currently spread out across multiple Federal agencies, many State and local governments, and countless private-sector entities. It also leads the development of our

Nation's cyber defense plans by working across the public and private sectors to unify deliberate crisis and action planning, while coordinating an integrated execution of these plans. Our goal with the JCDC is to bring together key Federal partners with private sector and SLTT partners who have critical visibility and ability to understand the threat landscape by virtue of their businesses and responsibilities, and to plan and exercise against the most serious threats to our Nation.

The JCDC's initial focus is on tackling ransomware and developing a planning framework to coordinate incidents affecting cloud service providers. Almost 2 months into this collaboration, we are already seeing good progress. Our relationships with our private-sector partners continue to grow as we share more information and collaborate around key operational issues. We are also validating and sharing information daily across broad swaths of partners in multiple sectors. For example, last month, CISA, the Federal Bureau of Investigation, and the National Security Agency issued guidance to help critical infrastructure entities protect themselves against BlackMatter ransomware as a service, using information provided by JCDC members.

While it is early days, the JCDC is already leveraging the skill sets, expertise, capabilities, and visibility of its members to better protect critical assets against cyber threats. This shifting paradigm will enable us to transform public-private partnerships into public-private joint action, and information sharing into information enabling—timely, relevant, and actionable. Together, Government at all levels, industry, and our international allies—because cybersecurity does not begin or end at our borders—will bring to bear our collective capabilities to sustainably shift the balance of power in favor of cyber defenders. We will plan together, exercise together, and act in unison to address both immediate threats and overcome longer-term strategic and systemic cybersecurity challenges. Ultimately, we envision that this integrated public-private collaboration will drive the collective defense of cyber space to create a secure and resilient cyber ecosystem for all Americans, and we look forward to expanding this operational collaboration going forward.

Election security also remains a top priority for CISA. As you know, a number of elections concluded just yesterday as part of the 2021 cycle, including prominent gubernatorial races in Virgina and New Jersey. In support of our election security efforts, CISA hosted an Election Operations Room at our Arlington Office, and virtually around the country, to present an integrated Federal coordination point for support to State and local election officials holding elections this cycle. Partners from the interagency and the election community collaborated in real time to share information about election risks and be prepared to respond as needed. In addition, I recently announced that secretary of state Kim Wyman will be joining CISA as our new election security lead. Kim has recently been the secretary of state in Washington, and she is joining to help ensure that we have a senior member of the election community guiding our efforts to address a range of threats to America's democratic process to include cyber and physical threats, as well as mis- and disinformation. I am extremely excited to welcome Kim to CISA.

Another area I want to highlight is CISA's on-going work to implement the May 12, 2021, Executive Order 14028, Improving the Nation's Cybersecurity signed by President Biden. This Executive Order aims to directly address the persistent and increasingly sophisticated malicious cyber threats the Nation has faced over the past several months, and tasks Federal agencies to make bold changes to improve the Nation's cyber posture. The efforts outlined in the Order aim to improve Federal cybersecurity posture and incident response capabilities, limit supply chain risk to the Federal Government, and increase CISA's visibility across Federal and contractor networks. CISA has been tasked with leading or supporting over 35 unique efforts, many with short time lines highlighting the urgency of the work to be done. I am proud to say that CISA met all of our deadlines in support of the Executive Order, to include:

- Driving adoption of modern, secure, and resilient networks, including through the Cloud Technical Reference Architecture, released for public comment earlier this month and co-developed with the U.S. Digital Service and GSA's FedRAMP program;
- Advancing the adoption of leading security practices necessary to address highly adaptive adversaries in collaboration with OMB and other Federal partners, including publication of a Secure Cloud Technical Reference Architecture and a Zero-Trust Maturity Model;
- Raising the bar for incident response by publishing a Vulnerability and Incident Response Playbook to Federal agencies, which will ensure that all agencies will operate from the same sheet of music during incidents, and enable a coordinated a whole-of-Government incident response effort, building on lessons learned in recent incidents;

- Ensuring that CISA has access to all necessary information about incidents affecting Federal agencies by providing recommendations to the Federal Acquisition Regulatory Council that require broader sharing of data by Government contractors, in response to incidents. Such sharing will include the Federal agency holding the contract, as well as with CISA. The recommendations to the FAR also establish procedures for sharing appropriate information with interagency partners to aid in their collective, on-going cyber defense operations;
- Establishing a plan to dramatically expand our visibility into cybersecurity risks affecting Federal networks through deployment of endpoint detection and response (EDR) capabilities and enabling "persistent hunt" activities as authorized by Section 1705 of the fiscal year 2021 National Defense Authorization Act; and
- Prioritizing Federal supply chain security by working with OMB to direct a review of over 650 unique cybersecurity-related contract clauses in place across the agencies and recommending to the FAR Council a baseline for cybersecurity that Federal contractors must meet to lower risk to the Federal systems they support.

The work outlined in the Executive Order is no small task; the administration asked CISA and agencies to rethink how we approach vulnerability and incident response, how we approach purchasing IT goods and services, how we design and secure our networks, and how we work together to share information. Our work applies not only to the Federal Government, but also to government at all levels, and the private sector, as we seek to work to ensure that we collectively drive adoption of strong security practices to materially reduce cybersecurity risks.

Building on the Executive Order, this summer, the President also issued a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. The reality is that cybersecurity needs vary among critical infrastructure sectors, but we cannot evolve our Nation's cybersecurity posture without baseline cybersecurity goals that are consistent across all sectors. Additionally, there is also a need for security controls for select critical infrastructure that is dependent on control systems. Working in partnership with the National Institute of Standards and Technology (NIST), at the end of last month, we issued the preliminary cybersecurity performance goals based on 9 categories of best practices. These goals are part of a whole-of-Government effort to meet the scale and severity of the cybersecurity threats facing our country. Our safety and security rely on the resilience of the companies that provide essential services such as power, water, and transportation and these performance goals should be the standard cybersecurity practices and postures that the American people can trust and should expect for such essential services. It takes all of us committed to action, and that requires harnessing the power of operational collaboration.

Our successes would not be possible without the outstanding and dedicated CISA workforce. For me, it is all about the people—we will be successful because of our people. While I am committed to working to attract and retain world-class talent, one of my top priorities is also to build a workforce that looks like America and has the skills needed to meet the threats of the future. To that end, I am very proud that, in addition to DHS's collaboration with the Girl Scouts of the USA, CISA recently announced a partnership with Girls Who Code, with the intent of closing the gender gap in cybersecurity and developing pathways for young women to pursue careers in cybersecurity and technology. Partnering with Girls Who Code will provide real solutions to tackle diversity disparities and bring together a stronger community of women in technology and cyber. CISA and Girls Who Code will work hand-in-hand to improve the awareness of these careers in cyber, while building tangible pathways for young women, especially young women of color, to get hands-on experience and find opportunities—whether in the private sector, non-profit sector, or part of Government.

CONCLUSION

Our Nation faces unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals, and CISA is at the center of our National call to action. In collaboration with our partners and with the support of Congress, we will make progress in addressing this risk and maintain the availability of services critical to the American people.

Thank you again for the opportunity to appear before the committee. I look forward to answering your questions.

Chairman THOMPSON. I thank the witnesses for their testimony.

I remind each Member that he or she will have 5 minutes to question the witnesses.

I now recognize myself for questions.

This is a question to both of you. The recent surge of high-profile cyber attacks, from Colonial Pipeline to JBS, has called into question the Federal Government's voluntary framework for securing critical infrastructure. Certainly the security directives issued by TSA earlier this year marks a significant shift in the Federal Government's approach. Just last week, as I indicated in my opening statement, the administration urges Congress to give EPA more authority over cyber standards for water.

With that in mind, do you envision the administration moving to impose security standards on additional critical infrastructure sectors? If so, and I guess my—do you envision it, yes or no?

Mr. INGLIS. Mr. Chairman, thank you very much for the question. It is an important question.

I would say that the answer to the question is yes. I think the context matters greatly. This must be done in partnership and collaboration with the private sector insomuch as we work together to determine what the shape, the form, the function is of digital infrastructure to ensure that innovation, capacity, generation, continues to take place in the private sector. We allow market forces and the leadership of the private sector to take their proper role. Then, by exception, when necessary impose the further non-discretionary standards that are required. We have done that in other industries, like the aviation safety industry or the automobile industry. I think that this is an equally appropriate place to do that for the critical services that our Nation depends on.

Chairman THOMPSON. Well, thank you. So you said yes and then you went on to define the role. So thank you very much.

Director Easterly.

Ms. EASTERLY. Thank you for question, Chairman.

I would agree with everything that National Cyber Director Inglis said. I would add two points. As we know, 85 percent of critical infrastructure is in private hands. So this really is based on a voluntary regime, as you pointed out. We know that collaboration and trust is absolutely critical to the model of how CISA works with the private sector. So we are going to continue to build that trust and build that collaboration. Notwithstanding whatever regulations may come into place, we are going to focus on the collaboration piece.

I would add though, in order to support any regulation that may come into force, we are doing a lot of work on articulating what are the cybersecurity baseline standards and goals. At the end of September we released those goals specific to industrial control systems and we are working on other goals that were tasked out by the White House National Security Memorandum.

So we are at least at a minimum letting all of our critical infrastructure sectors know what is expected to ensure the security and resilience of their infrastructure.

Chairman THOMPSON. Thank you very much.

I think, Director Inglis, you kind-of addressed this question, but—in your opening statement—do you have the necessary authorities and resources to do your job?

Mr. INGLIS. Mr. Chairman, thank you very much for that question.

I believe that I have sufficient authorities and resources, given the appropriations that we expect in the very near term, to make the difference that is expected. We will, based upon experience, come back and determine whether or not they need to be refined in some way, shape, or form. But for the moment I believe I have the authorities and expected resources to make the difference expected.

Chairman THOMPSON. Director Easterly.

Ms. EASTERLY. Well, first of all, thank you very much to this committee because you have done a lot to give us the authorities and resources. But we appreciate what is in potential upcoming legislation, to include cyber incident reporting, a recognition of grant programs for our State and local partners, the codification of CyberSentry and our role in ICS.

To the resource question, we have gotten a lot of resources and I think it is great to get resources specifically for cyber defenders and infrastructure defenders. I would say though what is also very important to us are those mission enablers that will help us execute the resources and the funding that we are getting, human resources, our people, our chief human capital officer, our finance, our acquisition authorities. So we are going to need to bolster those mission enablers to enable us to actually execute everything that you have given us.

Chairman THOMPSON. Thank you.

So if I hear you correctly, with that you are going to still have to find some bodies, right, to carry that mission forward?

Ms. EASTERLY. Say that again, Chairman.

Chairman THOMPSON. I think you are going to have to have some people or bodies to carry the missions forward.

Ms. EASTERLY. Absolutely.

Chairman THOMPSON. As a committee we have heard quite often that somehow we don't have enough qualified individuals to staff our agency. Do you find the lack of staff is a potential problem for CISA?

Ms. EASTERLY. We are working hard to build out our capability and capacity. We have a lot of vacancies that we are working very hard to fill. Two of the things that I am trying to do deal with this, first of all to really do an analysis of how we can accelerate our hiring. All of the steps that are required, how do we actually create some efficiencies on that because having just come from 4½ years in the private sector, I think it takes way too long to be able to bring people into the Federal Government. I think that is incredibly important to be able to streamline that process, sir.

The second thing that we are doing is really leaning into cyber talent management system authorities, which come into force the 15th of November that will give us greater flexibility to be able to hire based on aptitude and attitude, not based on degrees or certifications. It will allow us to be able to pay closer to market. So that flexibility I think will really help us close the gap to enable us to bring on the talent that will make us the agency that the Nation deserves.

Chairman THOMPSON. Thank you.

I yield to the Ranking Member.

Mr. KATKO. Thank you, Mr. Chairman.

Director Inglis, a quick question for you.

It is pretty clear that the authorities that CISA has and a cyber director are pretty well laid out and I understand the interaction between you two. One of the ones I kind-of struggle with is what is the role of the National Security Council within the cyber realm? If there are some issues that we need to work on there, what are they?

Mr. INGLIS. Yes, thank you for that question. That is a question we are asked on a fairly frequent basis and one that I think deserves a solid crisp answer.

I would say that as we look at it—I believe I am speaking for both Jen and myself—there actually is the need for a National Security Council leadership role in cyber for the following reasons: Typically in any domain of interest, cyber being one of those, we should consider bringing all instruments of power to bear, our intelligence assets, our diplomats, our financial abilities, our legal remedies. Typically bringing those instruments to bear in a coordinated fashion to achieve the appropriate desired conditions in the domain of interest, cyber being one of them, is traditionally the role of the National Security Council. We believe that that that remains appropriate in this space and therefore our colleague, deputy national security advisor for cyber emergency technology, Anne Neuberger, we think appropriately and fully fills that role as a complement to what Jen and I then do within the realm of cyber space.

Mr. KATKO. OK. I will leave it at that.

Director Easterly, I mentioned in my opening statement, I mentioned it several times before, we are getting to the point now where we are going to start having more requirements on the private sector. We also ask them many times to get us more information. I think the more information they get on their cyber attacks the better you can understand the playing field. The better you can understand the playing field, the better you can help them going forward. A common refrain you heard from the private sector is a lot of stuff goes to CISA—and this is before you time, mind you—a lot of information goes to CISA and not a lot of operational information comes back.

How are you doing trying to fix that issue and what do you plan to do going forward?

Ms. EASTERLY. Thanks for the question, Ranking Member Katko.

So it has been about 110 days. I think we are doing pretty good. But it is just a start.

Mr. KATKO. You don't have everything fixed in 110 days?

Ms. EASTERLY. I know, I failed miserably.

You know, I have a great appreciation for those comments because I spent the past 4½ years in the private sector and sometimes my observations were that the Government seemed disjointed, not coherent, and a black hole. So, frankly, I think we are doing a lot under Director Inglis' leadership and the leadership across the Federal Government to really ensure a coherent approach, that we are speaking with a coherent voice to the private sector. Frankly, it is one of the reasons why I am so excited about the Joint Cyber Defense Collaborative, the JCDC, because by statute it is the only cyber entity that brings together CISA and NSA and FBI and DoD and DoJ and ODNI and the Secret Service and the National Cyber Director. So that is a place where the private sector can come and expect accountability in one place and can go and say, we have given you this information, what are we getting back?

So that real-time conversation is happening. I will tell you we are already leveraging those partnerships from cloud security providers, from cybersecurity companies, to take that information to enrich what the Federal Government has and then to get that back, both to those companies, but importantly to critical infrastructure owners and operators and the State and local. As I said in my statement, we are looking to do not just sharing, but truly enabling. Because if we can't get information to network defenders in a timely way that allows them to use that information and that it is relevant and actionable, there is really no point in sharing information.

So we are looking to change that paradigm and I am very focused on ensuring that we are giving feedback and enriching what we get from the private sector.

Mr. KATKO. Thank you very much.

Following up on the critical infrastructure. I appreciate our discussion last week at CSIS on the importance of CISA having the capability to identify the most critical of critical infrastructure. Because, as you know, if everything is critical infrastructure then nothing is, right.

So while we may disagree on the best acronym for the effort, I think you said PSIES is a new one—Mr. Chairman we have got to learn now another one—it is clear we are seeking the same outcome here, right. It is paramount that we are understanding the single points of failure and layers of systemic importance across this ecosystem that have the potential for a cascading impact of compromise.

So can you briefly just discuss with me the importance and current state of play with CISA's Systemically Important Critical Infrastructure effort?

Ms. EASTERLY. Yes. Thanks very much for the question.

I do think it is incredibly important that we are able to articulate that infrastructure that is absolutely critical to Americans' way of life. We look at the lifeline sectors, water, transportation, communications, energy, we look at all of the 16 infrastructure sectors, but we also analyze them, sir, through the lens of National critical functions. Because, as we know, in today's society everything is connected, everything is interdependent, and therefore everything is potentially vulnerable as it rides on that technology backbone.

So, you know, inspired by some of the good work that came out of the Cyberspace Solarium Commission, the Systemically Important Critical Infrastructure, SICI, we have done some work on what we are calling PSIES which does sound like a better acronym, the Primary Systemically Important Entities. Again, those that have economic centrality, network centrality, and have logical dominance in those National critical functions. So we think it will end up to be about 150–200 entities that we really focus in on to be able to provide information. It goes back to the benefits and burdens question, but I absolutely think that we need to codify this.

So, to your point, sir, if everything is a priority, nothing is a priority. So I am a big proponent of the effort.

Mr. KATKO. Thank you very much.

Before I yield back I just want to note it is very important that you continue your collaborative relationship. I think the way you have things set up, you should be very proud and, like I said, you are a symbol for other agencies to follow. Instead of having turf battles you are getting things done and that is important.

Also know that with the Chairman and myself, don't wait for hearings, if you need something just pick up the phone and call us, OK.

All right. I yield back, Mr. Chairman.

Ms. EASTERLY. Thank you, sir.

Chairman THOMPSON. The gentleman yields back.

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

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank you for holding this hearing today and thank you and the Ranking Member for your bipartisan collaboration on cyber and many other issues.

I could not be more pleased to have the two witnesses we have before us today, two outstanding appointments. Take great pride in seeing the Nation's first National Cyber Director before us after more than a decade of trying to establish that position. I am glad it is finally established and that Director Inglis is the first inaugural director.

Five minutes is going to go by fast, so I am going to get right into my questions. But deeply appreciate the leadership you are both providing that are protecting the Nation's cyber space.

Director Inglis, I will start with you. In your testimony you mentioned that we can expect the Office of the National Cyber Director to "Issue more routine explicit statements of priorities and guidance on a year-to-year basis to support departments and agencies in their own planning and operational prioritization." I commend you for initiating this work. These year-to-year statements of priorities and guidance will address gaps in our medium-term planning that translate our cyber strategy into day-to-day work carried out by agencies.

Incidentally, this kind of activity is exactly what Congress intended for the National cyber director.

So on the subject of your Office's roles and responsibilities you testified before the Senate Homeland Security and Government Affairs Committee about a possible Executive Order in development that would delineate processes for your office, including around setting these yearly cyber priorities.

Can you update the committee on any plans to issue such an order?

Mr. INGLIS. Yes, Congressman Langevin. Thank you very much for the question.

I think that the statute has gone a long way and the policies that we have described have gone a further distance in describing what the roles and responsibilities are of the various players in this space. An Executive Order, we believe, is the essential capstone to that, to crisp up, at least for the moment, based upon the experience and the expectations we have, where we should then take this further. We are in discussion within the White House about when and how to effect an Executive Order that would bring additional clarity to these roles and responsibilities. I am confident that we will work our way through in weeks' to months' time to deliver such a thing.

Mr. LANGEVIN. Very good. Thank you. I do also want to commend you and thank you for your work on this Cyberspace Solarium Commission. It is a privilege to serve with you on that Commission.

Director Easterly, first of all congratulations and I thank you for the BOD that was issued earlier today. It is exactly the type of thing we need to do to get out ahead of cyber vulnerabilities, so thank you and CISA for that leadership.

We had a discussion a little bit earlier about the public-private collaboration, JCDC. So I was very pleased when you announced the creation of the Joint Cyber Defense Collaborative, or JCDC, in August and I think the JCDC will significantly improve the ability of the public-private sectors to collaborate on cyber defense efforts.

I would be curious on your further views on the importance of the public-private collaboration and I hope you can share—and, again, any further updates on CISA's progress in standing up JCDC. Anything you would like to add.

Ms. EASTERLY. No, sir. I mean we are really, really appreciative of those authorities. I know you championed the Joint Cyber Planning Office, which is a significant part of the Joint Cyber Defense Collaborative. I think it is really the thing that will make the difference, being able to be proactive as opposed to reactive in planning against the most serious threats to the Nation. I think it is something unique across the Federal Government from a cyber defense perspective. So I am really looking forward to putting that into action.

Mr. LANGEVIN. Very good. Thank you.

Also, Director Easterly, one idea to further the public-private collaboration developed by the Cyberspace Solarium Commission and adapted by Congressman Gallagher and into an amendment in this year's NDAA would create critical technology security centers to evaluate and test the security of devices and technologies underpinning our Nation's critical functions.

I would be curious to hear about your thoughts on this measure and how it could complement JCDC?

Ms. EASTERLY. I am very supportive of that measure, Congressman. I think it is incredibly important that we have an ability to understand. In particular, given everything that we have seen with respect to intrusions in our supply chains, that we understand the technology that is underpinning all of these infrastructures. So fully supportive. Would want to be able to leverage the JCDC and the partners within the JCDC to be able to understand some of the information that could be tested at some of those technology centers. So would look forward to that.

Mr. LANGEVIN. Last, very quickly, I took note of your comments that Aspen Cyber Summit on bureau cyber statistics and the need for better cyber metrics, your thoughts on potentially housing that at CISA?

Ms. EASTERLY. I am a huge fan of that. I think it is hard to say that you have reduced risk unless you know how to measure it. So believe we should have that Bureau of Cyber Statistics and I think it would make sense to house it at CISA.

Mr. LANGEVIN. Very good.

Thank you again for your answers, your outstanding leadership. I look forward to our future collaborations.

Mr. Chairman, I yield back. Thank you.

Chairman THOMPSON. The gentleman yields back.

The Chair recognizes Mr. Garbarino for 5 minutes.

Mr. GARBARINO. Thank you, Mr. Chairman, thank you, Ranking Member Katko, for having this hearing and thank you, Directors Inglis and Easterly for both coming today.

Director Easterly, I really enjoyed our conversation last week. We talked about a lot of different things, even with my babysitters I thought it was pretty productive. We talked about, and you brought it up in your opening testimony, about the cybersecurity pipeline and what you have been planning. You have talked now about—you know, and it is not all under your control, but it is a concern that you show that it is you show that you are fully staffed and now with the cyber talent management system coming on-line with the rules. What do you see as your job or the CISA's Office of the Chief Human Capital Officer, taking those rules and making sure that they work to make sure that CISA is fully staffed and properly staffed with the right people?

Ms. EASTERLY. Yes. Thank you for that question, because you know I think it something we are both passionate about.

I should first say we have fabulous people at CISA and this really is the best job in Government. But I believe that there is nothing more important than people. So we have actually spent a lot of the last 3½ months doing a couple of things. First, defining the core values and the core principles that underpin CISA's culture, identifying how we are going to build a talent management ecosystem that allows us not just to recruit the best people, but to ensure that we are training and certifying and mentoring and coaching and retaining those best people. That is incredibly important. We have done a careful analysis of all of the 20-plus steps that it takes to actually hire somebody into the Federal Government, which is way too onerous. You know, we were able to reduce by 13 percent the number of days that it takes to hire somebody, but it is still way too long. It is over 200. In the private sector I could bring somebody in like 60 days. So we need to fix all of that. But we are making progress on that. We have hired 500-some people, whereas last year it was just 200-some. So we are getting there, but not fast enough in my view.

So we are going to figure out how to fix the current process. I may come back to you and ask for your help if I need it.

Then we are going to aggressively implement CTMS, which allows me much greater flexibility, both to hire but also to figure out how to retain people and incentivize them. At the end of the day people want to come to CISA to defend their Nation, but given the competitive environment we also want to be able to pay closer to market.

So these new authorities will allow us to do that, sir.

Mr. GARBARINO. I appreciate it. Sounds like it is easier to get elected to Congress than to hire someone at CISA.

On a separate note, Ranking Member Katko and I have increasingly been concerned about the security of the Nation's information and communications technology. Specifically, we are concerned about the lack of progress from the Federal Acquisitions Security Council. We appreciate the transparency that CISA has provided to the committee regarding its role in FASC, but we understand that CISA is only one part of it.

Director Inglis, can you speak to the lack of progress we have seen from FASC and why now 3 years in there isn't much to show for it?

Mr. INGLIS. Yes. So thank you for the question. It is an important question, especially given the role that the Federal Acquisition Management Supply Chain Committee plays on the acquisition of the material that underpins the digital infrastructure that underpins our critical missions.

Having said all of that, 3 years is a long time, but I am pleased to report that in August of this year we concluded the rule-making process, gave CISA a leadership role on the FASC, have now charged the leader of that committee, who is one and the same as the deputy for Federal cybersecurity within the National cyber director, but at these same time the Federal chief information security officer, to move off in beginning to apply those rules, those processes, to determine how we manage the Federal supply chain.

We have a solid agenda for fiscal year 2022, the year that we are in, and we have every expectation that we will make significant progress in the time ahead. I would be happy to come back to this committee or to deal personally with any committee Member who is interested as to what those specific plans are, but to demonstrate progress in the very near-term.

Mr. GARBARINO. Great.

Well, and for either your or Director Easterly, with the authorization of FASC coming back in 2023, is there something that Congress should consider changing or—you know, you giving CISA a more essential role or is there something we should do differently in the re-authorization or change?

Mr. INGLIS. I think it is a very appropriate question. I think that you should hold us accountable for delivering value with the process and the authorities that we have at the moment. I do believe that it should be sustained past fiscal year 2023. We will come back to you to tell you what refinements we think are necessary.

Mr. GARBARINO. Director Easterly.

Ms. EASTERLY. Nothing to add.

Mr. GARBARINO. Great. I appreciate that.

I yield back. Thank you.

Chairman THOMPSON. The gentleman yields back.

The Chair recognizes the gentleman from New Jersey, Mr. Payne, for 5 minutes.

Mr. PAYNE. Thank you, Mr. Chairman and Ranking Member, for having this timely, timely hearing.

Let us see. The Colonial Pipeline ransomware attack was a stark reminder that cyber attacks on critical infrastructure can have physical real-world consequences that ripple across sectors throughout the economy. The longer it takes to restore operations, the more of those downstream effects can snowball in ways that matter for the health, safety, and financial stability of individuals and families and communities.

Director Easterly, what is CISA doing to promote not just the security but also the resiliency of critical infrastructure like pipelines to make sure they are able to get back up and running in the event of a cyber-related disruption?

Ms. EASTERLY. Well, thanks very much for that question.

You are absolutely right. What we have seen this year is cyber attacks that are manifesting against our critical infrastructure and having real effects on the American people, whether it is gas at the pump or food at the grocery store or money at the banks. So couldn't agree with you more that we really need to lean into CISA's statutory role as the National coordinator for critical infrastructure resilience and security.

So a lot of this is—we have two main roles actually. We are what I call "left of boom", as a retired military officer. We are focused on resilience and prevention of attacks. Then we are there to be able to respond effectively to a victim to help them recover and to mitigate risk to their business and to also leverage the information that we get in an anonymized way so that we can warn other victims and prevent them from being hacked. But it comes down to our ability to work very closely with our partners at the State and local level and within critical infrastructure to ensure that they have the resources, the technical assistance, and the information that they need to be able to protect themselves. Because at the end of the day we know that over 90 percent of successful cyber attacks start with a phishing email and that you are 99 percent less likely to get hacked if you implement multi-factor authentication.

So all of these standards and goals and information that we put out, working closely with the critical infrastructure owners and operators, incredibly important. That is why we work closely with TSA as they articulated new standards specifically to pipelines. That is why we are working with 20-plus pipeline CEOs twice a month to help them instantiate the technology that they need to protect their networks and systems and assets.

Mr. PAYNE. Thank you. Thank you.

How will the Joint Cyber Defense Collaborative help build our National resiliency by fostering collaboration, planning, and exercising to prepare for specific cyber attack scenarios?

Ms. EASTERLY. Yes, great question.

I am super excited about the JCDC. I really think this is a different and unique capability for the Nation. It is the place that by statute brings together the full power of the Federal Government with the innovation, imagination, and ingenuity of the private sector. The reason why we chose those plank-holder partners, the infrastructure companies, the cloud security providers, cloud service providers, and the cybersecurity vendors is because they afford global visibility into infrastructure that the Government doesn't have and shouldn't have. So that is how we see the dots, connect the dots, and then reduce risk at scale.

So that is how that collaboration in near-real time, information being shared to enable security and resilience, and also to inform planning against the most serious threats to the Nation so we can drive down risk at scale. It is one of the things that I am most excited about and we are already seeing dividends form the JCDC, sir.

So thanks for the question.

Mr. PAYNE. Well, thank you for those responses.

With that, Mr. Chairman, I yield back 20 seconds.

Chairman THOMPSON. The gentleman is so kind.

The Chair recognizes the gentleman from Louisiana, Mr. Higgins, for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman. I thank the Ranking Member and our witnesses for being here today.

Everyday importance of our cybersecurity systems grows as a matter of National security. The number of publicly-reported cyber attacks and breaches for 2021 unfortunately on track to be the highest and most impactful in history. The cost of ransomware damage is expected to reach $265 billion by 2031—and personally I think that is a light number.

Our foreign adversaries are rapidly increasing their cyber skills and stealth. We are also currently seeing the disastrous consequences involved with supply chain vulnerability. Supply chain cyber attacks have risen by 42 percent just in the first quarter of this year. According to BlueVoyant, a third-party cyber risk management company, 97 percent—97 percent of firms have been negatively impacted by cybersecurity breach in their supply chain. Further, 1 out of 5 small businesses fall victim to a cyber attack in the United States, and of those 60 percent go out of business within 6 months. This is a serious problem. Our adversaries should have a clear understanding that the United States can and will execute effective and timely consequences if they attack our National critical cyber infrastructure.

Deterrence and response, in my opinion, are critical aspects to our mission to address the cyber threats that we are currently experiencing and the threats of tomorrow.

Director Inglis, non-state criminal actors are responsible for many cyber attacks in the United States, including last year's ransomware attacks on our hospital systems and the Colonial Pipeline attack. The United States has had difficulty, however, in the past to executing counter attack strikes against cyber terrorists. For example, in 2016 the U.S. Cyber Command worked to destroy ISIS communications and remove pro-ISIS propaganda which only worked for a couple of days. They were right back up. Certainly wasn't an effective counter strike.

So, in your professional opinion, is the United States capable of launching an effective cyber counter strike against cyber criminals world-wide? Because this is the question that Americans want to know, can we strike back? Do we have the will, do we have the capability? If we do have the will and the capability, then why are we not lighting these criminals up with counter strike cyber attacks?

I ask you for your response.

Mr. INGLIS. Congressman, thanks very much for the question. I am sure that is the question on the mind of many people who are aware and watching the growing threat in cyber space.

I agree with your characterization of the growing seriousness of these threats and the perception that we are falling further behind.

I would offer that it is important to bring transgressors to justice. I would offer that the set of tools we should bring to bear is considerably larger than simply finding and shooting at them using cyber activities in and through cyber space. So that is an important part of the solution, but equally important is a campaign that covers all the ways that we can thwart their efforts. We need to begin with increased resilience and robustness in the technology, in the skills of our people, in the doctrine, in the roles and responsibilities. We are talking a lot today about how do we collaborate as opposed to achieve simply a division of effort such that these transgressors have to beat all of us to beat one of us. Having established a defensible enterprise, we then need to actually defend it. That is a very proactive set of endeavors. Jen Easterly at CISA and other sector risk management agencies are leading the collaboration of the Federal enterprise with the critical information and critical sector to do just that.

Finally, we need to align actions to consequences. An important piece of that, as you suggest, is finding and bringing to justice these transgressors, stopping their further efforts. But we need to use all the instruments of power at our disposal. We need to be able to——

Mr. HIGGINS. Thank—sir, in the interest of time—I have 10 seconds remaining. Let me just close. Thank you for your answer.

In my opinion we need to have a lightening-fast cyber counterstrike. There needs to be immediate consequences. Then we still bring them to justice. That takes a long time.

Mr. Chairman, I yield and I encourage my colleagues to support a very proactive and aggressive cyber counterstrike as we face these on-going attacks.

Thank you for holding this hearing today.

Mr. INGLIS. Mr. Chair, I would be happy to follow up——

Chairman THOMPSON. The gentleman yields back.

The Chair recognizes the gentleman from Missouri, Mr. Cleaver, for 5 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman, for the hearing, for a variety of reasons.

I am on the Homeland Security, but I am also on Financial Services and we also have a great deal of interest in and ability to work with CISA.

Director Easterly, thank you. You know, since CISA was created back a couple of years ago, you know, the agency now has a recognizable name. I think when CISA first was created, a lot of people, who you said CISA and they thought it was a hip hop band. But, you know, now I think it is recognizable. You know, you are serving a great purpose with security, public and private.

You know, but you have a far-flung and almost cryptic kind of a mission. You know, I am wondering, you know, what would you want your grandchildren to brag about when they become adults as it relates to what you were able to do at CISA? I mean what do you envision down the road as something that is significant that you really want to do and may even need the help of the Chair, the Ranking Member, and this entire committee in getting it done?

Ms. EASTERLY. Thank you for that great question, sir.

My son is 17 and I often tell him how excited I am to someday be a grandmother, which I think it is a little off-putting to him since he is a junior in high school, but I am excited for that day because I like babies.

But it is a great question. You know, I have thought about this through my career, through 21 years in the military, several combat tours, working at the White House, working in the intelligence community. Much of what I am doing is motivated so that my parents and my brothers and sisters and my son and my husband are proud of me. I would hope that my grandkids could say she helped make America safer. So that is my goal, to ensure the security and resilience of the infrastructure that Americans rely on every hour of every day, to get power, to get water, to get food at the grocery store, to get money at the bank, to get gas at the pump. These are the networks that underpin our lives and my mission is to ensure that they are secure and resilient.

Mr. CLEAVER. Is there a priority? Is there something that is so critically important to the agency that you want a direct as much attention to it as possible? The No. 1 thing. Or is the mission so massive that it is difficult to set anything aside?

Ms. EASTERLY. Well, I don't think it is—I mean it is a big mission and I think it is a critically important issue, sir.

Mr. CLEAVER. It is.

Ms. EASTERLY. But I think it is pretty simple. You know, our mission is to lead the National effort to understand, manage, and reduce risk to cyber and physical critical infrastructure. We do that in two main ways. We are the operational lead for Federal cybersecurity and we are the National coordinator for critical infrastructure security and resilience.

My top priority to ensure that this agency is successful is to make sure that we have the talent we need to be able to operationalize our various missions. But my goal, again, is to really ensure that infrastructure, whether it is owned by—critical infrastructure owners at the State and local level or with the Federal Government is secure and resilient to cyber attacks from nation-state actors and cyber criminals.

Mr. CLEAVER. Thank you very much.

Mr. Chairman, I would like to beat Mr. Payne and I will yield back 50 seconds.

Chairman THOMPSON. The gentleman is real kind.

The Chair recognizes the gentleman from South Carolina, Mr. Norman, for 5 minutes.

Mr. NORMAN. Thank you, Chairman Thompson.

I want to thank our guests for testifying and for being here. From reading your backgrounds for both of you, you all really have the background to do a great job with what I consider the threat that this country is facing every day. You know, we have got so many that we know about, but the ones we don't know about—and I am from small business and know a lot of businesses that would not report the attacks on their particular company because of loss of stock value. You know, the fact that they just do not want it publicized. But with—and I know you all have not been on the job but, you know, 6–8 months, but if what you put in place, and since you have been there for the time that you have, would the Colonial attack be able to occur now or do you have the mechanisms in place to stop that?

Mr. INGLIS. Mr. Congressman, thank you very much for the question. It is an excellent question.

I can't say for certain whether we would prevent the next Colonial Pipeline attack. I believe that we are in a much better position to detect it, if not deter it. The things we have done ensure that to the extent that any one of us has a small piece of understanding about what might be transpiring in the share domain of cyber space, we are now in a better position to share that richly, quickly, and a granularity that it is then useful, it is actionable intelligence.

We are also able at this point to better respond to those activities, such that we can surge support to the point of need and restore not simply resilience and robustness to the system quickly, but confidence that the systems will work on our behalf. But I have to be quite clear, quite honest about saying the technical debt—the lack of investment for so many years is long in the making. It won't be turned around in a fortnight. We need to make sure at this moment we are making best use of the components, the authorities, and that we apply those in an integrated and collaborative fashion, such that increasingly an adversary needs to beat all of us to beat one of us. That should be a daunting proposition for them.

Mr. NORMAN. What about—you know, we have got an open border. This country is petrified of what is going on with the border. Anybody and everybody from any country is coming in. We don't know who they are, we don't what country they represent. All we know is we are not doing any background, we just—they basically are coming across the border unfettered. How you—and this is for either one of you—how are you all dealing with that and what threat is this that we face known or unknown that you see?

Mr. INGLIS. Mr. Congressman, I will start with a question. I assume that you are extending that analogy into cyber space. I think it is quite apt. You know, cyber is essentially a set of open borders which we might confer some degree of jurisdiction based upon geography. But in cyber space geography means very little absent the authorities that are bound within the United States, based upon that geography. So we have to make sure that we understand what is happening across those borders, that we can better identify the transgressors who come at us from across those borders, and that we can better deal with the sum of the authorities we bring to bear based upon both domestic and National security authorities. All of that is a very daunting proposition, the borderless space of cyber space. I believe we have the means to do that, but we have to better identify those threats, better security the infrastructure that we mean to defend, and collaborate on top of that to bring all our resources to bear.

Ms. EASTERLY. Would only add, absolutely. I mean some of the complexity—a large part of the complexity of our job, sir, is that we are dealing with cyber space, which is borderless.

But just to add to Director Inglis' comments from earlier, I think we are making progress in ensuring that there are fewer Colonial Pipeline-type hacks, but at the end of the day, the Government can only do so much. A lot of this is the private sector making sure that they are implementing the standards and the cyber hygiene that they need to protect their systems and networks. We are here as a trusted partner to provide assistance, to provide standards, to provide information, but a lot of this has to be the basics of cyber hygiene.

So I look forward to continuing to work with small businesses, the private sector so that they have the information that they need to be able to protect themselves.

Mr. NORMAN. Yes. You all play a vital role with that and I hope you—I realize cybersecurity doesn't have a border, but what we are doing is letting people in that are embedded in our communities that are coming to our country. We have got Duke Power in my district and EMP attacks, which is—an attack on this country is of great concern to all of us.

Thank you so much. I think my time is up.

I yield back, Mr. Chairman.

Chairman THOMPSON. The gentleman yields back.

The Chair recognizes the gentlelady from New York, Ms. Clarke, for 5 minutes.

Ms. CLARKE. Thank you, Mr. Chairman. I thank our Ranking Member and our witnesses for appearing today and lending their expertise to the subject matter.

Let me start with Director Inglis. As you know, Congress established the Office of National Cyber Director in part to address the long-standing inter-agency coordination challenges and turf wars that existed between CISA, sector risk management agencies, and other Federal agencies with cyber missions. Can you distinguish between the role ONCD plays as opposed to the role played by the National Security Council and CISA's role as the lead Federal coordinator for critical infrastructure protection?

Mr. INGLIS. Yes, Congresswoman. That is I think an important question and so I think the answer would be that those roles are complementary, they are applied concurrently. They are not necessarily hierarchical. At the same time that CISA is the on-field quarterback equipped with resources and authorities to coordinate the defense within the Federal enterprise and the support of the Federal Government to the critical infrastructure, the National cyber director has to make sure that the roles and responsibilities, as you indicate, of CISA and the sector risk management agencies is clear, that they are prepared to act in a complementary fashion, and that their performance is up to par in terms of our expectations. At the same time, the National Security Council, and in the form of Anne Neuberger, who is the deputy National security advisor for cyber and emerging technology, applies instruments of power that are outside of cyber space to bring about desired conditions inside cyber space, our intelligence assets, our military assets, our diplomatic assets, our legal assets, our financial assets. All of that is traditionally the role of the National Security Council.

If we do those three roles concurrently they can complement one another such that the sum of the parts is greater than the arithmetic sum.

Ms. CLARKE. Wonderful.

So in your experience thus far as the first-ever U.S. National cyber director, how confident are you that ONCD will be able to unify Federal cyber efforts around a common vision and shared purpose?

Mr. INGLIS. I think I am not in a position to ultimately judge my own performance, but I think that we can make a difference. I think that that is the point of accountability that should be imposed on me. Did the system perform better, are we in fact more coherent, cohesive in the application of these very impressive pieces at the end of the day? I think we can and will make a difference.

Ms. CLARKE. Awesome.

Director Easterly, would you care to weigh in on the dynamics between ONCD and CISA and whether you see these roles as complementary of each other and any areas for improvement?

Ms. EASTERLY. Thanks so much for the question, Congresswoman.

As Chris and I have talked about—and we go back about 15 years, so we have known each other for a while—and I think—you know, I often say technology is easy, people are hard. So you have to have that trust to build that collaborative partnership. Fortunately Chris and I have been friends for a long time. We talk about our relationship as he being the coach, me being the quarterback, but we know that there are all players on the field. I think even in just the last 3½ months we have forged a highly collaborative, highly cohesive relationship with our teammates across the Federal Government.

You know, this is about one team, one fight, cyber is a team sport, no drama, no ego, no tribalism, no turf. It is about getting the job done. So it is not Cobra Kai versus Miyagi-Do, it is Cobra Kai and Myagi-Do against all the bad guys.

Ms. CLARKE. Wonderful. It is so refreshing to hear that response. We are maturing as an agency.

Director Inglis, in the wake of the Colonial Pipeline ransomware attack we saw what I would describe as a breakdown of the PPD–41 framework and a failure to execute the National Cyber Incident Response Plan. Specifically, the Department of Energy was given the lead role in the Federal Incident Response efforts despite being neither the lead for asset response under PPD–41 nor the sector risk management agency for the pipeline sub-sector.

What guardrails have been put in place since then to ensure that the next time the United States has to respond to a significant cyber attack on our Nation's critical infrastructure the lines of effort articulated under PPD–41 will be observed?

Mr. INGLIS. Thank you for the question.

As you indicate, PPD–41 remains a quite useful and appropriate document to guide our efforts in the moment of contingency or crisis, say a repeat, god forbid, of the Colonial Pipeline. I think that what we have done since then, and certainly in the last 3½ months now that Director Easterly and I have assumed these roles, is to double down on our efforts to understand what the role of CISA is—it is increasingly clear what the role is, it is the coordinator—to double down on how then that relates to the sector risk management agencies to understand what the lanes of effort are, how they complement one another such that in the heat of the next contingency or crisis we will be based upon not simply what the rules are laid out in PPD–41, but tested and exercised roles and relationships based upon not simply professional trust but the personal relationships that we have established to know how we would respond in that crisis.

Ms. CLARKE. I thank you, Mr. Chairman. Thank you for your indulgence.

I yield back.

Chairman THOMPSON. So, Mr. Inglis, so let me understand what you just said. You said personal relationships. Are you saying those personal relationships override the policy?

Mr. INGLIS. I do not, sir. So thank you for your question and the opportunity to clarify.

I think those professional relationships are well described in law, in policy, and ultimately in the administrative roles that are established. The personal relationships can complement those and ensure that you affect those not simply as a division of effort, but in a collaborative fashion.

I spend quite a lot of time trying to understand what the challenges and the authorities are of Jen Easterly or the sector risk management agencies so that I can put myself in their stead and understand what I need to do to support them. That is based upon personal trust as much or more as executing fully and faithfully the authorities and the rules that are inculcated in statute and policy.

Chairman THOMPSON. But you do recognize that the policies at the end of the day——

Mr. INGLIS. I do, sir, without equivocation——

Chairman THOMPSON [continuing]. Should be the driving force behind what you do.

Mr. INGLIS. Without equivocation.

If I might, I would just say that I think that a transformative feature of what we are proposing is that we can fully and faithfully execute the law and the policies in a way that might equate to a division of effort, that we then meet at seams that are defined by those laws and policies, which are very important. But we also need to go further to try to understand what more we can do to aid and abet the activities to the left of us, to the right of us, to achieve a degree of collaboration, which means that we have to work harder and essentially have a degree of personal addition to those as opposed to subtraction from those.

Chairman THOMPSON. But somebody has to be in charge.

Mr. INGLIS. At any moment in time we need to know who is is accountable for what, yes, sir.

Chairman THOMPSON. Absolutely.

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

Mr. CLYDE. Thank you, Mr. Chairman.

Our Nation's safety and security are being challenged by our enemies through cyber space. As we have seen over the last year, these attacks can lie dormant for many months before being detected and can have devastating consequences on our economy and our way of life.

Further complicating these threats is the fact that cyber attacks can be carried out by both state and non-state actors and can be relatively inexpensive to execute. There seems to be limited tools at our disposal that enable us to immediately respond to a cyber attack and hold perpetrators accountable. In many ways cyber attacks have emerged as a near-perfect weapon against our Nation—especially the civilians in our Nation.

So both of you, thank you for continuing to provide valuable insight into what steps are needed to strengthen our cybersecurity and to respond appropriately when the attacks are successful.

As my colleague from Louisiana, Mr. Higgins, highlighted, I think the best defense is a good offense, but we definitely need both. The civilian sector needs a stronger defense, but they have got to know what resources are there to help them too.

So my first question is for CISA Director Easterly. Director Easterly, this past month was cybersecurity awareness month and CISA launched their annual effort to educate the public on good cyber hygiene practices and the resources that CISA offers. Numerous Members in Congress, including myself, did what we could to amplify your agency's message with our constituents. Things like public service announcements, speaking on the House floor directing people to your CISA website for further education, speaking to local clubs, including Rotaries and that sort of thing, but what other steps can Members take to support CISA's mission in each of our district? Because, you know, honestly, when I spoke to a local Rotary, there was only one person in that room—and there was a number of folks there that actually knew what CISA was. You know, you bring tremendous resources to the table. How can we make America more aware of what you have got?

Ms. EASTERLY. Yes. So first of all, thank you very much for your leadership and your support. It is great to have Members weighing in on this important issue. So thanks for that.

You know, we are the newest agency in the Federal Government. We are going to have our third birthday here on November 16. so it is probably not terribly surprising that some folks don't know who CISA, what CISA is, how to correctly pronounce CISA. But at the end of the day, I do think, sir, we are making progress. Part of that is the help of Congress, but also we have a fantastic field force. We have over 500 people, cybersecurity advisors, protected security advisors out there working with State and local, your constituents, other constituents, and critical infrastructure owners and operators to render assistance, to ensure they have the information they need to be able to protect themselves. So we are going to continue with this campaign, but I agree with you, we need a campaign like "Click It or Ticket", or "Smokey the Bear", or "This is your brain on drugs", something that really makes an impact on the American people so they know exactly what they need to do to protect themselves and to implement multi-factor authentication.

Mr. CLYDE. Thank you.

Follow up on that, you recently discussed CISA's initial work to map out our Nation's primary systemically important entities. As you know, there are legislative proposals that would require CISA to accomplish this goal, including one authored by Ranking Member Katko and Mr. Garbarino. I applaud your agency for taking the initiative without Congress having to get involved. However, could you tell me, has CISA run into any obstacles in identifying these entities that are critical to our Nation's security and do you believe legislation would help CISA overcome these obstacles? Is there any way that we can help in that regard?

Ms. EASTERLY. You know, as I have said, I think it would be very useful to codify systemically important critical infrastructure, or what we call PSIES, Primary Systemically Important Entities, but we are going to do that work notwithstanding. We have not hit any obstacles, but I will tell you, I mean we want to do this right. So ensuring we have the rigorous methodology to be able to identify these systemically important entities based on network centrality, economic centrality, logical dominance, and National critical functions. That is a tough effort. It is an important effort. But we have to be able to identify them and then we have to measure how we reduce risk. This can't just be about advising on risk or managing risk, it has to be about reducing risk. We have to measure what matters, and part of that is being able to articulate those SICIs or PSIES in the first principles.

Mr. CLYDE. All right. Thank you.

In just a couple of seconds left, Director Inglis, you know, as I said, I am very interested in and support a great offense.

Chairman THOMPSON. The gentleman's seconds have expired.

Mr. CLYDE. OK. Thank you.

I yield back.

Chairman THOMPSON. The Chair recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you very much, Mr. Chairman. I thank the Ranking Member. I think this has been a very informative hearing and I regret that I have been in another hearing and have not been able to follow all of what has been—and I am still being in two places at once, it is difficult to achieve.

Let us start with what I believe the public perceives as an issue. Just the mere notion that the Federal Government cannot protect its networks. It is probably hard for the typical consumer to understand how the Federal Government can't protect its networks and if it can't, then there is probably a belief that it is going to be difficult for the private sector to secure its networks.

Perhaps this has been answered, but do we have—in collaborating with the private sector, have we identified the private-sector networks that are so important to our country that we the Federal Government should have a greater hand in protecting them?

Whoever would like to respond.

Mr. INGLIS. Congressman, if I could start with that and then defer to my counterpart, Jen Easterly, to complete the answer.

I think first and foremost you properly point to the public's expectation that Federal networks will be properly built, properly defended to deliver the functions, the services that they expect. We have taken aggressive effort to that. The Executive Order in May, the finding operational directive that Ms. Easterly talked about earlier in this hearing are both aimed at doing just that. But we have further work to do.

As to whether we should take then further effort to define the critical functions that serve the public, both within and without, within the private sector, there is further work to be done in that regard. We call that systemically critical infrastructure. It is a challenge to define what that is, given there are so many possibilities and therefore so many components that underpin those possibilities. But CISA has taken that work on. With the support of this Congress and this committee in particular, I think that we can make progress.

Mr. GREEN. Does the lady desire to have a comment?

Ms. EASTERLY. Sir, is that for me?

Mr. GREEN. Yes, ma'am. Sorry. Did you have a response?

Ms. EASTERLY. Yes, thank you.

You know, I would just add to Director Inglis' points, we are in fact moving out on identifying that primary systemically important entities. It is a serious and complex effort. We are working through it and so I am hopeful that we will have a preliminary view on that in the coming months.

I would absolutely agree with you that the Federal Government has to lead by example. The private sector can't look at us and expect us to not be able to defend our own networks. So all of the work we are doing pursuant to the President's EO to modernize our Federal civilian Executive branch networks to create visibility to ensure that we can actually manage that enterprise as an enterprise, not as 102 separate little tribes, we are working very aggressively to do that and I am optimistic that we are going to make a real difference. Because I think we all know that the status quo is unacceptable.

Mr. GREEN. Thank you.

With my 1 minute and 10 or so seconds left, let us talk quickly about diversity, work force diversity. It is my understanding that CISA recently announced a $2 million grant or grants to bring cybersecurity training to rural and diverse communities. What are the processes that we are putting in place to make sure that we do this in an efficacious way? My concern is that rural and minority communities too often are left behind and this is a great opportunity to make sure that they are brought into the fold.

Can you give me some sense of what the process will be to make sure that we are doing this appropriately from past attempts?

Thank you.

Ms. EASTERLY. Yes, thanks for asking that question. I am hugely passionate about this. I am a big believer that you have to build a talent management ecosystem that allows you to tap into diverse pipeline because that diversity that looks like America will enable us to solve the toughest problems. I have always believe that since my early days as one of the few women at West Point and in my time in the private sector where I built an organization that was 50 percent women, 25 percent black and Hispanic. So the kind of things that we are moving out on are lessons that I have drawn from previous aspects in my career.

You point to the GREAT grants—$1 million for N Power, $1 million for the Cyber Warrior Foundation focused on developing unrealized talent in under-served communities. That is just the beginning. We are also working to create a pipeline with things like the Girl Scouts. We just created a collaborative relationship with Girls Who Code. I am looking forward to working with folks on this committee to be able to tap in to historically black colleges and universities to create a vibrant pipeline there. I am open to all great ideas.

So I would love to work with you, Congressman, if this is a passion of yours as well.

Mr. GREEN. It is a passion.

Mr. Chairman, thank you so much for the time.

That is one of the better answers that I have heard. I look forward to working with you, ma'am. If you will contact my office.

Thank you so much.

Ms. EASTERLY. Thank you, sir.

Chairman THOMPSON. The gentleman's time has expired.

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

Mr. GUEST. Thank you, Mr. Chairman.

Director Inglis, in your written testimony on page 4 you talk about 3 categories of threat that warrant continued effort and attention. I want to specifically talk about the third category. You say that we must remain laser-focused on maintaining the integrity of our information and telecommunications infrastructure against high-risk actors. Large portions of the hardware supply chain underpinning our most critical—such technologies are located in countries that could leverage it for intelligence gathering or disruption at global scale.

So can you talk a little bit about the supply chain challenges that we are seeing today?

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

I think that there is a growing awareness that the digital infrastructure that supports critical functions, or for that matter, personal functions broadly across our society is at risk. It is at risk because it has not been built to be by design resilient and robust. It is at risk because we don't collaborate and integrate in the defense of that. Essentially the stove pipes that sit side-by-side-by-side add primary value to those supply chains without understanding what the resilience and robustness is from start to finish across those supply chains. As you have indicated, many of those lie outside our physical boundaries, our borders, such that we have to then depend upon the collaboration of others, other nations to effect the resilience, robust, and assume the defense of same.

Approaching that then means that we have to reconsider how do we build those supply chains, invest resilience and robustness in those supply chains, how do we defend those supply chains? An important piece of that will be collaboration between the private sector and the public sector. Some of that might mean that we have to re-shore some of those supply chains to find places where we can build the key components, manufacture, and add value to those components with like-minded nations or within this Nation. All of that work before us I think transcends both cyber and the physical space. So it is in fact a strategy that is under way and it is a collaborative activity between the private and the public sector.

Mr. GUEST. Yes, outside of Congress incentivizing companies to return and manufacture many of these critical components in the United States, is there anything else that we can do as a Congress to try to bring those supply chains back here domestically so we are not depending upon countries, particularly countries in the Far East? I think of China and the growing threat of China, how many of the components that we need for things that we do on a regular basis are manufactured in China. We have seen the CCP continue to grow. You even list here in your testimony that countries can use some of the hardware manufactured in other countries for intelligence gathering.

So I guess my first question is outside of incentivizing companies, giving tax relief, tax breaks for companies to bring production back to the United States, is there anything that we can do as a Congress to continue to encourage that?

Mr. INGLIS. I think there are three broad points of influence that we can bring to bear. You mentioned one of those, incentives. Trying to create market forces that will essentially push, right, these supply chains, these supply lines in the right direction for resilience and robustness and the confidence that pertains.

Another is simply awareness. There is insufficient awareness about what the true challenge is, where these supply chains lie. We then find ourselves surprised, right, in a Solar Winds escapade to understand where this comes from and how perhaps adversaries might insinuate themselves into that. The Congress can be very helpful and this committee has been specifically and particularly helpful in that regard.

Finally, some degree of accountability. When market forces fail, when incentives fail, we need to understand what are the truly critical functions that our Nation depends upon and ensure that those parties who are responsible for delivering that and defending that are specifically held accountable.

Director Easterly and I sit before you as accountable parties to kind-of make sure that the Federal Government is doing its part. The private sector also has a part to play. By exception we need to understand what those roles and responsibilities are and affect accountability.

Mr. GUEST. Have you seen specific instances where countries have used their supply chain being a critical component for intelligence gathering? I know you list that here in your written testimony. First, have you seen examples of that and then, No. 2, are there any that you could share with this committee? I know there may be things which you have awareness of that you are not able to share in this type of setting. But just specifically if there are any that you could share, I would appreciate that.

Mr. INGLIS. I would be pleased in the appropriate setting to speak to intelligence matters that would kind-of point to the opportunities that various nations might have given the current disposition of supply chains. Unfortunately, for the purposes of this discussion, those are matters that are likely Classified in terms of those opportunities.

Mr. GUEST. Yes, sir. Thank you very much.

Mr. Chairman, I yield back.

Chairman THOMPSON. The gentleman yields back.

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

Ms. SLOTKIN. Great. Thank you, Mr. Chairman. A warm welcome to our witnesses. Really glad to have excellent experts. I echo Ranking Member Katko's comment that I feel like we have the best team in place and we are working in a really positive bipartisan way on something that is an issue that really connects high policy in Washington to every family back home in our districts. It is rare that that happens. But after the attacks on Colonial Pipeline and JBS, I find myself increasingly in front of communities, often in rural communities, where I am, you know, there to talk about something very different and the first question they ask me, from farmers to school teachers and superintendents is, what are we doing to protect ourselves from this onslaught of attacks. I would note, I had a big group of superintendents in my office yesterday and every single one of them had had ransomware attacks and many had paid the ransom to get the school data back.

But what I want to know I think echoes some of my colleagues. I want to be able to tell people back home that we are doing everything we can to defend them. I understand that a lot of our offensive things are Classified and we don't talk about them in public, but I am interested in the defensive side. In particular what the President laid down on the 16 different categories of infrastructure that he told Vladimir Putin were off-limits.

Can you lay out for us, since the summit between the President and Putin and the President laying down that marker, have we seen attacks from Russian-based groups, particularly those groups that were responsible for some of our biggest, you know, disruptions, have you seen a decrease, an increase, or no change in their level of attempts to attack us?

Mr. INGLIS. I will start with that.

Thank you very much for that excellent question. I am sure on the minds of most, if not all, of our citizens.

I think that, answering the question head-on, we have seen a discernible decrease. It is too soon to tell whether that is because of the material efforts undertaken by the Russians or the Russian leadership. It may well be that the transgressors in this space have simply kind-of lain low understanding that this is for the moment a very hot time for them. We need to make sure that that continues to be the case, that we continue to build resilience and robustness in our infrastructure, we continue to work hard to understand who is transgressing across that infrastructure and use all of the resources at our disposal to bring them to justice.

I think in the longer term we will be able to measure in a qualitative and a quantitative fashion what the diminishment of those efforts are. For the moment, I think it is too soon to tell. We therefore need to ensure that our strategy is solidified and brought to bear.

Ms. SLOTKIN. OK. So I would just ask for your commitment. Since we know that some of these groups sometimes go dark for a short time while the media's attention is on them and then they come back to life. I would offer we should have that conversation again iteratively in this committee to make sure that the Russians are living up to a basic commitment to stop what is going on based out of their territory.

I think the other issue I think Ms. Easterly is—I think one of my colleagues mentioned—you know, I don't think the American public knows the 9–1–1 number to call when their school, when their farm, when their processing plant, when their local government is attacked. Of course there are State offices that handle some of these things, but is it appropriate to think of CISA as the Federal 9–1–1 that we call when we see one of our infrastructure nodes being attacked?

Ms. EASTERLY. Certainly. We welcome first of all the cyber incident reporting legislation where if there is an attack of some sort people would come to us and let us know because we are there to render assistance, but we can also use that information to prevent others from being hacked. So I would want people to recognize CISA both as those people that you call to get help, but really those people who are helping to raise the whole cybersecurity baseline and creating goodness for the entire defense of the Nation. So I hope to get to that point, Congresswoman, and I would love to partner with you on that.

Ms. SLOTKIN. Yes. Then last I would say, you know, the best, you know, offense is a good defense. We know that our private sector has an important role to play. Do the companies you engage with get that they are part of our National security apparatus, that they have a role to play, particularly in infrastructure, in protecting the United States, and therefore have to maintain the highest standards, unlike some of our pipelines and others that we have seen recently?

Ms. EASTERLY. Yes. I would certainly say that I have been incredibly encouraged, both from my time in the private sector within finance, but since then I arrived at CISA and have been working directly with private-sector companies, to include ISP, CSP, cybersecurity vendors, infrastructure providers, who get that this is a National security imperative. So have been encouraged, am optimistic, but we are going to continue to collaborate and strengthen those partnerships to make sure that this is really a National endeavor to protect the country.

Ms. SLOTKIN. Thank you very much.

I yield back.

Chairman THOMPSON. The gentlelady yields back.

The Chair recognizes the gentlelady from Iowa, Ms. Miller-Meeks, for 5 minutes.

Ms. MILLER-MEEKS. Thank you, Chairman Thompson, Ranking Member Katko. I appreciated the questions by all of my colleagues and Representative Slotkin, who just spoke, especially in reference to cyber attacks and ransomware.

So JBS is in my district and it was affected—less so the plant within my district than, you know, the entire infrastructure of JBS. I have also, as a State senator, worked on legislation for ransomware attacks that our local government had experienced when they had been hacked. Interestingly enough, when people communicated to me in my district about the provision in the reconciliation bill with the increase in IRS agents and looking into accounts where there was a $600 transaction, often I was asked about hacking and did this make us less secure.

So I think this is an extraordinarily important topic and I appreciate Chairman Thompson bringing this forward today.

Director Easterly, on the topic of the new CISA authorities provided in last year's NDAA, one of the more important provisions authorizes CISA to subpoena internet service providers to obtain contact information for critical infrastructure operators where CISA has identified vulnerable devices on the internet and so that these devices can be secured before they are attacked.

Can you provide the committee a status update on the implementation, how many subpoenas has CISA issued to date?

Ms. EASTERLY. Yes. Thanks for the question.

It is a really, really important authority. We have issued over I believe 35 administrative subpoenas to date and we have seen—because we go back and we re-scan the infrastructure where we saw those vulnerabilities—we have re-scanned that and we saw those vulnerabilities actually get closed. So we believe this tool is enabling us to mitigate and remediate vulnerabilities and to make folks aware of vulnerabilities that they probably were not tracking.

So we have used that aggressively since we have gotten it and I am really pleased to say that we have operationalized it in a way that is helping us reduce risk.

Ms. MILLER-MEEKS. So you answered one of my follow-up questions, so I am going to go to the next one.

Have you identified any shortcomings of the program that you think need to be addressed?

Ms. EASTERLY. Well, since we are just in the—I guess about 6 months, 9 months of operationalization, I have not yet seen specific shortcomings, but I will absolutely come back to you and let you know if we need something different or more from this authority.

Ms. MILLER-MEEKS. I think with the recent attacks, you know, people are much more aware of this now, so it is a topic of conversation.

So thank you. We would appreciate the feedback.

I also think that we are—all of us are in agreement that we need to double-down on our efforts to provide proactive vulnerability identification to critical infrastructure entities, particularly those that identify as being particularly critical for economic and National security. I think we have heard this from several Members.

We don't want a single point of failure resulting in cascading impact for the country at large. Do we have the processes and technology in place to execute on this proactive vulnerability identification and notification at scale? Are we effectively looking at vulnerabilities across critical infrastructure community through the eyes of an attacker?

Ms. EASTERLY. I will start and happy for Director Inglis to weigh in.

I think it is exactly the right question. As we know, everything is connected, everything is interdependent these days. Everything sits on that technology baseline and therefore everything is potentially vulnerable. So we work very hard to make sure that business owners, small and large, critical infrastructure owners and operators, State and local, the American people have a good understanding of what they need to do to ensure that their software is patched, to ensure that we are taking care of vulnerabilities, and to have the basics that we need.

I would also commend the incredible research community, those researchers, those academics, those hackers out there who were doing yeoman's work in being able to help identify these vulnerabilities, bring them to us through the coordination vulnerability disclosure platform, because that helps make us all safer and more secure.

I would point to the Binding Operational Directive, ma'am, that we issued today that I think is really groundbreaking in that for the first time this is really giving time lines to remediate those specific vulnerabilities that we know have been actively exploited by adversaries, not just all vulnerabilities, but the ones that we think are most dangerous. I think that can make a real difference, not just for Federal agencies, but from a signaling perspective for our critical infrastructure owners and operators and for businesses, large and small around the country.

Ms. MILLER-MEEKS. Thank you so much.

Director Inglis, I apologize. I have run out of time so I won't be able to get your answer to this. But thank you so much and thank you, Chairman Thompson.

I yield back.

Chairman THOMPSON. The gentlelady yields back.

The Chair recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Mr. Chairman, if I could, I have to run to vote in another committee. I would like to delay my 5 minutes.

Thank you very much. I will come back to the committee when I finish voting. Thank you.

Chairman THOMPSON. The Chair recognizes the gentlelady from Nevada, Ms. Titus, for 5 minutes.

Ms. TITUS. Thank you, Mr. Chairman. I didn't realize I was going to be next, but I appreciate it.

I would like to ask Mr. Inglis and Ms. Easterly both a couple of questions.

One is in our Subcommittee on Transportation and Marine Policy, last week we learned that there are many cybersecurity vulnerabilities in our travel hubs, including airports. I represent McCarran Airport and we know that as people travel we want them to be safe physically, but we also want their data to be safe. You see everybody plugging in their computers everywhere and working on them. Then when they get on the plane they continue to use wifi from the airlines for in-flight services. I wonder if you two could address what we might be doing to make that more secure?

Mr. INGLIS. Thank you very much for the question. I will start and Director Easterly, I am sure, will complement that.

I think there are at least two dimensions to this. One is, as per some earlier conversations we have had, there are in these locations systemically critical infrastructure upon which the public depends. How do we coordinate the flow of air traffic, how do we ensure that flight plans are securely communicated, how do we make sure that the data flows that underpin the safety of that industry is properly defended? The work that CISA and others are doing to determine what those systemically critical components are and the entities responsible for those will allow us to focus the very precious resources we have in a prioritized way to increase resilience and robustness in the defense of safe.

To the extent that individuals make use of individual services for their personal and perhaps their business activities, we need to make sure that as a matter of the commodities provided to them that security is built in. We also need to make sure that they are aware of what their alternatives are and that in the case where there is a risk that we haven't found a way to buy down, that they understand that that is a risk that they can choose to take or not take.

So some degree of cyber education, training, and awareness is also essential and we need to kind-of get that into our people skills at the earliest possible moment.

Ms. EASTERLY. Yes. I would only add—I completely agree with that. A lot of this, clearly from a standards perspective, we work closely with TSA as they are the sector risk management agency for aviation, for rail, but this also comes down to public awareness, making sure people understand the basics of password hygiene, updating their software, implementing multi-factor authentication, making sure that if you are a business you are patching those vulnerabilities.

So we have got to come at it from both angles, from a personal angle but also from a Government Federal agency angle. It has got to be a team sport.

Ms. TITUS. Thank you.

Speaking of Government agencies working with others, I would ask you about the relationship with universities and how we can strengthen that. I represent the University of Nevada, Las Vegas and they have a cyber center that has been recognized by DHS and the NSA as the National—it is a National center of academic excellence in cyber defense education. They are working to create a clinic where students can help small businesses if they get hacked because we know if a small business is hacked, 60 percent of them go out of business as a result of that.

So could you talk about maybe how we could strengthen the relationship between the Federal Government and the universities to do things like help small businesses?

Ms. EASTERLY. Sure, absolutely.

First of all, I love that clinic idea. I would love to come visit, if that is cool.

Ms. TITUS. You are welcome any time.

Ms. EASTERLY. Awesome. So you mentioned the centers of academic excellence that is sponsored by both DHS and NSA. It is a fantastic program and it is really part of our strategy to be able to tap into these schools, as well as community colleges, historically Black universities and colleges to create that pipeline for the next generation of cyber talent. So the kind of things that you are doing are exactly what we want to amplify. We want to tap into some of those students that are already cyber superstars. Our cyber talent management system will allow us to hire these folks based on their aptitude and their collaborative attitude as opposed to somebody having to get a Ph.D. or a Master's degree.

Mr. INGLIS. If could double down on that and commend the clinic in a particular and specific way, which is the clinic idea actually has many, many beneficiaries. Of course it benefits the local businesses that are serviced by those clinics, of course it is a component of those students, but importantly, it bridges the gap between education and practice in ways that so many institutions have been challenged. When a student arrives with a degree or a certificate that the front door of a business that they want to work for, they often lack the experience necessary to prove that they can do the job at the very first moment. So I think you have solved a number of challenges in one fell swoop. So I would commend that for others to follow.

Ms. TITUS. Well, thank you. I am glad to hear that. I will let UNLV know your comments.

Thank you, Mr. Chairman, I yield back.

Chairman THOMPSON. The gentlelady yields back.

The Chair recognizes the gentleman from Kansas, Mr. LaTurner, for 5 minutes.

Mr. LATURNER. Thank you, Mr. Chairman. Good afternoon.

I was on the phone conversation yesterday—phone call yesterday with a constituent of mine who owns a small business in Kansas. He had a ransomware attack and they asked for $900,000, which is a lot for this business—it is a lot for any business, but certainly a lot for this one. I asked the question, I said did your insurers or did the lawyers or the technical experts at any stage tell you you need to report this to a Federal agency, that you need to make this known. He said, no, to the contrary, they said it is a waste of time.

Now, I don't think you would agree that it is a waste of time and I would like you to address that. Assuming that you don't think it is a waste of time, how do we begin to change this narrative across the country?

Ms. EASTERLY. I am happy to start. Or you go ahead, please.

Mr. INGLIS. Go ahead.

Ms. EASTERLY. So first of all, I have great empathy for these small businesses that are getting hacked. They are put in a terrible position and I think they often do pay. Now, we say as a Government, you should not pay because it incentivizes that criminal ecosystem, but a lot of these folks——

Mr. LATURNER. They got it down to $600,000, but they were losing $2 million a day, you know.

Ms. EASTERLY. Yes, it is an incredibly tough decision.

Mr. LATURNER. So it is a tough spot.

Ms. EASTERLY. I totally hear you.

So part of this is making sure that businesses have everything that they need to prevent getting hacked. Frankly the resources and assistance and information we provide can help with that. But at the end of the day we have a field force that can actually render assistance to help folks understand if they get hacked what they can do about it, how they can recover and mitigate risk. If they do report to us, I think very importantly—which is why I am a fan of this legislation—we can use that information to prevent others from being hacked. But I would tell you, you should tell your constituent go to stopransomware.gov, which has been looked at uniquely almost 500,000 times. There is a huge amount of information, what ransomware is, how do you deal with it, how do you prevent yourself from getting hacked.

Mr. INGLIS. It is hard for me to add value to that answer. I think it is a complete and fulsome answer. I think that they should call such that then we can better support them in the time of need, that we can take the information necessary and invest in the future. But it our job as the Federal Government working in collaboration with the private sector to prevent these events in the future. Stopransomware.gov in an excellent kind of body of information to allow individuals, businesses to kind of act in their own defense, but there is more that we can do to get ahead of this to make sure that we are left of that event.

Mr. LATURNER. But you are both certainly aware of that attitude being very prevalent throughout the country in the business sector?

Mr. INGLIS. We are. The Government needs to actually—it needs to lead with the practice such that when you call the Government, the Government actually responds with meaningful support. What Director Easterly has laid out is an initiative, a set of initiatives across the Federal Government that had begun to do that. But we need to demonstrate that value such that the first thinking of an individual business or citizen is I need to call the Government because they have shown themselves willing and able to assist me in this time of need.

Mr. LATURNER. Let us talk about the JCDC. So I know it just launched in August officially. Talk about the promise of that and how you think that is going to help the coordination. Because that is one of the big concerns that I have is that there is so many different departments that have a piece of this. You know, for example, the White House chose the Department of Energy to deal with the Colonial attacks. So what is the promise of that and how are you going to make sure that we are actually coordinating and that Congress in our oversight function can actually hold someone accountable? Because it is incredibly frustrating when it is so spread out.

Ms. EASTERLY. Yes, absolutely. It is a great question.

I am incredibly motivated on this one, sir. I will come back and ask this committee for help if I need it. You can hold me accountable if the JCDC fails, but I will tell you, I am motivated because even though I spent 27 years in Government before I went to the private sector, when I showed up in the private sector it felt like you needed a Ph.D. in Government to deal with the U.S. Government, right. You were getting different signal, different information from different agencies, it was totally unhelpful and incoherent, even as good as Government agencies and well-meaning as they are. So the beauty of the JCDC is by law it brings together the power of the Federal Government, not just CISA, but NSA and FBI and DoD and DoJ and ODNI and Secret Service and the National Cyber Director as one entity to collaborate with State and local, with critical infrastructure owners and operators and with those cybersecurity companies, ISPs and CSPs that have the global visibility to allow us to illuminate those dots so we can connect them and drive down risk at scale.

This is not about just weekly meetings on partnership, hey, how are you, let us have coffee together. It is really about how do we operationally collaborate in a professional intimate, shoulder-to-shoulder—whether that is virtual or physical—way to make a difference for this defense of our Nation.

Mr. LATURNER. I appreciate that. I want you both to succeed and am happy to do anything that I can to help along the way.

Mr. INGLIS. Thank you, sir.

If I could, at the risk of 10 more seconds, simply add that I think that the JCDC is different in kind than what we have done before. This essentially is an agreement to collaborate essentially to find dots, to co-discover threats that no one can find alone. That is different. Authorized by the Congress, substantiated in law, we are now beginning to effect that.

Mr. LATURNER. Thank you both for your time.

I yield back, Mr. Chairman.

Chairman THOMPSON. The gentleman yields back.

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

Mr. TORRES. Thank you, Mr. Chair.

I must admit I continue to have a lack of clarity about cyber jurisdiction. I know you have been asked this question a few times, but the National Security Council exists to play a coordinating role on matters of National security, which increasingly include cybersecurity. What is the central difference between the coordinating role of the National cyber director and the coordinating role of the National security advisor for cybersecurity? Earlier, in response to Congressmember Clarke you said the two roles are complementary. But I am interested in knowing what makes them distinct, not complementary.

Mr. INGLIS. At the end of the day if there is an event that requires the application of instruments of power outside of cyber space, the various instruments kind-of in the hands of Government, like intelligence or military or diplomacy, that is the traditional and sustained role of the National Security Council. My job is to ensure that the resources inside of cyber space are prepared, complementary, and effected for the purpose intended such that chief information security officers, CISA, sector risk management agencies, all of whom operate inside cyber space, that they do the job that is required.

Mr. TORRES. I want to revisit a point that Congressmember LaTurner made. So there are 16 critical infrastructure sectors and each sector has a sector risk management agency. The role of CISA is to partner with those sector risk management agencies to secure critical infrastructure. Even though the TSA is the sector risk management agency for pipelines, the Federal Government designed the Department of Energy as the lead agency on response to the Colonial incident.

Do you worry, as I do, that the designation of the Department of Energy as the lead agency perpetuates confusion about who exactly is in charge, about cyber jurisdiction?

Mr. INGLIS. Congressman, I think is an excellent question. Neither Director Easterly nor I were here at the time and therefore are unable to illuminate that choice. I would say that from this day forward, from the moment we got here, we strongly relayed that the playbook should be followed. That when we allocate roles and responsibilities, to the question asked earlier, policy matters. It must be effected as intended. Therefore in the future we intend to exercise, allocate, and essentially respond according to those policies and laws.

Mr. TORRES. To be clear, who in the administration decides which agency takes the lead on a cyber incident response?

Mr. INGLIS. I think that we define that ahead of the time, such that that agency knows at the moment that that occurs that that is in fact what they should do. Again, within cyber space my responsibility is to ensure that those agencies understand those roles, they are prepared, and that they then execute those roles. As the on-the-field quarterback Jen Easterly would then ensure that that is actually being effected.

Mr. TORRES. Director Easterly, I appreciated your allusion earlier to Cobra Kai.

Ms. EASTERLY. Thank you.

Mr. TORRES. I am a fan of the show. You said earlier there is a limit to what we can do in Government, that there is no substitute for cyber hygiene from the private sector. I agree with your assessment. It seems to me the breach of both Colonial Pipeline and JBS demonstrates that the laissez-faire approach to cybersecurity that the Federal Government has long taken has been a profound failure. A voluntary framework will only take you so far. There is no substitute for mandates.

So I have a few questions. Should every owner and operator of critical infrastructure report major cyber incidents to the Federal Government? Yes or no?

Ms. EASTERLY. Yes.

Mr. TORRES. Should every owner and operator of critical infrastructure have a chief information security officer?

Ms. EASTERLY. Yes.

Mr. TORRES. Should every said owner and operator have multifactor authentication?

Ms. EASTERLY. Yes.

Mr. TORRES. Should every owner and operator have password updates and software updates and third-party assessments?

Ms. EASTERLY. Yes.

Mr. TORRES. So if you agree that every owner and operator of critical infrastructure should adopt these cross-sector standards of cyber hygiene, as you describe them, then when is the administration going to mandate them universally?

Ms. EASTERLY. Well, we have begun a lot of that work with mandating it within the Federal Government. That is the work that we are doing with the EEO. All of those things are part of on-going efforts and that is signaling to our private-sector partners, who own that infrastructure and—you know, as you know, it is not owned by the Federal Government, but we are doing everything we can to ensure that we are signaling by leading by example and then by articulating the goals and standards that private infrastructure needs to implement to make themselves safe——

Mr. TORRES. With respect, signaling is different from mandating. Like the only reason we have mandates for pipeline cybersecurity is Colonial Pipeline. There is a sense in which I feel like we are reacting to events rather than governing. I want to govern proactively.

Ms. EASTERLY. Yes. I think there is—I agree with you, bottom line. I think there is a role for insuring that we are holding those who own and operate critical infrastructure accountable for ensuring that their systems and networks are secure and resilient. I think you are starting to see some of that being implemented here by the Government.

Mr. TORRES. I want to quickly squeeze in a question. I am curious, Director Inglis, what is your opinion on General Nakasone's cyber strategy of defense forward and what impact, if any, has Solar Winds had on your opinion on that strategy?

Mr. INGLIS. I think the strategy, which has now been in place for 3½ years is an appropriate strategy. It follows on the heels of what we have done in other domains of interest. NATO is defend-forward, the pre-positioning of U.S. Forces in South Korea is defend-forward. It should be followed by the application of all instruments of power in a similar fashion such that we have an early discernment of threats against us and early action to engage those threats such that we no longer wait on shore to receive those threats as they arrive in a distributed fashion.

Chairman THOMPSON. Thank you very much. You see why he is Vice Chair of the Committee, right?

The Chair recognizes the gentleman from Michigan, Mr. Meijer, for 5 minutes.

Mr. MEIJER. Thank you, Mr. Chairman, and thank you to our Ranking Member and our witnesses for being here today.

I actually want to follow up on what the subcommittee Vice Chair was asking about regarding that strategy, and specifically, you know, there have been prior question around the concept of deterrence, so I don't want to go back and rehash that ground, but I serve on both Homeland Security and Foreign Affairs and a lot of these issues really—cybersecurity issues are at that nexus when it comes to foreign adversaries, you know. I know we have been working on a broader multilateral strategy deterrence on the diplomatic side, but there are also unique vulnerabilities—or I should say unique protections within the United States and the way that our intelligence community is structured that I think can be—are very well-intended, but could have negative consequences.

So I guess for both witnesses, are our foreign adversaries exploiting restrictions of our intelligence community by using U.S.-based tech firms in order to launch attacks using virtual private servers?

Ms. EASTERLY. I think we saw that pretty clearly in both Solar Winds, as well as Microsoft Exchange. It is not a surprise. These adversaries are sophisticated, they are going to do everything they can. They are entrepreneurial. So it is one of the reasons why we have put together the Joint Cyber Defense Collaborative with those companies that have the visibility into domestic and global infrastructure that we don't want the intelligence community or the U.S. Government to have. These companies are able to provide this information in an anonymized way so the privacy is protected, but that we understand those vulnerabilities and then we can do something about it as rapidly as possible.

Mr. MEIJER. Would you say that would level out the benefit to our adversaries of using U.S.-based platforms rather than using foreign platforms that may fall under a different set of guidelines for IC?

Ms. EASTERLY. Well, certainly it will help increase our visibility as we know we have better visibility overseas given some of our intel capabilities. But I think actors have shown themselves to try and take advantage of the blind spots. So we need to use creative ways to be able to create those dots, connect the dots to drive down risk at scale.

Mr. MEIJER. Are there legislative solutions that may help to further drive down that risk at scale and connect those dots further?

Ms. EASTERLY. At this point in time I really don't know. I don't think so. We need to get this model right and ensure that the information is shared in a way that is enabling and collaborative. But I will definitely come back to you, sir, if I think we need more authorities to instantiate this visibility that we need to defend the Nation.

Mr. MEIJER. Thank you. I would welcome that conversation. I think, you know, as you saw we are passionately committed to doing what we can on talent, recruitment, and retention, on making sure that authorities are in place on recognizing that this is a critical and pressing vulnerability for our country. So I think there is strong bipartisan support to do what we can to shore it up, but some of that may trip into other areas that I think we are happy to discuss on-line or off-line.

Then, Director Inglis, in your testimony you identified burden reallocation across the cyber ecosystem as a major key objective. In order to take those unfair responsibilities off of the most vulnerable entities in cyber space, such as individuals or small businesses, you know, local governments that may have the least amount of resources are least well-equipped to deal with the magnitude of the threat—I guess, to put it briefly, how are you approaching this problem, which stakeholders in this space do you feel should bear the largest share of responsibility for systemic cyber risk in the digital ecosystem?

Mr. INGLIS. Thank you very much for the question.

I think that if you are an individual consumer of cyber services far too often you have to provide for your own security in a way that a consumer of an automobile does not. A consumer of an automobile does not have to go out and negotiate for an airbag or antilock breaks, they are built in. So we need to start with that. The systems that we provide to our citizens, to users, have to actually be resilient and robust by design, at scale, commodity scale.

No. 2, we need to make sure that those who would transgress, who would essentially hold them at risk all the same, that we understand who they are, how they operate, and that we find them and bring them to justice using all the instruments at our disposal, legal means, financial sanctions, diplomacy. This is an international threat.

We also need to make sure that in a time of extremis, contingency, or crisis, that the Government provides resources as appropriate to help those individuals or businesses at that moment in time. All of those combined I think can make a determinative difference in the life and the progress of our individual citizens and businesses in using this, and increase confidence that those systems will be used for the purposes intended and not for transgressors.

Mr. MEIJER. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. The gentleman yields back.

The Chair recognizes the gentlelady from Texas for 5 minutes, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman, and to the Ranking Member for holding this important hearing. Congratulations to Director Easterly and Director Inglis for their ascending to important responsibilities.

I believe that we are in an era that Dr. King wrote about as relates to civil rights. I think that era has raised its head again as relates to civil rights, why we can't wait. I think as it relates to the whole issue of cybersecurity, we are at a time and place in America and around the world that we cannot wait to be aggressive in addressing the questions that are going to come at us or the issues that we are going to confront rapidly.

So, Director Easterly, you mentioned key stats from 2020 about attacks against America. In 2020 alone there were more than 12,000 explosive-related incidents and more than a 70 percent increase in domestic bombings, according to the Department of Justice and U.S. Bomb Data Center. My question to you would be where CISA is in the role of prevention but also aggressiveness as relates to the cyber engagement in that. Do you believe that the mindset of CISA should be aggressive in its protection and engagement with the entities around the Nation, but more importantly in its collaboration of the incidents that may come from outside of the United States? Director Easterly.

Ms. EASTERLY. Yes, ma'am. It is a really important question. Thank you for asking it.

You know, one thing that I didn't realize before I came to CISA was the power of our field force. We actually have over 500 folks and based on the force structure analysis that we are doing I suspect that number should grow. But these are our front-line defenders for both infrastructure and cyber. Our cybersecurity advisors, our State coordinators, our protective security advisors that are there working to ensure that at the State and local level, at the small business level, at a critical infrastructure owner and operator level, that all of these individuals have the guidance, the information, the resources that they need to be able to protect themselves. So I think those field forces are a very important part of what gives the magic to CISA to allow us to reduce risk to the Nation's cyber and physical infrastructure.

Ms. JACKSON LEE. Thank you.

Director, do you sense with the administration—and you are obviously a voice for the policy of the administration and actions—sense the urgency of creative policies and the why we can't wait concept? Are you all creatively meeting and looking at ways to meet this aggression in addition to the able staff that comes under CISA?

Ms. EASTERLY. Yes, ma'am. I believe we really have that sense of urgency, that sense of aggressiveness. Director Inglis and I are on the phone regularly. We are in contact with all of our partners across the Federal Government, and importantly, our partners at State and local and at private sector. I think everybody—you can't look at Solar Winds and Microsoft Exchange and Pulse Secure and Kaseya and JBS and Colonial Pipeline and get anything but a sense of urgency. So we are powerfully motivated to defend the Nation and we are working at it every minute of every day.

Ms. JACKSON LEE. Thank you.

This question will go to both, but I would like Director Inglis—and congratulations on your position. The pace of innovation and integration of new technologies are posing new challenges to cybersecurity. So how are you, the administration, and working with CISA integrating emerging threats and risks into the strategy for keeping security measures currently and focused on nimbleness? 5G, deep learning, artificial intelligence, and quantum computing advancements are just a few of the challenges.

I have been steady on the issue of zero-day occurrences. Obviously we are sort-of advanced beyond that, but you understand the concept, which is when all things go awry.

Director Inglis.

Mr. INGLIS. Thank you very much for that question, Congresswoman. I think that that is a very, very important dynamic.

In the earlier question you I think suggested that as opposed to simply responding to the transgressions, the initiatives of others who would hold us at risk, we need to establish our own initiative, we need to make sure that we reacquire the sense as to what we want this domain to do for us, not to us, and to achieve that. Technology, innovation, and best practices are a place where the United States—and like-minded nations, but the United States in particular can and must lead. The technologies you have addressed will play a critical role in that and American innovation will play a critical role in understanding how those might make a difference. We need to do that and therefore our investments need to be made accordingly, such that we build in resilience and robustness and this domain then can achieve our aspirations, not our worst dreams.

Chairman THOMPSON. The gentlelady's time has expired.

The Chair recognizes——

Ms. JACKSON LEE. I thank you, Mr. Chairman.

Chairman THOMPSON [continuing]. The gentlelady from Florida, Ms. Cammack, for 5 minutes.

Ms. CAMMACK. Well, thank you, Mr. Chairman. Thank you to all my colleagues for this very important discussion here today.

I would be remiss if I didn't mention that the work that I did as a student at the United States Naval War College was centered around cyber, so this topic is very exciting to me.

I would love to just use my time to talk about an initiative that is very near and dear to my heart. I would love for Director Inglis as well as Director Easterly to weigh in on the concept, logistics, challenges of potentially the creation of the next service academy of the United States, the United States Cyber Academy. We have worked to create a framework that would address more of our cyber work force challenges and I would love to hear from you about what something like that might look like that would be beneficial in meeting the needs from both a military standpoint, but also Federal service, as well as the public-private partnership that we need with our private partners in this space. How we might be able to better develop this and take advantage of the incredible talent that we have amongst our youth.

I think it is very exciting about next generation of cyber warriors that we can foster, educate, and deploy into this space through the creation of a next generation Cyber Academy a la West Point or the Naval Academy.

So I am just going to start with Director Inglis first and then, Director Easterly, if you want to weigh in. I am all ears.

Mr. INGLIS. Well, thank you, Congresswoman for the question. You are probably aware that both of us are service academy graduates. I am sure you meant to say the Air Force Academy first, but that being said—so we are both clearly aware of the value that a deep and sharp education in a disciplined domain of interest holds. I think we are also aware that the proponency that is provided by the parent service is essential. So if we were to define a service academy construct for cyber, we would have to attend not simply to the work that would take place there that would inculcate the sense of what the technology, the doctrine, the practices, would bring to bear, but we would have to make sure that we attended to the generation of what is the mandate that should be taught and inculcated there and who would then receive the proceeds from that.

Now, in the case of cyber, you probably have many claimants on the graduate of those institutions such that they could then take that forward. You would then have to determine whether you are going to physically instantiate this in a single place or whether you broadly would separate or spread this across, you know, many institutions that have already shown themselves able to do it.

But I think your idea is very solid insomuch as we need to dedicate time and attention to understanding the domain of cyber space and the practices that best work inside of it such that we can then avail ourselves of a cadre of people who have thought their way through this. I would tell you that cyber was declared a domain by the United States Department of Defense not because the intention was to militarize it, but because it was sufficiently different, it was sufficiently new and novel, that unless we study it and understand how it works and how it behaves, we will continue to be befuddled by it.

I think that there are a number of institutions who have done yeoman's work in helping us get to that place, but there is further work to be done.

Ms. CAMMACK. I appreciate your comments.

Ms. EASTERLY. Yes, I would only add first, beat Air Force, because it is that time of year.

But also I think it is incredibly important to explore creative solutions. You know, I stood at the Army Cyber Battalion in 2008. We helped—Chris and I helped to build United States Cyber Command. I think there is a lot of creativity in the services that we can benefit from and some really good ideas out there.

I am very proud to say that CISA is 42 percent veterans. Particularly proud to say that during Veterans Appreciation Month. But I think there is so much innovation and creativity in the military that we should figure out how we can create connectivity with that community and really amplify and emphasize it.

Ms. CAMMACK. I appreciate both of your comments. As the sister to a career airman, I appreciate the nod and hat tip to the Air Force.

Of course, one of the things that we have always struggled with I believe is that joint operability across the services. Then, of course, as the space has gotten bigger, how do we navigate that divide between Federal service and the various intelligence agencies, as well as the military and then beyond.

So I think there is something really here and you will definitely be hearing from my office as we continue to build up a framework for this.

Thank you again for your time and testimony today. Much appreciated.

With that, I yield back.

Mr. INGLIS. We will look forward to working with you on that.

Ms. EASTERLY. Thank you.

Chairman THOMPSON. The gentlelady yields back.

The Chair recognizes the Ranking Member.

Mr. KATKO. Thank you, Mr. Chairman, for indulging me for a moment.

Before we close, I just wanted to say thank you again for the great conversation and testimony today. I think it is very helpful. It is very encouraging to see everyone on the same page and trying to do the right thing here.

As you may know, I issued in the past what I consider the five pillars of how we fight the cyber intrusions in this country. The last one has to do with offensive capabilities, or clapping back against bad guys. I don't want to talk about them in this setting, but, Director Inglis, I am asking you specifically on behalf of my colleagues, many of whom have asked me this very question, if we could get a briefing in a secure setting on where we stand with respect to our offensive cyber capabilities so we can have a better understanding of the entire playing field. Obviously I don't want to do it here, but I want to ask you a commitment to set something up soon to brief all of us on the committee.

Mr. INGLIS. We will commit to doing that in the appropriate venue.

Mr. KATKO. Thank you very much.

I yield back.

Chairman THOMPSON. The gentleman yields back.

One of the things I would like to thank both witnesses for is your frankness and your willingness to address the known and unknown challenges. I think the Academy prepared both of you for the ability to make adjustments.

Part of what the Vice Chair talked about is some of the going-forward challenges that I think we will have to meet. The fact that if we have a policy, we need to follow it. That is it. If not, change the policy.

So what we saw with the Colonial Pipeline situation is a concern, but from both of you we have heard a commitment to follow the policy and to try to get other partners to do likewise so that they understand it. That is important.

The other part is to the extent—piggybacking on the Ranking Member's comment—some of the countries who give us the most heartburn we have to continue to engage with. The public is somewhat befuddled that here we know nation-states are doing things to us, but yet we are still engaging them on a daily basis. We go into space together, we do a lot of other things together, and sometimes we have to be clearer with our messaging so the public is not confused.

Last, this notion of work force, it is an absolute concern. Congressman Green left the confines of his office to come to the end of the hearing because he is not going to let you get away without closing that deal today. But that is the point, that we are all interested in helping building the work force because we are in this together. To the extent that we can make that work force look like America, the better off we are.

So I join Mr. Green in that effort also.

But just let me thank you for your testimony and the Members for their excellent questions today.

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

The Chair reminds Members that the committee record will remain open for 10 business days.

Without objection, the committee stands adjourned.

[Whereupon, at 12:22 p.m., the committee was adjourned.]

APPENDIX

Question From Honorable Michael Guest for Jen Easterly

Question. Director Easterly, the time line for entities to report has been a significant point of contention during the debate on mandatory cyber incident reporting legislation. As you know, both the House and Senate Homeland bills have a 72-hour time line. You have served a significant amount of your career in Government, but also recently in the private sector. How do we strike the right balance here of not overburdening industry, but still getting CISA the information it needs to protect others?

Answer. The private sector, which owns and operates most of the Nation's critical infrastructure, plays a vital role in working with CISA to improve our Nation's cybersecurity. A mandatory incident reporting law would increase visibility into the cybersecurity threat environment, which in turn would inform and augment the U.S. Government's ability to develop and disseminate actionable information to help protect our Government and private-sector partners. CISA, in concert with other Federal agencies responsible for responding to cybersecurity incidents, look forward to working with both Congress and industry to make cyber incident reporting legislation a reality.

CISA's goal is to avoid overwhelming companies and our own Federal team. The balance should be between getting meaningful and relevant information in a timely manner that can then be analyzed and provided to industry in an actionable format while avoiding undue burden on a company trying to manage a live cyber incident. Timely information can be the difference between containing an incident and seeing its effects cascade across sectors and the economy impacting thousands of other companies. Without timely notification to CISA, critical analysis, mitigation guidance, and information sharing is severely delayed, leaving our Nation and our critical infrastructure vulnerable.

For example, CISA estimates that hundreds of millions of devices in use around the world were potentially susceptible to the Log4j vulnerability. We know malicious actors are actively exploiting this vulnerability in the wild. However, the Federal Government simply does not have the level of information it needs to definitively understand the breadth or nature of intrusions occurring as a result of this severe vulnerability. A cybersecurity incident reporting law would help the Government and our partners receive timely information about successful exploitation of critical infrastructure networks quickly after they are discovered, enabling us to help victims mitigate the effects, stop the spread to additional victims, and better track the size, scope, and scale of any adversary campaigns to exploit wide-spread vulnerabilities like Log4j.

Hearing from all stakeholders, through a formal and consultative rule-making process with publicly-sought input, will achieve balance by accounting for the concerns of industry and the benefits to the whole Nation. We recognize that Government agencies across critical infrastructure sectors have a need for cyber incident reporting for regulatory and other purposes. We believe that it is important that Congress support CISA's role in coordinating a National incident reporting system so that a thoughtful and consistent approach can be applied across the entire economy. CISA is built on a partnership model and we are committed to working with Congress and with industry to strike the right balance with these principles in mind.

○