S. Hrg. 117–266

# NATIONAL CYBERSECURITY STRATEGY: PROTECTION OF FEDERAL AND CRITICAL INFRASTRUCTURE SYSTEMS

## HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 23, 2021

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
47–628 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
MICHAEL A. GARCIA, *Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
ANDREW DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*
WILLIAM H.,W. MCKENNA, *Minority Chief Investigator*
PATRICK T. WARREN, *Minority Investigative Counsel*
CARA G. MUMFORD, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

# CONTENTS


| Opening statements: | Page |
|---|---|
| Senator Peters | 1 |
| Senator Portman | 3 |
| Senator Carper | 13 |
| Senator Hassan | 15 |
| Senator Ossoff | 23 |
| Senator Lankford | 26 |
| Senator Scott | 29 |
| Prepared statements: | |
| Senator Peters | 37 |
| Senator Portman | 39 |


WITNESSES

THURSDAY, SEPTEMBER 23, 2021


| | |
|---|---|
| Hon. Chris Inglis, National Cyber Director, Executive Office of the President | 5 |
| Hon. Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security | 7 |
| Christopher DeRusha, Federal Chief Information Security Officer, Office of Management and Budget | 9 |


ALPHABETICAL LIST OF WITNESSES


| | |
|---|---|
| DeRusha, Christopher: | |
| Testimony | 9 |
| Prepared statement | 54 |
| Easterly, Hon. Jen: | |
| Testimony | 7 |
| Prepared statement | 47 |
| Inglis, Hon. Chris: | |
| Testimony | 5 |
| Prepared statement | 42 |


APPENDIX


| | |
|---|---|
| Portman chart | 58 |
| Portman CISA Alert | 59 |
| Portman Communications Association Letter | 65 |
| Portman Financial Associations Letter | 70 |
| Portman Multi Association Letter | 73 |
| Portman Pipeline Letter | 76 |
| Additional statements for the Record: | |
| AAI | 80 |
| Responses to post-hearing questions for the Record: | |
| Mr. Inglis | 83 |
| Ms. Easterly | 88 |

# NATIONAL CYBERSECURITY STRATEGY: PROTECTION OF FEDERAL AND CRITICAL INFRASTRUCTURE SYSTEMS

**THURSDAY, SEPTEMBER 23, 2021**

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:15 a.m., via Webex and in room SD–342, Dirksen Senate Office Building, Hon. Gary Peters, Chairman of the Committee, presiding.

Present: Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley.

## OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. The Committee will come to order. I want to thank our witnesses for joining us here today and for their service to the American people. Your agencies and offices are vital to protecting Federal cyber networks and critical infrastructure systems.

Although it can often be difficult to understand the complexity and severity of many cyberattacks, they are only increasing in sophistication and frequency, and have a significant cost on our national security.

The Federal Bureau of Investigation (FBI) reported that there were 2,474 ransomware attacks in 2020, though experts believe that that number is actually much, much higher.

Just last month, in my home State of Michigan, about 1,500 patients were notified that their information had been exposed as a result of the breach of a file-sharing service used by their hospital. This breach, like the SolarWinds attack, is yet another example of how our adversaries target vendors and contractors, including small businesses, to find the weakest link and exploit our greatest vulnerabilities.

In order to prevent these types of attacks, potential victims, from the public sector to the private sector, must be aware of these ever-changing threats, and have the right information to safeguard their networks. Whether it is widespread spyware or a ransomware attack, the Federal Government needs to know when cyber incidents have occurred so they can determine if there are patterns, also future potential targets, and help seal up vulnerabilities.

[1] The prepared statement of Senator Peters appears in the Appendix on page 37.

This information is especially vital when it comes to our nation's critical infrastructure, 85 percent of which is privately owned and operated. Despite this vulnerability there is currently no national requirement for all critical infrastructure owners and operators to report to the Federal Government when they have been hit with a significant attack, and that needs to change.

As we have seen from recent attacks on an oil pipeline, water treatment plants, food processing facilities, and hospitals, these breaches can cause serious economic and national security concerns, and disrupt our daily lives. If multiple critical infrastructure entities, like energy companies for example, are reporting similar attacks, then Cybersecurity and Infrastructure Security Agency (CISA) and other Federal entities should be able to warn others, prepare for potential impacts to that sector or other related sectors, and help prevent further widespread attacks.

Ranking Member Portman and I are currently working on legislation that we plan to introduce soon, to require critical infrastructure companies that experience cyber incidents, and other entities that make ransomware payments, to report this information to CISA. This requirement will ensure CISA and other Federal officials have better situational awareness of ongoing cybersecurity threats, who those targets are, how the adversary is operating, and how best to protect the Nation.

I am looking forward to hearing from our witnesses today about how an incident reporting law could help each of your organizations assist victims in recovering from an attack and prevent them from happening in the first place. But we also need to ensure the Federal Government is sharing this same information in a timely manner.

The last time Congress substantially addressed Federal cybersecurity was in 2014, when this Committee, led by then Chairman Carper, passed the Federal Information Security Modernization Act (FISMA). Since then, our technology has developed rapidly, along with the sophisticated threats that we face. When that legislation was passed, CISA had not yet even been created.

We need to pass updated legislation that clarifies CISA's roles and responsibilities in Federal information security, improves how incidents on Federal networks are reported to Congress, and ensure that our cybersecurity resources are effectively aligned with emerging threats. Ranking Member Portman and I are also working on legislation that would help achieve these goals.

We also need a better understanding of how the Federal Government is balancing its responsibility to bring cybercriminals to justice and helping victims recover from an attack.

We learned earlier this week that in one instance, the FBI withheld a digital key that could have aided victims for several weeks to pursue its investigation. In order to conduct thorough oversight, this Committee needs to know more about the Federal Government's processes for assisting the victims of attacks and how your agencies weigh investigative, national security, and economic needs.

Finally, I want to acknowledge the important actions the Biden administration has already taken to bolster our cybersecurity defenses, improve information sharing, and apply the lessons learned

from previous breaches to avoid future attacks. The President's Executive Order (EO) "On Improving the Nation's Cybersecurity," for example, is paramount to securing our Nation.

This is a top priority for both myself and Ranking Member Portman, and I look forward to today's discussion and working productively with these vital Federal agencies to ensure we are addressing this threat.

Ranking Member Portman, you are now recognized for your opening comments.

**OPENING STATEMENT OF SENATOR PORTMAN[1]**

Senator PORTMAN. Thank you, Mr. Chairman, and thanks for convening this critically important hearing. I look forward to the dialog and it is great to have people in place who are now in charge of our cybersecurity system at the Federal Government level. Our strategy for protecting our cyber networks and critical infrastructure is something that we have been struggling with, frankly, and to have the leadership in place is very important to get that strategy right.

One important part of that, in my view, is accountability, and I hope to have a conversation about the appropriate roles and responsibilities for the many different cybersecurity positions within the Federal Government, who is in charge, who is making decisions, who is accountable. I also look forward to discussing how cyber incident reporting legislation might better inform that strategy, as the Chairman has just said. I think that is very important, and if we can get that right and if we can get a bipartisan product on that.

In recent years, hostile cyber adversaries, both foreign and domestic, have executed some of the most damaging cyberattacks ever, and we all know about these. We have had hearings about them, Colonial Pipeline most recently. Both the Federal Government and private sector companies have been targeted. We held hearings on SolarWinds, Colonial Pipeline, and others. These events are stark reminders of the wide-ranging and real-world impacts of sophisticated cyberattacks and impacts on people.

These attacks have become more and more common, and so it is important that we work to protect ourselves and our networks. One of the best strategies for preventing these attacks, of course, is to improve baseline cybersecurity practices, basic cyber hygiene. We also know that Federal agencies have failed to make meaningful progress on the implementation of these practices, as is actually required by law under FISMA.

In August, just last month, Chairman Peters and I released a report detailing the significant cybersecurity vulnerabilities of eight key Federal agencies: the Departments of Homeland Security (DHS), State, Transportation (DOT), Housing and Urban Development (HUD), Health and Human Services (HHS), Agriculture (USDA), Education, and Social Security Administration (SSA). This report follows a 2019 report I released with Senator Carper as Chair of the Permanent Subcommittee on Investigations (PSI), evaluating the same eight agencies.

[1] The prepared statement of Senator Portman appears in the Appendix on page 39.

In this year's report, only DHS had an effective cybersecurity program. Every other agency featured in the report failed to meet this standard. We also found the average grade across all government agencies was a C minus, close to failing. The report identifies several common agency vulnerabilities, including the failure to adequately protect personally identifiable information (PII); maintain an accurate and up-to-date list of the agency's information technology (IT) assets; install security patches in a timely fashion; and retire vulnerable legacy technology that is no longer secure.

Securing fragmented networks against increasingly sophisticated attackers is not an easy or trivial task. It would be unfair to suggest otherwise. Yet, in the nearly seven years since FISMA was last updated in 2014, agencies still have the same vulnerabilities, year after year.

Accountability is a critical aspect of any strategy. All three witnesses with us here today have heard me discuss the importance of it for Federal cybersecurity in particular. At all of your confirmation hearings and in our conversations we talked about the need to ensure that we have appropriate accountability for these Federal networks and the agency systems. Among the three of you and the Deputy National Security Advisor for Cyber, I believe that we will continue to see these inconsistencies or vulnerabilities, because of the question about accountability, unless we are clear about who is in charge, who is in charge to better prevent, who is charge to better respond to cyberattacks. I look forward to continuing that discussion today again of how we can best achieve that accountability.

We are also here to discuss another important topic of overarching strategy, and particularly, cyber incident reporting. As I said, recent attacks on critical infrastructure, particularly through ransomware, demonstrate how prompt notification to the government can benefit both the government and its victims. In the case of Colonial Pipeline, the FBI was able to recover part of the ransom paid by Colonial to the attackers. There is a balance between getting information quickly, letting victims respond to an attack without imposing onerous requirements on them, and getting accurate information. We understand that balance and we want to try to reach the right balance to be sure that we are actually doing what we intend to do, which is to help the private sector and government agencies deal with cyberattacks. I look forward to the witnesses' perspectives on how to balance those competing priorities.

Again, Mr. Chairman, I appreciate the witnesses being here—glad you are in place—and I look forward to the dialog.

Chairman PETERS. Thank you, Ranking Member Portman.

It is the practice of this Committee to swear in witnesses, so if each of you would please stand and raise your right hands.

Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. INGLIS. I do.

Ms. EASTERLY. I do.

Mr. DERUSHA. I do.

Chairman PETERS. You may be seated.

Our first witness today is National Security Director (NSD) Chris Inglis. Director Inglis has over 41 years of Federal service and has held a variety of senior leadership assignments at the Department of Defense (DOD) and the National Security Agency (NSA). He initially began his career at NSA as a computer scientists within the National Computer Security Center, eventually serving seven and half years as a senior civilian and deputy director. His work included tours in information assurance, policy, time-sensitive operations, and signal intelligence operations.

In addition to his civilian work, Mr. Inglis' military career includes over 30 years of service in the U.S. Air Force (USAF), nine years on active duty, and 21 years in the Air National Guard (ANG), from which he retired as a brigadier general in 2006.

Mr. Inglis, thank you for all of your service to the American people. I know this is the first time you have come before this Committee since your confirmation, and we expect you will be here many times in the time ahead.

So welcome. You may proceed with your opening comments.

**TESTIMONY OF THE HONORABLE CHRIS INGLIS,[1] NATIONAL CYBER DIRECTOR, EXECUTIVE OFFICE OF THE PRESIDENT**

Mr. INGLIS. Thank you, sir. As do I. With your permission, I will remove my mask for the duration of my remarks.

Chairman PETERS. Certainly.

Mr. INGLIS. Chairman Peters, Ranking Member Portman, 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 and Mr. DeRusha. 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.

I am mindful of the history of this moment, and appearing before you as the first National Cyber Director (NCD), a position that you created last year and confirmed me for following my 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 fruition, and for the cybersecurity and critical infrastructure investments that you have made and are proposing in follow-on vehicles like the Infrastructure Investment and Jobs Act. 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 the Office of the National Cyber Director is making progress in standing up as a full-fledged contributor to the various initiatives we will discuss today. While we are anxious to receive appropriations needed to implement our strategy fully, no resource in this business is more valuable than our people. As you well realize, cyber talent is in high demand everywhere, but we are pleased with the quality and the experience of the people we have recruited thus far, and we will continue to work with Congress to secure the resources we need to bring on key staff.

[1] The prepared statement of Mr. Inglis appears in the Appendix on page 42.

In the coming months, I expect our contribution from the Office of the National Cyber Director to the President's cybersecurity agenda to grow and focus on a few key challenges: accountability and follow-through on the implementation of cybersecurity policy and investments; securing technology supply chains and the broader cyber ecosystem; fostering collaboration across the public and private sectors; coordinating closely with the Office of Management and Budget (OMB) and CISA on the security, resilience, and coherence of the Federal network enterprise; and ensuring defensive cyber operation and planning we are equipped and postured for success.

I will also be working with my colleagues to continue implementing crucial initiatives, directed by President Biden, including working with my counterparts on the implementation of Executive Order 14028, on improving the nation's cybersecurity; initiatives to strengthen and proactively defend critical infrastructure cybersecurity; and the central challenge of building a cyber workforce to meet our needs well into the future.

To these ends, the Office of the National Cyber Director will endeavor to drive the Federal Government's efforts through the following priorities. First, the office will champion coherence across the Federal cyber enterprise, ensuring we speak with one voice, and more importantly, operate with unity, purpose and effort.

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

Third, we will carefully analyze the cyber maturity of Federal agencies and chart a path for ambitious cybersecurity goals against which the U.S. Government can effectively execute. We look forward to close partnership with OMB to align resources and authorities together with these ambitions.

Finally, the office will work to increase present and future resilience, not only within the Federal Government but across the American digital ecosystem. That is a big task for which we have started by exercising incident response and planning processes from which we have already learned much regarding how to evolve those processes into the future.

Through these and other efforts, we are working to ensure that our workforce, our technologies, our organizations, and our relationships are not only fine-tuned for today's needs but are futureproofed for service in an ever-changing world. These are daunting undertakings. While the Office of the National Cyber Director is young and small, once expected funding is in place, and with the partners we have today, along with the support of Congress, it will be in a strong position to succeed in delivering the expected returns.

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

Chairman PETERS. Thank you, Mr. Inglis.

Our next witness is Jen Easterly, Director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. As Director, Ms. Easterly leads CISA's efforts to protect and defend the security of the nation's cyber and physical infrastructure. Ms. Easterly has an established record of public service, including two tours at the White House, most recently as Special

Assistant to President Obama and Senior Director for Counterterrorism, and previously as Executive Assistant to National Security Advisor Condoleezza Rice in the George W. Bush Administration.

She is a veteran of the United States Army, with more than 20 years of service in intelligence and cyber operations, including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan.

Ms. Easterly, I know this is also your first time you have been before this Committee since your confirmation, and we expect to see you here on numerous occasions in the time ahead as well. Welcome, thank you for your service. You may proceed with your opening comments.

**TESTIMONY OF THE HONORABLE JEN EASTERLY,[1] DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. EASTERLY. Thank you Chairman. I look forward to it.

Chairman Peters, Ranking Member Portman, distinguished Members of the Committee, thanks for the opportunity to testify on behalf of CISA on what I believe is the most important national security imperative, our nation's cyber defense. I am grateful for your trust in confirming me to this position, and as I have shared with my team on each of my first 73 days in this office, I have the best job in government.

As I always say, cybersecurity is a team sport, so I am truly honored to testify today alongside Chris Inglis and Chris DeRusha, my teammates and partners in cyber defense.

I have spent the past two and half months getting to know my teammates within CISA and engaging with partners across the Federal Government at the State and local level, in private industry, and across the globe. Based on those observations, I want to outline my priorities for CISA and thoughts for how to move forward collectively to raise our cybersecurity baseline.

As the Director of CISA, I am focused on building our workforce, strengthening the resilience of our Federal civilian enterprise, and elevating the security of our nation's cyber ecosystem. First, people are CISA's No. 1 asset, and I am intently focused on making CISA the world's premier cyber and infrastructure defense agency, the place where the best network defenders want to work.

When I arrived at CISA I found a dedicated, innovative, and inspiring team. I intend to expand upon that foundation to build a culture of excellence and a talent management ecosystem that prizes teamwork and collaboration, innovation and inclusion, trust and transparency, ownership and empowerment. I am equally focused on building a workforce that reflects the diversity of our Nation, not just because it is the right thing to do but because it is the smart thing to do. Diversity of experience, background, and thought enables better problem-solving.

Incidents like SolarWinds and Colonial Pipeline, JPS Foods, and the scourge of ransomware attacks that you mentioned on our schools and hospitals and small businesses illustrate how cybersecurity impacts our daily lives. They also highlight the need to address shared cybersecurity risk, and it truly is shared. Together we

[1] The prepared statement of Ms. Easterly appears in the Appendix on page 47.

have to focus on strengthening our cyber defenses, investing in new capabilities, and fundamentally reimagining how we think about cybersecurity for the Nation.

To that end, CISA is pursuing capabilities that increase visibility into cybersecurity risks across Federal agencies and critical infrastructure. One such capability, CyberSentry, helps identify sophisticated threats to critical networks. We are excited about the results from the pilot and appreciate Congress' efforts to fully resource it.

CISA, as an agency, as you know, was designed to be something different and special, built on the foundation of collaboration with partnerships at the core of our mission. Recognizing that no single entity has all the answers, my goal is to shift the paradigm, transform public-private partnerships into operational collaboration, transformation information-sharing into information-enabling, making sure that the data we deliver to network defenders is timely, relevant, and most importantly, actionable.

We are going to do this, in part, through the newly established Joint Cyber Defense Collaborative (JCDC), and I want to thank you for authorizing it. JCDC harnesses the power of the Federal cyber ecosystem and the private sector to create a common operating picture. Our goal is to be able to see the dots, to connect the dots, and then to drive action to enable collective defense.

All of these efforts align with the imperatives conveyed in the President's Executive Order, as you mentioned, as well as the last year's National Defense Authorization Act (NDAA). They seek to further CISA's implementations of those requirements, and with respect to the EO in particular, I am pleased to note that CISA has fully met the highly aggressive deadlines for each of the 35 unique implementation efforts we were charged to lead.

That said, we have a lot of work ahead of us and we need Congress' help. As you know, there is no single mandatory Federal requirement for the reporting of cyber incidents, and without timely notification to CISA critical analysis, mitigation guidance, and information-sharing is severely delayed, leaving infrastructure vulnerable. Incident reporting must be timely, broad-based, and not limited by incident type or sector impacted. It also has to provide enforcement mechanisms to drive compliance.

Finally, legislation should provide CISA with the flexibility to define the scope of requirements in consultation with our partners, including importantly, the Department of Justice (DOJ) and FBI, balancing the benefit of reporting against the burdens to industry and government.

Finally, I would like to thank the Committee for the efforts on FISMA reform. As you said, FISMA is outdated. The status quo clearly is not working. A modernized FISMA should shift the spotlight from compliance and docs checking to true risk management. It also should recognize and codify CISA's role as the operational lead for Federal cybersecurity. As these efforts move forward, I really look forward to working with the Committee and our partners on it. It is hugely important.

Our nation faces an unprecedented array of cyber risks. Now is the time to act to deepen our collaboration, to strengthen our ability to defend the government's network to drive targeted action. We

must address this risk collectively to defend today and secure tomorrow.

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

Chairman PETERS. Thank you, Director Easterly. Thank you for being here.

Our final witness is Chris DeRusha. Mr. DeRusha has broad experience managing cybersecurity and critical infrastructure programs, plans, and operations in both the Federal Government and private sector. He has held roles at the Department of Homeland Security and at the White House, where he served as Senior Cybersecurity Advisor in the Obama Administration. He also previously served as the State of Michigan's Chief Information Security Officer (CISO).

Mr. DeRusha, as the Federal Chief Information Security Officer, you are charged with implementing and coordinating many of the efforts that we will be discussing here today, and based on your strong record in my home State of Michigan and your extensive experience, I have every confidence that you are up to this challenging task.

Welcome, Mr. DeRusha. You may proceed with your opening remarks.

**TESTIMONY OF CHRISTOPHER DeRUSHA,[1] FEDERAL CHIEF INFORMATION SECURITY OFFICER, OFFICE OF MANAGEMENT AND BUDGET**

Mr. DERUSHA. Thank you, Chairman Peters and Ranking Member Portman, distinguished Members of the Committee. Thank you for the invitation to testify about the administration's cybersecurity priorities. I am pleased to be here today with Directors Easterly and Inglis. The three of us work closely together in service of a common mission, to build a more secure Federal enterprise.

This Committee took decisive action earlier this year by supporting $1 billion in emergency funding to the Technology Modernization Fund (TMF). I would like to provide a brief update. To date, we have received more than 100 project proposals, requesting over $2.3 billion. Seventy-five percent of those proposals are focused on cybersecurity improvements. The need is clear. As the board prepares to release its first round of awards for this emergency funding, we are focused on learning what works well for one agency and translating that into successful outcomes for all.

These are challenging times to manage cybersecurity for any enterprise. It is not the time for us to maintain a steady course. We need to embrace bold ideas. We need to form enduring partnerships. Above all, we must act with a sense of urgency.

I would like to now highlight three areas of focus where the administration is taking decisive action on Federal cybersecurity. The first is zero trust. Earlier this month, we released, for public comment, a draft strategy to move the U.S. Government toward zero trust principles. This term, "zero trust," refers to a security model where every person, device, and network is considered untrusted and potentially compromised. This is a significant shift from the

[1] The prepared statement of Mr. DeRusha appears in the Appendix on page 54.

traditional model we have used throughout the public and private sector.

We have proposed an ambitious, multiyear plan that establishes a new baseline for government security and will require us to iterate and adjust over time. Our strategy directs agencies to adopt known, trusted technologies and practices that make harder for even sophisticated adversaries to defeat our defenses. The approach is purposeful and specific, yet flexible, for agencies to learn and adjust along the way. OMB will require agencies to develop funding and implementation plans to demonstrate earlier iterative progress, and, most importantly, to work together as one community in implementation.

The second area I would like to highlight is the Executive Order on improving the nation's cybersecurity. In May, the President issued Executive Order 14028, with the intent of dramatically improving the nation's cybersecurity, by deploying critical capabilities governmentwide, by improving information-sharing between U.S. Government and the private sector, and by strengthening the United States' ability to respond to incidents when they do occur.

We recently passed the 120-day milestone since the EO was issued. Over that time, OMB, National Security Council (NSC), and now the NCD have been working closely with agencies to execute key deliverables, which include a definition of critical software as well as accompanying security guidance from National Institute of Standards and Technology (NIST); the recommendation of new contract causes that will enhance how the Federal Government aims to work together to address cyber threats; OMB memoranda to help agencies identify and secure their most critical software; and set requirements for storing and sharing security data to support incident detection and response activities.

Finally, as I described a moment ago, it drives zero trust strategy and key supporting technical guidance developed by CISA designed to raise the security baseline of the entire Federal civilian government.

The final area I would like to highlight is FISMA reform. The Federal Information Security Modernization Act of 2014 describe the roles and responsibilities that underpin much of the policy and oversight work that my office does today. We appreciate the opportunity to work with Congress in reforming this flagship piece of legislation to improve the government's ability to manage risk. We share Congress' view that we should be more clearly oriented toward security outcomes, and we are actively updating guidance to agencies in support of this goal.

In conclusion, this administration is dedicated to making cybersecurity the immediate priority in Federal IT. Since January, we have been balancing a national response to a series of significant cyber events, well weighing the strategic groundwork for the future. As we move forward, we are focused on supporting agencies as they work to implement these priorities with diligence and that sense of urgency.

As I have said today, none of us can do this alone. It is a partnership where collaboration is key, with my colleagues here today, but more importantly with the personnel across the Federal Government that work tirelessly every day to safeguard our nation's

digital assets. I appreciate this Committee's leadership in this field, and I am confident that with your partnership and frank discussions, we are going to build a more secure and resilient Federal enterprise together.

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

Chairman PETERS. Thank you, Mr. DeRusha.

All of you are well aware that Ranking Member Portman and I are working together on an incident reporting bill that would require specific companies to report to CISA regarding cyber intrusions and when they make ransomware payments as well. Certainly after thousands of cyberattacks, including SolarWinds, the Microsoft Exchange, and the Colonial Pipeline ransomware attack, I think it is probably well past time for us to have some sensible legislation put forward to make sure that we are getting timely information about these incidents.

My first question is for Director Easterly. If our incident reporting bill were enacted, what would CISA do with this information, and how would you be able to help victims?

Ms. EASTERLY. Thanks very much for your question, Chairman. First of all, we really appreciate this effort. We absolutely agree it is long past time to get cyber incident reporting legislation out there, and we are excited to work with you on this.

CISA plays a critical role as the national coordinator for critical infrastructure resilience and security. As I think about CISA's superpower that we use on behalf of the Nation and the American people is our ability to share information rapidly to enable us to protect other potential victims.

What we could do with this information is not only render assistance to the victim and help them remediate and recover from the attack but we can use that information, we can analyze it, and then we could share it broadly to see whether, in fact, evidence of such intrusions were found across the sector or, frankly, across other sectors, or across the Federal civilian Executive Branch.

We think that timely and relevant reporting of cyber incidents is absolutely critical to help us raise the baseline and protect the cyber ecosystem.

Chairman PETERS. Mr. Inglis, my next question is for you. Would the type of information being collected by CISA, as laid out in the draft legislation that we are working on, help NCD formulate a national strategy and develop policies to prevent these attacks from happening in the first place? Clearly we want to be a deterrent for them to occur. Would this be helpful?

Mr. INGLIS. Thank you for the question, Mr. Chairman. I wholeheartedly support what Director Easterly just said, and do believe that information would be profoundly useful for the determination of an appropriate strategy. To reprise, that information is useful to help us be more efficient and to prioritize our response in the moment, to inform investments that we should make to get left of the event, to prevent these from happening in the future, and ultimately as a foundation of true knowledge, factual-based knowledge, such that we can create strategies that cover the gamut of cybersecurity activities.

Chairman PETERS. Mr. DeRusha, the incident reporting data from the bill that we are talking about, as well as a FISMA reform bill that we are also working together on would help protect Federal networks by indicating when intrusions have occurred on both private and government-owned systems, much like we saw after FireEye announced the SolarWinds attacks.

Is there anything else from the OMB's perspective that we should consider as we are developing the text in both of these bills?

Mr. DERUSHA. Senator, I believe it is crucial that Federal civilian agencies are included. We need to ensure that we have one common standard that everyone is following. That has been my experience, both at the State and Federal level, that there is patchwork of reporting requirements and they need to come together. It is really burdensome, and we are not focused on the right security outcomes.

The other thing I would say, though, is we have a really good partnership with CISA sharing threat information in a timely way to Federal agencies, and what we need is we need to increase the pipeline of information and getting it faster.

Those are the things that I would be really focused on.

Chairman PETERS. This next question is for all three of you, and I will start with you, Director Easterly. We will go in the same order that we just went through.

Each of you has a lot of experience in the private sector, and part of what we are looking at here is mandating companies to submit these reports, but we have to make sure they actually comply with that to get this information. I would love to hear your thoughts, and the Committee would love to hear your thoughts on the right enforcement mechanism to make sure that that information actually gets submitted. What should we be focused on. Director Easterly.

Ms. EASTERLY. Yes, thanks for the question, Chairman. As I mentioned in my opening remarks I do think a compliance and enforcement mechanism is very important here. I know some of the language talks about subpoena authority. My personal view is that is not an agile enough mechanism to allow us to get the information that we need, to share it as rapidly as possible, to prevent other potential victims from threat actors.

I think that we should look at fines. Fines are obviously used across industries. I just came from four and half years in the financial services sector where fines are a mechanism that enable compliance and enforcement. I realize this is a complicated issue, and I really look forward to working through it with you, because I think it is important that we are able to get the information that we need in a timely way.

Chairman PETERS. Thank you. Mr. Inglis.

Mr. INGLIS. Mr. Chairman, I support that view strongly. I would observe that most of the 50 States have reporting requirements of a similar sort, and the vast majority of those have an enforcement mechanism. Many of those use fines. There may be some best practices in there, if we do a thoughtful survey of how they have actually addressed this and how that has worked, and whether that has imposed an unfair burden on the victims.

We, of course, do not want to impose an unfair burden on the victims, but this information is essential for the welfare of the whole. There should be rewards for good behavior. If you have performed well and thoughtfully in this, the benefit should obvious, which is that we can provide better services, both in response and in preventing this in the future.

Chairman PETERS. Mr. DeRusha.

Mr. DERUSHA. Yes, Senator. I also agree, enforcement is needed, and I share the views of my colleague, and I would be happy to work with this Committee.

Chairman PETERS. Thank you. Before I recognize Senator Carper for his questions I need to step aside and attend another committee. As you can see from attendance we have committees. We are actually in the middle of a vote, so Members will be coming and going as this hearing continues. Senator Hassan, will chair in my absence. But as I leave, Senator Carper, you are recognized for your questions.

**OPENING STATEMENT OF SENATOR CARPER**

Senator CARPER. Senator Peters, can you hear Ms. Easterly?

Chairman PETERS. I can hear you.

Senator CARPER. All right. That is great. I can hear you too. Welcome to all of our witnesses today and thank you for your leadership and what you do with your lives.

My first question is for Director Inglis. Have I pronounced your right name correctly?

Mr. INGLIS. Yes, sir. Precisely correct. Thank you.

Senator CARPER. That is great. I have worked with colleagues, not just Democrats but colleagues on the other side of the aisle for many years on Federal data security and breach notification legislation that would protect the consumers' sensitive personal information. As you know, Director Inglis, each State as well as the District of Columbia and several territories have some form of their own breach notification law. There is, however, as has been said, there is no national standard.

In 2019, while I was privileged to lead the Permanent Subcommittee on Investigations, Senator Portman and I released a report dealing with Equifax's repeated failures to protect sensitive information for 145 million Americans, a lot of people. Director Inglis, can you take a moment to speak to the importance of having Federal data being breached standard and whether or not it would help covered entities have consistency in cyber-best practices and places to protect Americans' personal information?

Mr. INGLIS. Thank you for the question, Senator. As you may well know, the administration has no formal position on that at the moment, but I would observe the following, which is that given that 50 States have essentially addressed this, each one in their own way, if you are a company that operates across those 50 States you then have 50 challenges in terms of doing breach notification. I imagine that most of those companies are trying to get it exactly right, so they have to do it 50 times.

To the degree that we can harmonize and standardize that essential requirement to provide the breach notifications so that we can assure that the victims are properly notified and the recovery ef-

forts address their needs at that moment of vulnerability, I think that Federal legislation would be useful.

Senator CARPER. All right. Thank you for those comments.

Next, Jen Easterly, how are you?

Ms. EASTERLY. I am great, sir. How are you?

Senator CARPER. Good. How are things at CISA?

Ms. EASTERLY. They are awesome. Best job in government.

Senator CARPER. That is good. Would you work for nothing?

Ms. EASTERLY. Yes. I almost do.

Senator CARPER. All right. We are looking for ways to bring down the deficit. I will pass that on. [Laughter.]

Seriously, as we saw from the Colonial Pipeline ransomware attack earlier this year, when disaster strikes in the cyber world folks do not always know who to call. In fact, the Chief Executive Officer (CEO) of Colonial Pipeline, Joseph Blunt, was actually before our Committee earlier this year. He placed his first call, he told us he placed his first call to the FBI, but the FBI did not put him in touch with CISA. This incident, I think, makes clear that we need a plan for who to contact when a cyber incident occurs, and we need to better communicate that plan with not just our Federal partners but with State and private partners too.

Director Easterly, is there a clear and well-communicated plan in place for the Federal Government and for critical infrastructure entities to implement should they be subject to a cyber, or in the case of Colonial Pipeline, to a ransomware attack?

Ms. EASTERLY. Thanks so much for the question. A hugely important issue.

Senator CARPER. Who are you going to call? Ghostbusters. How are you going to call? They are not around these days, so who are we going to call?

Ms. EASTERLY. I think we are the new Ghostbusters, actually, Senator.

It is a hugely important question, and I would just say, I watched the hearing with Mr. Blunt from Colonial and I think it was great that FBI immediately reached out to CISA. We have a fabulous partnership with FBI, and that has only been confirmed over my last two and half months how important and how strong that partnership is.

But I think your point speaks to the larger issue and why this cyber incident reporting legislation is so important, because we need to get reports both about breach, as you were just talking to Director Inglis about, about ransomware, but really about all flavors of cyber incident. Because it is very important for us to both be able to render assistance to any entity that suffers an attack but to be able to analyze that information and to share it more widely, because we know that in today's world everything is connected, everything is interdependent, and everything is vulnerable.

So having that information in a timely way so that CISA can share it both with our partners across the Federal Government but, importantly, with our partners across critical infrastructure, and then, of course, at the State and local and tribal and territorial (SLLT) level, so that we can collectively raise the baseline of the cyber ecosystem. I think it is incredibly important to instantiate that in legislation, sir.

Senator CARPER. I agree. Thanks for that response.

I have a question, as well, if time will allow, to ask of all three witnesses. Let us start with you, Director, and then we will go to the other witnesses. As I believe you know, each of you mentioned, I think, in your testimony, in May 2021, earlier this year, President Biden signed the Executive Order aimed at strengthening our cybersecurity as well as our authority to respond to cyber incidents when they occur. I am pleased to see that we are shifting to a more proactive as opposed to a reactive posture in the cybersecurity space.

My question would be this for the three of you. To that end, could each of you take a moment to share with us how you are working in concert with one another to implement President Biden's Executive Order and what you need from Congress in order to implement these changes?

Director Easterly, why don't you go first.

Ms. EASTERLY. Great. Thanks so much, sir. Yes, I agree, it was a very significant Executive Order and I think it will really help make a difference for both the Federal cyber ecosystem as well as the broader ecosystem.

We have been working very closely with all of our partners, in particular our partners with Federal CISA, with my good teammates, Chris DeRusha here, and Chris Inglis, to make sure that we are implementing all of the tasks that were assigned to us. I think we had 35 total, and we have met all the deadlines to date.

As you said, this is about a paradigm shift and how we protect the Federal cyber ecosystem, improving information-sharing from Federal contractors, modernizing the infrastructure to move to zero trust architecture, as Mr. DeRusha already talked about, making sure we have cloud-secure instantiations, and then making sure that we are implementing what we call endpoint detection and response (EDR) technology, which allows us to not just focus on the perimeter but really to focus in depth, all the way down to the host level, at the workstation, at the server, to ensure that we can see what threats are out there, detect suspicious activity, and ensure that we are able to mitigate and remediate it as soon as possible.

So those aspects of it, plus all we are doing about secure software, software bill of materials, and then finally, everything we are doing to improve detection around logging.

So a lot of work done. I look forward to keeping the Committee updated, sir, on the important work. Thank you.

Senator CARPER. Thank you, ma'am. Mr. DeRusha, really the same question. Talk to us a little bit about——

**OPENING STATEMENT OF SENATOR HASSAN**

Senator HASSAN [Presiding.] Senator Carper, I am going to ask each witnesses to respond to your question, but you are over by about a minute, and so we need to move along.

Senator CARPER. OK. Thank you. All right. I will yield. Thank you.

Mr. DERUSHA. Yes, Senator. Look, it was a very large, aggressive action plan, which we felt completely appropriate for the moment. We are focused, and made a lot of progress already on baseline hygiene measures. Director Easterly just described some of those.

We have also set in place a multi-year strategy and plan, and, what we are going to need from Congress is, we are going to need some new resources to implement this plan. But what we have done is we have really laid out, in pretty descriptive detail, what we need to do to become more secure as a Federal enterprise. We really look forward to working with Congress on those priorities.

Mr. INGLIS. Senator, I will answer quickly. I am largely in agreement with all of those remarks. I was impressed with the audacity of the plan—very aggressive. I am pleased with the performance. We have met or exceeded the objectives that were established. I am sobered by the idea that it is simply a down payment. To Mr. DeRusha's point, we have much more work to do, and we, therefore, need to redouble our efforts to do that.

Senator CARPER. Thank you all very much.

Senator HASSAN. Thank you, Senator Carper. Because Senator Portman is not back yet I am going to recognize myself for a round of questions, and I want to thank Chair Peters and the Ranking Member for this hearing, and I also want to thank the three of you not only for your service but for your testimony today and your commitment to improving the country's cybersecurity.

My first question goes to Directors Easterly and Inglis, and I will start with Director Easterly. One of the biggest impediments to improving cybersecurity is the shortage of qualified cybersecurity professionals at Federal, State, and local level. I have introduced, along with Senator Cornyn, the Bipartisan Federal Cybersecurity Workforce Expansion Act. The act would authorize a registered cybersecurity apprenticeship program at CISA, and it would also create a veteran cybersecurity training program at the Department of Veterans Affairs (VA).

Director Easterly, how would an apprenticeship program help address workforce challenges at CISA?

Ms. EASTERLY. Thanks for the question. I love that. I love apprenticeships. We have already started talking about how we could implement apprenticeships at CISA. I would love to work with you on that legislation.

I think we need to be as creative as possible in all our approaches to deal with the deficit that we have across the country and then across the Federal cyber workforce. So programs like rotational programs, apprenticeships, internships, and I am very excited, in particular, about implementing our Cyber Talent Management System (CTMS), finally, to enable us to more flexibly hire people from all walks of life, basically based on their aptitude, not based on certifications or degrees.

So anything to do with workforce, Senator, I would love to work with you and your team and this Committee.

Senator HASSAN. Great. I would look forward to that.

Director Inglis, what do you think of cyber apprenticeships and a veterans' training program, and are there other ways we can increase the talent pipeline to build a larger cybersecurity workforce?

Mr. INGLIS. Senator, once again I am in that position where happily I agree strongly with both the premise that you have established and Director Easterly's remarks. I think apprenticeships are essential, not simply because they provide experience for its own sake, but they bridge the gap between aspiration that is often sup-

ported by training and education and the real experience that employers need or want when you show up at that door. It helps to transition from one phase to another, in terms of one's work life.

To the extent that that is something we can pilot, at CISA or within the Veterans Administration or other places, I would hope that we make that broadly available to the rest of government.

As to what else we can do, I think that it falls into three broad buckets, which are not unrelated. We need to increase awareness, so that every citizen, every person who experiences cyberspace has what is necessary to cross the digital cyber street in the same way that we teach children to cross actual streets, and that they are aware of the opportunities in this space.

It would be to make sure that we invest some more training and education in those who make decisions that implicate cybersecurity but they do not know it, whether they are lawyers or logisticians or system engineers.

Then, of course, we need to double down on filling the jobs that have cyber and IT in their job title. I think we need to be as broad-based as possible. To Ms. Easterly's point, we need to encourage diversity, because that is a mission-essential strength. But at the same time let us relook those jobs skills to make sure we are asking for the right things. You do not need a bachelor of science in computer science for every one of those jobs.

Senator HASSAN. Thank you very much.

Director Easterly, the Office of Management and Budget recently released a draft zero trust strategy, and it was nice to hear Mr. DeRusha talk about it. It states that the continuous diagnostics and mitigation (CDM) program run by CISA is a foundational element of the Federal Government's cybersecurity. I introduced legislation with Senator Cornyn last Congress to codify the program, and we are working on reintroducing CDM legislation this Congress.

When do you expect all civilian Federal agencies to have their electronic assets inventoried and continuously monitored via CDM?

Ms. EASTERLY. Thanks for the question. It is a great one. Having a lot of experience in this space, and certainly in the private sector, asset inventories and ensuring that you know exactly what is in your network is not a trivial endeavor.

All that said, I am told that we are at about 85 percent of an understanding of the Federal endpoints, and so I think we will get there in the near term, and I am happy to keep you updated on the course of our progress.

Senator HASSAN. OK. A related issue, of course, is whether CISA is re-evaluating previously approved CDM tools to ensure that they still meet the newest best practices and our zero trust strategy. So is that happening as well?

Ms. EASTERLY. Yes, ma'am, absolutely, as part of our entire modernization effort to make sure that we are able to provision the right capabilities through the CDM program, and some of the most important ones, as you are aware of, are EDR capabilities.

Senator HASSAN. OK. Another question for you, Director Easterly. Next week I am going to lead a Subcommittee hearing on the Federal Government's IT management resources. The service is available to agencies to modernize their aging systems and ways to

improve those programs while also saving taxpayers money. Mr. DeRusha, I am looking forward to hearing from your colleague, Federal Chief Information Office (CIO) Clare Martorana on this topic.

An important aspect of ensuring the cybersecurity of Federal systems is modernizing outdated and obsolete IT systems, which are difficult, if not impossible to properly secure. Director Easterly, how is CISA supporting agency efforts to modernize their aging IT systems to improve cybersecurity?

Ms. EASTERLY. We are taking a very aggressive approach, because we understand the urgency here. That said, Senator, this is a very complex endeavor, dealing with years and years of legacy systems. It is why, as my colleague, Mr. DeRusha, mentioned, the TMF fund is so important to enable that modernization.

We are working hand-in-hand with departments and agencies to ensure that they have the capabilities that they need to enable them to build out networks in a different way, and it really goes to zero trust architecture, the secure cloud systems, the maturity model. We are pushing as hard as we can, Senator. It is a big project, and it is really one of the reasons why I am excited about FISMA reform, because we need to ensure that we can do this the right way, and secure an enterprise, not 102 separate departments and agencies.

Senator HASSAN. Thank you.

Last question for you. I was delighted to hear your testimony and by the recent announcement from CISA about the Joint Cyber Defense Task Collaborative.

Ms. EASTERLY. Like ACDC.

Senator HASSAN. I know, yes, except not. But yes. It is intended to improve planning, information-sharing, and collaboration among interagency, intergovernmental, and private sector partners. However, several of our critical infrastructure sectors, particularly the health care and education sectors, are severely under-resourced when it comes to cybersecurity, especially compared to the JCDC's initial private sector partners.

What lessons is CISA learning to learn from its initial industry collaboration that will help it and the JCDC support health care, education, and other sectors that are often under-resourced? I see that I am over time, so if you can make your answer brief. I can follow up with you as well.

Ms. EASTERLY. I will do my best. The whole idea of those initial plankholders were those who had massive visibility, so they can drive action at scale, Senator. The fact that we have the Content Security Policy (CSPs), the Internet Service Provider (ISPs), the cybersecurity vendors, that see the dots so we can connect them, will allow us to have that information and provide it to the other critical sectors, so that we can help health care and education and all of the, what I would call, target-rich, sometimes resource-poor sectors. So they will accrue benefit from what we are building in the JCDC.

Senator HASSAN. Thank you very much. Senator Portman.

Senator PORTMAN. Thank you, Madam Chair. I want to start, if I could, by asking unanimous consent (UC) to put something in the record that has to do with reporting. This is some of the feedback

that we have received from industry and government with regard to our cyber notification legislation. I think the bill is better for this input, and I think it would be appropriate to have these letters included in the hearing record.[1] All three relate to the legislation. One is from 18 trade associations, one is from the financial sector, one is from the communications sector, and the fourth is from the oil and gas sector, expressing their concerns in that case about lack of consultation with the pipeline industry before issuing security directives.

Senator HASSAN. Without objection, so ordered.

Senator PORTMAN. Thank you, Madam Chair. Let me start with something urgent. I am really eager to get to the accountability issue because, as you know, I think that is critical for us to be able to organize ourselves properly going forward. But unfortunately, we live in a state of constant attacks, and we just had another one.

There is a joint publication by CISA, the FBI, and the U.S. Coast Guard (USCG) last week that indicates an advanced, persistent threat, meaning right now, timely, a threat, targeting a software program used to authenticate users when they log onto their computer. According to this publication it is widely used by several critical infrastructure sectors. The hackers have covered their tracks, much like we saw with SolarWinds.

Again, I would hope we could talk about the important, not just the urgent, but the urgent is upon us again. I would ask you, Ms. Easterly, can you briefly explain, what this is and why it matters?

Ms. EASTERLY. Yes. Thanks very much for asking that question, Ranking Member Portman, because it does speak to, I think, a really good-news story and the collaboration and how we use data to help protect other sectors of critical infrastructure.

So you are referring to something called ManageEngine ADSelfService Plus, which is this password management and single sign-on capability. We worked with the U.S. Coast Guard on a vulnerability at the Port of Houston and found out about this. We worked with our FBI partners and our Coast Guard partners to better understand that vulnerability, and then to be able to get that information out, to see whether, in fact, we saw the same vulnerability across the Federal cyber ecosystem and in our critical infrastructure partners. This was actually one of the early successes for JCDC, because we were able to share that information across our JCDC partners to see if they could find additional victims to notify.

To this point in time, we see that the campaign thus far is limited, but we are continuing to work through it, and I am happy to keep you apprised.

Senator PORTMAN. I appreciate that. I guess I am glad to hear that, that you feel like, in this case, we have a handle on it. I did speak to one of your prominent JCDC members yesterday, and I support what you are doing there, including bringing the private sector expertise in. I think it is critically important.

The alert indicates that this advanced persistent threat and these actors have been exploiting vulnerabilities but also covering their tracks. What does that mean, and does that mean if it is a

[1] The letters referenced by Senator Portman appears in the Appendix on page 65.

nation-state actor, as an example, we are not going to be able to determine who it is?

Ms. EASTERLY. As you know, Ranking Member Portman, attribution can always be complicated in terms of being able to positively say who that threat actor is. Certainly the most sophisticated threat actors go to great winds, as we saw with SolarWinds, to be able to cover their tracks and obfuscate their presence, so that they can live for long times in networks and be able to extract data.

But we are working very closely with our interagency partners and the intelligence community (IC) to better understand this threat actor so that we can ensure that we are not only able to protect systems but ultimately to be able to hold these actors accountable.

Senator PORTMAN. Right. But in terms of this one, can you tell us who you think it is?

Ms. EASTERLY. At this point in time I would have to get back with my colleagues, but I do think it is a nation-state actor, sir.

Senator PORTMAN. Concerning, yes.

Ms. EASTERLY. Yes, sir.

Senator PORTMAN. OK. We look forward to hearing more as you have it, perhaps even in a classified setting, to understand what we can do to be able to respond, as you say, to be able to push back against these nation-state actors who continue to probe and to commit these crimes against our public and private sector entities, in this case critical infrastructure.

OK. Accountability. I am going to show a chart[1] here. It is a chart that tries to explain what the roles are. Maybe it is just me, but it seems like there is a lot of overlapping responsibility, including, by the way, among the three of you. The question is, who is in charge, who is accountable.

We talked about this latest hack, and you mentioned that you are involved, as the, CISA lead, which is good. But also you indicated that there are other entities involved. The question is, who is in charge and who will take accountability as things happen?

This chart has, with regard to the strategic side, the National Cyber Director, who is here with us today, and the Deputy National Security Advisor, who has been with us here before. She is not with us today but she has a role that she has indicated is, in some ways, quite similar to your role. Then we have OMB, of course, the Federal CIO, and the Federal CISA role. Then the CISA Director and the FBI CISA Director for Cyber are more on the operational side.

On the strategic side, of course, every agency head has to be involved, and should be, and then, of course, the agency CIOs and the CISA in the agencies, and that goes to our FISMA issue we talked about earlier.

I guess I would start with you, Mr. Inglis, and again, I am glad you are where you are. I wish you had more staff to be able to do your job, which is another topic we will discuss. Under your authorizing statute, you are the principal advisor to the President on cybersecurity and cybersecurity strategy. Is that correct?

Mr. INGLIS. That is correct, sir.

---

[1] Thge chart referenced by Senator Portman appears in the Appendix on page 58.

Senator PORTMAN. Does that mean that you are the single point of accountability for Federal cybersecurity within the Executive Branch?

Mr. INGLIS. I think I am the single point of accountability for Federal cybersecurity on owned or leased estates, to include the Federal Government and the critical infrastructure. When we determine that we need to use instruments of power outside of owned or leased estates, then military diplomacy, financial instruments of power, the National Security Council (NSC) is the natural place to essentially coordinate those instruments of power, and, therefore, they would interact to determine what that strategy should be to do the rest of what is required.

But for purposes of preparation, synthesis of the big picture, defense of owned and leased estates, performance assessments, I am the accountable person.

Senator PORTMAN. So are you accountable, as an example, if the Department of Homeland Security does not have proper cyber hygiene in place? Probably not a good example because they are one of the few agencies that we found, of the eight, that was doing some of the right things. But let us say the Department of Health and Human Services or the Department of Energy (DOE). Are you the one responsible?

Mr. INGLIS. Yes, sir. I am ultimately the accountable person. Now, my job is to ensure that that accountability has been allocated property to agency and department heads, to CISA for being the operational entity coordinating the defense, to OMB for issuing the right directives. As the coach—as we have used that term before—I need to ensure those roles are properly assigned, properly executed, and ultimately to do performance assessments to ensure that we are meeting the need.

Senator PORTMAN. Let me ask you this. This organizational chart, again, we have talked about, in the past, the overlap, and you just talked about the National Security Council overlap with what you are doing. Do you think the Federal Government's organizational structure is effective right now, and do you think that the lines of responsibility are clear?

Mr. INGLIS. I think it is reasonably effective. Can we make it better? We can, and we will. The three of us at this table talk on a daily basis about how to actually ensure that these roles complement one another.

I would observe that the chart does not show sector risk management agencies. That is a further complication of what they on the edge of the enterprise that they represent. All of those strengths represent diversity, which properly applied can be a huge strength for us. It is perhaps then less complicated than the U.S. Department of Defense or an American football team, which, if it has the right strategy, if it has the right roles, if the life forces that course across it create coherence, Unity of Purpose, Unity of Effort, it can, in fact, be quite useful. That is our job, is to make sure that the video actually makes sense, even if the static picture does not.

Senator PORTMAN. You make the football analogy. There you have a coach, who is ultimately responsible. You have a quarterback responsible for the offense. The question is, how do you have that with this more diffuse structure?

Is there any thought of issuing an Executive Order or some other rulemaking to more clearly delineate what the——

Mr. INGLIS. I think there is, sir. I think that is essential. We are actually taking our time, not because we are complacent in any way, shape, or form, but taking our time to actually let a modest amount of experience drive our efforts to then clarify, in writing, what we believe is the right and proper way to describe that chart in action.

I think you would have hopefully seen, over the last three or four months, there were several times when we reported informally to this Committee not on a major incident but an incident we thought was reflective of the work that we do together, where we surged to the point of maybe to assist an agency that was encountering some difficulty. We checked the rest of the enterprise, the Federal enterprise in that case, to ensure that that had not been something experienced by others. We visited with the investment strategy, using OMB resources to ensure that we were making the proper investments to get ahead of this, and reworked that according. Then ensure that ultimately those best practices became something that everyone could benefit from.

That is complicated. That is hard to do, but it is the necessary work of the leadership that you have charged to undertake coherence in that diagram behind you.

Senator PORTMAN. Let us go to one of those points that you just made, which is the cybersecurity budget for the agencies. Mr. DeRusha is here with us, on the panel, and you are here on the panel, yet both of you have that responsibility as I understand it. You have responsibility over the agency cybersecurity budgets and what they ought to be. Is that true, Mr. DeRusha?

Mr. DERUSHA. Sir, OMB does, absolutely.

Senator PORTMAN. So say it again?

Mr. DERUSHA. I am sorry, sir. Yes, OMB has the responsibility. It is a shared responsibility between the management side, but largely the budget side, the resource management officers.

Senator PORTMAN. OK. I do not want to put Mr. Inglis on the spot here, but would you agree with that, Mr. Inglis, that you do not have responsibility for cybersecurity budgets?

Mr. INGLIS. I do not have unique and solitary authority over that. I agree.

Senator PORTMAN. Not unique and solitary, but Mr. DeRusha just said that it is OMB who has unique and solitary over that, that responsibility, and my understanding is that you believe you have responsibility for it too.

Mr. INGLIS. Oh no, sir, I do not. By statute I have the responsibility to report on performance. I do not have the authority to direct dollars. I do not have the authority to move dollars. But I think I have a useful and necessary function to report on performance.

I think by example what we have done has actually joined those two responsibilities in a way that it is coherent. Take the Technology Modernization Fund in hand, as earlier described by Mr. DeRusha. There is $1 billion allocated by the Congress for that purpose. There is $2.3 billion in applications. OMB, using its authority, has described what the requirements are that would allow

them to judge the merits of any particular application. They have been paneled aboard.

I have looked at those requirements. I have judged that the panel is an appropriate panel to adjudicate this, and I look at each of the applications and each of the awards to ensure that they are consistent with our overall cyber strategy. I therefore am in a place where I am performing my responsibility to ensure performance, at the same time allowing OMB to perform their statutory responsibility to be accountable for the budget.

Those two nicely, but in a complicated way, intersect at this thing we call cyber. I think that is, by statute, where we are. We could possibly clarify that to a greater degree in the FISMA modernization and other bills, but the things that I think that we are enjoying at the moment, we can achieve coherence with the roles as they are defined.

Senator PORTMAN. OK. I am over time already and I apologize to my colleagues. Let me read the statute for what you are supposed to be doing: "Reviewing the annual budget proposals for relevant Federal agencies and departments and advising the heads of such departments and agencies whether such proposals are consistent with the national cyber policy and strategy." It sounds like you are involved in the budgets. But I look forward to further conversation in the second round.

Thank you, Mr. Chairman.

Chairman PETERS [Presiding.] Thank you, Ranking Member Portman.

Senator Ossoff, you are recognized for your questions.

**OPENING STATEMENT OF SENATOR OSSOFF**

Senator OSSOFF. Thank you, Mr. Chairman, and thank you to our panel. Thank you for your service.

Mr. DeRusha, you have responsibility as Chair of the Federal Acquisition Security Council (FASC) for risk management in the supply chain for Federal agencies. We saw Apple rush out an iDevide Operating System (iOS) patch a couple of weeks ago, an exploit that allowed targeted, remote jailbreaking of iOS devices, which it appears had been outstanding for at least several months, and was used to target certain individuals, was revealed.

What is your assessment of your capabilities and the capabilities of the private sector partners you work with, your interagency partners at identifying zero-day exploits that could be used to target senior government executives by foreign intelligence services or to penetrate public sector or private sector networks, and what additional authorities or reforms to procedure or law might be contemplated to improve our ability to get ahead of that kind of exploit?

Mr. DERUSHA. Senator, I will respond first, but there is also a shared equity with this entire group, in particular at CISA and FBI and other partners.

I will speak a little about the role of the FASC. We are primarily focused on supply chain risks that have a nexus to national security, foreign threats, and others. There is an acute focus of the FASC and its responsibilities, however, in our ability to make rec-

ommendation of exclusion or removal orders for the Federal Government.

We also take on the responsibility, strategically, to ensure that we are providing the right guidance and risk information to Federal agencies. We are working on some new OMB guidance on that front, and we also work closely with NIST to ensure that they have the appropriate understanding of the standards that sit behind the effective risk management programs that they need to build at each Federal agency to secure itself. There is partnership there.

We have efforts to engage all the key stakeholders, both industry and other committees, like in Team Telecon and the Committee on Foreign Investment in the United States. There are a lot of groups and bodies that need to be pulled together to address the risks that you have described.

In particular to what you were talking about, vulnerabilities of that sort are, unfortunately, fairly pervasive across the entire ecosystem, and, that has not traditionally been the explicit focus of the FASC itself. But I would be happy to have a discussion regarding that further.

Senator OSSOFF. OK. We will come back to this topic in a moment. Mr. Inglis, I want to come to you for a moment and then hear from you, Ms. Easterly, on this as well. What changes to policy or operational posture of executive agencies have been made in response to lessons learned from the Colonial Pipeline breach?

Mr. INGLIS. Thank you for the question, Senator. In response to the Colonial Pipeline breach, what we have done is to shore up our response mechanisms. Ms. Easterly can talk at some length about that. We have engaged the CEOs of the pipeline sector to ensure that they understand what the Federal Government is prepared to do, but at the same time what we have an expectation of that they need to do in terms of increasing resilience and robustness, and they have responded in kind.

We have, therefore, kind of articulated what we believe the requirements are for the pipeline sector. We will probably do that for other sectors as well. We have worked closely with the private sector to make sure that that is understood and reasonable, and ultimately develop a response plan such that we can help them in the moment of need in a way that is timely, efficient, and prioritized.

Senator OSSOFF. Thank you. Ms. Easterly?

Ms. EASTERLY. Yes. I think as you know, Senator, there were security directives that were issued in the wake of the Colonial Pipeline incident, one of which, importantly provides the requirement to report cyber incidents to CISA. This is a way that we are able to gather the information to protect the larger sector and also connected sectors, so that is one very important thing.

Also, as part of the White House's Industrial Control System (ICS) Initiative, that first looked at energy, it is now looking at pipeline. We are actually working with major companies about what we can do to help them shore up their security to include instantiating technology that will allow them to detect more rapidly and to remediate and respond to any intrusions, one of those programs being CyberSentry, which we appreciate that Congress is focused on permanently authorizing.

Senator OSSOFF. Thank you, Ms. Easterly. I share the Ranking Member's concerns about the complexity of this bureaucracy. I recognize you are making good-faith efforts every day to rationalize it and streamline, apply the right authorities through the right agencies.

But I am curious, Ms. Easterly, based on your experience thus far, surely there is room for improvement. What is the most significant impediment to operational efficiency or effectiveness that you have experienced and observed in your time in this position?

Ms. EASTERLY. To be honest, Senator, it has been a pretty good experience thus far. At the end of the day, I think CISA's role is pretty clear. We have two primary roles. We are the operational lead for Federal cybersecurity, and I hope that gets formally instantiated in FISMA reform, and by statute we are the national coordinator for critical infrastructure, resilience, and security.

Both of those missions necessarily are team sports. It implicates partners across the Federal Government, as well as partners across critical infrastructure. We will never own that mission wholly because, as the Chairman said, over 85 percent is privately owned.

I feel very comfortable with the partnerships that we have forged to date, across the Federal cyber ecosystem, as well as with the private sector. As I said earlier, Senator, I am very excited about what we are building with the Joint Cyber Defense Collaborative.

Senator OSSOFF. I appreciate that, Ms. Easterly, and yet there must be obstacles in efficiencies and impediments to effectiveness that you do encounter on a daily basis, and the Congress needs to hear them, because we can learn lessons about modifications to statute or reforms to policy based upon your testimony. I would like to hear from you. What is not working? We need to know.

Ms. EASTERLY. With respect to Federal cybersecurity, I think with FISMA reform I would ask that the Congress do three things. First, that we codify CISA's role in Federal cybersecurity as the operational lead, that we make sure that we are holding departments and agencies specifically accountable for the investments that they make in their cybersecurity teams. They are making tradeoffs every day. They need to take that seriously and invest in cybersecurity and give some of those authorities between OMB and NCD and make that more explicit. Finally, we need to move from this compliance and box-checking to true operational risk management. I think instantiating all of that in FISMA reform will be incredibly important and helpful for our role.

Finally, I do think the cyber incident notification legislation is incredibly important to establish our ability to receive reports and then share them agilely and rapidly with the rest of the community so we can raise the baseline on the cyber ecosystem. I am sure as I progress in this job I may have some more things to come back to you on, Senator.

Senator OSSOFF. In addition to your deep experience in the Army, you have also worked in the financial services sector. How resilient and robust do you believe that sector's cybersecurity is, and what changes, either within the industry or at the regulatory level, need to be made to protect our markets from what could be a devastating cyberattack that could lead to a financial crisis or significant economic damage?

Ms. EASTERLY. Thanks for the question. It is a great one. Since 2012, when Wall Street was subject to a massive distributed denial of service attack there has been significant investments made by the financial services sector, billions of dollars to ensure that there is the right process, the right technology, the right people. That is why I think finance is generally in such good shape.

This is just my experience at Morgan Stanley—I think with respect to regulatory regime I always found it necessary to try and harmonize that, and I think we need to think about that with respect to cyber incident reporting, because it is very important that we are not asking a company, a business, that is under duress during a cyber incident to report to seven different entities, whether it is CISA for cyber incidents or to other regulatory agencies. The harmonization piece, I think is important.

But one other really important aspect of this, as good as finance can be it does not matter if electricity is not working, if the telcos are not working. Even as we look at these sector models, sir, we really have to look at this functionally, right? We have to look at the national critical functions. I think that is a very important lens, because everything is interdependent. Everything is connected. Everything is vulnerable. At the end of the day that is why I think CISA's statutory role as the national coordinator is so important because we have to look across the whole critical infrastructure ecosystem and make sure that it is as protected as it is connected in cyberspace.

Senator OSSOFF. Thank you. Mr. Chairman, I am over time. I have a couple more questions, if there is time for it later. But I yield.

Chairman PETERS. Very good. Thank you, Senator Ossoff. Senator Lankford, you are recognized for your questions.

**OPENING STATEMENT OF SENATOR LANKFORD**

Senator LANKFORD. Mr. Chairman, thank you. Thank you all for the work that you are doing. It is exceptionally important for the country, and I am grateful that you are engaging in this.

Mr. Inglis, let me walk back to something that Senator Portman was talking about before on the budget issues. You have a fairly unique situation here all of a sudden, that your office requested about $15 million to be able to stand up the office. The infrastructure bill gave you $21 million, and then the House Appropriations bill has allocated almost $19 million more. So you suddenly went from a $15 million request to, it looks like, a $40 million allocation. Is that what you are hearing, seeing?

Mr. INGLIS. My understanding is that there are three numbers. The $15 million was imagining that we would get a slow start in fiscal year (FY) 2022, therefore not be able to execute at a flat, high level across the whole year. Therefore you might take a $21 million figure, which is probably about the right number, and reduce that, because you are not going to expend all those resources if you do not have the same number of people at the start of the year as you do at the end.

With respect to the other budgets, my understanding is they are not additive, that they are kind of one or the other, those will hold sway.

Senator LANKFORD. OK. That is helpful, because we are trying to be able to track this as well, as you are trying to be able to stand this up.

Ms. Easterly, thanks again for your engagement on this. Obviously, after the Colonial Pipeline whole incident a lot of pipeline folks awakened to vulnerabilities that were out there, and that has been in the long-term conversation for years with a lot of the pipeline companies and some areas of vulnerability on this.

They made lots of hard decisions on this, but directives came out immediately that were emergency directives. What I am hearing now from a lot of the companies, not only pipeline companies but in others, saying, "Will we get to be at the table when the final version is done?"

Help us understand what you think that would mean, for them to be at the table, because obviously every single company is not going to be able to be there. There is a notice and comment period that allows every single entity and company to be able to contribute, but what does that look like now in the days ahead, when we start getting a finally ruling on this? Because there were some really good actors that had additional requirements put on them, or had to redo some things, but they were doing all the right things already on this. So they got consequences even though they were actually doing all the right things originally.

What does this look like, to be able to have more cooperation?

Ms. EASTERLY. Yes, thanks for the question. You are absolutely right. Some companies were doing the right things. Some were not. I think the objective of the security directive was to set baselines, and I think that is incredibly important. As you know, we have been working with pipeline companies for many years. Some of those vulnerabilities that we illuminated in the security directive had not been remediated for years, and we felt it was incredibly important to be able to really make aggressive progress on this.

So we absolutely recognize, and as I mentioned earlier, we are working closely with the big pipeline companies. We have a task force that has been set up. I was on the phone with them earlier this week. Understanding that there was some unhappiness from the community, I know that my colleague, Administration Pekoske briefed them on the security directive the other week and they were quite happy with having that opportunity to consult and collaborate on the way forward.

That is absolutely my approach going forward, Senator. Everything we do has to be in partnership, and I am looking forward to furthering those conversations.

Senator LANKFORD. Great. How do we start proactively sharing intelligence information, not just with pipeline companies but everybody in the infrastructure world, that actually has some context to it, if I can say it that way. Because sometimes different reports come out and they look so neutral that it really does not look like hair's on fire, do something right now. It is just a hey, be aware of, but there is no real context to it.

How do we help provide information to people proactively, to say we are hearing this, seeing this, take action immediately on this, in a way that has context to it and has some clarity to it of what to be able to do?

Ms. EASTERLY. Yes, that is a fabulous question. You sound like me when I was at Morgan Stanley. What we wanted was not just indicators but real context, because you have to take action against something, and if it unclear information it does not help a network defender. That is why we are so focused on timely, relevant, actionable, contextual information. We are making improvements on what is called automated indicator sharing (AIS). That is a program that has been around for a while, and we actually are adding context from things like the MITRE attack network that all network defenders use, to give more granular information for defense.

We are also looking to use CSPY, which is our cyber information-sharing collaboration platform, about 300 companies there, to ensure that we have regular analytic exchanges to include classified exchanges, to make sure that everybody has the information they need to shore up their networks.

Then finally, with respect to the JCDC, that is a way to be able to share information very rapidly, both within that small ecosystem and then within the larger community, to help enforce across the board what companies need to do to protect themselves in cyber.

I am optimistic about making progress, exactly as you are saying, contextual.

Senator LANKFORD. All right. That is helpful. If you are a large energy company you have lots of support on that. If you are a local co-op, you do not have the same level of support on that. As we are communicating with these companies, how are we getting to the co-op the same as we are getting to an Edison?

Ms. EASTERLY. That is a great question. I would answer it two ways. First of all, we are constantly putting out information through our platforms. We manage the Critical Infrastructure Partnership Advisory Council (CIPAC), which reaches all aspects across infrastructure to put out this information. We have resources, education, technical guidance, and assistance.

But one of the greatest things about CISA is our field force. We are 10 regions, 500 people across the country, security advisors that are in touch at the State and local level, with some of those smaller businesses, to ensure they have what they need to be able to make those changes to improve their cybersecurity baseline.

Senator LANKFORD. OK. That is helpful. Let me ask a question as you walk into this. Just perception at this point. Is the IC, the intelligence community, doing enough to be able to actually reach into areas for critical infrastructure protection, as was discussed earlier, to get left of some of these challenges, to be able to make sure that we are seeing into it, to see what is actually developing? We do a lot on our national security side, as we should, trying to be able to protect our larger systems and how we operate as well.

Are there things that we can do to be able to help engage with him more, to be able to raise the level of priority there?

Ms. EASTERLY. I think with respect to the intel community, in the past two and half months I have had many engagements across the board, and I have been, as I always was when I was in government, incredibly encouraged and impressed with the power and capability of our intel community.

I would say, though, Senator, with respect to some of the more exotic and sophisticated actors that take advantage of the blind

spots in domestic infrastructure—we saw that with SolarWinds, we saw it with Microsoft Exchange—I do not think that that should be an IC role. I am sure you agree with me on that.

Strongly, though, that is really the motivating impetus for the JCDC. The plankholder partners are those that have incredible visibility across the ecosystem, so they are able to see into things that the government cannot and alert us to trends in malicious cyber actor behavior and suspicious activity, to enable us to use that information to make the ecosystem safer. I think that is how we solve the dots issue. We solve the dots issue by the visibility through our partnership construct that we are building out now.

Senator LANKFORD. OK. Thank you.

Ms. EASTERLY. Thank you.

Chairman PETERS. Thank you, Senator Lankford. Senator Scott, you are recognized for your questions.

**OPENING STATEMENT OF SENATOR SCOTT**

Senator SCOTT. Thank you, Chairman Peters. Thanks for being here.

How important is the existing satellite system that the Federal Government uses to cybersecurity, and how risky do you think the satellite system is, as far as its ability to, in any time that somebody wanted to have a conflict with us, that it would be still viable?

Mr. INGLIS. I appreciate the question, Senator. Without having the details in hand, but happy to respond to that in further detail, I would say that the question is probably equally apt of how important is cybersecurity to those satellites. Satellites often perform critical functions for the Nation, whether it is weather observations or military command and control, and so on and so forth. We need to ensure that we have invested as much in them as we have in any other piece of critical infrastructure. Cybersecurity is essential for them. I think our adversaries would clearly hold those at risk if they thought they had the means or the ability to do so, and therefore it has to be in scope.

Senator SCOTT. Jen, what do you think?

Ms. EASTERLY. I would agree with that, Senator. Obviously, anything that is critical to our national security is something that we need to make sure is protected and secure. In today's technology world, we know that many things are connected and almost everything is vulnerable. It is why we work so hard to ensure that all sectors are raising their cybersecurity baseline. I very much agree with the Director on this.

Senator SCOTT. The way to think about it is, it is more they need you to make sure that they are not damaged rather than the other way around.

Mr. INGLIS. I agree. I talked with a gentleman a couple of weeks ago and he gave me a wonderful analogy. He says, "You know why race cars have bigger brakes? So they can go faster." The point he was making is that the reason we have cybersecurity, the reason we lay it on, is not for its own sake, and that is what we can be proud that we have done that, but so that we can enable a critical mission. I think that is the case with satellites or any other piece of our critical infrastructure.

Senator SCOTT. OK. What is the administration doing to go after these nation-states that target our critical infrastructure? I was Governor of Florida so we had all these hurricanes, a lot of them. The first thing you realize is you have to get the power back up and you have to get your communication back up, because eventually, if you do not get that done, you are going to run out and get food and water out to everybody.

What do you think we should be doing to deal with these nation-states that are targeting our critical infrastructure and central services, and are we doing enough?

Mr. INGLIS. Senator, I will start. I think that the administration's strategy, take ransomware as an example but it is not the only example where a nation-state would hold us at risk, there are four lines of effort currently in that strategy. One is you have to disrupt the infrastructure and the actors, determine what it is they make use of and try to hold that at risk, using all instruments of power, not simply cyber instruments of power. But use your legal remedies, your diplomatic remedies, your financial remedies, all of that, to essentially make it such that they cannot succeed.

Two, promote resilience, such that we are simply a harder target. That is sometimes less satisfying because you do not see kind of some flash in the night, but actually if you simply avoid the event it is far more meritorious than kind of working your way through it.

Three, address the abuse of virtual currency, which is underpinning. It is a huge fuel inside of this fire, and we——

Senator SCOTT. Can I interrupt you? Do you think that is doable?

Mr. INGLIS. I think it is doable, maybe not to the 100th percentile, but I do think it is doable.

Senator SCOTT. Good.

Mr. INGLIS. Right. So the sanctioning that occurred, what, two days ago, of MUEX, which has shown itself to be involved in so many of these transactions of virtual currency turning into hard currency, or vice versa, we can essentially kind of lock those down if we know that they are engaged in illicit activities, and actually try to hold the virtual system accountable for the same requirements that the hard currency system does.

Finally, I think that the fourth element, not independent of the other three, is to do this in the broadest possible coalition. This is an international issue, not a U.S.-only issue. We need to, if we are bringing pressure to bear on Vladimir Putin because he gives sanctuary or permissive action, we need to bring a coalition to bear to hold him at risk, to determine what it is he cares about, to use all of our powers across nation who have this same problem, who are like-minded in their desire to achieve the outcomes in this space.

Senator SCOTT. Do you want to add anything?

Ms. EASTERLY. I think it is a great rundown. I mean, this really is a whole-of-nation effort, where CISA's role, of course, is in that promoting resilience phase. We also do response and recovery. But I would be failing if I did not take this opportunity to just say that, yes, there are sophisticated and highly dedicated actors, sir, but much of the attacks that we see could be prevented with good cyber hygiene. And so incredibly important that all entities do the basics, to include, most importantly, in my view, implementing multi-fac-

tor authentication. We are going to spend Cybersecurity Awareness Month in October making sure that everybody has what they need to implement the basics.

Mr. INGLIS. Sir, if I might jump back in, just to complement Jen on this, if you go to StopRansomware.gov, a site set up by CISA, you actually learn quite a lot about how you can actually be your own best defense.

Senator SCOTT. Mr. DeRusha, do you want to add anything?

Mr. DERUSHA. No, sir. I think that it was well stated by my colleagues. The only thing I would say is, as the lead for Federal civilian we take an approach of anything of value is going to be a high target, so we have the high value asset approach. Then we prioritize our efforts around looking at the threats and vulnerabilities of those assets first. So that aligns completely with the concerns you raised and expressed here.

Senator SCOTT. Good. According to the U.S. Office of the Director of National Intelligence (ODNI) 2021 Annual Threat Assessment, China presents a prolific and effective cyber espionage threat, possesses essential cyberattack capabilities, and presents a growing influence threat. I think everybody would pretty much agree with that.

Can you describe some of the risks we face when it comes to cyberattacks from—let us pick on one—I would pick on Communist China?

Mr. INGLIS. Sir, I can, and I will try to go fast. I think we know all of this, and it is just a summary of what I think is already out there.

First and foremost, there is the theft of intellectual property that constitutes hard-won competitive advantage of our businesses, our industries to aid and abet the development of their own industries. That is simply wrong, and it an unlevel playing field that we need to challenge.

Second, kind of stealing some of that materiel, those secrets, they can hold our maneuvers, our actions at risk, our legitimate actions in the realm of diplomacy or military actions, hold that at risk in ways that are inappropriate.

Finally, they can attack our confidence by making it such that we might come to the conclusion that this digital infrastructure will not work for us when, and as it should, and that perhaps is the most insidious, pernicious threat of all.

The answer to all of this——

Senator SCOTT. I think that is true. Right? Don't you think most people believe it will not be there when we need it?

Mr. INGLIS. I think it is possibly true. I think it our job to ensure that we have sufficient confidence. I think that we can agree that the infrastructure that we make use of can never be perfectly secure, and it will not defend itself. So we can make it defensible—Jen has described many ways to do that. We then must actually defend it, and we must have a transcendent, resilient idea of who we are and where we are going such that that is the thing that they have to challenge, such that we essentially achieve our aspirations through momentum as much as more as they are knocking down, right, the efforts that somebody else undertakes to hold that at risk.

Ms. EASTERLY. I do not think I can say it better.

Senator SCOTT. OK. All right. Thank you, Chairman.

Chairman PETERS. Thank you, Senator Scott. Ranking Portman, I know you have a question that you would like to ask, you are recognized for it.

Senator PORTMAN. Yes, thank you, and again, thanks for the opportunity today to dig into some of these issues, including the good dialog we just had with Senator Scott. There is so much that needs to be done to tighten up our defenses and respond more effectively, but one is this reporting requirements legislation we talked about earlier. We would like to get legislation passed that is bipartisan, that you all can work with. The bottom line is it would require entities to report to you, Ms. Easterly, in a more expedited fashion and, in some cases, clarifying that that is a responsibility, because it is not, as we saw with Colonial Pipeline, when they got the FBI and did not contact you, based on our hearing testimony.

So for you to be able to properly disseminate that information that you get to the right agencies and, therefore, to have the right analysis—I suppose you need to do that—what do you need? In other words, if we have a reporting requirement, what do you need to make it effective so that CISA can take that information and get it out immediately to the right actors?

Ms. EASTERLY. Thanks for the question, Senator. That is what we do every day. We receive a variety of reports across the Federal civilian Executive Branch. We receive a variety of reports at the State and local level, and then, of course, at critical infrastructure. We analyze those reports to ensure that if there is information that needs to be shared with other entities to help us raise the cybersecurity baseline of the cyber ecosystem that we are doing that. That really is what I describe as our super power, is to share that information, and the authorities that we were given by the Congress to do that, I think, are exactly what we need.

If this legislation goes into place—and I am a huge supporter of it and I think, as I said earlier, we need to craft it in such a way that it enables enforcement, it is timely, but we are going to need to put in place a process to be able to handle this information at even greater scale and make sure that we can share it as agilely as possible.

I think that the JCDC that we are standing up will help enable that, because again, that gives a construct to share many to many. Uniquely, it is the only Federal cyber entity in statute that brings together NSA, FBI, CISA, United States Cyber Command (CYBERCOM), DOD, ODNI with the private sector, so that we can share that many to many. That is the dots visibility issue that we are trying to solve, Ranking Member Portman, and I am optimistic that we will be able to leverage any new legislation to share that information as agilely as possible.

Senator PORTMAN. I appreciate that. My colleagues want to ask some additional questions and I want to make sure they get the chance to. We will have more follow-up on this as we move the legislation through the process. But we want your input. We want to make sure that this works right and does not unduly burden those who get hacked at a time when they have to be able to respond. That is why there is a time period here, to give them time where

they are not filling out paperwork but they are, in fact addressing the attack. So there is a balance there, and we understand that, but ultimately we want to have a reporting requirement, and we want to make sure that you have the resources to be able to properly take that information and get it out to the right Federal agencies and others as quickly as possible.

Ms. EASTERLY. Can I respond to that?

Senator PORTMAN. Yes.

Ms. EASTERLY. I totally agree with you. I mean, we went through this in the private sector at Morgan Stanley. What we do not want is to have CISA overburdened with erroneous reporting, and we do not want to burden a company under duress when they are trying to actually manage a live incident. That is why I think the rulemaking process that will be consultative with industry will really be important to getting this right.

We do not want to be flooded with reports saying we detected something and we are not sure whether there is actual impact or not. I think we need to make sure that there is determined impact, and then we can get that information and we can do something with it that will help ensure the cybersecurity baseline is raised. But erroneous noise is not what we need. We need signal.

Senator PORTMAN. Yes, I could not agree more. You noted that, at the outset, we introduced into the record letters we have received from the private sector, and I think you will see, in some of that information, the input that you are talking about. It is a balance, and we will try to achieve that balance but also provide some discretion so that we get it right. We look forward to working with you.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Ranking Member Portman. Senator Ossoff, if you have an additional question or two you may proceed.

Senator OSSOFF. Thank you, Mr. Chairman. I know time is short and there is a vote on the floor. Two final questions for you please, Mr. Inglis. The first is, what do we all need to do, as public leaders, what would we call upon the private sector to do to build a privacy culture in this country such that citizens understand the risks associated with engagement online with the use of technology so that basic cyber hygiene principles, practices like patching and using complex passwords and preferring encrypted messaging apps, avoiding reckless public disclosure that can put one at risk or one's family at risk or invite financial intrusion, what can we all do to make that something that is closer to our core understanding of citizenship?

Mr. INGLIS. Senator, thank you for that terrific question. I would say many things. First, I would say follow the best examples of this Committee in two key ways. One, this is, by every kind of representation, a nonpartisan and bipartisan issue. You all speak with equal fervor about the nature of what this means to us and what we should do about that. That is extraordinarily important.

Two, you have taken it seriously such that you have asked us questions, you demand that we give you good answers. We will continue to work our way through that. This is an issue that all of us

have as a responsibility, not simply the people that have "IT" or "cyber" in their name.

Three, to the point that you have mentioned some things that people should know, regardless of whether they are Python coders or IT experts, I think that we assume too much about people raised in the midst of technology that they are digital natives. They are generally not. They are app natives. They understand how to use this stuff. They have no idea about what the security consequences are.

In as much as we teach our children how to walk across a busy street, especially when they are in an environment where perhaps the traffic goes the wrong way, we need to spend an equal amount of time teaching them something about the basics of cyber space—how that works, what happens when you touch a link, what perhaps are the responsibilities, who is defending your stuff when you store it in whatever the cloud is. We need to tell them a little bit more about those. Those are basic, fundamental issues.

Finally, I would say that we need to redouble our efforts to imbue critical thinking in our people, because we cannot predict all of the situations they are going to encounter. They, therefore, need to have foundational abilities to say does this make sense, and make a choice based upon some facts that are kind of solid underneath them.

I think if we do all of those things we are in a better place.

Senator OSSOFF. Thank you, Mr. Inglis, and let us continue the conversation on this subject. My final question, and it is a brief one, Mr. Chairman, for you, Mr. Inglis. In your capacity you have to consume threat intelligence, work with the intelligence community, work with law enforcement agencies. You have a background at the National Security Agency. What is your involvement, if any, with respect to policy decisions, operational decisions, legal interpretation that touches on intelligence collection that may be related to or include collection of data, information, or anything pertaining to U.S. persons?

Mr. INGLIS. Senator, as you indicate I am an avid consumer of that, not simply for my own sake, so that on behalf of those I represent, the institutions that are charged with cyber defense, that we can be properly informed about the true nature of threat. That would, in turn, have an effect on what they then attempt to collect and how they then produce that. But I am not able to direct that with a hands-on ability, as appropriate to my limited responsibilities with respect to offensive or intelligence capabilities.

Senator OSSOFF. Thank you. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Ossoff.

A couple of final questions here for the panel, but I will start with Mr. Inglis on this question. I think all of you know right now we are in the middle of an investigation into the Kaseya hack, so I know you will be limited as to what you can say.

But I think this Committee needs to understand, particularly with some of the information that came to light just recently regarding the FBI's action, that we need to understand how the administration balances the need for investigating a cyberattack and providing relief to the victims as well.

As National Cyber Director, could you explain the process that the government uses to evaluate investigative needs compared to assisting victims in attacks, and do you coordinate with the FBI? Give us a better picture of how this happens.

Mr. INGLIS. Yes, sir. Thank you for the question. First I would say that the overwhelming bias is to assist the American people to essentially provide the government's resources focus its time and attention to assist them, as opposed to develop, for its own sake, some instrument of power for its own sake.

The article the other day, that probably showed up first in The Washington Post, had a headline that indicated that there potentially was an undue delay in the kind of provision of the key. But when you read the article, the article itself, actually, I think, thoughtfully said that there was, in fact, a very strong focus on how do we help Kaseya, how do we help the downstream or upstream customers, and that challenge, which is the first and foremost priority, has to take into consideration how can we do this in a way that is at once time and has the most significant impact. Those two things, sometimes when you align them, you wind up not trading one for the other, but not achieving an optimal effect on both of them at the same time.

But I would say that the government starts with how do we actually assist the private sector in the most impactful way, how do we then use all of the instruments at our disposal to do that, and how do we then have a full-fledged discussion across those instruments of power in as timely a way as possible to come up with the strategy, the play.

I will defer to Jen for the rest of the answer.

Chairman PETERS. Ms. Easterly.

Ms. EASTERLY. Yes. Just to add to that, I have to say I was not here during those discussions. Certainly having managed live incidents in real time it is a very complex process, and certainly there are competing goals around doing what you can for current victims and then protecting potential victims.

What I would say is I would expect to be part of any of those discussions going forward, and at CISA what I would do would be advocating for doing everything that we can to ensure that victims have the tools that they need to recover, remediate, and get their businesses back up and running, and that we have the information that we need to protect future victims. That is why your cyber incident legislation is so important.

Chairman PETERS. Mr. DeRusha, we will do a final question for you. We have been discussing some of the legislation that we are working on here in the committee to reform FISMA, and we have heard from the other witnesses, some good input related to that. I wanted to give you an opportunity to suggest any reforms that you think are needed to FISMA to protect our Federal networks.

Mr. DERUSHA. Absolutely, Senator, and I appreciate the opportunity. As you know, we are working closely with your Committee staff on the bill, and we are excited about that opportunity. Director Easterly stated a lot of our priorities already, but I would reiterate that clarifying roles and responsibilities is crucial, and we are committed to that. Really moving toward tested security, away from attested security so that we can determine, through contin-

uous monitoring and testing where the greatest risks are and address those first, and having supportive legislation of that.

Having legislation that ensures that we are not being overly burdensome with multiple compliance requirements and regimes that are going toward agencies, and so that we can streamline some of that and maybe provide some relief on how often they need to do that so they can focus on remediating the vulnerabilities that they are finding through test and mechanisms.

Also moving toward automation. There is a skills gap in this space—we are working to address it—but we cannot do that fast enough. We have to an on the technology and integrate that into our processes.

I think those priorities are well aligned and shared, and we look forward to the right language to codify this into law.

Chairman PETERS. Thank you for that answer, and once again thank you to our witnesses for joining us today. I appreciate all of your efforts to strengthen our cybersecurity defenses. It is a big challenge. All three of you are certainly up to that challenge, and I appreciate you taking the time today to discuss these issues with the Committee. I think you can tell this Committee is very focused on these issues. All of the Members are very engaged, and we understand the seriousness of what we are dealing with and we want to support you in your efforts each and every day.

We have to stay vigilant against these breaches and ransomware attacks, and effectively addressing these is going to require strong coordination between our offices and work in a bipartisan way.

I look forward to continuing my work with Ranking Member Portman to introduce bills that will strengthen the cyber incident and ransom payment reporting requirements for key public and private sector entities and ensure that Federal Government networks are also prepared to deal with these evolving threats.

I think we heard today that there is a clear need for our offices to get this information, which can help you connect the dots and who is behind these attacks, and help prevent potential targets from being potential victims. I look forward to continuing to work with all of you and my colleagues on this Committee to do everything in our power to strengthen our cybersecurity defenses.

The record for this hearing will remain open for 15 days, until 5 p.m. on October 8, 2021, for the submission of statements and questions for the record.

This hearing is now adjourned.

Ms. EASTERLY. Thank you, Chairman.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]

# APPENDIX

**Chairman Peters Opening Statement As Prepared for Delivery**
**Full Committee Hearing: National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems**
**September 23, 2021**

I want to thank our witnesses for joining us today and for their service to the American people. Your agencies and offices are vital to protecting federal cyber networks and critical infrastructure systems.

Although it can often be difficult to understand the complexity and severity of many cyber-attacks, they are only increasing in sophistication and frequency, and have a significant cost on our national security.

The Federal Bureau of Investigation reported 2,474 ransomware attacks in 2020, though experts believe the actual number is much, much higher.

Just last month, in my home state of Michigan, about 1,500 patients were notified that their information had been exposed as a result of the breach of a file-sharing service used by their hospital.

This breach, like the SolarWinds attack, is yet another example of how our adversaries will target vendors and contractors, including small businesses, to find the weakest link, and exploit our greatest vulnerabilities.

In order to prevent these types of attacks, potential victims, from the public sector to the private sector, must be aware of these ever-changing threats, and have the right information to safeguard their networks.

Whether it's widespread spyware, or a ransomware attack, the federal government needs to know when cyber incidents have occurred, so they can determine if there are patterns, alert future potential targets, and help seal up any vulnerabilities.

This information is especially vital when it comes to our nation's critical infrastructure, 85% of which is privately owned and operated.

Despite this vulnerability there is currently no national requirement for all critical infrastructure owners and operators to report to the federal government when they have been hit with a significant attack. That needs to change.

As we have seen from recent attacks on an oil pipeline, water treatment plants, food processing facilities, and hospitals, these breaches can cause serious economic and national security concerns, and disrupt our daily lives.

If multiple critical infrastructure entities, like energy companies for example, are reporting similar attacks, then CISA and other federal entities should be able to warn others, prepare for potential impacts to that sector or other related sectors, and help prevent further widespread attacks.

Ranking Member Portman and I are currently working legislation that we plan to introduce soon, to require critical infrastructure companies that experience cyber incidents, and other entities that make ransomware payments, to report this information to CISA.

This requirement will ensure CISA and other federal officials have better situational awareness of ongoing cybersecurity threats, who the targets are, how the adversary is operating, and how best to protect the nation.

I'm looking forward to hearing from our witnesses today about how an incident reporting law could help each of your organizations assist victims in recovering from an attack and prevent them from happening in the first place.

But we also need to ensure the federal government is sharing this same information in a timely manner.

The last time Congress substantially addressed federal cybersecurity was in 2014, when this Committee, led by then Chairman Carper, passed the *Federal Information Security Modernization Act*.

Since then, our technology has developed rapidly, along with the sophisticated threats we face. When that legislation was passed, CISA had not yet been created.

We need to pass updated legislation that clarifies CISA's roles and responsibilities in federal information security, improves how incidents on federal networks are reported to Congress, and ensures that our cybersecurity resources are effectively aligned with emerging threats. Ranking Member Portman and I are also working on legislation that would help achieve these goals.

We also need a better understanding of how the federal government is balancing its responsibility to bring cybercriminals to justice and helping victims recover from an attack.

We learned earlier this week that in one instance, the FBI withheld a digital key that could have aided victims for several weeks to pursue its investigation.

In order to conduct thorough oversight, this Committee needs to know more about the federal government's processes for assisting the victims of attacks, and how your agencies weigh investigative, national security, and economic needs.

Finally, I want to acknowledge the important actions the Biden Administration has already taken to bolster our cybersecurity defenses, improve information sharing, and apply the lessons learned from previous breaches to avoid future attacks. The President's Executive Order "On Improving the Nation's Cybersecurity," for example, is paramount to securing our nation.

This is a top priority for both myself and Ranking Member Portman; and I look forward to today's discussion and working productively with these vital federal agencies to ensure we are addressing this harmful threat.

**OPENING STATEMENT**
**RANKING MEMBER ROB PORTMAN**
*NATIONAL CYBERSECURITY STRATEGY: PROTECTION OF FEDERAL AND CRITICAL INFRASTRUCTURE SYSTEMS*

September 23, 2021

Thank you, Chairman Peters for convening this hearing to continue our bipartisan oversight of Federal cybersecurity.

We are here today to discuss the Federal Government's strategy for protecting our cyber networks and critical infrastructure. One important part of that strategy is accountability and I hope to have a conversation about the appropriate roles and responsibilities for the many different cybersecurity positions within the Federal Government. I also look forward to discussing how cyber incident reporting legislation might better inform that strategy.

In recent years, hostile cyber adversaries, both foreign and domestic, have executed some of the most damaging cyberattacks in our history. Both the Federal Government and private sector companies have been targeted. We held hearings on several of these incidents here in this Committee—including the SolarWinds and Colonial Pipeline attacks. Both of these events are stark reminders of the wide-ranging and real world impacts of sophisticated cyberattacks.

As these attacks become more and more common, it is important that we work to protect ourselves and our networks. We know that one of the best strategies for preventing these attacks is to improve baseline cybersecurity practices. We also know that Federal agencies have failed to make meaningful progress on the implementation of these practices as required by the Federal Information Security Modernization Act or FISMA.

In August, just last month, Chairman Peters and I released a report detailing the significant cybersecurity vulnerabilities of eight key Federal agencies—the Departments of Homeland Security, State, Transportation, Housing and Urban Development, Health and Human Services, Agriculture, and Education, and the Social Security Administration. This report follows a 2019 report I released with Senator Carper as Chairman of the Permanent Subcommittee on Investigations evaluating the same eight agencies.

In this year's report, only DHS had an effective cybersecurity program. Every other agency featured in the report failed to meet this standard. We also found the average grade across all Government agencies was a C minus. The report identifies several common agency vulnerabilities including the failure to: (1) adequately protect personally identifiable information; (2) maintain an accurate and up to date list of the agency's IT assets; (3) install security patches in a timely fashion; and (4) retire vulnerable legacy technology that is no longer secure.

Securing fragmented networks against increasingly sophisticated attackers is not a trivial task. It would be unfair to suggest otherwise. Yet, in the nearly seven years since FISMA was last updated in 2014, agencies still have the same vulnerabilities year after year.

Accountability is a crucial aspect of any strategy. All three witnesses with us here today have heard me discuss the importance of it for Federal cybersecurity in particular. Without appropriate accountability for Federal networks and agency systems, among the three of you and the Deputy National Security Advisor for Cyber, I believe that we will continue to see these consistent and long-standing vulnerabilities. We need to be clear about who is in charge to better prevent and respond to cyber attacks. I hope we can continue the discussion of how we can best achieve that accountability here today.

We are also here to discuss another important topic in the development of an overarching strategy: cyber incident reporting. Recent attacks on critical infrastructure, particularly through ransomware, demonstrate how prompt notification to the government can benefit both the government and victims. In the case of the Colonial Pipeline attack, the FBI was able to recover part of the ransom paid by Colonial to the attackers. There is a balance between getting information quickly, letting victims respond to an attack without imposing onerous requirements on them, and getting accurate information. I look forward to the witnesses' perspectives on how to balance these competing priorities.

I appreciate the witnesses being here, and I look forward to your testimony on these important issues. Thank you.

**Testimony of the National Cyber Director**

**J. Chris Inglis,**

**United States Senate**

**Committee on Homeland Security and Governmental Affairs**

September 23, 2021

Chairman Peters, Ranking Member Portman, 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 and Mr. DeRusha. 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 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 has created and appointments he has made, as well as the unmatched speed with which the Administration has acted to modernize our defenses and bolster our security in nine 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, a position that you 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 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 in standing up as a full-fledged contributor in those imperatives. Cyber talent is in high demand everywhere, but I will continue working with Congress to secure the resources we need to bring on key staff. While we continue to work with the Office of Management and Budget (OMB) and Congress on funding amounts, organizational planning, and timelines, we are determining how our office and limited team can begin helping the Administration confront the critical challenges facing us.

And as the ONCD organizes for that purpose, I see those responsibilities falling into a few major areas of emphasis to bolster the President's cybersecurity agenda:

- Informing and helping develop policy and strategy around cybersecurity, technology supply chains, and, the resilience of the cyber ecosystem across the people, processes, and technology that constitute cyberspace.
- Ensuring accountability and follow-through on implementation and providing recommendations on agency investments in cybersecurity to ensure they align with national strategy and priorities;
- Engaging with the private sector and our international partners, in collaboration with the rest of government, to find opportunities for greater integration and collaboration;
- Coordinating with OMB and the Cybersecurity Infrastructure Security Agency (CISA) on security and resilience of the Federal civilian network enterprise; and,
- Ensuring defense cyber operations and planning have the policies, plans, procedures, and coordination mechanisms necessary to be successful.

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 colleagues sitting alongside me – Director Easterly and Mr. DeRusha – and many others serving in the Federal cyber ecosystem.

Cyberspace 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 the shared spaces of cyberspace. Cyberspace allows a global reach and efficiency of scale unrivaled in any other domain, meaning that our geopolitical competitors can have global reach and strategic effect and criminals and extremists can have wield an unprecedented level of impact and coercion. Malign actors big and small often believe they can evade consequence for acts and crimes that in most other realms would provoke swift and severe responses.

The complexities of holding actors accountable applies not only to malign actors, but also to our friends and partners. This is true in both the positive and negative sense; across the public and private sectors alike, there are rarely clear lines defining what it means to "do the right thing" when preparing or responding to a cyber incident. And the reward for success can be even more elusive, as it is hard to quantify and even harder to celebrate 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. We have the good fortune of having two domestic agencies at the forefront of cyber incident preparation and response—CISA and FBI—whose roles complement one another and who, working together, strengthen our defense of cyberspace 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.

These are just some of the challenges that President Biden sought to address in Executive Order 14028, Improving the Nation's Cybersecurity (signed May 12, 2021). The President took 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. Our hope is that the federal government's purchasing power is great enough that these requirements will echo 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. And 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 seeing this real-world example will catalyze stakeholders

across the public and private sectors to implement security controls commensurate with the importance of their operations.

The Office of the National Cyber Director will build on this momentum, fill in gaps and seams in the government's current approach, and bring a unique perspective and direction by focusing on the following priorities:

- First, the Office will champion coherence across the Federal cyber enterprise – from coordinating with NIST in standards and guideline development, supporting CISA in providing operational support to federal agencies, and working in partnership with OMB to resource these key cybersecurity initiatives. That means ensuring that we are speaking with one voice and moving in the same direction, particularly in areas like common standards and guidelines in hardware and software, in propagating best practices, acting with unity of purpose and effort in the actual defense of our digital infrastructure, and ensuring that the good work Sector Risk Management Agencies are doing is not only improving their respective sectors, but also adding value across the Federal enterprise.
- Second, the Office will highlight the importance of improving public-private collaboration. We will work closely with Director Easterly and Mr. DeRusha and seek to expand engagement and partnership across this sectoral line to new level – because tackling the cyber challenges we face requires nothing less. The new Joint Cyber Defense Collaborative, hosted by CISA and leveraging authorities, capabilities, and talents of the federal cyber ecosystem in partnership with industry, can play an important role in this effort, and I look forward to working with the JCDC and other associated initiatives across the Federal government.
- Third, we will ensure that the US government is aligning their resources to their aspirations and accounting for the execution of cyber resources entrusted to their 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 are not being made or those that are not quite singing from the same general sheet of Federal music.
- Finally, the Office will work to increase present and future resilience, not only within the Federal government, but also across the American digital ecosystem. 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, or technologies, and our very structures and organizations are not only fit for purpose today, but are future-proofed for tomorrow.

These are daunting undertakings, but with the support of this Congress, we are excited to undertake them.

Finally, I'd like to draw the Committee's attention to our cyber workforce. Your investment in education, training, and workforce programs like the National Initiative for Cybersecurity Education at NIST, CyberCorps: Scholarship for Service, and the special hiring authorities afforded to the Department of Defense and CISA have made very real progress in ensuring the U.S. Government can attract and retain the talent it needs. In the months and years ahead, we will need to ensure that all portions of the Federal government that have a strong, central role in our collective cyber defense also benefit from the best recruitment and retention tools we have to offer. The ultimate purpose should be to create a shared, interoperable community of interest that operates with unity of effort and unity of purpose across the U.S. Government.

These are all important undertakings. The Office of the National Cyber Director is a young and still small office, but once funding is in place and with the partners we have today, and with the confidence and support of this Congress, it will be in a strong position to succeed. Thank you for the opportunity to testify before you today, and I look forward to your questions.


**Testimony**

**Jen Easterly**

**Director**
**Cybersecurity and Infrastructure Security Agency**

**U.S. Department of Homeland Security**

**FOR A HEARING ON**

**"National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems"**

**UNITED STATES SENATE**

**HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE**

**September 23, 2021**

**Washington, D.C.**

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for the opportunity to testify on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) on our Nation's cybersecurity.

I am truly honored to appear before this Committee with our National Cyber Director and our Federal CISO. As I often say, cyber is a team sport, and Chris and Chris are certainly two of my best teammates. Let me begin by outlining CISA's priorities for accomplishing its mission, which include building and investing in our workforce, strengthening and defending federal networks, and working collaboratively with industry, both pre-event and in response and recovery. I will also share more information about our efforts to implement the President's Executive Order 14028, on *Improving the Nation's Cybersecurity*, and our perspective on cyber incident reporting legislation and FISMA reform. As I have shared with my team on just about each of my first 73 days, I have the best job in government.

First, people are CISA's number one asset. One of my principal goals is to make CISA the place where our nation's best cyber defenders want to work. I'm 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, Secretary Mayorkas and I are committed to attracting and retaining world-class talent by implementing a vibrant, end-to-end talent management ecosystem that spans from recruiting and hiring, to onboarding and integration, mentorship and coaching, certification and training, recognition and promotion, to 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 DHS Cybersecurity Service, also known as the Cyber Talent Management System (CTMS). Under the Secretary's leadership, the Department of Homeland Security (DHS) and 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. To that end, my goal is to make CISA a leader in diversity among both the Federal Government and the broader tech workforce.

**Defending the Nation's Networks**

In the wake of the recent Solar Winds and Pulse Secure campaigns targeting federal networks and the Colonial Pipeline and JBS Foods intrusions targeting our nation's critical infrastructure, we are working to address our nation's shared cybersecurity risk. We must collectively and with great urgency strengthen our nation's cyber defenses, invest in new

capabilities, and reimagine how we think about cybersecurity to recognize that all organizations are at risk and our efforts must focus on ensuring the resilience of essential services. To that end, as the National Coordinator for critical infrastructure security and resilience, CISA is acting with utmost resolve to drive reduction of cyber risk across Federal networks and the National Critical Functions. Achieving the outcomes we seek will require progress in several key areas.

First, CISA is currently investing in, and growing capabilities to increase visibility into cybersecurity risks across federal agencies and our critical infrastructure partners. As we all know, if we can't see it, we can't defend it. Therefore, we must enhance our ability to detect potentially nefarious network activity before it becomes systemic. This approach embodies a fundamental change, in which CISA conducts persistent hunts for threat activity, ingests and analyzes security data at all levels of the network, and conducts rapid analysis to identify and act upon identified threats. CISA leverages the results from threat hunting for adversary activity to inform its efforts to protect both federal networks and critical infrastructure, as the results from reported insights helps to drive our efforts, regardless of sector. At the same time, CISA is driving adoption of defensible network architectures, including implementation of zero-trust environments in which the perimeter is presumed compromised and security must focus on protecting the most critical accounts and data. Going forward, we must take lessons learned from our investments in federal cybersecurity to support organizations across sectors in driving similar change.

Second, CISA is working with all partners to gain increased visibility into national risks. With increased visibility, we will be able to better identify adversary activity across sectors. By identifying cross-sector trends, we can produce more targeted guidance and identify earlier how to prioritize and scale any potential response. As one element of this effort, CISA offers a pilot program called CyberSentry, which deploys technologies and analytic capabilities to monitor activity between business (IT) and operational technology/industrial control system (OT/ICS) networks for sophisticated threats. CyberSentry is a voluntary partnership with private sector critical infrastructure companies. This capability is not a replacement for commercial solutions; rather, the capability complements such solutions by allowing CISA to leverage sensitive threat information already being captured by network defenders. CyberSentry has shown significant benefit in practice and has been used to drive urgent remediation of threats and vulnerabilities.

Third, CISA continues to invest in and mature our voluntary partnerships with critical infrastructure entities. These partnerships with industry enable us to better understand the nature of vulnerabilities pre- and post-disclosure and in turn provide timely and thorough mitigation guidance to government agencies and critical infrastructure. CISA collaborates with private industry on significant risks, developing sector and threat focused products, and providing briefings on new trends, threats, and capabilities across the sectors.

The newly established Joint Cyber Defense Collaborative (JCDC) is building on these partnerships to lead the development of the Nation's cyber defense plans by working across the public and private sectors to help defend against cyber threats to the nation. Authorized in the National Defense Authorization Act for FY 2021, the JCDC brings together the authorities, capabilities, and talents of the interagency – CISA, the National Security Agency, the Federal Bureau of Investigation, Cyber Command, the Department of Justice, and the Office of the

Director of National Intelligence – with the power of industry to enable shared situational awareness of the threat landscape, to plan and exercise against the most significant threats to the nation, and to implement cyber defense operations against these threats. This new collaborative promotes national resilience by coordinating across federal agencies, to include Sector Risk Management Agencies (SRMAs); state, local, tribal and territorial (SLTT) partners; and industry to protect against, identify, detect, and plan for and respond to malicious cyber activity targeting U.S. critical infrastructure. Finally, the JCDC will leverage CISA's broad authorities to share information about threats and vulnerabilities to enable early warning and prevent other victims from being attacked. This shifting paradigm will enable us to transform information sharing into information enabling – timely, relevant, and actionable.

**Cyber Executive Order Implementation Update**

As you are aware, on May 12, 2021, President Biden signed Executive Order 14028, *Improving the Nation's Cybersecurity*. 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, large-scale 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, consulting, or supporting over 35 unique efforts, many with short timelines highlighting the criticality and 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;
- Raising the bar for incident response by publishing a Vulnerability and Incident Response Playbook, which will ensure that all agencies will operate from the same sheet of music during incidents, and allow CISA to confidently coordinate 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 in response to incidents with the contracted agency as well as with CISA, and establishing procedures for sharing appropriate information with interagency partners to aid in their collective ongoing 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 FY21 National Defense Authorization Act; and
- Prioritizing federal supply chain security by directing 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.

**Cyber Incident Reporting Legislation**

Facing repeated attacks on our Nation's Federal networks and critical infrastructure, CISA will continue to pursue ways to increase visibility into federal and critical infrastructure networks. We must also continue to rely on network owners and operators to identify and report anomalous and potentially nefarious activity on their networks to CISA and our partners.

Although some reporting requirements exist within certain sectors, there is currently no single mandatory federal requirement to report cyber incidents. Rather, entitities must assess the complex disclosure requirements imposed by an array of agencies at the Federal and State levels. Moreover, when a victim does seek to do the right thing and report an incident to the Federal government, they may not know which agencies to contact, delaying their reporting during an emergency situation. Among the harms this may cause is a lag in availability of critical mitigation guidance to the operators who are positioned to take action.

We appreciate the work of members of Congress in both the House and the Senate who have drafted or introduced bills on cyber incident notification over the past several months, including members of this Committee. The earlier that CISA, the Federal lead for asset response, receives information about a cyber incident, the faster we can conduct urgent analysis and share information to protect other potential victims.

To that end, cyber incident reporting must be timely, ideally within 24 hours of detection. Reporting should be broad-based, and not limited by type or sector, with CISA and DOJ having the joint authority, in coordination with other relevant departments and agencies, to set reporting thresholds and requirements for covered entities. These entities include critical infrastructure, federal agencies, and government contractors. It should also provide clear and compelling enforcement mechanisms that ensure compliance. We encourage Congress to adopt a cyber incident notification reporting approach that appropriately focuses broadly on cybersecurity incidents, including cyber supply chain and ransomware attacks, and provides CISA and DOJ, in coordination with other relevant agencies, the flexibility to modify the scope of the requirements as necessary, balancing the benefits of reporting against burdens to industry and government.

**Federal Information Security Modernization Act (FISMA) Reform**

Lastly, I'd like to thank the Chairman and the Ranking Member for your efforts to review and update the Federal Information Security Modernization Act or FISMA. Enacted in 2002,

FISMA, it recognized the importance of information security, and defined roles and responsibilities for the Federal Government. However, the rapid evolution of both technology and vulnerabilities are outstripping a policy-to-implementation process last updated in 2014. When faced with threats and vulnerabilities, corrective action can be stifled, especially when incidents span multiple agencies. Disparities in senior leadership engagement and cyber expertise across federal agencies, resource constraints, and a complex policy and governance environment impair risk management efforts. These hurdles are even more challenging since the networks supporting federal agencies are difficult to defend due to design, age, and insufficient investment.

In this operating environment, the legal framework governing management of Federal information security must enable all of government to lean into these challenges to seek effective, efficient, and coordinated solutions. However, in its current form, FISMA reflects the roles and responsibilities of nearly a decade ago, while the Federal Government still struggles to affect the level of oversight, accountability, and performance that was envisioned in FISMA 2014. There have been many changes in the intervening years, including the establishment of CISA, and the creation of the National Cybersecurity Director as part of the 2021 National Defense Authorization Act. Together with my teammates in cybersecurity, Chris Inglis, the National Cyber Director and Chris DeRusha, the Federal CISO, we stand ready to tackle the challenges facing the federal cybersecurity enterprise together. Clearly, the status quo is not acceptable. I welcome efforts by Congress to modernize FISMA to address the dynamic and challenging cyber landscape, targeting strengthened risk management and implementation, and recognizing CISA's role as the operational lead for federal cybersecurity.

CISA is appropriately positioned to identify and address unacceptable risk within and across Federal civilian executive branch agencies. CISA has the capability, expertise, and access to define and drive the right level of security to protect federal agencies in coordination with the Office of Management and Budget, the National Institute of Standards and Technology, and the National Cyber Director. Existing and planned CISA shared services, as well as continued modernization of our flagship cyber programs, namely the Continuous Diagnostics and Mitigation Program and National Cybersecurity Protection System, will provide an avenue for agencies to confidently enhance their own cybersecurity capabilities, where they are working, and also provide a backstop for agencies struggling to fill capability gaps. CISA is modernizing National Cybersecurity Protection System capabilities to support the increasing adoption of cloud services and other emerging technologies and improve CISA's ability to collect, process, analyze, and share cyber data with its partners. CISA will have a single analytical environment scaled to support the full spectrum of our services.

A modernized FISMA should shift the spotlight from compliance to risk management and implementation. This approach has led to an operating environment with heavy compliance requirements that do not always contribute to the intended outcome and in some cases distract from it. Instead, an environment that fosters implementation should ensure that cybersecurity actions enable agency missions and that agency leadership decisions appropriately prioritize and fund the security of their systems and networks.

We at CISA look forward to working with Congress to modernize FISMA to better align with the realities of modern information security, enabling a more effective Federal government through an updated law that balances security and reporting, and empowers information security leaders. As this effort moves forward, I will remain committed to working with my fellow agencies to champion the defense and security of federal systems.

**Conclusion**

Our nation faces unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals. Now is the time to act – 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.

September 23, 2021

Testimony of the Federal Chief Information Security Officer

Christopher J. DeRusha

United States Senate

Homeland Security and Governmental Affairs

Hearing on

National Cybersecurity Strategy:
Protection of Federal and Critical Infrastructure Systems

Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for the invitation to testify about the Administration's cybersecurity priorities. I am pleased to be here today with Director Easterly and Director Inglis. The three of us work closely together, in partnership with the National Security Council (NSC), to leverage our unique authorities in the service of our common mission—to build a more secure federal enterprise. My goal as the Federal Chief Information Security Officer is to focus on enterprise-wide outcomes, and ensure that we are taking a holistic approach to addressing common challenges while taking advantage of shared opportunities.

This committee took decisive action earlier this year by supporting the allocation of $1 billion in emergency funding to the Technology Modernization Fund (TMF). To date, we have received more than one hundred project proposals from agencies, requesting more than $2 billion. Seventy-five percent of those proposals are focused on cybersecurity improvements. As the TMF Board prepares to release the first round of project approvals, there is a strong focus on learning what works well for one agency and translating those experiences and lessons into successful outcomes for many agencies.

These are challenging times to manage cybersecurity for any enterprise, even more so when the enterprise is as attractive a target as the federal government. This is not the time to maintain a steady course. We need to embrace bold new ideas, form enduring partnerships, and above all to act with a sense of urgency. I would like to highlight a few areas where this administration is taking decisive action.

**Zero Trust Security**

Earlier this month, we released for public comment a draft strategy to move the U.S. Government toward zero trust cybersecurity principles. The term "zero trust" refers to a security model where every person, device, and network inside of an organization is considered untrusted and even potentially compromised. This is a significant shift from the traditional model used by many enterprises throughout the public and private sectors. Our strategy calls for agencies to make this shift, and envisions a federal zero trust architecture that:

- Bolsters strong identity practices across federal agencies;
- Relies on encryption, authentication, and application testing instead of perimeter security;
- Recognizes every device and resource the government has;
- Supports intelligent automation of security actions; and
- Enables safe and robust use of cloud services.

This is an ambitious, multi-year strategy that establishes a new baseline for government security and requires us to iterate and improve over time. To start, our strategy requires agencies to adopt known, trusted technologies and practices that make it harder for even sophisticated actors to compromise an organization. We also recognize that some areas of zero trust are too complex to address through prescriptive technical requirements. In these areas, the federal government will continue to find flexible and innovative solutions to overcome practical and technical hurdles. Our strategy requires agencies to grapple directly with these challenges by developing long-term

plans, demonstrating early, iterative progress, and working together to share information and develop best practices.

We also recognize that implementing zero trust principles is a paradigm shift for security, so we sought input and recommendations from experts by sharing the strategy for public comment. We are excited to see what can be strengthened and improved in this strategy before we release the final version.

**Executive Order on Improving the Nation's Cybersecurity**

In May, the President issued Executive Order 14028, with the intent of dramatically improving the nation's cybersecurity by requiring critical cybersecurity capabilities to be deployed government-wide, improving information-sharing between the U.S. government and the private sector, and strengthening the United States' ability to respond to incidents when they occur.

We recently passed the 120-day milestone since the Executive Order was issued. Over that time, OMB and NSC have been leading the execution across government. Key deliverables include:

- Over the summer, NIST, in consultation with OMB, CISA, ODNI, and NSA, provided a definition of critical software as well as accompanying security guidance. NIST also published minimum standards for vendors to test their software source code as part of a broader initiative to improve the security and integrity of the software supply chain, which will continue into FY 2022.
- OMB and DHS worked closely with key stakeholders to develop recommendations for new contract clauses that will enhance how the federal government and industry work together to address cyber threats. These clauses will streamline the sharing of threat intelligence and notification of incidents, and support a more rapid and coordinated response when security incidents occur.
- OMB released Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures,* which builds upon NIST guidance by helping agencies identify their most critical software and prioritize security requirements for that software.
- OMB then released Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.* This policy was developed in collaboration with DHS and establishes a comprehensive set of requirements for the logging of security-relevant data, centralization of access to those logs, and information sharing across agencies to support incident detection and response.
- NIST also recently held two days of workshops to get private sector input on criteria for consumer cybersecurity labeling programs for both internet of things devices and consumer software.

**FISMA Reform**

The Federal Information Security Modernization Act of 2014 describes the responsibilities and rules of the road for federal cybersecurity that underpin much of the policy and oversight work that our office does today. We appreciate the opportunity to work with Congress on reforming this flagship piece of legislation to improve the government's ability to manage risk. We share

Congress' view that federal cybersecurity management should be more clearly oriented towards security outcomes, and we are already updating our own FISMA oversight processes in service of this goal. What OMB asks agencies to measure and report should be the things that matter most and help determine whether agency cybersecurity investments are producing results.

We also need to emphasize the right roles for our current federal organization. For example, an updated FISMA should reflect CISA's heightened role in collecting and sharing risk information across the federal enterprise, providing cybersecurity operational support to agencies, and providing surge support capabilities when agencies respond to incidents. It should also maintain and strengthen the role of NIST in developing cybersecurity and privacy standards and guidelines, and clearly describe the responsibilities of the new National Cyber Director in regards to federal cybersecurity.

**Conclusion**

This administration is dedicated to making cybersecurity the immediate priority in federal IT. Since January, we have been extremely active in both responding to incidents and laying the strategic groundwork for the future of federal cybersecurity. As we move forward, we will be focused on helping agencies implement these priorities with the diligence this work requires and the speed the moment demands.

As I have said before, none of us can do it alone. This is a partnership where collaboration is key–collaboration with my colleagues here today and, most importantly, collaboration with all of the cybersecurity personnel who support the Federal government and work tirelessly to safeguard our nation's digital assets. I appreciate this Committee's leadership, and I am confident that through partnership, mutual transparency, and frank discussions about where we need additional improvement, we will build a more secure and resilient federal enterprise.

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

Civilian Federal Cybersecurity Roles
Government-wide
Individual Dep'ts & Agencies
Strategic
Operational
Strategic
Operational
Executive Office of the President
National Cyber Director (NCD)
Deputy National Security Advisor for Cyber and Emerging Technology
OMB
Federal CIO
Federal CISO
Department of Homeland Security
CISA Director
Department of Justice
FBI Assistant Director for Cyber
Cabinet Secretary or Agency Head
Agency CIO
Agency CISO
National Institute of Standards & Technology: Develop standards & best practices for cybersecurity & risk management.

# Alert (AA21-259A)

More Alerts

## APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus

Original release date: September 16, 2021

## Summary

*This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise for referenced threat actor tactics and for techniques.*

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), United States Coast Guard Cyber Command (CGCYBER), and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of a newly identified vulnerability (CVE-2021-40539) in ManageEngine ADSelfService Plus—a self-service password management and single sign-on solution.

CVE-2021-40539, rated critical by the Common Vulnerability Scoring System (CVSS), is an authentication bypass vulnerability affecting representational state transfer (REST) application programming interface (API) URLs that could enable remote code execution. The FBI, CISA, and CGCYBER assess that advanced persistent threat (APT) cyber actors are likely among those exploiting the vulnerability. The exploitation of ManageEngine ADSelfService Plus poses a serious risk to critical infrastructure companies, U.S.-cleared defense contractors, academic institutions, and other entities that use the software. Successful exploitation of the vulnerability allows an attacker to place webshells, which enable the adversary to conduct post-exploitation activities, such as compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files.

Zoho ManageEngine ADSelfService Plus build 6114, which Zoho released on September 6, 2021, fixes CVE-2021-40539. FBI, CISA, and CGCYBER strongly urge users and administrators to update to ADSelfService Plus build 6114. Additionally, FBI, CISA, and CGCYBER strongly urge organizations ensure ADSelfService Plus is not directly

accessible from the internet.

TLP:WHITE

The FBI, CISA, and CGCYBER have reports of malicious cyber actors using exploits against CVE-2021-40539 to gain access [T1190] to ManageEngine ADSelfService Plus, as early as August 2021. The actors have been observed using various tactics, techniques, and procedures (TTPs), including:

- Frequently writing webshells [T1505.003] to disk for initial persistence
- Obfuscating and Deobfuscating/Decoding Files or Information [T1027 and T1140]
- Conducting further operations to dump user credentials [T1003]
- Living off the land by only using signed Windows binaries for follow-on actions [T1218]
- Adding/deleting user accounts as needed [T1136]
- Stealing copies of the Active Directory database ( `NTDS.dit` ) [T1003.003] or registry hives
- Using Windows Management Instrumentation (WMI) for remote execution [T1047]
- Deleting files to remove indicators from the host [T1070.004]
- Discovering domain accounts with the `net` Windows command [1087.002]
- Using Windows utilities to collect and archive files for exfiltration [T1560.001]
- Using custom symmetric encryption for command and control (C2) [T1573.001]

The FBI, CISA, and CGCYBER are proactively investigating and responding to this malicious cyber activity.

- FBI is leveraging specially trained cyber squads in each of its 56 field offices and CyWatch, the FBI's 24/7 operations center and watch floor, which provides around-the-clock support to track incidents and communicate with field offices across the country and partner agencies.
- CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.
- CGCYBER has deployable elements that provide cyber capability to marine transportation system critical infrastructure in proactive defense or response to incidents.

Sharing technical and/or qualitative information with the FBI, CISA, and CGCYBER helps empower and amplify our capabilities as federal partners to collect and share intelligence and engage with victims while working to unmask and hold accountable, those conducting malicious cyber activities. See the Contact section below for details.

Click here for a PDF version of this report.

Click here for indicators of compromise (IOCs) in STIX format.

TLP:WHITE

## Technical Details

TLP:WHITE

Successful compromise of ManageEngine ADSelfService Plus, via exploitation of CVE-2021-40539, allows the attacker to upload a `.zip` file containing a JavaServer Pages (JSP) webshell masquerading as an x509 certificate: `service.cer`. Subsequent requests are then made to different API endpoints to further exploit the victim's system.

After the initial exploitation, the JSP webshell is accessible at `/help/admin-guide/Reports/ReportGenerate.jsp`. The attacker then attempts to move laterally using Windows Management Instrumentation (WMI), gain access to a domain controller, dump `NTDS.dit` and `SECURITY/SYSTEM` registry hives, and then, from there, continues the compromised access.

Confirming a successful compromise of ManageEngine ADSelfService Plus may be difficult—the attackers run clean-up scripts designed to remove traces of the initial point of compromise and hide any relationship between exploitation of the vulnerability and the webshell.

### Targeted Sectors

APT cyber actors have targeted academic institutions, defense contractors, and critical infrastructure entities in multiple industry sectors—including transportation, IT, manufacturing, communications, logistics, and finance. Illicitly obtained access and information may disrupt company operations and subvert U.S. research in multiple sectors.

### Indicators of Compromise

*Hashes:*

```
068d1b3813489e41116867729504c40019ff2b1fe32aab4716d429780e666324
49a6f77d380512b274baff4f78783f54cb962e2a8a5e238a453058a351fcfbba
```

*File paths:*

```
C:\ManageEngine\ADSelfService Plus\webapps\adssp\help\admin-guide\reports
\ReportGenerate.jsp
C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\adap.jsp
C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org
\apache\jsp\help
C:\ManageEngine\ADSelfService Plus\jre\bin\SelfSe~1.key (filename varies
with an epoch timestamp of creation, extension may vary as well)
C:\ManageEngine\ADSelfService Plus\webapps\adssp\Certificates
\SelfService.csr
C:\ManageEngine\ADSelfService Plus\bin\service.cer
C:\Users\Public\custom.txt
C:\Users\Public\custom.bat
```

TLP:WHITE

`C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help (including subdirectories and contained files)`

TLP:WHITE

*Webshell URL Paths:*

`/help/admin-guide/Reports/ReportGenerate.jsp`

`/html/promotion/adap.jsp`

Check log files located at `C:\ManageEngine\ADSelfService Plus\logs` for evidence of successful exploitation of the ADSelfService Plus vulnerability:

- In access* logs:
  - `/help/admin-guide/Reports/ReportGenerate.jsp`
  - `/ServletApi/../RestApi/LogonCustomization`
  - `/ServletApi/../RestAPI/Connection`
- In serverOut_* logs:
  - `Keystore will be created for "admin"`
  - `The status of keystore creation is Upload!`
- In adslog* logs:
  - `Java traceback errors that include references to NullPointerException in addSmartCardConfig or getSmartCardConfig`

*TTPs:*

- WMI for lateral movement and remote code execution ( `wmic.exe` )
- Using plaintext credentials acquired from compromised ADSelfService Plus host
- Using `pg_dump.exe` to dump ManageEngine databases
- Dumping `NTDS.dit` and `SECURITY/SYSTEM/NTUSER` registry hives
- Exfiltration through webshells
- Post-exploitation activity conducted with compromised U.S. infrastructure
- Deleting specific, filtered log lines

*Yara Rules:*

```
rule ReportGenerate_jsp {
  strings:
    $s1 = "decrypt(fpath)"
    $s2 = "decrypt(fcontext)"
    $s3 = "decrypt(commandEnc)"
    $s4 = "upload failed!"
    $s5 = "sevck"
    $s6 = "newid"
  condition:
    filesize < 15KB and 4 of them
}
```

```
rule EncryptJSP {
```

TLP:WHITE

```
    strings:
      $s1 = "AEScrypt"
      $s2 = "AES/CBC/PKCS5Padding"
      $s3 = "SecretKeySpec"
      $s4 = "FileOutputStream"
      $s5 = "getParameter"
      $s6 = "new ProcessBuilder"
      $s7 = "new BufferedReader"
      $s8 = "readLine()"
    condition:
      filesize < 15KB and 6 of them
}
```

## Mitigations

Organizations that identify any activity related to ManageEngine ADSelfService Plus indicators of compromise within their networks should take action immediately.

Zoho ManageEngine ADSelfService Plus build 6114, which Zoho released on September 6, 2021, fixes CVE-2021-40539. FBI, CISA, and CGCYBER strongly urge users and administrators to update to ADSelfService Plus build 6114. Additionally, FBI, CISA, and CGCYBER strongly urge organizations ensure ADSelfService Plus is not directly accessible from the internet.

Additionally, FBI, CISA, and CGCYBER strongly recommend domain-wide password resets and double Kerberos Ticket Granting Ticket (TGT) password resets if any indication is found that the `NTDS.dit` file was compromised.

### Actions for Affected Organizations

Immediately report as an incident to CISA or the FBI (refer to Contact Information section below) the existence of any of the following:

- Identification of indicators of compromise as outlined above.
- Presence of webshell code on compromised ManageEngine ADSelfService Plus servers.
- Unauthorized access to or use of accounts.
- Evidence of lateral movement by malicious actors with access to compromised systems.
- Other indicators of unauthorized access or compromise.

## Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at https://www.fbi.gov /contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.
- To report cyber incidents to the Coast Guard pursuant to 33 CFR Subchapter H, Part 101.305 please contact the USCG National Response Center (NRC) Phone: 1-800-424-8802, email: NRC@uscg.mil.

## Revisions

September 16, 2021: Initial Version


September 9, 2021

The Honorable Gary Peters
Chairman, Committee on Homeland Security & Government Affairs
United States Senate

The Honorable Rob Portman
Ranking Member, Committee on Homeland Security & Government Affairs
United States Senate

The Honorable Mark Warner
Chairman, Select Committee on Intelligence
United States Senate

The Honorable Marco Rubio
Vice Chairman, Select Committee on Intelligence
United States Senate

The Honorable Bennie Thompson
Chairman, Committee on Homeland Security
United States House of Representatives

The Honorable John Katko
Ranking Member, Committee on Homeland Security
United States House of Representatives

The Honorable Yvette Clarke
Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
United States House of Representatives

The Honorable Andrew Garbarino
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
United States House of Representatives

Dear Chairman Peters, Chairman Warner, Chairman Thompson, Chairwoman Clarke, Ranking Member Portman, Vice Chairman Rubio, Ranking Member Katko, and Ranking Member Garbarino:

We have been closely following Congressional activity around the important and timely issue of cyber incident reporting. In the aftermath of major cyber incidents, it is important that key cybersecurity professionals in the U.S. government have timely access to accurate information about such incidents in order to make strategic and operational assessments, provide support if requested, and improve overall situational awareness.

Legislation to adopt cyber incident reporting requirements should be grounded in key principles of flexibility, practicality, and constructive collaboration between industry and the Federal government, minimizing the burden on businesses and ensuring government has the information it needs to be effective. Legislation should direct the Cybersecurity and Infrastructure Security Agency (CISA) to establish a program for reporting confirmed cyber incidents and should entrust key determinations to experts at CISA. CISA is in the best position to adapt to evolving threats and react dynamically, while also providing industry with assurances that are integral to the public-private partnership's success.

A regime in which every single instance of an actual or potential unauthorized access to an information system triggers a reporting obligation would contravene each of the key principles. It

would burden industry with reporting requirements for incidents that were transitory and/or non-harmful, and burden the Federal government with a regime that encourages over-reporting, which could distract key resources away from the matters of the greatest concern to our national and economic security. No reporting obligation should be triggered unless and until the affected entity has had the opportunity to assess and **confirm an incident has met applicable** criteria and thresholds.

We also urge Congress not to lose sight of the tremendous investment and collaboration that already occurs in many sectors to keep government partners informed about cyber threats and intrusion. The communications sector has collaborated with DHS (CISA and the Secret Service), the Federal Bureau of Investigation, the Commerce Department, the Federal Communications Commission, and other government entities and officials within the intelligence community on a broad array of cybersecurity initiatives, ranging from securing critical infrastructure, cyber threat information sharing, bolstering defenses against botnet attacks, addressing supply chain risks and vulnerabilities, and much more. The communications sector has long-established cyber incident reporting relationships with DHS, the FBI and the Secret Service, along with outage reporting obligations overseen by the FCC. Communications providers are also subject to the SEC requirement for publicly-traded companies to disclose cyber incidents.[1] The sector also closely partners with DHS across multiple venues to enhance the nation's cyber readiness.

As the U.S. government considers changes to existing policies and new requirements for cyber incident reporting, it is important to deeply engage private sector partners – not only because the private sector is on the front lines and directly impacted by these proposals, but also because owners and operators of critical infrastructure have unique operational insights that can help the government effectuate its security goals with greater efficiency. The focus now should be on strengthening and coordinating public-private partnerships and interagency processes that are in place and centralizing coordination of those efforts at CISA. Below, we offer guidance on some specific priorities for incident reporting legislation.

**1. Reporting obligation criteria should filter out incidents that do not raise significant cyber risks and only confirmed (not potential) incidents should be reported.**

Defining reporting thresholds is a highly technical exercise that requires extensive subject matter expertise. Not every incidence of unauthorized access or service interruption should be deemed to be a cyber incident. A service interruption caused by maintenance crew's unintentional cut of a fiber line or a brief, unauthorized penetration of an information system that is quickly rebuffed or mitigated by security tools without any harm to the public or other third parties should not be reportable events, otherwise there will be a significant risk of over-reporting.

Reporting criteria need to be specific enough to avoid ambiguity, so that industry knows exactly how to comply with the reporting requirements. Given these complexities, policymakers should consider directing federal agency experts to define thresholds in consultation with industry, rather than attempting to include thresholds in legislation.

---

[1] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

As a baseline, however, only *confirmed* cyber incidents should be subject to any new compelled reporting framework (not potential incidents) or else both government and industry resources will be strained by the problem of over-reporting. The thresholds need to be grounded in criteria that are verifiable, attributable, and actionable. When defining reporting thresholds, it is important to avoid imposing the assumptions of one entity upon another. For instance, what counts as a major attack for one business may be far less significant for another business.

**2. The reporting timeline should be flexible in order to encourage reporting and reflect the need for industry to investigate and assess incidents.**

When a possible incident occurs, industry will need at least enough time to investigate the validity of an incident, determine whether reporting criteria have been met, and comply with applicable best practices. Rather than establishing one-size-fits all time requirements in legislation, Congress should consider giving CISA (or some other relevant federal agency) discretion in establishing reporting windows with reasonable parameters. For example, while some types of incidents may be reportable within 72 hours, situations will arise where more time is necessary to avoid diverting resources from active mitigation and response efforts. Therefore, flexibility should be built into the reporting requirements in recognition that no two events are exactly the same.

Hours in the reporting window should only start counting after an incident has been determined to meet reporting criteria. Otherwise, out of an abundance of caution, industry would likely have to report many events that ultimately do not meet reporting criteria because of the remote possibility of escalation. This over-reporting will require additional industry resources and could strain government resources, thus being counterproductive for both sides of the public-private partnership.

**3. Federal incident reporting should include protections for industry that promote the objective of timely sharing of key information while averting aggravation of the harms and adverse effects of cyberattacks.**

There are a number of important protections Congress should grant industry partners who report cyber incidents. To begin with, liability protections and safe harbors are essential. Congress should also ensure reported information is not used for regulatory purposes. These liability limitations should encompass not only the act of submitting a report but should preclude the use of any information contained in such a notification as a basis for any cause of action by any litigant. Nor should information contained in such a notification be subject to discovery in any civil action or otherwise available or accessible via compulsory process to any litigant or non-Federal entity.

Other considerations include protection of trade secrets; waiver of ex parte communications restrictions; and protection from disclosure for reported information (e.g., commercial, financial, proprietary). A good place to begin is the protections in the Cybersecurity Information Sharing Act of 2015, but there is no substitute for consulting industry. Different players may provide unique insights into how incident reporting affects them legally and operationally.

Consistent with creating good incentives, incident reporting legislation should avoid financial penalties or other policies that create disincentives to industry investment in sophisticated threat monitoring capabilities.

**4. The federal government should take steps to protect reported data.**

When the government collects sensitive information from industry partners, it has a responsibility to protect that information. To that end, legislation should include provisions to ensure data from incident reports is not shared inappropriately or leaked once it is made available. There should be a rule to ensure victim names reported to CISA (or some other relevant federal agency) are not shared outside the agency. This is essential to ensure the information is safeguarded appropriately and not misused. Incident reporting should be covered either by CISA's Protected Critical Infrastructure Information (PCII) Program[2] or an equivalent program.

**5. Reporting obligations should reside with the entities whose systems or data are targeted by malicious actors.**

Incident reporting responsibilities should lie with the entities whose information systems or data are targeted for attack by malicious actors, and not any intermediary transport or retransmitting entities or contractors. While such intermediaries should be covered by a cyber incident bill when their own information systems are attacked in a manner that triggers a reporting obligation, they should not have a duty to report their customers' or other compromised entities' incidents to the government, as such a policy would implicate privacy concerns, disrupt business relationships and operations, and create potential legal issues associated with compelled disclosures of incidents affecting third parties.

**6. Public-Private Interactions will not be limited to CISA.**

Any new, mandatory reporting requirements should not overlook the extensive collaboration that industry currently has with federal law enforcement, specifically the FBI. While CISA has a role to play in analyzing threat information about significant incidents, other federal agencies will continue to be engaged with the private sector. Indeed, consistent with the federal government's recommendation, many companies contact federal law enforcement if they have a cyber incident. If a company has a significant intrusion, its first reaction may be to reach out to the FBI, which could take appropriate actions against cyber criminals (e.g., seize back some of a ransom payment). Industry should be able to trust that federal agencies are in the best position to share reported information as appropriate with one another, while ensuring that necessary safeguards are in place. Policymakers should ensure that any new reporting regime does not inadvertently penalize a private entity for heeding the government's advice or put the entity in the middle of two government agencies that may both have an interest in cyber collaboration with the private sector.

[2] https://www.cisa.gov/pcii-program

**7. Flexibility is critical because cybersecurity best practices will continue to evolve.**

Threats and countermeasures will continue to evolve during the life of any cyber incident reporting scheme. Mechanisms should be considered to pilot cyber approaches to determine effectiveness before implementing industry-wide, and to create a public-private board that periodically (e.g., at least yearly) reviews and modifies the practices industry must follow.

By following these principles, Congress and policymakers in federal agencies can move the conversation forward and develop incident reporting legislation that enhances the public-private partnership that is foundational to bolstering the country's cyber readiness and resilience.

Sincerely,

CTIA

NCTA – The Internet & Television Association

USTelecom – The Broadband Association

August 16, 2021

The Honorable Mark Warner
Chairman
Senate Select Committee on Intelligence
Washington, DC 20510

The Honorable Marco Rubio
Ranking Member
Senate Select Committee on Intelligence
Washington, DC 20510

Dear Chairman Warner and Ranking Member Rubio,

In the wake of recent ransomware and other cybersecurity attacks, we appreciate your efforts to improve the resilience of federal agencies and private critical infrastructure, emphasizing the importance of public-private collaboration in this ongoing fight. The financial services sector shares your commitment to cybersecurity and the value in sharing threat and incident information and supports Congressional efforts to fortify the Cybersecurity and Infrastructure Security Agency (CISA) as a leader in this space. We have concerns, however, with several provisions within the Cyber Incident Notification Act of 2021, which we believe would, in practice, conflict with cybersecurity requirements already in place for financial institutions.

As Congress considers this legislation, we urge you to ensure that any new requirements for reporting, oversight and enforcement are harmonized with existing regulatory requirements for financial institutions – both to avoid confusion and also because those requirements have proven their worth over the years. Below are changes that we believe are necessary to achieve our shared goal of protecting the nation's critical infrastructures:

1. **Extend the timeline for reporting to 72 hours after confirmation an incident has occurred.** As drafted, the legislation requires the filing of a report within 24 hours of a cybersecurity incident. The initial stages of an incident response require "all hands on deck" to focus immediately on understanding the incident and implementing mitigation and response measures. Filing government reports would not only distract from that work but also result in reports that are premature and likely erroneous. Here it is important to distinguish between notification and a formal report. The European Union's NIS Directive as well as the recent Notice of Proposed Rulemaking on Computer-Security Incident Notification Requirements from U.S. financial regulators recognize that within the first 24-36 hours, firms will have limited information on an event and thus call for a simple *notification* that a cyber incident of a sufficient materiality has occurred, with more detailed *reporting* to follow.

   Extending the reporting timeline in the legislation to 72 hours *after* confirmation an incident has occurred would also be more consistent with the bill's definition of a "cybersecurity intrusion" which includes incidents involving nation-states or advanced persistent threats – both of which firms would be unable to determine within a 24-hour period given the need for assistance and confirmation of attribution from federal agencies.

2. **Narrow the scope of reporting to incidents causing actual harm.**
   The bill requires reporting of "potential incidents," which would create near-constant reporting to CISA by financial services firms based on the number of incidents those firms see on a daily basis. Collecting information on potential incidents would add noise to the signal of material incidents, and thus overwhelm rather than enhance CISA's analytical efforts. We recommend that the legislation require reporting of incidents that cause actual harm.

3. **Ensure alignment with existing regulations and avoid duplication with Sector Risk Management Agencies (SRMA).**
   As you are aware, financial services firms are already subject to significant cyber reporting requirements.[1] As drafted, the legislation requires reporting to both CISA and the SRMA. For the financial sector, U.S. Treasury serves as SRMA, but not as regulator as implied in the legislation. Primary regulators that would receive additional reporting include the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Securities and Exchange Commission, among others. We have no objection to reporting to CISA; however, we recommend that the legislation include a mandate for CISA to work with all the other regulatory agencies to develop a common reporting form and streamlined process that would be good for one and good for all. Otherwise, still more time will be spent by first responders working with firms' legal and compliance teams to ensure that each agency's requirement is met rather than focusing those efforts on protecting critical infrastructure.

4. **Ensure the rulemaking process allows for meaningful dialogue with critical infrastructure.**
   The rulemaking process should include greater coordination and discussion with critical infrastructure, as many of the details around definitions, the scope of reporting, and specific requirements will be determined through this process. Getting these details right is essential, and the process would benefit from an initial 90-day consultation period with industry followed by a 90-day comment period.

5. **Harmonize financial penalties for non-compliance with the existing regulatory framework.**
   The legislation includes penalties for firms that fail to report, and we agree that any requirement must come with an enforcement mechanism. Our concern is that financial services firms could be subject to multiple enforcement actions and multiple penalties for the same reporting violation. Here again, we would recommend that the legislation mandate that CISA coordinate any enforcement action and ensure that there are not duplicative penalties for the same conduct.

6. **Develop mechanisms to notify a critical infrastructure entity when an incident affects a federal system holding the entity's sensitive data.**
   Many government agencies and regulatory authorities hold sensitive financial institution data that, if breached, could pose risks to national security. Legislation should encourage bi-directional information sharing and greater collaboration between government and critical infrastructure. Should a federal agency experience a cyber incident affecting the operations and security of systems holding sensitive private sector data, notifying the private entity would allow institutions to take proactive measures to mitigate potential attacks.

We deeply appreciate your longstanding work on this issue and your efforts on this legislation and stand

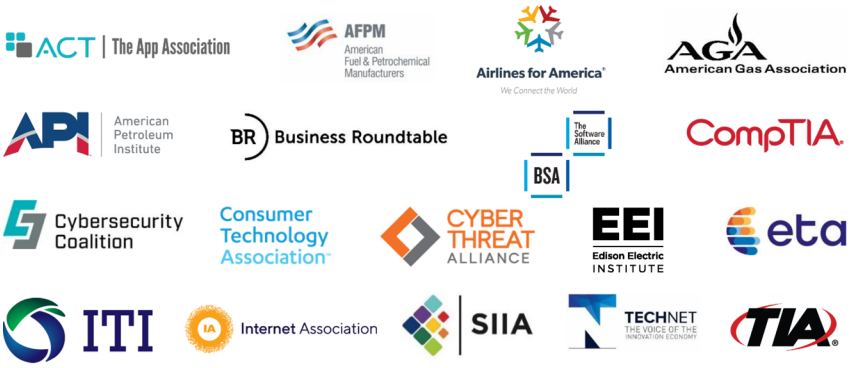
[1] Summary of incident reporting requirements

ready to work with you on all the issues described above; as drafted, however, we do not support the legislation as we believe that it would hinder rather than enhance cybersecurity for the financial services sector. We welcome further discussion on how to better protect our nation's critical infrastructure while ensuring front-line cyber defenders can continue to focus on security threats.

Sincerely,

American Bankers Association
Bank Policy Institute
Consumer Bankers Association

**CC: Senator Susan Collins, Senate Select Committee on Intelligence**




August 27, 2021

The Honorable Gary Peters
Chairman, Committee on Homeland Security & Government Affairs
United States Senate

The Honorable Rob Portman
Ranking Member, Committee on Homeland Security & Government Affairs
United States Senate

The Honorable Mark Warner
Chairman, Select Committee on Intelligence
United States Senate

The Honorable Marco Rubio
Vice Chairman, Select Committee on Intelligence
United States Senate

The Honorable Bennie Thompson
Chairman, Committee on Homeland Security
United States House of Representatives

The Honorable John Katko
Ranking Member, Committee on Homeland Security
United States House of Representatives

The Honorable Yvette Clarke
Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
United States House of Representatives

The Honorable Andrew Garbarino
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
United States House of Representatives

Dear Chairs, Vice Chairman, and Ranking Members:

The undersigned associations, representing major sectors of the American economy, including the owners, operators, and those that support and maintain the nation's critical infrastructure, appreciate Congress's ongoing focus on cybersecurity incident reporting legislation. Our industries recognize the value of public-private collaboration facilitated by mutual sharing of actionable information on significant cybersecurity incidents and intrusions with federal agencies. Incident Reporting legislation pending in Congress, when harmonized with the requirements of Section 2 of President Biden's *Executive Order on Improving the Nation's Cybersecurity*, have the potential to improve the nation's cybersecurity posture if appropriately developed and implemented.

To ensure an effective incident reporting regime that leverages the limited resources of federal agencies, enables regulatory compliance, provides liability protections, and advances national cybersecurity interests, we believe that policymakers in Congress should, at a minimum, follow five key principles:

**Establish feasible reporting timelines of no less than 72 hours.** Cybersecurity incidents are crisis moments for victim organizations. To ensure that the Cybersecurity and Infrastructure Security Agency (CISA) and its interagency partners receive actionable information on truly significant incidents, it is essential to give incident responders time to evaluate the intrusion to determine its impact. Shorter timelines also greatly increase the likelihood that the entity will report inaccurate or inadequately contextualized information that will not be helpful, potentially even undermining cybersecurity response and remediation efforts. A formal report on a verified, significant incident should not preclude less-fulsome notifications to CISA on a more flexible timeline."

**Limit reporting regulations to verified incidents and intrusions.** Incident reporting should focus on verified incidents rather than potential incidents or "near misses." Reporting verified incidents, that have been well defined and scoped, will avoid a culture of overreporting that will strain limited incident response capacity and capabilities inside and outside the government. It also can help ensure that information received is useful and actionable.

**Limit reporting obligations to the victim organization, rather than third-party vendors or providers**. Any legislation should ensure that the reporting obligation falls only on compromised affected entities. Vendors and third-party service providers should not be required to report cybersecurity incidents to the US Government that have occurred on their customers' networks and vice versa. Such a requirement would pose numerous challenges to normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of that customer or breach their contractual obligations. Requiring third-parties to report incidents could even disincentivize companies from employing outside cybersecurity services to the detriment of those companies' own security and resilience.

**Harmonize federal cybersecurity incident reporting requirements**. It is imperative that Congress streamline and normalize federal reporting requirements to ensure resources are used to combat malicious cyber threat activity, rather than customizing reports on the same incident to multiple agencies. Numerous federal agencies currently have disparate incident reporting requirements, many of which are just being implemented. Reported information should be aggregated, anonymized, analyzed, and shared, with government and industry, in a manner to assist in the mitigation and/or prevention of future cyber incidents.

**Ensure confidentiality and nondisclosure of incident information provided to the government.** It is imperative that any legislation have strong and transparent rules about the confidentiality of incident information that is shared with or by federal agencies. Such rules should govern not only the dissemination of incident information with relevant interagency partners, but should specifically preclude direct or indirect use of such information by the Federal government. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual, intellectual property, and privacy obligations.

Our industries strongly believe that securing the nation's digital assets is a shared responsibility requiring collaboration between the private sector and federal partners. We stand ready to assist policymakers as they develop their proposals on this important national security issue.

Sincerely,

ACT | The App Association

Airlines for America (A4A)

American Fuel & Petrochemical Manufacturers

American Petroleum Institute

American Gas Association

Business Roundtable

BSA | The Software Alliance

The Computing Technology Industry Association

Consumer Technology Association (CTA)

Cyber Coalition

Cyber Threat Alliance

Edison Electric Institute

Electronic Transactions Association

Information Technology Industry Council (ITI)

Internet Association

Software & Information Industry Association

TechNet

Telecommunications Industry Association (TIA)

August 24, 2021

The Honorable David P. Pekoske
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598-6020

Administrator Pekoske,

The included pipeline trade associations, AFPM, AGA, AOPL, API, APGA, INGAA, and GPA Midstream appreciate the opportunity to provide feedback on the recent Security Directive 2021-02, issued on July 19, 2021 (Directive). These trade associations represent almost all aspects of U.S energy pipeline operations that serve customers reliably across North America. The associations' members represent refineries and petrochemical operators -- through which pipelines receive and distribute products, regional and local natural gas distribution pipelines, liquids pipelines, integrated and midstream natural gas and oil companies, operators of municipal natural gas systems, natural gas transmission pipelines, and natural gas product pipelines and processors. Across the industry, our members all share the same concerns with the implementation of Security Directive 2021-02 and the process with which it was developed. For nearly two decades, we have worked along-side TSA in a structured oversight model applying risk-based methodology that properly balanced pipeline security with operational reliability and safety. We understand the ongoing situation presented by ransomware and other cyber threats to critical infrastructure and are committed to working with TSA to continue sound pipeline security practices and policies.

Open communication, process transparency, and timely engagement with the industry have been hallmarks of the TSA pipeline security program. Concerningly, these fundamental elements of a strong security partnership were not fully realized during the process used to develop the Directive. We wish to reemphasize the need for TSA to work efficiently with affected companies on successful Directive implementation, especially now that compliance deadlines are approaching. We encourage TSA and its technical experts to work closely with industry experts to ensure mutual understanding of how requirements in the Directive could impact operational reliability.

While we appreciate that TSA published an initial list of frequently asked questions (FAQs) focused on administrative matters, there remain several unanswered technical questions submitted by the associations and our members to which TSA guidance is critical for compliance. These unanswered questions have left operators with significant uncertainty about what is required for compliance. We urge TSA to release the technical FAQs in a timelier manner—TSA's timeline to responding to questions should be consistent with the rapid deadlines established under the Directive. We also ask TSA to apply learnings from the recent Directive development process to improve the agency's procedures for


obtaining stakeholder input on future pipeline security initiatives and avoid recreating the implementation challenges and uncertainty our members are now experiencing.

Operational reliability and safety are extremely important to the pipeline industry. The Directive's potential to cause operational disruptions or threaten safe operations remains a concern of affected pipeline operators. Our pipeline operators have expert knowledge regarding their assets, how they are managed to meet customer needs, and how to comply with the various state and federal regulations under which they are required to operate. As the Directive was developed, industry conveyed highly probable operational safety and reliability concerns that could arise by imposing prescriptive cyber requirements and untenable timelines without specific understanding of a company's existing cybersecurity protections and operations. We appreciate that TSA addressed some of our recommendations and responded to our feedback. Regretfully, significant concerns remain. The broad scope and prescriptive nature of the Directive create potential conflicts with TSA pipeline Security Guidelines and with existing cybersecurity and safety regulations from other federal government entities. The prescribed implementation schedule creates safety and reliability concerns. We urge TSA to work closely and quickly with operators on Directive implementation to ensure affected pipelines do not have to choose between complying with the Directive and ensuring continued safety and reliable operations.

The Directive allows operators flexibility to submit alternative compliance options to TSA for consideration, and TSA has stated it will respond promptly to these submissions. We recognize TSA believes operator concerns may be addressed through this alternative submittal option. However, the usability of this option is limited without further clarity on TSA's anticipated criteria and timelines for review of alternative proposals relative to the Directive's deadlines, what recourse operators have if TSA disagrees with proposed alternative compliance options, and how TSA will address scenarios where an operator determines that extensive equipment retrofits will take longer time periods than envisioned by TSA. Furthermore, TSA should ensure operators are not penalized for awaiting TSA's clarification of these issues and approval of alternative proposals as the Directive's deadlines approach.
Pipeline operators also face challenges applying the Directive in the context of broader corporate structures, given that cybersecurity for some pipeline operations is managed across individual companies and countries as part of enterprise-level cybersecurity and information technology systems that also cover non-pipeline operations. As the Directive is currently written, and without clarity from TSA, some operators are in the position of guessing what nonoperational networks (e.g., finance, HR, etc.) are impacted by the Directive and may be applying prescriptive measures that divert resources while not addressing the actual risks to pipeline operations. We urge TSA to provide more clarity on the scope, so that operators can make more sound determinations of what is necessary to avoid disrupting operations or threatening pipeline safety.

We also urge TSA to reconsider its process for implementing pipeline security initiatives in the future to ensure better input on the compatibility of proposed security requirements with pipeline operational technology. It is important TSA make timely updates to its pipeline security policies to keep up with


evolving threats. At the same time, it is equally important TSA's process does not sacrifice input from the regulated industry for the sake of speed. TSA's authorizing statute[1] and the Administrative Procedures Act require that the agency use formal notice-and-comment rulemaking as the primary vehicle for issuing new requirements. In this case, we believe the robust stakeholder input and advisory committee review provided by a notice-and-comment rulemaking would have resolved many of the substantive challenges created by the current Directive text and promoted stronger public-private partnership for pipeline security. We acknowledge that TSA may wish to protect certain aspects of its proposed requirements as Sensitive Security Information and note that procedures other than formal notice-and-comment can also be successful in soliciting and incorporating necessary input on a timely basis.

Our associations are also concerned that, as you testified to the Senate Commerce Committee on July 27, 2021, there is additional threat information driving the urgency of the Directive and the timelines that have been set. This threat intelligence has not been shared with potentially affected companies. Pipeline operators are best positioned to design mitigations to defend their systems against new threats based on their risk-based security programs. They are unable to effectively prepare for threats about which they have not been briefed. While we do appreciate the recent offer of a Secret level briefing to a limited group of associations within the Beltway, we again highlight the need for TSA, and the broader intelligence community, to ensure they are sharing the most timely and relevant information directly with the potentially impacted operators. We urge TSA, and other agencies that have threat information relevant to pipelines, to brief all potentially affected companies as soon as possible to ensure they can appropriately defend against current threats. We also encourage TSA to work with the broader intelligence community (IC) to provide regularly scheduled briefings to pipeline industry experts to ensure operators are appropriately informed about the evolving threats to their systems. TSA should also work with the IC to provide as much timely, unclassified information as possible to operators to ensure it is actionable and can be disseminated to operators who do not possess security clearances.

Listed below is a summary of our requests.

- TSA and its technical experts should work closely and quickly with industry experts to ensure mutual understanding of how requirements in the Directive could impact operational safety and reliability.
- TSA should release the technical FAQs immediately.
- TSA should provide clarity on anticipated criteria and timelines for review of alternative proposals, including addressing operator recourse if TSA disagrees with the alternative proposal and how TSA will address supply chain limitations.
- TSA should ensure operators are not penalized for awaiting TSA's review of alternative proposals.

[1] 49 U.S.C. § 114(l)(2)(A).


- TSA should provide more clarity on the Directive's scope so that operators can make more sound determinations of what is necessary to avoid disrupting operations or threatening pipeline safety.
- TSA should reconsider its process for implementing pipeline security initiatives in the future to ensure better input on the compatibility of proposed security requirements with pipeline operational technology.
- TSA and pertinent government intelligence community should brief all potentially affected pipelines on relevant cybersecurity threat intelligence as soon as possible.

The associations and our members are committed to supporting efforts to build pipeline cyber security capability, and we look forward to further discussing our concerns and potential solutions to ensure the Directive implementation can be successful.

ALLIANCE FOR AUTOMOTIVE INNOVATION

September 28, 2021

The Honorable Gary Peters
United States Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Rob Portman
United States Senate Committee on Homeland Security & Governmental Affairs
442 Dirksen Senate Office Building
Washington, DC 20510

**RE: Discussion Draft – Cyber Incident Reporting Act of 2021 (MIR21D05)**

Dear Chair Peters and Ranking Member Portman:

The Alliance for Automotive Innovation ("Auto Innovators") greatly appreciates your leadership on the important issue of cybersecurity incident reporting and critical infrastructure protection. As the singular, authoritative, and respected voice of the automotive industry, Auto Innovators welcomes the opportunity to provide feedback on the Cyber Incident Reporting Act of 2021 discussion draft. Securing the automotive ecosystem is critical to realizing the transformational benefits of the future of personal mobility. For this reason, members of Auto Innovators remain committed to building cybersecurity into their products and services and to managing evolving cybersecurity risks through information sharing, adoption of cybersecurity best practices, and cross-sectoral and public-private partnerships.

Focused on creating a safer, cleaner, and smarter transportation future, Auto Innovators represents the manufacturers that produce nearly 99 percent of cars and light trucks sold in the United States. Comprised of motor vehicle manufacturers, original equipment suppliers, technology companies, and others within the automotive ecosystem, Auto Innovators understands the importance of remaining nimble and agile in responding to a dynamic cybersecurity threat environment, particularly as connectivity, electrification, and automation results in the integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders.

Although the draft Cyber Incident Reporting Act of 2021 has a number of positive aspects – such as requiring the Cybersecurity and Infrastructure Security Agency ("CISA") to consider and harmonize with existing regulatory reporting requirements and allowing entities to report via third parties like information sharing and analysis organizations – there are several provisions that unnecessarily complicate our shared objective of protecting critical infrastructure and developing an effective and efficient cybersecurity incident reporting regime.

**Entities Subject to Reporting Requirements**

While the draft legislation defines "covered entity" as "an entity that owns or operates critical infrastructure," the text does not specify that "critical infrastructure" means the statutory definition of the term in the USA PATRIOT Act of 2001 (42 UC 5195c(e)). Auto Innovators maintains that "covered entity" should reference the existing statutory definition of "critical infrastructure" to give

CISA and entities more certainty about who will be in scope and alignment with existing reporting relationships.

**Types of Incidents Subject to Reporting**

Auto Innovators contends that cybersecurity incident reporting should be limited to material events that occur in the United States to focus CISA's limited time and resources on significant incidents that could have a debilitating effect on national security, national economic security, or national public health and safety. We also assert that entities should only have to report confirmed incidents.

**Reporting of Cybersecurity Incidents**

The discussion draft's exemption for covered entities from the reporting requirement if they provide substantially similar information to another federal regulatory authority applies only if the entities comply with the same reporting timelines for the proposed Cyber Incident Review Office and the other federal regulatory authority has an agreement to share such reporting within 24 hours of receipt. Auto Innovators maintains that the reporting of cybersecurity incidents to other regulatory authorities should be deemed sufficient for the purposes of this legislation if such reporting is done in compliance with that regulator's requirements. In addition, we suggest that the proposed Office be required to publish the list of agencies with which agreements for transmittal are in place.

**Timelines for Reporting Cybersecurity Incidents**

Auto Innovators appreciates that the discussion draft provides CISA with a date range for requiring covered entities to submit cybersecurity incident reports, *i.e.*, no earlier than 72 hours and no later than 7 days. Despite this, we contend that it is critical that CISA not take a one-size-fits-all approach on the reporting deadlines. As CISA itself notes, "[c]yberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks." Auto Innovators suggests that CISA be provided with the flexibility to develop different reporting deadlines for different categories of reporting entities.

**Use of Cyber Incident Reporting for Enforcement Action**

Unlike the draft Cyber Incident Reporting for Critical Infrastructure Act of 2021 (proposed by Congresswoman Yvette Clarke (D-NY-9) and Congressman John Katko (R-NY-24)), this discussion draft does not include any provisions to ensure that Federal, State, Tribal, and local authorities cannot use such information contained in cybersecurity incident reports for regulatory or enforcement purposes. Such provisions allow for continued collaborative information sharing. Auto Innovators strongly encourages the adoption of similar language from the Clarke/Katko draft legislation in this discussion draft.

**Traditional, Complete Rulemaking Process**

The discussion draft calls for CISA to issue an interim final rule, outlining the processes and procedures for entities to report cybersecurity incidents to the proposed Cyber Incident Review Office. While Auto Innovators appreciates the 60-day consultative period and the 90-day public comment period provided for in the draft, we recommend that the legislation allow for a traditional, complete rulemaking process with CISA starting with a notice of proposed rulemaking to provide more opportunities for public input and agency accountability in the formulation of these new regulatory requirements.

Auto Innovators and its members share the Committee's goals and desire to improve critical infrastructure protection. We stand ready to work with the Committee in a bipartisan, bicameral way in pursuit of an effective and efficient cybersecurity incident reporting regime that advances situational awareness for the government and non-Federal entities in a collaborative manner.

Sincerely,

Garrick C. Francis

Garrick C. Francis
Vice President, Federal Affairs
Alliance for Automotive Innovation

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Chris Inglis**
**From Senator Jacky Rosen**

**"National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems"**
**September 23, 2021**

1. GAO has identified the consistent shortage of cybersecurity personnel at federal agencies as a high risk to national security. Recent unprecedented cyber-attacks, like the SolarWinds and the Colonial Pipeline breaches, demonstrate the urgency of equipping the U.S. government with the cyber talent needed to prevent & respond to attacks. To address this gap, Senator Blackburn and I introduced the Civilian Cyber Security Reserve Act –which was marked up and passed by this committee –to establish a civilian cyber reserve at CISA and CYBERCOM to call up cybersecurity in response to significant cyber incidents.

   a. What is your strategy to equip the Federal Government with the cyber talent required to protect critical infrastructure?

   ***ONCD Response:*** *The Office of the National Cyber Director is developing the National Cyber Workforce and Education Strategy in coordination with other elements of the Executive Office of the President as well as Federal departments and agencies, with input from key public and private stakeholders. Among other topics, the National Cyber Workforce and Education Strategy will aim to address the challenges and opportunities in the Federal cybersecurity workforce.*

2. I'd like to focus on addressing vulnerabilities to the energy and water sectors in particular. Attacks like those recently targeting Colonial Pipeline and a Florida water treatment facility will only become more frequent, and potentially deadly, unless we shore up our cyber defenses. To protect our electric grid, I recently re-introduced the Cyber Sense Act, bipartisan legislation that would create a voluntary Cyber Sense program at the Department of Energy to test the cybersecurity of products and technologies intended for use in the bulk-power system. I'm glad that my bill was included in the bipartisan infrastructure bill passed by the Senate.

   a. While the program established by my bill would be for electric utilities, I know that the water sector is one of the most vulnerable of all critical infrastructure sectors. Given this, do you think a similar program for water systems would be helpful?

***ONCD Response:*** *The Energy Cyber Sense Act, as enacted by Sec. 40122 of the Infrastructure Investment and Jobs Act of 2021 (PL 117-58), is integrating and enhancing Department of Energy's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program, which is a consortium of six of the National Labs conducting intelligence-informed cyber vulnerability testing and enumeration for critical components in control systems in partnership with industry manufacturers and asset owners. A large portion of the most prevalent components in control systems are common across utility systems including electricity, oil and natural gas, hydroelectrics, and water systems.*

3. In May, operations of the Colonial Pipeline were brought to a halt due to the malicious actions of foreign hackers. The impacts were devastating and disruptive to millions of Americans throughout the country. I have serious concerns about similar cyber-attacks that are being directed at numerous utilities around the country on a daily basis.

   We must protect devices and assets connected to the electric grid, including our substations, power plants, and fuel transportation systems, from nefarious actors that are constantly attempting to compromise our networks. No single layer of cyber protection is sufficient to mitigate these types of attacks, and additional layers are needed to protect critical infrastructure.

   a. The Federal Power Marketing Administration (PMA) markets and delivers power across 34 states, including Nevada. The consequences of a cyber-attack on these utilities could be devastating. What is being done to protect critical infrastructure in the field when networks are compromised, such as we saw with Colonial; and do you agree with the multiple layer approach to ensure assets in the field are adequately protected?

   ***ONCD Response:*** *The Colonial Pipeline incident involved criminal ransomware actors compromising part of the information technology (IT) system of the company. Fortunately, the ransomware actors were unable to move from the IT system in to the operational technology systems that run the physical infrastructure. The asset owner in this case elected to halt operations out of an abundance of caution, but the resulting disruption and potential for more significant impacts have catalyzed action.*

   *In response, the Administration issued the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems which established the Industrial Control Systems Cybersecurity Initiative to improve visibility on these critical systems, and directed the development of Critical Infrastructure Cybersecurity Performance Goals to accelerate the adoption of*

*cybersecurity baselines. ONCD continues to coordinate with the National Security Council, Cybersecurity and Infrastructure Security Agency, and the sector risk management agencies in implementing these critical initiatives.*

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Chris Inglis**
**From Senator Kyrsten Sinema**

**"National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems"**
**September 23, 2021**

1) In your testimony, you briefly mentioned the importance of building a cyber workforce and having agencies speak with one voice and operate with unity of purpose and effort. As my staff has collaborated with several agencies on a draft bill that seeks to improve cybersecurity education nationally and increase the pool of cybersecurity professionals, it became clear that agencies are involved in several educational efforts but that there has been no clear coordination amongst these efforts.

   i) Do you believe that one critical area for improving our nation's cybersecurity posture is addressing the need for a coordinated cyber education strategy to increase general cybersecurity knowledge across the US population and expose and thus encourage more people to pursue careers in cybersecurity?

***ONCD Response:*** *The Office of the National Cyber Director is developing the National Cyber Workforce and Education Strategy in coordination with other elements of the Executive Office of the President as well as Federal departments and agencies, with input from key public and private stakeholders. Among other topics, the National Cyber Workforce and Education Strategy will aim to address the challenges and opportunities in this critical area, improve collaboration across government-wide efforts, help align resources to aspirations, and implement Biden-Harris Administration priorities on education and workforce development.*

   ii) If so, do you foresee that the Office of the National Cyber Director will oversee the overall day-to-day coordination and ongoing evaluation of these efforts?

***ONCD Response****: The Office of the National Cyber Director will lead the coordination of implementation of the previously mentioned National Cyber Workforce and Education Strategy.*

   iii) Will the National Cyber Strategy that you are crafting include a component focused on education and workforce development?

***ONCD Response:*** *The Office of the National Cyber Director is developing the National Cyber Workforce and Education Strategy which is dedicated to addressing the challenges and opportunities in both cyber education and the cyber workforce.*

2) Now that you are confirmed in your role as the National Cyber Director, what steps are you taking to outline the structure and operations of the office and the budget you will need to support those plans? Do you have the resources that you need?

***ONCD Response**: In October 2021, the Office of the National Cyber Director (ONCD) released, "A Strategic Intent Statement for the Office of the National Cyber Director." This document outlined the vision for the office and our path to execute the Biden-Harris Administration's cyber agenda through four principal outcomes: federal coherence; improving public private collaboration; aligning resources to aspirations; and increasing present and future resilience. The document further describes ONCD's lines of effort, to include National Cybersecurity; Federal Cybersecurity; Strategy and Budget; and Technology and Ecosystem Security. For Fiscal Year 2023, the President requested $21.9M to carry out ONCD's operations. ONCD thanks Congress for funding the ONCD at the President's Budget Request level for Fiscal Year 2023.*

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Jen Easterly**
**From Senator Kyrsten Sinema**

**"National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems"**

**September 23, 2021**

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | CISA Workload |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Kyrsten Sinema |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Within the past year, there have been a number of actions within the Administration and legislation passed by Congress to improve the nation's cybersecurity. These efforts have rapidly expanded CISA's workload. CISA is still a young organization and has yet to fully implement its organizational plan. It is also an agency that requires professionals with a particular skillset that is in high demand across the country.

Are you concerned that Congress is asking CISA to do too much too quickly?

What efforts are you taking to assess CISA's capabilities and scale the workforce and programs accordingly to ensure these efforts are successful?

What do you need from Congress to help ensure that you can successfully implement and scale these efforts?

**Response:** The Cybersecurity and Infrastructure Security Agency (CISA) does not believe Congress is asking the Agency to do too much, too quickly. CISA has benefited tremendously from the strong support of Congress, which has provided the Agency with important authorities, as well as additional resources to begin implementing new programs and activities. We look forward to implementing the cyber incident reporting law, the new Cyber Response and Recovery Fund (CRRF), and, along with our partners at the Federal Emergency Management Agency, the State, Local, Tribal, and Territorial (SLTT) Cybersecurity Grant Program recently passed by Congress. The cyber incident reporting law will give CISA, our federal partners, and stakeholders across our nation's critical infrastructure sectors a much better understanding of the scope and scale of cyber incidents impacting our networks and critical infrastructure. The CRRF resources CISA to provide response and recovery services to victims during a major cybersecurity incident. And the SLTT Grant Program provides SLTT partners with additional resources to enhance the security and resilience of their networks against cyber-

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | CISA Workload |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Kyrsten Sinema |
| **Committee:** | HOMELAND SECURITY (SENATE) |

attacks. CISA is moving quickly to stand up new program offices and develop processes and procedures to guide implementation of these and other new initiatives directed by Congress in recently passed legislation. Any additional resources required to sustain the execution of these, and other critical mission priorities will be identified and communicated to Congress via the annual President's Budget.

We appreciate Congress recent passage of the FY 2022 Omnibus Appropriations Act, which provided $2,593,666,000 for CISA in FY 2022, $598.7M above the FY 2021 Enacted and $460M above the FY 2022 President's Budget. This law provides the additional resources CISA needs to successfully implement a variety of new and emerging mission requirements. Should Congress decide to include funding increases above and beyond the annual President's Budget in future appropriations cycles, it is important to consider whether complimentary investments in mission enabling functions such as talent management, financial management, procurement, acquisition, and other program support services are warranted. It is imperative that as we grow CISA capabilities and service offerings, we continue to mature these essential business and mission support services.

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | Cybersecurity Curriculum |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Kyrsten Sinema |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** When we focus on cyber education and workforce development, we tend to focus more on developing cybersecurity professionals. However, in this connected world, it seems every professional would benefit from more enhanced cyber education. CISA partnered with Office of Personnel Management's Federal Executive Institute to develop and deliver a curriculum to managers in the Federal government who do not have cybersecurity in their mission. This is the type of program we need across the Federal government. Is this program continuing and if so, how is CISA scaling it to support more professionals in the Federal workforce?

**Response:** People are CISA's number one asset. Secretary Mayorkas and I are committed to attracting and retaining world-class talent by implementing a vibrant, end-to-end talent management ecosystem that spans from recruiting and hiring, to onboarding and integration, mentorship and coaching, certification and training, recognition and promotion, to succession planning and retention. To this end, CISA is utilizing the U.S. Department of Homeland Security's (DHS) new Cyber Talent Management System launched in November 2021, thanks to Congress' earlier actions. CISA will use this system to grow the future cybersecurity workforce and ensure it represents the people it is designed to serve, including diverse backgrounds at all levels of the agency and in all positions in the workforce.

Even as we focus on CISA's own workforce, we have a critical role in building a world-class cybersecurity workforce across our country that reflects the diversity of America. This requires both cultivating today's cyber workforce and recognizing that our efforts also play an important role in helping build the cyber workforce of tomorrow. CISA has maintained a partnership, over two fiscal years, with the Office of Personnel Management's (OPM) Federal Executive Institute and just concluded the Second Federal Executive Cyber Training Cohort to prepare senior leaders to understand the dynamic cybersecurity environment. CISA and OPM shared lessons learned throughout the partnership and are currently evaluating ways to have higher return on investment through improved scalability that optimizes participation and availability. Additionally, CISA is piloting an internal program that will evaluate cybersecurity baseline training for entry-level personnel and personnel looking to develop the necessary skills to enter the cybersecurity profession.

More broadly, as cybersecurity threats to our communities continue to rise, CISA strives to provide innovative tools to help prepare, grow, and sustain a talented, diverse workforce to defend against these threats. In August 2021, CISA released the Cybersecurity Workforce Training Guide for current and future federal and SLTT cybersecurity/IT professionals. The Guide helps staff develop a training plan based on their current skill level and desired career

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | Cybersecurity Curriculum |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Kyrsten Sinema |
| **Committee:** | HOMELAND SECURITY (SENATE) |

path. CISA offers over 100 training courses (including some certification prep materials), as well as cybersecurity resources from across the federal government to help professionals stay current and advance their careers.

Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up to date on skills and evolving threats. CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Jen Easterly**
**From Senator Jacky Rosen**

**"National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems"**

**September 23, 2021**

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | Identify SICI |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Recent cyberattacks targeting critical infrastructure, from pipelines to our food supply, have exposed significant vulnerabilities in our networks. Our adversaries are constantly hunting for cyber targets in key sectors that would have the greatest destructive impact. And yet, according to the Cyberspace Solarium Commission, "the U.S. government still lacks rigorous, codified, and routinely exercised processes for identifying, assessing, and prioritizing critical infrastructure risks across the federal government and between the public and private sectors." In simpler words, if everything is critical, nothing is critical.

As you know there are multiple bipartisan legislative efforts to provide clarity on what systems, assets, and networks are Systemically Important Critical Infrastructure, or SICI. Could you provide an update on CISA's work to identify SICI entities, and how you are and separately, how you are evaluating the performance of each Sector Risk Management Agency in reducing cybersecurity risks in key sectors?

**Response:** CISA has a statutory responsibility to identify and prioritize the systems and assets that are most critical to national security, health, and prosperity. CISA has gathered lessons learned from previous incidents and combined with an improved understanding of the Nation's rapidly changing risk environment and systemic risk, is working to develop prototypes of new methods to identify, assess, and prioritize critical infrastructure and the risks to critical infrastructure. Specifically, the Nation's COVID-19 response provided CISA with a wealth of lessons learned that are informing our prototype development.

We coordinate across CISA to identify what the Cyberspace Solarium Commission called Systemically Important Critical Infrastructure (SICI). These SICI entities, which CISA refers to as Systemically Important Entities, are private/public entities that provide products and services that, if disrupted, would have an outsized impact on our national and economic security. CISA

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | Identify SICI |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

has previously developed lists of infrastructure, such as the National Critical Infrastructure Prioritization Program lists and the Section 9 list, which have served as initial efforts to identify critical entities. CISA is actively striving to simplify the recognition of indicators of the systemic importance of critical infrastructures at a national level. CISA's focus on the National Critical Functions (NCFs) is designed to mature CISA's prioritization methodologies by identifying critical infrastructure primarily based on the cascading effects of loss or compromise of a nationally critical function that a system or asset supports. Additionally, CISA has created a cross-agency working group to apply our NCFs Framework.

Core elements of this framework include:

- The entities' ownership or operational responsibilities for critical infrastructure meet criteria for systemic importance.
- They are candidate primary partners that help CISA lead the nation to more secure and resilient practices, or they are other systemically important entities who are likely to have subtle but important roles and need our assistance.
- We are using draft criteria to help identify systemically important entities and will evaluate and apply lessons learned.
- Early results of prototype analytic methods have been developed through our National Infrastructure Simulation and Analysis Center.

CISA will engage Sector Risk Management Agencies (SRMAs) and other relevant federal partners for review and coordination; their participation will also be critical in the initial identification of systemically important entities. Upon completion of these efforts, CISA will focus its service deliveries to prioritize engagements with SICI in adaptive risk reduction efforts. With more mature partners, this may lead to rapid optimized risk reductions through operational collaboration. While progress may be slower with less mature partners – and may require a different set of services - working with these entities can yield improvements in the nation's risk landscape of even greater significance. CISA aspires to eventually build on this success to engage our state, local, territorial, and tribal government partners in adaptive risk reductions within their areas of responsibility.

CISA's work on National Critical Functions and the development of a National Risk Register continues and will support and illuminate areas of National Risk that we will collaborate with partners to enhance risk mitigation. Furthermore, CISA, the National Institute of Standards and Technology, and the sixteen critical infrastructure sectors are coordinating to establish cybersecurity performance goals to ensure that the critical infrastructure owners and operators have shared understanding of target cybersecurity capabilities across entire sectors. Additional goals will be established by each sector to ensure that the specific needs of each sector are

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | Identify SICI |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

incorporated into the broader set of sector specific cybersecurity goals. CISA will continue to support partners with resources, assessments, and information sharing.

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | Cybersecurity Surge Capacity |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** GAO has identified the consistent shortage of cybersecurity personnel at federal agencies as a high risk to national security. Recent unprecedented cyber-attacks, like the SolarWinds and the Colonial Pipeline breaches, demonstrate the urgency of equipping the U.S. government with the cyber talent needed to prevent & respond to attacks. To address this gap, Senator Blackburn and I introduced the Civilian Cyber Security Reserve Act -which was marked up and passed by this committee -to establish a civilian cyber reserve at CISA and CYBERCOM to call up cybersecurity in response to significant cyber incidents.

On the heels of last month's White House cybersecurity summit with business leaders, how can CISA utilize preexisting links between the private sector and the Federal Government to mobilize a cybersecurity surge capacity at times of greatest need?

**Response:** Managing cybersecurity threats requires a whole-of-nation response that brings together the best capabilities of government and the private sector. For this reason, we recently established the Joint Cyber Defense Collaborative (JCDC). The JCDC is focused on bringing key federal government partners, along with private sector entities, together to plan proactively for and respond to cybersecurity threats like those that impacted SolarWinds, Microsoft Exchange Server, and Colonial Pipeline.

The JCDC will expand CISA's existing information sharing approach by incorporating a robust planning element and focus on cyber defense operations. The goal of the JCDC is to have these federal and private sector partners share information to better understand cyber risks and develop an operational plan to address a specific cyber risk that defines how each entity will use their capabilities to prevent or mitigate the risk. These joint plans aim to strengthen the nation's collective cyber defense posture through collective and unified action.

The JCDC will provide comprehensive, whole-of-nation planning to address risk both during steady-state operations and during an incident. As we've learned from recent events, the time to plan for how to bring together these unique capabilities, and to determine who to have at the table, is not during the stress of an active incident. Instead, the JCDC will advance the state of national cybersecurity by providing the first place where the public and private sectors can come together to plan how to reduce the most significant risks, exercise those plans together to ensure they operate as expected, adapt plans as circumstances change, and jointly execute plans to actively reduce risk.

The unique value of the JCDC is to create a proactive capability for government and private sector to work together closely before an incident occurs to strengthen the connective tissue and

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | Cybersecurity Surge Capacity |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

ensure a common understanding of processes. Through coordinated cyber defense with interagency, SLTT and private sector partners, the JCDC will work to drive down risk before an incident and to unify actions should an incident occur. The JCDC will help equip the nation as a whole with the collective capabilities needed to prevent and respond to major cyber incidents. We look forward to working with Congress to explore future strategies necessary to meet the evolving nature of cybersecurity risks.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | Water Systems Program |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** I'd like to focus on addressing vulnerabilities to the energy and water sectors in particular. Attacks like those recently targeting Colonial Pipeline and a Florida water treatment facility will only become more frequent, and potentially deadly, unless we shore up our cyber defenses. To protect our electric grid, I recently re-introduced the Cyber Sense Act, bipartisan legislation that would create a voluntary Cyber Sense program at the Department of Energy to test the cybersecurity of products and technologies intended for use in the bulk-power system. I'm glad that my bill was included in the bipartisan infrastructure bill passed by the Senate.

While the program established by my bill would be for electric utilities, I know that the water sector is one of the most vulnerable of all critical infrastructure sectors. Given this, do you think a similar program for water systems would be helpful?

**Response:** Ensuring the supply of safe drinking water and treatment of wastewater is essential to modern life and the Nation's economy. Every day, more than 150,000 public water systems provide drinking water to millions of Americans and U.S. wastewater treatment facilities process approximately 34 billion gallons of wastewater. Considered NCFs, both the ability to "supply water" and "manage wastewater" are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

CISA tests for and simulates cybersecurity risks affecting critical infrastructure sectors, including the Water and Wastewater Sector. Through our Control Environment Laboratory Resource (CELR) government, academic, and private industry partners can demonstrate and experience the effects of kinetic cyber-physical events in a safe, isolated, and secure environment. CELR can simulate high-consequence cyber scenarios that would otherwise introduce unacceptable risk to real production environments. Using CELR, researchers, operators, and utility owners can have access to several test environments that use real components to demonstrate the effects of cyber-physical disturbances. These test environments, called skids, can be accessed in-person, through remote connection, or shipped across the United States. Each skid contains real operational technology, which allows CELR to effectively simulate and assess the risks and consequences of an attack, a vulnerability, or integration of new equipment on an existing simulated infrastructure – such as a chemical plant or a natural gas pipeline compressor station. Using CELR's resources, researchers can improve methods for defending industrial computer technology.

This work is just one part of our ongoing focus on the Water and Wastewater Sector.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | Water Systems Program |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

To enhance the security of these functions, CISA is working with the private sector, government agencies, and other key stakeholders to manage the most significant risks to these important functions. On October 14, 2021, CISA released a joint cybersecurity advisory with the Federal Bureau of Investigation, the Environmental Protection Agency (EPA), and the National Security Agency to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology and operational technology networks, systems, and devices of U.S. Water and Wastewater Systems Sector facilities. On January 27, 2022, the Biden Administration announced the Water Sector Action Plan which was developed in close partnership with EPA and CISA. The Action Plan is part of the Administration's ICS Cybersecurity Initiative, a voluntary collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of technologies and systems that provide cyber-related threat visibility, indicators, detections, and warnings.

CISA supports efforts to increase SRMAs' ability to identify, monitor, and manage risk within their sectors. However, we need to ensure that we are making the best use of the tools currently available to the Federal government. If not done thoughtfully, addressing risks on a sector-by-sector basis could result in overlapping responsibilities, duplication of resources, and inadvertent barriers to information collection and sharing. Where there is systemic risk – as is often the case with cybersecurity – we should leverage CISA's existing authorities and expertise, while supporting EPA's ongoing efforts to secure this vital sector.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | Climate Change |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** This week, the GAO released a report finding that FERC and the Energy Department have not acted on a number of GAO recommendations for improving electricity grid resilience. One of these recommendations includes better managing climate-related risks. How is CISA identifying and planning for the impacts of climate change on the cybersecurity of our critical infrastructure?

**Response:** CISA will ensure that the risks posed by climate change are reflected in the data and analytic products of the agency, and guides its engagement with our stakeholder community. E.O. 14008 directs the Secretary of Homeland Security to "consider the implications of climate change to NCF." CISA is leading this analysis for DHS. The response will include an analysis of how flooding, extreme tides and sea-level rise, tropical cyclones and hurricanes, severe storm systems, extreme cold, extreme heat, wildfire, and drought are expected to impact the execution of NCFs in the years 2030, 2050, and 2100 under the following two scenario conditions:

- High Emissions scenario: This scenario reflects the projected global mean temperature change by 2100 in the event of a sudden significant increase in future global emissions and/or a higher climate sensitivity that results in higher magnitudes of climate change per unit of emissions. This is equivalent to global warming of approximately 5 C (9 F) by the end of the century.
- Current Policies scenario: This scenario reflects the projected global mean temperature change by 2100 given current global emissions levels and national commitments to emissions reductions. This is equivalent to global warming of approximately 3 C (5.4 F) by the end of the century.

The first iteration of this annually developed analysis will address expected impacts on 27 NCFs; subsequent updates will include both an analysis of the 28 NCFs that are not included in the initial response, as well as updates and revisions to the original 27 as needed. This analysis will guide how CISA allocates resources and develops strategies for collaborating with its partners as it prepares the nation's critical infrastructure stakeholders to address the threats posed by climate change.

We maintain a close working relationship with the Department of Energy as the Sector Risk Management Agency (SRMA) for the energy sector. Our work with DOE includes efforts to identify and address risks created or exacerbated by climate change.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | Climate Change |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

Additionally, CISA is examining multiple avenues for nexus points between cyber and climate security and look forward to guiding our stakeholder community on strategies to maximize their overall resilience to all-hazards.

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | CETAP Budget |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Last year, I worked with my colleague, Senator Cassidy, to introduce the PROTECT Act, a bipartisan bill to make permanent the Cybersecurity Education and Training Assistance Program - or CETAP - that provides cybersecurity career awareness, curricular resources, and professional development to elementary and secondary schools across the U.S., including direct, no-cost support to students and educators. I was surprised and disappointed, therefore, to see that funding for CETAP was zeroed out in the President's budget request.

Will you recommend to OMB that the CISA budget for Fiscal Year 2023 include funding for CETAP?

**Response:** CISA is not in a position to comment on the contents of the President's Budget Request for future fiscal years. That said, America needs well-trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation. CISA is committed to helping the administration and other interagency partners to strengthen the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of future cybersecurity leaders for tomorrow.

To help address the cybersecurity workforce shortage of skilled cyber workers, CISA is undertaking a variety of efforts. We have built pathways to help America's academic institutions prepare students for careers in cybersecurity, to include investing in the Scholarship for Service Program which provides scholarships for students interested in a career in cybersecurity in exchange for government service. Additionally, CISA has issued a $2M grant to non-traditional training providers to produce a supply of diverse and highly qualified cybersecurity professionals to solve the cyber challenges facing our nation.

Our K-12 program has provided cybersecurity curricula access to over 26,000 teachers to date, influencing over 3 million students to join the cybersecurity career field in the future. CISA intends to continue to find innovative and creative ways to engage students and educators that further influences national cyber awareness, education, training, and career pathways to cyber.

Recognizing the broad scale of the cybersecurity workforce challenge and the need to make measurable progress in the near term, CISA plans to prioritize the needs of the federal workforce, while influencing the national cyber-ecosystem and talent pipeline.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | Layers of Protection |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In May, operations of the Colonial Pipeline were brought to a halt due to the malicious actions of foreign hackers. The impacts were devastating and disruptive to millions of Americans throughout the country. I have serious concerns about similar cyber-attacks that are being directed at numerous utilities around the country on a daily basis.

We must protect devices and assets connected to the electric grid, including our substations, power plants, and fuel transportation systems, from nefarious actors that are constantly attempting to compromise our networks. No single layer of cyber protection is sufficient to mitigate these types of attacks, and additional layers are needed to protect critical infrastructure.

The Federal Power Marketing Administration (PMA) markets and delivers power across 34 states, including Nevada. The consequences of a cyber-attack on these utilities could be devastating. What is being done to protect critical infrastructure in the field when networks are compromised, such as we saw with Colonial; and do you agree with the multiple layer approach to ensure assets in the field are adequately protected?

**Response:** In today's rapidly changing world, our Nation's critical infrastructure continues to face new threats and challenges, many of which require an integrated risk management approach and close coordination between the government and private sector to address. CISA understands that securing our nation's electricity sector is a vast and complex system. Many of the necessities of modern society, from putting food on our tables to keeping lights on in our homes, depend on the reliability of our communications and power networks, and the devices that control them. As these systems become more complex, critical equipment is increasingly connected digitally making these systems more efficient, but also more susceptible to intrusions by our adversaries. Attacks on operational systems not only endanger the American ways of life but threaten to directly take lives. CISA is working with the companies that power America to ensure that their efforts to serve customers in new ways are designed with security principles fit for the 21st Century.

To accomplish this mission, CISA leads a collaborative effort to identify and drive reduction of the most significant cyber risks to critical infrastructure. This requires first identifying cyber risks through robust multi-directional information sharing, conducting risk and vulnerability assessments, and deploying threat detection technologies to critical assets. These efforts are made more effective through our interagency work with Sector Risk Management Agencies (SRMAs). We work to prioritize identified risks, including by leveraging the capabilities of our National Risk Management Center to understand relative criticality of critical infrastructure assets and working with our partners across government to understand our adversaries' potential

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | Layers of Protection |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

intent and capabilities. Finally, we drive collective action to reduce cybersecurity risks, including by providing incident response and threat hunting services, issuing alerts and guidance, and developing plans for joint cyber defense operations that bring together capabilities from government and private sector partners.

CISA maintains field-based cybersecurity advisors (CSAs) and cybersecurity state coordinators (CSCs). The CSAs/CSCs provide cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations and SLTT governments. CSAs/CSCs cultivate partnerships with participating organizations and initiate information sharing. CSAs/CSCs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources. CSAs/CSCs also collaborate with local and federal entities to facilitate delivery of cybersecurity services across the U.S. These services include cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, and incident coordination and support. During incidents, these CSAs/CSCs support victims with incident triage and share important information quicky such as indications of compromise with the greater cybersecurity community to reduce the risk of such activity. CISA also brings together the cyber/physical security nexus to help minimize the impacts of a single critical infrastructure entity outage. CSAs/CSCs work alongside field based CISA Protective Security Advisors, Emergency Communications Coordinators, Regional Analysts and other Regional office staff to provide information sharing, risk prioritization and dependency analysis, technical assistance, and capacity building across all 16 critical infrastructure sectors.

CISA has a longstanding relationship of cooperation and collaboration with the electricity subsector, in close partnership with the U.S. Department of Energy (DOE) as the SRMA for the energy sector, that we are keen to strengthen and evolve given the serious cybersecurity threats this vital sector faces every day. An example of this collaboration is the Administration's ICS Cybersecurity Initiative which was launched in 2021 as part of the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. The Administration worked closely with CISA, DOE, and the Transportation Security Administration (TSA) to establish Action Plans with the electricity and natural gas pipeline subsectors. The Initiative provides a voluntary collaboration mechanism between the federal government and the critical infrastructure community to facilitate the deployment of technologies and systems that provide cyber-related threat visibility, indicators, detections, and warnings.

Given the criticality of certain pipeline entities and certain other critical infrastructure assets, CISA works closely with TSA and the Department of Transportation who serve as co-SRMAs for the pipeline subsector to enhance pipeline security, safety, and resilience. CISA offers a pilot program called CyberSentry, which deploys technologies and analytic capabilities to monitor an organization's business (IT) and operational technology/industrial control system (OT/ICS)

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | Layers of Protection |
| **Hearing:** | National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems |
| **Primary:** | The Honorable Jacky Rosen |
| **Committee:** | HOMELAND SECURITY (SENATE) |

network for sophisticated threats. CyberSentry is a voluntary partnership with private sector critical infrastructure companies using CISA's unique statutory authorities, policy and privacy-focused solutions. This capability is not a replacement for commercial solutions; rather, the capability complements such solutions by allowing CISA to leverage sensitive threat information to enable increased protection for critical networks and systems. CyberSentry has shown significant benefit in practice and has been used to drive urgent remediation of threats and vulnerabilities.

Separately, in partnership with a National Laboratory, CISA is developing a suite of tools to assess cyber resilience through scenarios using specialized threat models and simulations to identify critical components within pipeline OT. Going forward, the Pipeline Cybersecurity Initiative (PCI) is planning a pipeline cyber table-top exercise to better understand the impacts of an OT compromise at a major natural gas transmission line and is collaborating with industry to integrate pipeline considerations into CyberStorm VIII – a CISA-led biennial exercise series that provides the framework for the nation's largest cybersecurity exercise – in Spring 2022. PCI's future efforts will center around determining the prevalence of major components within pipeline OT systems to identify potential vulnerabilities and inform supply chain risk efforts. Further, CISA plans to lead the development of a pilot tool focused on liquid pipelines that will allow users to explore how disruptions to pipelines can have cascading consequences on National Critical Functions.

Lastly, CISA is focused on driving resilience and functional continuity alongside improvements in security. We must advance business continuity exercises, even as we catalyze adoption of cybersecurity best practices; we must ensure that operational technologies are segmented from and can run independently from business networks even as we advance our ability to detect threats in both environments; and, we must reduce single points of failure across our National Critical Functions as we identify and harden identified nodes of systemic risk.