TRANSPORTATION CYBERSECURITY: PROTECTING PLANES, TRAINS, AND PIPELINES FROM CYBER THREATS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

AND THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

OCTOBER 26, 2021

Serial No. 117–34

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

46–812 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

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

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

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

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

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

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

BONNIE WATSON COLEMAN, New Jersey, *Chairwoman*

DONALD M. PAYNE, JR., New Jersey
DINA TITUS, Nevada
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
BENNIE G. THOMPSON, Mississippi *(ex officio)*
CARLOS A. GIMENEZ, Florida, *Ranking Member*
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
JOHN KATKO, New York *(ex officio)*

ALEX MARSTON, *Subcomittee Staff Director*
KATHRYN MAXWELL, *Minority Subcomittee Staff Director*
ALICE HAYES, *Subcomittee Clerk*

CONTENTS

TRANSPORTATION CYBERSECURITY: PROTECTING PLANES, TRAINS, AND PIPELINES FROM CYBER THREATS

Tuesday, October 26, 2021

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

The subcommittees met, pursuant to notice, at 2:04 p.m., via Webex, Hon. Yvette D. Clarke [Chairwoman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation] presiding.

Present: Representatives Clarke, Watson Coleman, Jackson Lee, Langevin, Titus, Slotkin, Rice, Luria, Torres, Garbarino, Gimenez, Norman, Van Drew, Harshbarger, Miller-Meeks, Clyde, and LaTurner.

Ms. CLARKE. The Committee on Cybersecurity, Infrastructure Protection, and Innovation and the Subcommittee on Transportation and Maritime Security will come to order for today's hearing entitled "Transportation Security: Protecting Planes, Trains, and Pipelines from Cyber Threats."

Without objection, the Chair is authorized to declare the subcommittees in recess at any point.

Let me start by thanking Chairwoman Watson Coleman and Ranking Member Garbarino, Ranking Member Gimenez, and our panel of witnesses for joining us today.

We are here to assess the administration's actions aimed at mitigating the cybersecurity challenges facing the transportation sector. Earlier this year, our subcommittees worked together to evaluate how the Federal Government partners with the private sector to respond to a ransomware attack against Colonial Pipeline which resulted in 5,500 miles of pipeline being shut down.

As panic led to fuel shortages at gas stations along the East Coast and airlines scrambled to find alternative fuel supplies, we learned that, No. 1, attackers infiltrated Colonial Pipeline's business network using a legacy VPN that did not require multifactor authentication; No. 2, the flow of information between Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency, and the Transportation Security Administration was slow, fueled in part by on-going confusion about which agency was in charge; and,

No. 3, despite repeated offers from TSA, Colonial Pipeline had not yet undergone an important security assessment, a validated architecture design review, and did not have a disaster response plan that contemplated a full—the full scope of cyber threats.

Shocked by what we learned during their oversight of Colonial Pipeline and other recent high-profile cyber incidents, Members of Congress have begun to question whether the Federal Government's approach to cybersecurity, which relies primarily on voluntary partnerships, actually works, or whether some security requirements ought to be mandated.

The notion that certain entities should be subject to cybersecurity standard mandates is not new. Almost 10 years ago, President Obama issued Executive Order 13636 on improving critical infrastructure cybersecurity. The Executive Order directed sector risk management agencies to evaluate whether they had sufficient authority to establish cybersecurity requirements for critical infrastructure entities for which a, "cybersecurity incident could reasonably result in catastrophic regional or National effects on a public health or safety, economic security, or National security," and report back to DHS and the White House with what they found.

To the best of my knowledge, no agency suggested they lacked authority to issue such requirements. Nevertheless, for nearly a decade, the Federal Government has continued to pursue security policies that rely primarily on voluntary partnerships with the private sector. That is why the security directives that TSA issued for pipelines and the requirements TSA plans to issue for rail, transit, and aviation deserve such careful attention. They mark a pivotal transition in the Federal Government's approach to cybersecurity.

As a representative from Brooklyn, I welcome TSA's renewed interest in improving the cybersecurity posture of the transportation sector. New York City is a transportation hub, home to two major airports, several rail lines, and the largest mass transit system in the Nation. Just 6 months ago, actors reportedly tied to the Chinese Government breached the Metropolitan Transit Authority's network. Fortunately, they did not gain access to operational systems that control rail cars, but I remain concerned about the cybersecurity of mass transit systems generally and MTA's network in particular.

Given the degree to which middle- and low-income people rely on public transportation, a cyber attack affecting mass transit could have a disproportionate impact on these populations. In light of the conversations I have had regarding cybersecurity threats to rail and aviation, I also support TSA's efforts to raise the bar on cybersecurity for these subsectors.

That said, as the Federal approach to securing critical infrastructure evolves, we must get it right. TSA's security directives on pipelines and pending securities directives on trail—excuse me—on transit, rail, and aviation present an opportunity to better understand the administration's security goals, how the security directives align with those goals, and the private sector's ability to effectively implement the directives.

Today, I hope to identify the lessons learned from the roll-out and implementation of the pipeline security directives so we can use them to inform future transportation security directives to en-

sure that they are buying down risk and yielding the security benefits we expect. More broadly, I hope today's conversation will provide insight into how we can raise the cybersecurity posture across critical infrastructure sectors.

I thank the witnesses for being here today, and I look forward to your testimony.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation and the Subcommittee on Transportation and Maritime Security will come to order for today's hearing, titled "Transportation Cybersecurity: Protecting Planes, Trains, and Pipelines from Cyber Threats." Without objection, the Chair is authorized to declare the subcommittees in recess at any point.

Thank you to Chairwoman Watson Coleman, Ranking Member Garbarino, Ranking Member Gimenez, and our panel of witnesses for joining us.

We are here today to assess the administration's actions aimed at mitigating the cybersecurity challenges facing the transportation sector.

Earlier this year, our subcommittees worked together to evaluate how the Federal Government partnered with the private sector to respond to a ransomware attack against Colonial Pipeline, which resulted in 5,500 miles of pipeline being shut down.

As panic led to fuel shortages at gas stations along the East Coast and airlines scrambled to find alternative fuel supplies, we learned that:

- attackers infiltrated Colonial Pipeline's business network using a legacy VPN that did not require multi-factor authentication;
- the flow of information between Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency, and the Transportation Security Administration was slow, fueled in part by on-going confusion about which agency was in charge; and
- despite repeated offers from TSA, Colonial Pipeline had not yet undergone an important security assessment—a Validated Architecture Design Review—and did not have a disaster response plan that contemplated the full scope of cyber threats.

Shocked by what we learned during their oversight of Colonial Pipeline and other recent high-profile cyber incidents, Members of Congress have begun to question whether the Federal Government's approach to cybersecurity—which relies primarily on voluntary partnerships—actually works, or whether some security requirements ought to be mandated.

The notion that certain entities should be subject to cybersecurity standard mandates is not new.

Almost 10 years ago, President Obama issued Executive Order 13636, on Improving Critical Infrastructure Cybersecurity.

The Executive Order directed sector risk management agencies to evaluate whether they had sufficient authority to establish cybersecurity requirements for critical infrastructure entities for which a "cybersecurity incident could reasonably result in catastrophic regional or National effects on public health or safety, economic security, or National security"—and report back to DHS and the White House with what they found.

To the best of my knowledge, no agency suggested they lacked authority to issue such requirements.

Nevertheless, for nearly a decade, the Federal Government has continued to pursue security policies that relied primarily on voluntary partnerships with the private sector.

That's why the security directives that TSA issued for pipelines—and the requirements TSA plans to issue for rail, transit, and aviation—deserve such careful attention. They mark a pivotal transition in the Federal Government's approach to cybersecurity.

As a representative from Brooklyn, I welcome TSA's renewed interest in improving the cybersecurity posture of the transportation sector.

New York City is a transportation hub—home to two major airports, several rail lines, and the largest mass transit system in the country.

Just 6 months ago, hackers reportedly tied to the Chinese government breached Metropolitan Transportation Authority's network.

Fortunately, they did not gain access to operational systems that control rail cars—but I remain concerned about the cybersecurity of mass transit systems, generally, and MTA's network, in particular.

Given the degree to which middle- and low-income people rely on public transportation, a cyber attack affecting mass transit could have a disproportionate impact on these populations.

In light of the conversations I have had regarding cybersecurity threats to rail and aviation, I also support TSA's efforts to raise the bar on cybersecurity for these subsectors.

That said, as the Federal approach to securing critical infrastructure evolves, we must get it right.

TSA's security directives on pipelines—and pending security directives on transit, rail, and aviation—present an opportunity to better understand the administration's security goals, how the security directives align with those goals, and the private sector's ability to effectively implement the directives.

Today, I hope to identify the lessons learned from the rollout and implementation of the pipeline security directives, so we can use them to inform future transportation security directives to ensure that they are buying down risk and yielding the security benefits we expect.

More broadly, I hope today's conversation will provide insight into how we can raise the cybersecurity posture across critical infrastructure sectors.

I thank the witnesses for being here today and I look forward to their testimony.

Ms. CLARKE. The Chair now recognizes the Ranking Member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, the gentleman from New York, Mr. Garbarino, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman Clarke and Chairwoman Watson Coleman, for holding this important hearing today. Thank to you my colleague, Ranking Member Gimenez, for his continued leadership on transportation security.

As you know, cybersecurity remains a bipartisan cooperation in Congress. Bringing together these two subcommittees is a continuation of the bipartisan spirit that makes this community function so well. But there remains room for improvement.

This year, the full committee and our Cybersecurity Subcommittee have held several hearings in the aftermath of major cyber incidents to review the state of our Nation's cyber preparedness and assess the overall efficacy of response mechanisms across the Federal Government within various industry sectors. This joint hearing is a great opportunity to continue that work, focusing on the transportation sector which impacts millions of Americans and many of my constituents.

Every day, Americans are already experiencing the impact of a pervasive supply chain crisis. Goods are becoming more expensive and harder to find. Nearly every sector of our economy has been affected by this problem, which is particularly acute in the auto industry. We have already witnessed the impact of a devastating ransomware attack on Colonial Pipeline which led to gas shortages on the East Coast. Imagine a similar attack on a major U.S. port, airline, or major logistics company as the holidays approach. We must ensure that there is a robust partnership between the Department of Homeland Security, particularly the Cybersecurity and Infrastructure Security Agency, the Transportation Security Agency, and the U.S. Coast Guard, and the owners and operators of our transportation systems.

I hope that this hearing reviews the cyber preparedness of our critical transportation systems and how agencies like CISA, TSA, and the Coast Guard can enhance their programs, services, and

guidance to best ensure entities can defend and mitigate the threat of cyber attacks.

I am particularly interested in learning more about DHS's use of security directives as a tool for enforcing new security standards. I would like to hear testimony and learn from our witnesses regarding the impact of security directives and how TSA is working with relevant partners to ensure robust industry input because they know their sector best. I would also like to hear from our witnesses on the extent to which industry expertise and feedback is utilized in the creation of these security directives.

Members of this committee, including myself, are actively engaged in crafting mandatory cyber incident reporting legislation to improve CISA's ability into cyber incidents impacting our Nation's critical infrastructure. I thank Chairwoman Clarke for her leadership and partnership on this effort.

I have also been working closely with Ranking Member Katko and Representative Spanberger to introduce bipartisan legislation to authorize the director of CISA to establish a stakeholder-driven transparent process for identifying the owners and operators of our Nation's most critical infrastructure, known as systemically important critical infrastructure.

How can we expect CISA and other sector risk management agencies to prioritize limited services if we don't know what is most critical? It is also incumbent on Congress to ensure such a program includes the appropriate guardrails, guidance, and built-in mechanisms for industry collaboration. Such an important program must be done right. I believe that securing systemically important critical infrastructure strives to these very principles.

I am disappointed that the committee held a mark-up this morning, this legislation was not included, despite months of industry collaboration and attempts to collaborate with the Majority. I hope it comes soon.

I do want to note Representative Langevin's leadership on this important issue and his transparency with the Minority. I look forward to working with him and with you, Chairwoman Clarke, on this legislation to continue the bipartisan nature of our subcommittee.

Last, I will just say that the issue of transportation cybersecurity hits close to home. It was shortly after New York's MTA systems were hacked in April and discovered in June in which Secretary Mayorkas announced intentions to create a new security directive for major rail and aviation entities.

I look forward to learning from our panelists here today about what this committee can do to help TSA, CISA, and the Coast Guard work toward an enhanced public-private partnership with owners and operators of our Nation's transportation system.

Thank you very much, Chairwomen. I yield back.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW GARBARINO

Thank you, Chairwoman Clarke and Chairwoman Watson Coleman for holding this important hearing today. And thank you, Ranking Member Gimenez, for your continued leadership on transportation security.

As you know all, cybersecurity remains an area of bipartisan cooperation in Congress.

Bringing together these two subcommittees is a continuation of the bipartisan spirit that makes this committee function so well, but there remains room for improvement.

This year, the full committee and our Cybersecurity Subcommittee have held several hearings in the aftermath of major cyber incidents to review the state of our Nation's cyber preparedness and assess the overall efficacy of response mechanisms across the Federal Government and within various industry sectors.

This joint hearing is a great opportunity to continue that work, focusing on the transportation sector, which impacts millions of Americans.

Everyday Americans are already experiencing the impact of a pervasive supply chain crisis. Goods are becoming more expensive and harder to find. Nearly every sector of our economy has been affected by this problem, which is particularly acute in the auto industry.

We have already witnessed the impact of a devastating ransomware attack on Colonial Pipeline, which led to gas shortages on the East Coast. Imagine a similar attack on a major U.S. port, airline, or major logistics company as the holidays approach.

We must ensure there is a robust partnership between the Department of Homeland Security, particularly the Cybersecurity and Infrastructure Security Agency (CISA), the Transportation Security Agency (TSA), and the U.S. Coast Guard and the owners and operators of our transportation systems.

I hope that this hearing reviews the cyber preparedness of our critical transportation systems and how agencies like CISA, TSA, and the Coast Guard can enhance their programs, services, and guidance to best ensure entities can defend and mitigate the threat of cyber attacks.

I am particularly interested in learning more about DHS's use of security directives as a tool for enforcing new security standards.

I would like to hear testimony and learn from our witnesses regarding the impact of security directives, and how TSA is working with relevant partners to ensure robust industry input, because they know their sector best.

I would also like to hear from our witnesses on the extent to which industry expertise and feedback is utilized in the creation of these security directives.

Members of this committee, including myself, are actively engaged in crafting mandatory cyber incident reporting legislation to improve CISA's visibility into cyber incidents impacting our Nation's critical infrastructure. I thank Chairwoman Clarke for her leadership and partnership on this effort.

I've also been working closely with Ranking Member Katko and Rep. Spanberger to introduce bipartisan legislation to authorize the director of CISA to establish a stakeholder-driven, transparent process for identifying the owners and operators of our Nation's most critical infrastructure—known as systemically important critical infrastructure. How can we expect CISA, and other Sector Risk Management Agencies to prioritized limited services if we don't know who is the most critical?

It is also incumbent on Congress to ensure such a program includes the appropriate guard rails, guidance, and built-in mechanisms for industry collaboration, such an important program must be done right. I believe that the Securing Systemically Important Critical Infrastructure Act strives for these very principles. I'm disappointed that the committee held a mark-up this morning, and this legislation was not included despite months of industry collaboration and attempts to collaborate with the Majority.

I do want to note Rep. Langevin's leadership on this important issue, and his transparency with the Minority. I look forward to working with him, and you Chairwoman Clarke on this legislation, to continue to bipartisan nature of this subcommittee.

Last, I'll just say that the issue of transportation cybersecurity hits close to home. It was shortly after New York's MTA systems were hacked in April, and discovered in June, in which Secretary Mayorkas announced intentions to create a new security directive for major rail and aviation entities.

I look forward to learning from our panelists here today about what his committee can do to help TSA, CISA, and the Coast Guard work toward an enhanced public-private partnership with owners and operators of our Nation's transportation system.

Ms. CLARKE. Thank you, Ranking Member Garbarino.

The Chair now recognizes the Chairwoman of the Subcommittee on Transportation and Maritime Security, the gentlelady from New Jersey, Mrs. Bonnie Watson Coleman, for an opening statement.

Mrs. WATSON COLEMAN. Thank you, Chairwoman Clarke. To our Ranking Members Gimenez and Garbarino, thank you for coming together around this very important issue. To our witnesses, thank you for being willing to discuss this critical topic.

I want to be crystal clear. When it comes to transportation cybersecurity, inaction is not an option. When gas stops flowing due to a cyber attack, it doesn't just impact the pipeline owner; it means Americans struggle to fill up their tanks. If hackers succeed in bringing down a plane or derailing a train, it is not an airline or railroad that would pay the steepest price. Indeed, the real cost would be borne by the passengers injured or even killed.

Simply put, when you own critical infrastructure, people's lives and livelihoods depend on your cybersecurity. Yet despite the stakes, most transportation operators currently have no obligation to meet even baseline cybersecurity standards.

The status quo is dangerous. We are all familiar with the attack on Colonial Pipeline, but just this year, hackers have also targeted New York's MTA, as stated, the Massachusetts ferry system, the Port of Houston, one of the largest repositories of airline passenger records, a leading pipeline maintenance company, and global freight railroads. The list goes on.

Unquestionably, our Nation's transportation systems are facing a crisis. Fortunately, TSA has begun the process of requiring critical operators to take basic cybersecurity precautions. The recent cybersecurity directors for pipelines and Secretary Mayorkas' announcement of forthcoming requirements for rail, transit, and aviation are justified, necessary, and an important first step. But more action is even needed.

For instance, TSA must ensure all transportation moves are covered. Particularly as vehicles become increasingly connected and autonomous, the cybersecurity of motor carriers and busses cannot be forgotten. Meanwhile, the Coast Guard needs to hold ferries, ports, and other maritime systems to similar standards.

There is also the question of implementation and enforcement. If an operator proposes an alternative procedure that maintains robust cybersecurity, TSA needs to provide timely, substantive feedback.

By the same token, if operators fail to comply, leaving our Nation's critical infrastructure vulnerable to attack, TSA must have the resources to enforce the rules. Ultimately, TSA should pursue traditional notice-and-comment regulations so that stakeholders can offer meaningful input.

But these conversations around implementation shouldn't distract from the fundamental fact: There is no substitute for mandatory transportation cybersecurity requirements like those that are announced by TSA and Secretary Mayorkas.

While many operators employ best practices, invest in cybersecurity talent, and coordinate with Government voluntarily, some cut corners and put us all at risk. Without requirements, there is nothing to compel those companies to improve. That is a prospect we cannot take lightly, because in the 21st Century, physical security and cybersecurity are two sides of the same coin.

Historically, to hijack a plane, you had to clear TSA's checkpoint and then breach the cockpit. Today, it may be possible to hijack a

plane by hacking it. The same is true for railroads, subways, and other modes. Cameras and guards are no match for a hacker seeking to control or derail a train.

This isn't science fiction. This is the future, and cybersecurity requirements for all modes are the way to prepare for it, as well as tackle today's immediate threats, such as ransomware and state-sponsored data theft. A recent study found that only 60 percent of transit agencies have a cybersecurity preparedness program in place. The surge in cyber attacks against railroads, airlines, airports, and maritime assets suggest an equally grim picture in these modes.

This is our moment to ensure that every transportation operator in America prepares themselves for 21st Century threats. We can't wait until a hacked plane falls from the sky or a breached railroad gridlocks our Nation's supply chain to take action. I look forward to hearing from our panel today about what can be done to shore up the cyber defenses of our transportation system.

Again, I thank the witnesses for joining us.

Madam Chairwoman, I yield back.

[The statement of Chairwoman Watson Coleman follows:]

STATEMENT OF CHAIRWOMAN BONNIE WATSON COLEMAN

Thank you Chairwoman Clarke, and thank you to our witnesses for joining us today to discuss this critical topic.

I want to be crystal clear: When it comes to transportation cybersecurity, inaction isn't an option.

When gas stops flowing due to a cyber attack, it doesn't just impact the pipeline's owner. It means Americans struggle to fill up their tanks.

If hackers succeed in bringing down a plane or derailing a train, it's not an airline or railroad that would pay the steepest price. The real cost would be borne by the passengers injured or killed.

Simply put, when you own critical infrastructure, people's lives and livelihoods depend on your cybersecurity. Yet despite the stakes, most transportation operators currently have no obligation to meet even baseline cybersecurity standards.

The status quo is dangerous. We're all familiar with the attack on Colonial Pipeline, but just this year, hackers have also targeted New York's MTA, the Massachusetts ferry system, the Port of Houston, one of the largest depositories of airline passenger records, a leading pipeline maintenance company, and global freight railroads. The list goes on.

Unquestionably, our Nation's transportation systems are facing a crisis. Fortunately, TSA has begun the process of requiring critical operators to take basic cybersecurity precautions.

The recent cyber security directives for pipelines—and Secretary Mayorkas' announcement of forthcoming requirements for rail, transit, and aviation—are justified, necessary, and an important first step. But more action is needed.

For instance, TSA must ensure all transportation modes are covered. Particularly as vehicles become increasingly connected and autonomous, the cybersecurity of motor-carriers and buses cannot be forgotten. Meanwhile, the Coast Guard needs to hold ferries, ports, and other maritime systems to similar standards.

There's also the question of implementation and enforcement. If an operator proposes an alternative procedure that maintains robust cybersecurity, TSA needs to provide timely, substantive feedback.

By the same token, if operators fail to comply—leaving our Nation's critical infrastructure vulnerable to attack—TSA must have the resources to enforce the rules.

And ultimately, TSA should pursue traditional notice-and-comment regulations so stakeholders can offer meaningful input.

But these conversations around implementation shouldn't distract from a fundamental fact: There's no substitute for mandatory transportation cybersecurity requirements, like those announced by TSA and Secretary Mayorkas.

While many operators employ best practices, invest in cybersecurity talent, and coordinate with Government voluntarily, some cut corners and put us all at risk. Without requirements, there is nothing to compel those companies to improve.

That's a prospect we cannot take lightly, because in the 21st Century, physical security and cybersecurity are two sides of the same coin.

Historically, to hijack a plane, you had to clear TSA's checkpoint and then breach the cockpit. Today, it may be possible to hijack a plane by hacking it.

The same is true for railroads, subways, and other modes. Cameras and guards are no match for a hacker seeking to control or derail a train.

This isn't science fiction. This is the future, and cybersecurity requirements for all modes are the way to prepare for it, as well as tackle today's immediate threats—such as ransomware and state-sponsored data theft.

A recent study found that only 60 percent of transit agencies have a cybersecurity preparedness program in place, and the surge in cyber attacks against railroads, airlines, airports, and maritime assets suggests an equally grim picture in those modes.

This is our moment to ensure that every transportation operator in America prepares themselves for 21st Century threats. We can't wait until a hacked plane falls from the sky or a breached railroad gridlocks our Nation's supply chain to take action.

I look forward to hearing from our panel today about what can be done to shore up the cyber defenses of our transportation systems.

Again, I thank the witnesses for joining us, and I yield back.

Ms. CLARKE. I thank the gentlelady from New Jersey.

The Chair now recognizes the Ranking Member of the Subcommittee on Transportation and Maritime Security, the gentleman from Florida, Mr. Gimenez, for an opening statement.

Mr. GIMENEZ. Thank you, Chairwoman Clarke and Watson Coleman, for holding this important hearing today, and to Ranking Member Garbarino as well. I am glad that we can bring these two subcommittees together to discuss how to protect our vital aviation service, transportation, and maritime systems from cyber threats.

I know first-hand from my time as mayor of Miami-Dade County how important these systems are to the flow of people and goods and the overall health of our economy. As we are seeing right now with supply chain challenges and the increasing prices in everyday goods, keeping our transportation system operating at a high level is imperative.

The recent ransomware attack on Colonial Pipeline only served to highlight what owners and operators of these critical infrastructure systems already knew: A significant cyber incident has enormous ramifications to their systems and can cripple the goods and services that our Nation needs.

Transportation system owners and operators have enhanced their cybersecurity practices and real-time information sharing over the years, but there is always more that can be done to strengthen our defenses and it is imperative that we do so. As TSA moves forward with new cybersecurity directives for aviation, rail, and mass transit in the next few weeks, it is important that industry is fully consulted as these requirements are drafted and implemented.

The owners and operators know their systems the best and what is workable. Having a strong public-private partnership as new cyber requirements are imposed in the transportation sector is key. I look forward to hearing from the witnesses today on their perspectives on how to strengthen cybersecurity throughout our transportation system.

Madam Chairwoman, I yield back.

[The statement of Ranking Member Gimenez follows:]

STATEMENT OF RANKING MEMBER CARLOS GIMENEZ

Thank you, Chairwomen Clarke and Watson Coleman, for holding this important hearing today. And to Ranking Member Garbarino as well. I'm glad that we can bring these two subcommittees together to discuss how to protect our vital aviation, surface transportation, and maritime systems from cyber threats.

I know first-hand from my time as Mayor of Miami-Dade County how important these systems are to the flow of people and goods and the overall health of our economy. As we're seeing right now with supply chain challenges and the increasing prices in everyday goods, keeping our transportation systems operating at a high level is imperative.

The recent ransomware attack on Colonial Pipeline only served to highlight what owners and operators of these critical infrastructure systems already knew—a significant cyber incident has enormous ramifications to their systems and can cripple the goods and services that our Nation relies on.

Transportation system owners and operators have enhanced their cybersecurity practices and real-time information sharing over the years, but there is always more that can be done to strengthen our defenses.

As TSA moves forward with new cybersecurity directives for aviation, rail, and mass transit in the next few weeks, it's important that industry is fully consulted as these requirements are drafted and implemented. The owners and operators know their systems the best and what is workable. Having a strong public-private partnership as new cyber requirements are imposed in the transportation sector is key.

I look forward to hearing from the witnesses today on their perspectives of how to strengthen cybersecurity throughout our transportation systems.

Madam Chairwoman, I yield back.

Ms. CLARKE. I thank the Ranking Member from Florida, the gentleman, Mr. Gimenez, for his statement.

Members are also reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures.

Member statements may also be included for the record.

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

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

Thank you, Chairwomen Clarke and Watson Coleman, for holding today's hearing, and thank you to our panelists for being here with us.

Today's hearing occurs amid a shifting conversation on how to secure our Nation's transportation systems from cyber attacks.

The Transportation Security Administration has long relied on voluntary collaboration with industry partners to develop and implement cybersecurity measures.

The ransomware attack on Colonial Pipeline and the ensuing gas shortage earlier this year tested the effectiveness of this approach and highlighted the devastating potential effects of a successful cyber attack on transportation systems.

In the aftermath of the attack, the Biden administration moved swiftly to mandate cybersecurity requirements for owners and operators of critical pipelines through two security directives issued by the TSA, with support from CISA.

Over time, TSA will replace these security directives with full notice-and-comment regulations, marking the start of a new regulatory scheme for securing the transportation sector from cyber attacks.

Earlier this month, Secretary Mayorkas announced that TSA will also expand this mandatory approach to other modes of transportation by issuing new cybersecurity requirements for rail, transit, and aviation.

Indeed, while the attack on Colonial Pipeline dominated the headlines, it is far from the only recent cyber attack we have seen targeting transportation systems.

From the subway system in New York City to the Port of Houston, we have seen cyber attacks attempted across all modes of transportation.

I commend the Biden administration for taking the bold steps needed to address these emerging threats.

As DHS embarks upon this new approach, it must act deliberately to ensure its mandates deliver the intended security results.

First, TSA must work in close collaboration with CISA and industry experts to develop requirements that are intelligence-based, actionable, and crafted to achieve the greatest security benefit.

TSA must focus its enforcement efforts on desired outcomes and work with stakeholders to provide flexibility in how regulated parties achieve those outcomes.

Second, DHS must develop a plan for developing the cybersecurity expertise and resources it will need at TSA and CISA to carry out robust outreach and enforcement efforts—not just for the immediate implementation of new requirements, but as a regular way of doing business going forward.

Congress will need to fully fund these efforts, and I look forward to working with my colleagues to deliver the necessary resources.

Finally, as DHS considers plans for securing other critical infrastructure sectors from cyber attacks, the transportation sector may serve as a model for the prospect of mandating cybersecurity measures.

DHS must be transparent with Congress, stakeholders, and the public about its successes and failures.

Consistently evaluating the effectiveness of security efforts will be key to fixing what may not be working well and to considering whether to apply what does work well more broadly across critical infrastructure sectors.

I look forward to discussing these topics with our witnesses today, and I yield back.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

OCTOBER 26, 2021

I want to thank Congresswoman Yvette Clarke, Chair of the Cybersecurity, Infrastructure Protection and Innovation Subcommittee; and Congresswoman Bonnie Watson Coleman, Chair of the Transportation and Maritime Security Subcommittee and the respective Ranking Members of these committees Congressman Andrew Garbarino and Congressman Carlos A. Gimenez for holding today's hearing on "Transportation Cybersecurity: Protecting Planes, Trains, and Pipelines from Cyber Threats".

I thank today's witnesses for their service to their Nation; and I look forward to their testimony:

- Suzanne Spaulding, senior adviser, Center for Strategic and International Studies and former under secretary, National Protection and Programs Directorate;
- Patty Cogswell, strategic advisor, Guidehouse, and former deputy administrator, Transportation Security Administration;
- Jeffrey Troy, president & chief executive officer, Aviation Information Sharing and Analysis Center and former deputy assistant director, Cyber Division, Federal Bureau of Investigation; and
- Scott Dickerson, executive director, Maritime Transportation System Information Sharing and Analysis Center (MTS–ISAC) (Minority witness).

Today's hearing affords Members an opportunity to engage with former Federal cybersecurity and transportation security officials about the current state of cybersecurity across all modes of transportation, as well as recent and forthcoming regulatory actions to enhance transportation cybersecurity.

I look forward to learning more about how the Transportation Security Administration (TSA), Cybersecurity and Infrastructure Security Agency (CISA), the broader law enforcement, and intelligence communities, and transportation owners and operators can address the need for increased cybersecurity preparedness across the transportation sector.

Today's hearing is an important opportunity to view the cyber threat from a real-world perspective.

The threat is not limited to telecommunications, banking, transportation, health care, or critical infrastructure because of omnipresent and ubiquitous nature of attacks.

The Solar Wind attack was an equal opportunity abuser to any network that it invaded.

Colonial Pipeline was just one victim in a long line of victims, which ended with the consumer who curtailed travel plans due the impact on gasoline availability due to the attack.

Any networked device can be a vector for an attack, no matter how small.

The age of hyper-connectivity is upon us and we are not prepared to protect devices that are by design linked to share data traffic.

Cybersecurity is not something you can see or actively prove—it is established by each moment of each day that a network or computing device remains free of breaches by adversaries.

For too long the policy of local and Federal law enforcement was that some cyber crimes were too insignificant to waste limited resources on to investigate, conduct arrests, or prosecute—this must change.

We know from our work on this committee that determined adversaries will spare little to succeed in breaching U.S. networks even small efforts provide valuable insights that are applied to increase the likelihood of success for much more damaging attacks.

The goal of cybersecurity throughout the Federal Government must be to block adversaries when it is possible, detect and eradicate them quickly when it is not, and impose consequences to raise the costs and deter malicious behavior in cyber space.

For 4 years, Federal efforts to raise the National cybersecurity posture—across Federal networks, State and local governments, and the private sector—were stunted by a lack of steady, consistent leadership from the White House, leaving agencies to pursue piecemeal approaches to cybersecurity.

Congressional efforts to address the weaknesses in Federal cybersecurity include several Jackson Lee bills that comprise the following measures introduced in the 117th Congress:

- H.R. 119—Cyber Defense National Guard Act, which requires the Office of the Director of National Intelligence to report to Congress regarding the feasibility of establishing a Cyber Defense National Guard that may be activated during emergencies that affect the cybersecurity of the Nation or critical infrastructure.
- H.R. 118—Cyber Vulnerability Disclosure Reporting Act, requires the Department of Homeland Security to submit a report describing the policies and procedures developed to coordinate the disclosure of cyber vulnerabilities. The report shall describe instances when these policies and procedures were used to disclose cyber vulnerabilities in the previous year. Further, the report shall mention the degree to which the disclosed information was acted upon by stakeholders.
- H.R. 57, the DHS Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure Act" or the CAPITALS Act, which requires the Department of Homeland Security (DHS) to report to Congress on the feasibility of establishing a DHS Civilian Cyber Defense National Resource.

The goals of the Jackson Lee legislative efforts during the 116th Congress were to raise the baseline cybersecurity posture across the Federal and work with the private sector to reduce avoidable, opportunistic attacks and to refocus talent, time, and resources on preventing, detecting, and eliminating more sophisticated attacks.

The raising the Nation's baseline cybersecurity posture will require a systemic, whole-of-Government approach to cybersecurity.

The private sector has 85 percent of the Nation's critical infrastructure and much of it has some connectivity to the internet, which means they cannot adequately protect these National assets.

The vulnerabilities in computing technology from the most complex systems to the smallest devices are often found in its software.

This was true in the early 1990's when the first desktop computing technology was produced.

Desktop computing devices were quickly adopted for business and Government use.

The market and regulatory forces that should have forced security and safety improvements on computing technology never developed due to interference from Congress and the courts that excused or deflected culpability for known computing technology errors or omissions in product development or manufacturing that left systems open to attack.

The last defense for computing technology and systems are the concrete steps that organization, companies, and agencies can take to secure their computing assets; and business continuity measures that can be in place to allow meaningful recovery of operations should a successful cyber attack occur.

Business continuity refers to the capability of an organization to continue the delivery of products or services at acceptable levels following a disruptive incident, and business continuity planning or business continuity and resiliency planning is the process of creating systems of prevention and recovery to deal with potential threats to operations.

To survive in the current high-risk computing landscape both Government and private-sector entities must engage in risk mitigation strategies that assess operations from top to bottom to identify potential cyber threats and risk vectors.

This assessment should include both internal and external threats that could compromise business continuity.

Some risks are firmly within an organization's ability to control, such as the controls they implement to secure data and systems.

Continuity planning is also firmly under the control of organizations, and to not invest in proven strategies to survive a cyber attack, is not only irresponsible on the part of owners—but it creates unacceptable risks for their employees, customers, and investors.

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

This bill goes significantly further than the first Cybersecurity Vulnerability bill that I introduced in the 115th Congress, to address the instance of Zero Day Events that can lead to catastrophic cybersecurity failures of information and computing systems.

The ANS to H.R. 2980 responds to the recent cyber attacks on America's private sector and establishes the Federal Government as having a major role in fighting cyber attacks that target Government agencies and the private-sector critical infrastructure.

H.R. 2980, the Cybersecurity Vulnerability Remediation Act:

- Changes the Department of Homeland Security (DHS) definition of security vulnerability to include cybersecurity vulnerability,
- Provides the plan to fix known cybersecurity vulnerabilities,
- Gives the Department of Homeland Security the tools to know more about ransomware attacks and ransom payments, and
- Creates greater transparency on how DHS will defend against and mitigate cybersecurity vulnerabilities and lays the road map for preparing the private sector to better prepare for and mitigate cyber attacks.

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

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

In 30 years the world has gone from one divided by oceans to one that is interconnected through the internet.

An interconnected world has brought us closer together, created new opportunities for business, and citizen engagement, while at the same time given new tools to those who may wish to cause harm using cyber attacks.

In cyber space an attack against one entity or device can devolve into an attack against many.

The work that must be done to secure critical infrastructure from cybersecurity vulnerabilities that include oil and gas pipelines; the electric grid, water treatment facilities, and other privately-held infrastructure must occur with much more order and purposefulness.

The consolidation of cybersecurity for both the .gov domain and for the private sector is now under the jurisdiction of the Committee on Homeland Security was is an important step to better coordinating domestic cybersecurity.

THE NEED TO TAKE ACTION

Ransomware is a form of cyber crime where criminal actors compromise a victim's computer systems, preventing access or threatening to release sensitive information if the victim does not provide a ransom payment.

In recent years, the number of ransomware attacks has increased significantly, affecting school districts, police departments, hospitals, and numerous businesses, among others.

In 2020, an estimated 2,400 governments, hospitals, and school districts were victims of ransomware attacks in the United States.

Victims made an estimated $350 million in ransomware payments in 2020, with an average payment of $312,493.

In the first quarter of 2021, the average monetary demand associated with a ransomware attack increased to $220,298, up 43 percent from the previous quarter.

While many businesses suffer significant losses due to disruptions from ransomware and the cost of remediation or making ransom payments, when crimi-

nals groups target Government entities or other critical infrastructure, the effects can pose significant risks to public safety.

For example, there were 560 ransomware attacks on U.S. health care facilities in 2020, in some cases causing delays in treatment for serious illnesses.

In a growing number of ransomware attacks, the perpetrators engage in "double extortion" where they threaten to release sensitive data publicly if a ransom payment is not made.

Last week, the Washington, DC police department was hit by a ransomware attack that included the release of detailed background reports on 5 current or former police officers and the threat to release files publicly.

Ransomware can be delivered in various ways, the majority of which utilize email. Ransomware are real, but computers aren't infected just by opening emails anymore.

Just opening an email to view it is safe now—although attachments & links in the email can still be dangerous to open.

While it is not always possible to prevent a successful attack, engaging in general security best practices and implementing effective email protection can drastically reduce your risk.

The SolarWinds attack was a wake-up call on any notion that some companies are more trustworthy than others because a trusted software source was the cause of the company's 18,000 customers downloading a compromised version of Orion.

Nearly 40 Federal agencies downloaded the compromised SolarWinds Orion update, but evidence of further compromise has only been detected at 9 Federal agencies to date. Agencies that downloaded the compromised Orion update continue to hunt for indicators of compromise.

It is important to note that about 30 percent of both Government and non-Government victims of the Russian cyber campaign had no direct connection with SolarWinds.

According to news reports, hackers also breached networks by "exploiting known bugs in software products, by guessing on-line passwords and by capitalizing on a variety of issues in the way Microsoft Corp.'s cloud-based software is configured."

Bugs can also be called Zero Day Events that if exploited could cost significant disruption in the function of application or services that rely in computers or remote computing services.

The committee recently took action to address the lack of Federal law requiring private entities to report cybersecurity incidents, there is little public information on the number of victims that installed the infected versions of SolarWinds Orion or experienced second-stage intrusions.

The Cybersecurity and Infrastructure Security Agency should be empowered to more effectively coordinate and lead interagency cybersecurity and risk management activities that coordinate functions among critical infrastructure stakeholders.

Congress should provide CISA the authorities and budget that match its mission.

Over the past decade, the private sector has raised fair concerns about the value of many Federal cybersecurity programs and has used its concerns as an excuse for not fully participating, to the detriment of National cybersecurity efforts.

That must stop. The private sector has an important role to play to improve the Nation's cybersecurity posture and must step up.

Solving this cybersecurity challenge will require creativity from policy makers as we seek out new strategies to bolster security efforts for Federal and private-sector networks.

I look forward the asking questions of today's witnesses.

Ms. CLARKE. I now welcome our panel of witnesses. Ms. Suzanne Spaulding is a senior advisor to the Center for Strategic and International Studies. Before that, Ms. Spaulding served as the under secretary for the Department of Homeland Security's National Protection and Programs Directorate, which Congress redesignated as CISA in 2018.

Next we have Ms. Patricia Cogswell, a senior strategic advisor for the National Security at Guidehouse, who served as the deputy administrator for the Transportation Security Administration from 2018 through 2020.

I would also like to welcome Mr. Jeffrey Troy, the president and CEO of the Aviation Information Sharing and Analysis Center, or

the Aviation ISAC. Prior to the Aviation ISAC, Mr. Troy served as a deputy assistant director of the FBI's Cyber Division.

Finally, we will hear from Mr. Scott Dickerson, the executive director of the Maritime Transportation System Information Sharing and Analysis Center, or the MTS–ISAC.

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

I now ask each witness to summarize her or his statement for 5 minutes, beginning with Ms. Spaulding.

Ms. Spaulding, I think you have to unmute.

STATEMENT OF SUZANNE SPAULDING, SENIOR ADVISER, HOMELAND SECURITY, INTERNATIONAL SECURITY PROGRAM, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES; FORMER UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Ms. SPAULDING. Madam Chairwoman, can you hear me at this point?

Ms. CLARKE. Yes, I can.

Ms. SPAULDING. Excellent. All right. Thank you.

Chairwomen, Ranking Members, and Members of the committee, thank you for this opportunity to testify today in this joint hearing on TSA directives aimed at ensuring the security and resilience of the aviation, rail, and pipeline sectors against significant cyber incidents.

As the former under secretary at the Department of Homeland Security, where I led what is now called the Cybersecurity and Infrastructure Security Agency, and as a member of the Congressionally-created Cyberspace Solarium Commission, and even going back to my involvement with the Commission on Cybersecurity for the 44th President, which was run out of my current organization, CSIS, I have always favored voluntary market-based solutions to cybersecurity, as they are generally more efficient and flexible. However, I have reluctantly had to conclude that we cannot rely upon markets alone to ensure the continuity of Nationally-critical functions upon which the American public relies.

First, the purely voluntary approach simply has not gotten us to where we need to be, despite decades of effort. The threat is evolving much more quickly than our defense. Even in these key sectors where there has been significant progress on cyber, there is still a need to ensure continued investment across all vital assets. Even in a perfect market, there are external impacts on society and the Nation from inadequate cybersecurity that will simply not be captured in a business' bottom line or their calculation of return on investment.

Externalities have long justified regulation and mandates such as with pollution and highway safety. This is the thinking behind a number of recommendations from the Cyberspace Solarium Commission.

First, we looked at ways to improve the performance of relevant markets, including by providing better market incentives, greater transparency, more information, to improve the cybersecurity behavior of firms. But the Solarium Commission too ultimately concluded that the market alone was not going to be sufficient to pro-

vide the level of security and resilience that is urgently needed for the most important elements of our infrastructure, particularly with what the Solarium calls systemically important critical infrastructure.

We recommended creating a transparent methodology for identifying these most critical systems and assets and then building a closer relationship between the Federal Government and the firms that own and operate these systems. The Government should offer a suite of benefits, like improved intelligence sharing and operational support, but industries should also accept burdens, like requirements for security behavior and enhanced incident reporting.

Consistent with this thinking, I believe it is appropriate for TSA to use its existing authority to put basic requirements in place for the most critical assets in these three sectors. The details will be important. But as described, these directives seem like a step in the right direction. Collaboration with industry will continue to be an imperative as TSA further develops these directives and perhaps follow-on regulations.

Industry has a level of expertise that will be essential in understanding what needs to be done. It must be at the table to help craft directives that are ambitious but achievable, and Government must invite them early enough in the process to allow them to make a meaningful contribution. In addition, those who depend upon these critical sectors should also make their voices heard in this process.

Moreover, requirements should be informed by an awareness of the tools and technologies that are available to help these asset owners and operators gain visibility into their information technology and operational technology systems, detect malicious activity, and respond quickly and effectively.

To encourage continued innovation in this area, Government should lean toward open, performance-based standards that are technology-neutral and vendor-agnostic. Any new regulations should draw on existing guidelines, standards, and best practices. They should be harmonized with requirements in other sectors, particularly as between pipeline and electric sectors for which there is often significant overlap.

Finally, Congress needs to ensure that DHS has provided the resources necessary to effectively implement and monitor these mandates and continue its equally important voluntary work.

Time is not on our side. The threat environment grows more dangerous with each passing day. We should not wait for a tragedy caused by malicious cyber activity in one of these vital sectors before we take necessary action. The proposed TSA directives reflect a growing body of evidence that the risk of serious disruptions to critical infrastructure is not potential or in the future. It is here now, and it requires an urgent response.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Spaulding follows:]

PREPARED STATEMENT OF SUZANNE SPAULDING

TUESDAY, OCTOBER 26, 2021

Chairwoman Clarke, Chairwoman Watson Coleman, Ranking Member Garbarino, Ranking Member Gimenez, and distinguished Members of the subcommittees, thank

you for this opportunity to testify today in this joint hearing on the important issue of ensuring the security and resilience of the aviation, rail, and pipeline sectors against significant disruption from malicious cyber activity.

The safety and security of these 3 sectors falls under the Transportation Security Administration (TSA) at the Department of Homeland Security (DHS). This Spring, following a ransomware incident at Colonial Pipeline that disrupted fuel deliveries along the East Coast and led to panic buying, long lines, and higher prices at gas stations, TSA issued a security directive mandating that certain pipeline owner/operators—those deemed by TSA to be most critical—assess whether their current operations are consistent with TSA's Guidelines on cybersecurity, identify any gaps and remediation measures, and report the results to TSA and others. This was followed in July 2021 with an additional cybersecurity directive mandating implementation of cybersecurity mitigation measures; development of Cybersecurity Contingency Response Plans in the event of an incident; and an annual cybersecurity architecture design review, among other things.

Recently, the Secretary of Homeland Security announced that DHS would be coming out with similar mandates covering critical U.S. airport operators, passenger aircraft operators, and all cargo aircraft operators, as well as "higher-risk" railroad and rail transit assets.[1]

The pipeline directives have not been publicly released and the aviation and rail directives are still under development. However, they have generally been described as prescribing a relatively basic level of cybersecurity measures and plans for incident response. The latter, planning and exercising incident response to reduce the impact of a successful hack is one of the most important, and often underappreciated, elements of managing cyber risk.

The details will be important but, as described, these directives seem like a step in the right direction. Moving forward, TSA will need to operate collaboratively with these sectors to ensure that the requirements and time lines drive toward actual improvements in security and resilience. No directives or regulations will achieve perfect security. This is an exercise in risk management, not risk elimination, which is why planning for incident response is so crucial. The objective should be to ensure that the relevant industries are putting in place a common baseline of measures to strengthen the security and resilience of the highest-risk assets.

As the former Under Secretary at the Department of Homeland Security leading what is now called the Cybersecurity and Infrastructure Security Agency (CISA), as a member of the Congressionally-created Cyberspace Solarium Commission (CSC), and going back to my involvement with the Commission on Cybersecurity for the 44th President, which was run out of my current organization, the Center for Strategic and International Studies (CSIS), I have always favored voluntary, market-based solutions to cybersecurity. Markets are generally more efficient and, important for such a dynamic area as cyber, nimbler. However, over the last couple of years, I have reluctantly had to conclude that we cannot rely upon markets alone to ensure the continuity of Nationally-critical functions upon which the American public relies. I think there are several reasons for this.

The first is that the purely voluntary approach has not gotten us where we need to be, despite decades of effort. There has been significant progress and a growing level of maturity in industry and in Government on cyber, including in the sectors under discussion today. All three, aviation, rail, and pipelines, have worked collaboratively with DHS over the years to improve their physical and cyber security. But the threat is evolving much more quickly than our defense. There is an urgency to addressing this risk to the American public that the market simply cannot address fast enough.

One reason the market has not fully addressed this challenge is the paucity of information. Markets need information to function effectively. For example, information about the scale, scope, and cost of inadequate cybersecurity is needed to drive a demand signal that would prompt appropriate levels of investment and balance the "first-to-market" imperative. Yet, since most cyber incidents are not reported, and those that are do not provide details on costs, this information is lacking. Furthermore, such information is needed to calculate the return on investment (ROI) for security measures. Without it, security professionals often have a hard time convincing management to make needed investments.

Even in a perfect market, there are external impacts on society and the Nation from inadequate cybersecurity, particularly in assets that control essential functions, that will not be captured in a businesses' bottom line or ROI. Externalities have long justified regulation and mandates, such as with pollution and highway

[1] *https://thehill.com/policy/cybersecurity/575580-tsa-to-issue-regulations-to-secure-rail-aviation-groups-against-cyber?rl=1.*

safety. In the case of pipelines, rail, and aviation, the potential risks to public health and safety, as well as the potential for cascading economic consequences, calls for a Government role.

This is the thinking behind a number of the recommendations from the Cyberspace Solarium Commission. First, we looked at ways to improve the performance of relevant markets, including by providing better market incentives to improve the cybersecurity behavior of firms. Mandatory reporting of relevant cyber incidents can fill critical information gaps, particularly if paired with the establishment of a Bureau of Cyber Statistics. Bolstering the capabilities of cyber insurance underwriters can help that industry play the role it does in other risk categories to encourage appropriate investments in security and safety.

In addition to nudging firms in the sector toward better cybersecurity behavior, the Federal Government can do more to help these firms make better purchasing decisions regarding the security of the products and services they deploy as part of their business. More Government-sponsored security testing of critical technologies and applications—like industrial control systems—can help firms understand the security characteristics of the devices they deploy. The CSC recommended the creation of Government-sponsored critical technology security centers at places like Federally-funded research and development centers or National labs to fill this gap. Similarly, a clearer ecosystem of cybersecurity product certifications would allow procurement specialists at critical firms in the sector to more easily price security into their purchasing decisions and manage their supply chain risk.

But the CSC, too, ultimately concluded that the market was not going to be sufficient to provide the level of security and resilience that is urgently needed for the most important elements of our infrastructure, particularly what CSC calls Systemically Important Critical Infrastructure. The Solarium recommended creating a robust and transparent methodology for identifying these most critical systems and assets and then building a closer relationship between SICI firms and the Federal Government through a suite of benefits—like improved intelligence sharing and operational support—but also burdens—like requirements for security behavior and enhanced incident reporting.

Consistent with this thinking, I believe it is appropriate for TSA to use its existing authority to put basic requirements in place for the most critical assets in these three sectors. That said, the process is important. According to testimony from Kimberly Denbow Managing Director, Security & Operations American Gas Association, in front of this committee in September in support of the legislation to mandate cyber incident reporting across critical infrastructure, "The TSA Pipeline Group has been the epitome of innovation—leveraging the infrastructure subject matter expertise of pipeline operators, partnering with CISA and Idaho National Labs for in-house industrial control system cybersecurity knowledge, and collaborating with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) on cybersecurity reviews of control centers. AGA helped champion the CISA/TSA Pipeline Cybersecurity Initiative and promoted effortlessly the Pipeline Validated Architectural Design Reviews. The quality output has been the result of the dedication of TSA and CISA staff, in partnership with pipeline operators, toward a shared common goal—pipeline security."[2]

This level of collaboration should be the model as TSA, in partnership with CISA, works to develop the aviation and rail directives. Industry has a level of expertise that will be essential in understanding what needs to be done. Businesses rarely embrace Government mandates; that is not surprising. Nevertheless, industry must be at the table to help craft directives that are ambitious but achievable, and Government must invite them early enough in the process to allow to make a meaningful contribution.

It's also important to note that the security directive process allows the TSA administrator flexibility to work with businesses even after the directive is issued. For example, a company can propose alternative measures for achieving the objective(s), and the administrator can amend or issue new directives as conditions warrant.

DHS has indicated that these temporary directives will be replaced with regulations, presumably no later than 1 year from their issuance, when they are set to expire. The informal consultation with industry will, pursuant to the Administrative Procedures Act, be supplemented by a formal notice and comment process. Not only should the industries directly covered by the proposed regulations weigh in, those who depend upon these critical sectors should also let their voices be heard as the Government considers how best to ensure the security, safety, and reliability of these critical functions in the face of growing cyber risks. In addition, these regulations should be informed by an awareness of the tools and technologies that are

[2] *https://homeland.house.gov/imo/media/doc/2021-09-01-CIPI-HRG-Testimony-Denbow.pdf*.

available to help these asset owners and operators gain visibility into their information technology (IT) and operational technology (OT) systems, detect malicious activity, and respond quickly and effectively. To encourage continued innovation in this area, Government should lean toward open, performance-based standards that are technology-neutral and vendor-agnostic.

Furthermore, any new regulations should draw on existing guidelines, standards, and best practices. They should be harmonized with requirements in other sectors, particularly as between the pipeline and electric sectors, in which there is often significant overlap.

Finally, TSA has been working to build its cyber capacity, but it should not try to duplicate expertise that resides at CISA. These two DHS entities should continue to work closely together, with TSA bringing industry relationships and expertise together with CISA's cyber-specific and critical infrastructure resilience expertise. The work of the National Risk Management Center should inform the identification of highest-risk/highest-consequence functions. Congress needs to ensure that DHS is provided the resources necessary to effectively implement these mandates and to continue its equally important voluntary work with these vital industries.

Time is not on our side. The threat environment grows more dangerous with each passing day. In the recent words of one administration official, "the overall environment is more aggressive; more sophisticated; and more belligerent . . . "[3]

The general assessment is that neither state nor non-state actors have current intent to cause significant disruption. But cyber incidents can have unintended consequences. NotPetya came back to impact Russian companies. And if we are to believe the criminals involved in the Colonial Pipeline attack, they did not intend to disrupt pipeline operations. I am inclined to believe that, since it would've been hard to predict that an intrusion into the corporate IT system, as opposed to the OT system, would have such a significant impact on operations. It is a reminder that lack of intent should not give us great comfort.

Moreover, intent can change. Even short of a direct kinetic conflict in which an adversary might decide to disrupt our critical infrastructure, there is the prospect of an adversary using the credible threat of such disruption to deter us from taking actions in our National interest. Having this leverage could embolden China in the South China Sea or Russia in Ukraine or elsewhere, for example. It seems likely that Russia's cyber attacks on Ukraine's electric grid were designed not only to undermine the Ukraine government but to send a signal to the United States about Russia's capabilities.

Perhaps most troubling is the threat of a destructive attack on the safety systems of operations, leading not just to disruption but to potentially catastrophic deadly consequences. In 2017, a Saudi petrochemical plant was hit with malware later dubbed "Triton" which disabled the Safety Instrumented System (SIS). SISs are the last line of automated safety defense for industrial facilities, designed to prevent equipment failure and catastrophic incidents such as explosions or fire. Faulty code prevented that attack from succeeding but experts say the technique is replicable by others. Moreover, in 2019, the attackers behind the Triton malware, attributed to a Russian government-funded research institution, were reported to be scanning and probing at least 20 electric utilities in the United States for vulnerabilities.

The bipartisan co-chairs of the Solarium have noted that it was envisioned as a 9/11 commission to avert a cyber 9/11. We should not wait for a tragedy caused by malicious cyber activity in one of these vital sectors before we take the necessary action. The proposed TSA directives reflect a growing body of evidence that the risk of serious disruptions to critical infrastructure is not "potential" or in the future, it is here now and requires an urgent response.

Thank you and I look forward to your questions.

Ms. CLARKE. We thank you for your testimony, Ms. Spaulding.

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

STATEMENT OF PATRICIA F.S. COGSWELL, STRATEGIC ADVISOR, GUIDEHOUSE; FORMER DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Ms. COGSWELL. Chairwoman Clarke, Chairwoman Watson Coleman, Ranking Member Garbarino, and Ranking Member Gimenez,

[3] *https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr.*

and the distinguished Members of the subcommittees, thank you for the opportunity to testify before you this afternoon on transportation cybersecurity.

The insights I will share today are informed by my 24 years of Federal service, serving in varied capacities from the founding of DHS through my retirement as the deputy administrator of the Transportation Security Administration.

My first significant engagement in countering cybersecurity threats to industrial control systems was while I served as the special assistant to the President for Transborder Security at the National Security Council after the 2012 cyber attack on Saudi Aramco.

Since that time, I have seen the number of security threats increase, with an expanding number and type of threat actors, including both state and non-state actors such as transnational criminal entities; an increased focus by them on exploiting network-connected ICS vulnerabilities; and an increasing level of risk faced across our transportation infrastructure for both the combination of increased threat but also of consequence as we see how an attack on one entity can affect the entire sector.

I have also seen very strong partnerships across Government and industry to develop tools, programs, information-sharing mechanisms, and standards to mitigate the risks, including the NIST framework, TSA's pipeline security guidelines, and various multi-entity exercises.

I am pleased to be able to be here today and hope that I can assist you as you consider how best Congress can support and enable transportation cybersecurity.

I thank you for your willingness to call attention to this incredibly important topic. I want to recognize the work that this committee, along with Senate Homeland Security and Government Affairs and the Defense Armed Services Committee, are leading to promote and standardize cyber incident reporting.

As this committee further examines roles, responsibilities, and activities, I would highlight the following: First is the value of TSA's authority to issue security directives. Security directives have repeatedly demonstrated their value, providing a mechanism for TSA and industry to put immediate protective mitigation measures in place. They send a clear message to our adversaries, to the American people, and to our allies.

After the recent pipeline ransomware event, TSA security directives were the tool of choice. SDs are most effective, as you have noted, when TSA and the regulated industry are able to work together throughout the entire process from development of requirement through implementation.

Second, promote bidirectional partnership through analysis of reporting data. As I have spoken with industry and Government about the new cyber requirements, several colleagues expressed their interest in using this reporting to promote a deeper understanding of and engagement around cyber threats to critical infrastructure. There is a recognition that analyzing the threats of vulnerabilities associated with industrial control systems can tell us more about the prevalence and use of tactics, the effectiveness of measures to counter those tactics, and best practices to follow.

Continued investment in open standards development. NIST and DHS, through CISA and TSA, have established cybersecurity and standards environments for ICS and critical infrastructure. Continued evolution that provides transportation owners and operators with an opportunity to participate in that development and a mechanism to communicate direction to solutions developers and providers should be encouraged.

Finally, incentivizing and encouraging innovative approaches, while requiring transportation operators to achieve minimum standards. As DHS looks to advance regulatory requirements for transportation operators, I anticipate it will look to adopt a set of baseline requirements based on current best practices and recommendations, with the aim of continuing to update them over time. DHS and Congress should consider innovative mechanisms for how to achieve these goals, using a model that emphasizes performance-based outcomes and allows industry to use alternative methods to reach compliance.

This can be further encouraged through a regulatory model where transportation operators can use a qualified third party to complete the cybersecurity architecture reviews or planning required, similar to TSA's third-party canine program, and providing operators with access to a list of qualified entities who can provide such functions and services, such as GSA does for identity management and credentials, or providing other recognized criteria.

Cybersecurity, it is often said, is a team sport. Having many players on the field with standards-based interoperable solutions will enable innovation and enhance the protection of our critical infrastructure.

As you consider statutory language, I would encourage you to develop it in a way that will create an enduring framework that supports the evolution of cybersecurity as the threats and risks continue to change. A technology-neutral approach based on open standards that promote competition, innovation, and interoperability should be the core of such effort.

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

[The prepared statement of Ms. Cogswell follows:]

PREPARED STATEMENT OF PATRICIA F.S. COGSWELL

OCTOBER 26, 2021

Chairman Thompson, Ranking Member Katko, and distinguished Members of the subcommittees, thank you for the opportunity to testify before you this morning on Transportation Cybersecurity.

The insights I will share with the committee today are informed by my 24 years of Federal service, my long-standing tenure as a founding member of DHS serving on Day 1, and the varied capacities in which I have served the transportation security mission of DHS through my retirement as deputy administrator for the Transportation Security Administration.

My first significant engagement in countering cybersecurity threats to industrial control systems (ICS) was while I served as special assistant to the President for transborder security, at the National Security Council after the 2012 cyber attack on Saudi Aramco.

Since that time, I've seen:

- The number of cyber threats increase—with an expanding number and type of threat actors, including both state and non-state actors, including transnational criminal entities;

- Targeted exploitation of vulnerabilities in ICS-environment management practices;
- An increased recognition of the risk faced across our critical transportation infrastructure, from the combination of threat, vulnerability, and consequence; and
- Partnership across Government and industry to develop tools, programs, information-sharing mechanisms, and standards to mitigate the risk, including the NIST Framework for Improving Critical Infrastructure Security, TSA's Pipeline Security Guidelines, and various multi-entity exercises, such as 2020 Ohio Cyber shield.

I am pleased to be here today to speak before the committee, and hope that I can assist you as you consider how Congress can best support and enable critical infrastructure cybersecurity. I thank you for your willingness to call attention to this very important topic. I also want to recognize the legislation this committee, along with Senate Homeland Security and Government Affairs, and the Defense Armed Services Committee are leading to promote and standardize cyber incident reporting to DHS's Cybersecurity and Critical Infrastructure Agency (CISA).

As this committee further examines how to incentivize the right mix of roles, responsibilities, and activities across Government and industry, I'd highlight the following areas as important in our common interest in making progress:

- The value of TSA's authority to issue Security Directives. SDs have repeatedly demonstrated their value, providing a mechanism for TSA and industry, often in concert with DOT and other Federal entities, to put immediate measures into place—and sending a clear message to our adversaries, to the American people, and to our allies. After the recent pipeline ransomware event, there was an understandable interest across the administration, Congress, industry, and the public in taking action. TSA's authority to issue Security Directives for the transportation industry in response to emerging threats was the tool of choice to rapidly direct owners and operators of pipeline and natural gas facilities to implement necessary cyber protections. TSA's SDs are most effective when TSA and the regulated industries work together throughout the process to ensure that requirements are achievable under the time lines set and the regulated industries, all the way down the individual companies can work through implementation.
- Promote bi-directional partnership through analysis of reporting data. As I've spoken with individuals in industry and Government about the new CISA cybersecurity reporting requirements, several colleagues expressed their interest in using this to promote a deeper understanding and engagement of cyber threats to critical infrastructure, particularly where they can be done in a Classified setting. While there are significant differences in transportation modes of operation, there is a recognition that analyzing the threats and vulnerabilities associated with industrial control systems across critical infrastructure sectors can tell us more about the prevalence and use of adversaries' tactics, the effectiveness of measures to counter those tactics, and best practices to follow. That analysis is also critical to feed back to the industries required to report cyber incidents to provide them with that deeper understanding of the threats and vulnerabilities to proactively assess additional areas of focus for their own systems and operations. These should then be considered for adoption and reinforcement through regulatory programs.
- Invest in continued evolution of open standards. NIST and DHS, through both CISA and TSA, along with other agencies, have established a cyber standards environment for ICS and critical infrastructure. This environment provides transportation owners and operators with insight and visibility, as well as the opportunity to participate in standards development. It also creates a mechanism to communicate direction to solutions developers and providers.
- Incentivize and encourage innovative approaches, while requiring transportation operators to achieve minimum standards. Consistent with our approach to other transportation security issues, DHS should look to advance regulatory requirements for transportation operators. These could be a formalization of actions already encouraged now or recognized industry best practices, such as the validated architecture reviews, with the aim of changing over time as the standards evolve. By setting these baseline requirements, we can ensure that critical infrastructure operators are on an even playing field, and that the industry as a whole is less vulnerable to the actions of a small few.

The Government should also consider innovative mechanisms for how to achieve these goals, using a model that emphasizes performance-based outcomes, and allows industry to use alternative methods to reach compliance. A more open model also addresses the issues associated with vendor lock or over reliance on a single set of

tools, which can disincentivize innovation. Cybersecurity, it's often said, is a team sport. Having as many players on the field with standards-based solutions interoperable solutions will enable innovation and enhance the protection of our critical infrastructure.

I would also encourage DHS to establish a regulatory environment where a transportation operator can use a qualified third-party entity to complete the cybersecurity architecture reviews or planning required. From a statutory and regulatory perspective, this could look similar to how TSA established the third-party canine program. This type of model would increase speed of adoption, and provide transportation operators options for meeting the requirements. But, from industry colleagues I have talked to, transportation operators must have access to a list of Government-approved third-party entities, or be able to rely on firms that meet specified criteria. My understanding is that the pipeline industry is already working to begin to identify those criteria and identifying firms who could serve these needs. To scale this model effectively given the number of critical infrastructure entities, both public and private, that would benefit from industrial control systems cybersecurity expertise, it may make sense to look to GSA to manage the vendor qualification process, with DHS and other entities contributing their expertise, similar to other cross-cutting needs.

As you consider statutory language, I would encourage you to develop it in a way that will create an enduring framework that supports the evolution of cybersecurity as the threats and risks continue to change. A technology-neutral approach based on open standards that promote competition, innovation, and interoperability should be the core of any such effort.

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

Ms. CLARKE. Thank you, Ms. Cogswell, for your testimony.

Members should know that votes have been called, but we will continue to receive testimony from our final two witnesses today.

So I now recognize Mr. Troy to summarize his statement for 5 minutes.

STATEMENT OF JEFFREY L. TROY, PRESIDENT, CEO, AVIATION INFORMATION SHARING AND ANALYSIS CENTER; FORMER DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. TROY. Thank you, Chairwoman, Chairwoman, and Ranking Members, and Members of the committee.

Good afternoon. My name is Jeffrey Troy. I am president of the Aviation Information Sharing and Analysis Center.

The Aviation ISAC is a global nonprofit. Our members are on 5 continents and include air framers, airlines, airports, air navigation service providers, and more. Our mission is to make the aviation industry more resilient to cyber attacks.

Last time I came before you was in September 2018, and thank you for the opportunity to talk to you once again about the cyber risk landscape in aviation.

The cyber risks to the aviation industry have increased. Together, both private industry and the public sector have significantly increased cooperation and threat intelligence and best practices sharing, and now is the time for industry and Government to partner even more closely in creating and enhancing effective cyber risk reduction frameworks.

Over the past several years, ransomware has become a common term in aviation and many other sectors. The success of ransomware operators to extort money from their victims has greatly increased the level of skill and the number of persons willing to conduct ransomware attacks. The second-stage ransomware events, wherein additional ransoms are sought in exchange for de-

letion of sensitive records stolen as a part of the ransom operation, also highlights the risk, the theft of intellectual property, sensitive business information, and privacy data.

Ransomware can also shut down operations. This has the potential to be very impactful to the aviation industry. Pardon me. Ransomware—excuse me—it also becomes more complicated in the aviation industry because many of the operational technologies are mobile. The attack on Colonial Pipeline, which has been spoken of today, and the QNX real-time operating system vulnerability are two examples of where a cyber attack or a vulnerability in a product can have a ripple effect across many sectors.

Preventing, responding to, and limiting the impact of these attacks requires a team-of-teams approach. Our core values include creating and maintaining partnerships with numerous Government and private-sector entities. The Aviation ISAC is proud to have partnered with the Aviation Cyber Initiative, a joint partnership led by DOD, FAA, and the DHS, which is in the process of transferring this tri-chair seat to the TSA.

This year, the Aviation ISAC and the ACI significantly solidified our partnership by co-hosting a summit on aviation cybersecurity. We are also proud to partner with CISA. CISA is maturing well and has been put out timely, relevant guidance in direct response to recent cyber attacks on critical infrastructure and the supply chain. On 6 occasions our intelligence was used in CISA's intelligence bulletins and intelligence information reports.

Similarly, we have reached out to the TSA as they build their cybersecurity strategy and create a regulatory framework over cyber events in aviation. Our industry is also benefiting from a significant increase in cooperation between private entities. This includes the Aerospace Village, the Aerospace Industries Association, the American Institute of Aeronautics and Astronautics, along with Airlines for America.

The Aviation ISAC is also working with ICAO, the United Nations group—excuse me—International Civil Aviation Organization, and working with them on their aviation cybersecurity strategy and their cybersecurity action plan. We are also working several other initiatives, to include secure interoperability strategies across the globe.

As the United States considers legislation such as mandatory cyber reporting, the Aviation ISAC has been reaching out to educate stakeholders to ensure that the regulatory requirements are risk-based, achievable, cost-effective, and do not degrade the success the private sector has had in reducing cyber risks through ISACs like ours.

With respect to the mandatory reporting requirements, we believe it is important that the mandatory reporting is scoped to well-defined and confirmed cyber incidents, that mandatory reporting requirements should include robust liability protections, and it is critical that Congress streamlines the Federal and State reporting requirements to ensure that industry resources are used efficiently to combat malicious cyber threats rather than customizing reports on the same incident for multiple agencies. We also believe that the reporting program should encourage cooperation and strengthen

trust between the public and private sectors, which would include bidirectional information sharing.

Information reported to the Government needs to be properly aggregated, anonymized, analyzed, and shared with industry to help prevent future incidents.

Thank you again for the opportunity to come before you today and work on this important matter with cybersecurity and aviation.

[The prepared statement of Mr. Troy follows:]

PREPARED STATEMENT OF JEFFREY L. TROY

OCTOBER 26, 2021

Good afternoon. My name is Jeffrey Troy. I am the president of the Aviation Information Sharing and Analysis Center or Aviation ISAC. The Aviation ISAC is a global non-profit. Our members are on five continents and include air framers, airlines, airports, air navigation service providers, satellite companies, and more. Our mission is to make the aviation industry more resilient to cyber attacks.

The last time I came before you was in September 2018. Thank you for this opportunity to talk with you once again about the changes to the cyber risk landscape in aviation. The cyber risks to the aviation industry have increased. I will share with you about the good work being done by both the public and private sectors. Together both private industry and the public sector have significantly increased cooperation in threat intelligence and best practices sharing. Now is the time for industry and Government to partner even more closely in creating and enhancing effective cyber risk reduction frameworks.

INCREASE IN THREAT ACTOR ACTIVITY

Over the past several years ransomware has become a common term in aviation and many other sectors. A breach is a breach, but the success of ransomware extortionists to collect money from their victims, has greatly increased the level of skill and the number of persons willing to conduct cyber attacks. Second stage ransomware events, wherein additional ransoms are sought in exchange for the deletion of sensitive records stolen as a part of the ransom operation also highlights the risk to theft of intellectual property, sensitive business information, and privacy data.

Ransomware can also shut down operations. This has the potential to be very impactful on the aviation industry as the aviation eco-system is supported by many operational technologies.

Other cyber and cyber-related activity include business email compromises, ransom in lieu of a Distributed Denial of Service (DDoS) attack, and other frauds.

These attacks are both directly on segments of the aviation industry such as air framers, airlines, airports, etc., and their supply chains. The attack on the Colonial Pipeline and QNX Real Time Operating System (RTOS) vulnerability are two examples of where a cyber attack or a vulnerability in a product can have a ripple effect across many sectors.

INCREASED COLLABORATION

The aviation industry is a unique, global eco-system. Much of our critical infrastructure is mobile. Each industry segment, air framers, airlines, airports, services and more, are dependent on each other effectively monitoring and responding to their cyber risk. In the same way, as our assets move around the world, we benefit from trusted, global cooperation and intelligence sharing.

Preventing, responding to, and limiting the impact of these attacks requires a team of teams approach. The Aviation ISAC is primarily private-sector members. However, our core values include creating and maintaining partnerships with numerous Government and private-sector entities.

We are working with many Government agencies to make the industry more resilient by identifying and reducing cyber risks. The Aviation Cyber Initiative (ACI) is a joint partnership with the Department of Defense (DOD), the Federal Aviation Administration (FAA) and the Department of Homeland Security (DHS) which is in the process of transferring this tri-chair seat to the Transportation Security Administration (TSA). This year the Aviation ISAC and the ACI significantly solidified our partnership by co-hosting a Summit on Aviation Cyber Security. This 3-day event

included domestic and international leaders and cybersecurity experts from both the Government and private sector.

We are proud to partner with DHS's Cybersecurity and Infrastructure Security Agency (CISA). CISA is maturing well and has been putting out timely, relevant guidance in direct response to recent cyber attacks on critical infrastructure and the supply chain. The Aviation ISAC has shared intelligence on 18 occasions which were used in part in six of CISAs Intelligence Bulletins and Intelligence Information Reports. CISA has also been reaching out on vulnerability disclosures. It is also promising to learn the TSA is considering CISA as an agent for the collection of soon-to-be-required mandatory reporting of cyber events impacting aviation.

Similarly, we have reached out to the TSA as they build their cybersecurity strategy and create a regulatory framework over cyber events in Aviation.

The Aviation ISAC has been in the forefront of ringing the bell on the ransomware problem. We have been a strong voice in the crowd calling for action to reduce and eliminate this threat. We were honored to be a part of a group represented by the Government and private sector in the writing of the "Combatting Ransomware Report" issued in late April by the Institute for Security and Technology. The report has many actionable recommendations. The world needs a stronger international consensus on identifying ransomware operators and taking them out of action. Law enforcement efforts must be enhanced with private-sector expertise and a whole-of-Government as well as a whole-of-governments working together. We encourage continued action on the recommendations in this report.

Aviation is global. The Aviation ISAC has members on five continents and from many segments of the Aviation industry. We engage with global Computer Emergency Response Teams, the International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), Airports Council International, and many European Union entities, to name a few.

The public-private partnerships still have a long way to go, especially in the area of trust, which I will talk about in a few minutes. Our industry is also benefiting from a significant increase in the cooperation between "Private-Private" entities.

To highlight a few, the Aviation ISAC has partnered with the Aerospace Village. Each year, we sponsor a cyber skills event, also known as a capture the flag event. The Aerospace Village has many cyber security researchers as members. This is a great event for building bridges between industry and the researcher community.

We partner with the Aerospace Industries Association, contributing to discussions and development of a white paper on best practices in aviation cyber security.

We also partner with the American Institute of Aeronautics and Astronautics (AIAA) and have a regular dialog with Airlines for America.

The Aviation ISAC and our members are also building bridges with security researchers through the creation, promotion, and ease of access to Vulnerability Disclosure programs. These programs make manufacturers more accessible to security researchers who can make vulnerabilities known to manufacturers of software and hardware products.

CREATING AND ENHANCING EFFECTIVE RISK REDUCTION FRAMEWORKS

There are many efforts going on across the globe to increase the regulatory requirements related to cybersecurity in Aviation. Earlier I mentioned ICAO, a United Nations organization, which establishes guidance for the aviation industry around the world. The Aviation ISAC is working with ICAO and partners across the globe in updating ICAO's Aviation Cybersecurity Action Plan. We are also working on several other initiatives to include an aviation cybersecurity framework and secure interoperability strategies.

As the U.S. Government considers legislation such as mandatory cyber reporting, the Aviation ISAC has been reaching out to educate aviation stakeholders to ensure that the regulatory requirements are risk-based, achievable, cost-effective, and do not degrade the success the private sector has had in reducing cyber risk through ISACs like ours.

Regarding Mandatory Reporting Requirements

1. We believe it is important that mandatory reporting is scoped to well-defined and -confirmed cyber incidents. We must be focused on quality information sharing. Too much information will overload threat intelligence and incident response resources.

2. Any mandatory reporting requirements should include robust liability protections. The act of reporting a covered incident and the contents of any report, including supplemental reporting, should be protected from legal liability. Information contained in notifications should not be subject to discovery in any civil or criminal action. Reporting entities, in essence, should not be penalized after

the fact for complying with a legal obligation. In addition, only relevant information which will assist others in protecting and defending critical infrastructure systems should be required of the sector regulator.

3. Several critical infrastructure sectors have existing obligations to report significant cyber incidents to Federal and/or State regulatory agencies. It is crucial that Congress streamlines Federal and State reporting requirements to ensure that industry resources are used efficiently to combat malicious cyber threats, rather than customizing reports on the same incident for multiple agencies. A single report to one agency should suffice to meet legislative and regulatory mandates. For example, many aviation sector companies are also defense contractors. Reporting should be made either to CISA or the appropriate sector risk management agency (SRMA), which should then disseminate reports to other relevant agencies.

4. Cyber attack victims are victims. A reporting program should encourage cooperation and strengthen trust between the public and private sectors. A regulatory-based approach that focuses on punitive actions, such as fines or penalties, rather than mutual gains achieved through information sharing runs counter to the goal of creating a strong National partnership model to address the increasing cyber threats facing the United States.

5. The bills in draft would require CISA to take the lead in writing an interim final rule. Lawmakers are urged to step back from this line of thinking and call on CISA to first provide notice that it intends to promulgate a rule. With input from industry, the process will work faster as industry can assist in making the rules achievable. Industry is passionate about protecting our customers, employees, and our businesses. We are operators of critical infrastructure and our industry has incredible passion and cybersecurity talent working to protect it. The rule-making process must include coordination with impacted private industry stakeholders because many of the programmatic details, such as definitions and the contents of reporting, would be determined through the rulemaking process. At a minimum, we ask you to consider a rulemaking process which features an initial 90-day consultation period with industry followed by a 90-day comment period.

6. Cyber intelligence is a requirement to protect the sector. It is not a singular need of the Government, nor the private sector. Information reported to Government needs to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation and/or prevention of future cyber incidents. Nothing in future legislation or processes should limit or impede companies continuing to work together through ISACs. With respect to the Government sharing back information to the private sector, in many cases, the private sector will be able to enhance that information, keeping the intelligence cycle active and benefiting us all as we protect aviation. A persistent shortcoming experienced by businesses across many sectors is a lack of timely and effective action or feedback on cyber reports from Government. We need legislation that leads CISA, law enforcement, and other agencies to provide more timely, relevant cyber intelligence to industry groups' and sector businesses.

CONCLUSION

We have made great strides in coming together as a Government and an industry in making aviation more resilient to cyber attacks. We applaud the efforts of the Government to continue to strengthen the ability of our Government entities to investigate, prosecute, and dismantle ransomware gangs. We will continue to partner and engage with the Aviation Cyber Initiative and our many partners as we seek out vulnerabilities and develop best practices to protect, defend, respond to, and mitigate cyber attacks. We applaud the efforts of CISA in publishing vulnerability and best practices and encourage more bidirectional information sharing. Finally, thank you once again for the opportunity to come before you today on this important matter of cybersecurity in aviation.

Ms. CLARKE. Thank you, Mr. Troy, for your testimony.

I now recognize Mr. Dickinson—Mr. Dickerson—excuse me—to summarize his statement for 5 minutes.

STATEMENT OF SCOTT DICKERSON, EXECUTIVE DIRECTOR, MARITIME TRANSPORTATION SYSTEM INFORMATION SHARING AND ANALYSIS CENTER

Mr. DICKERSON. Thank you, Chairwomen, Ranking Members, and Members of the subcommittees. My name is Scott Dickerson, and I serve as the executive director of the nonprofit Maritime Transportation System Information Sharing and Analysis Center, the MTS–ISAC. A decade ago, helped create the Coast Guard Cyber Command, before serving in other civilian roles and supporting private-sector cybersecurity programs. Thank you for the opportunity to testify before the subcommittees today.

The MTS–ISAC is made up of public and private-sector stakeholders, including port authorities, vessel and terminal owners and operators, cruise lines, energy facilities, ferry operators, and other members of the maritime community. We focus on actionable, relevant, and timely cyber threat information sharing. We have supported cybersecurity guidelines on-board vessels, as well as cybersecurity guidelines for ports and port facilities, both of which are recognized by the U.N.'s International Maritime Organization.

Our efforts have resulted in significantly more cybersecurity advisories being distributed to our maritime community than those released by the 20-plus Federal Government organizations with the responsibility for maritime security combined. A key reason for the level of sharing we see is the anonymization of identities and the trust that this reinforces with the maritime community. Others may tell you we need billions of dollars in cybersecurity investment across the critical infrastructure sectors. We do need investment, but taxpayers may currently be overpaying for the results the critical infrastructure community is receiving from the Federal Government.

I want to share with you three common challenges I regularly hear from industry stakeholders related to the Federal Government's approach to cybersecurity and public-private partnership. First is the concern of redundant Federal cybersecurity efforts. Because of the critical intermodal connections that ports, terminals, and a variety of facilities have, some of our stakeholders are subject to multiple regulatory requirements, including the Maritime Transportation Security Act of 2002, as well as TSA's pipeline and soon-to-be-finalized rail security directives.

As a result, limited resources are often spent on redundant checklists, meetings, reports, audits, et cetera, as opposed to actively managing cyber risks to critical infrastructure. It seems like every time we turn around, there is a new effort unveiled by a Government agency, and often it seems to be repackaging the elements of an older program with a new name. The latest example is JCDC, elements of which have been in place for several years.

Second, there is a lack of trust with the Federal Government related to cyber incident reporting. Trust is critical when fostering collaboration and information sharing. The maritime community's trust in Federal agencies was yet again recently shaken in the aftermath of an incident at a port. This is because of three things.

No. 1, immediately following the incident, the 3 Federal Government agencies involved did not want industry-sharing actionable information for almost 3 weeks as zero-day vulnerabilities were ac-

tively being exploited. Of note, during this 3-week period, none of those agencies collaborated with the MTS–ISAC or the maritime industry writ large.

No. 2, CISA publicly released the name of the victim, with no prior coordination or notice to the victim. This may have been in violation of the Cybersecurity Information Sharing Act of 2015, and undermine trust.

No. 3, a Government agency for-official-use-only technical report with details surrounding the incident was leaked to the press, but it was not shared amongst maritime community members.

These were 3 distinct ways industry trust was undermined with just this one incident, and, unfortunately, incidents are occurring regularly.

Third, resource investments in people are needed. Experienced cybersecurity specialists are in short supply in all industries. Please review opportunities for partnering with ISACs for real-world hands-on cybersecurity training, internships, and educational opportunities. Also, Federal employees need to better understand the various cybersecurity funding opportunities the Government provides to align with their agency mission sets.

As an example, cybersecurity was the highest-stated priority for FEMA's 2020 Port Security Grant Program. Yet many stakeholder requests for cybersecurity investments were turned down by U.S. Coast Guard captains of the port, resulting in only about 12 percent of the $100 million program being invested in cybersecurity, the No. 1 priority.

MTS–ISAC and the stakeholders are hopeful that we can more effectively partner with the Federal Government to safeguard our National interests. I kindly request you include, support, and protect the mechanisms safeguarding trusted, anonymous information sharing, incident reporting, and other critical infrastructure cybersecurity efforts performed by ISACs and their communities in legislation.

Of note, CISA of 2015 remains significantly underutilized. Although it has been implemented, there remains resistance to fully trusting and using the provisions of the legislation. Perhaps we should focus on some of these underutilized efforts rather than creating some new ones.

Thank you again for the opportunity to provide this testimony, and I look forward to your questions.

[The prepared statement of Mr. Dickerson follows:]

PREPARED STATEMENT OF SCOTT DICKERSON

OCTOBER 26, 2021

I. BACKGROUND

Ranking Member Garbarino, Ranking Member Gimenez, and Members of the subcommittee: My name is Scott Dickerson and I serve as the executive director of the Maritime Transportation System Information Sharing and Analysis Center Institute (MTS–ISAC). Thank you for the opportunity to testify before the committee today.

The Maritime Transportation System ISAC was formed as a nonprofit by a group of U.S. maritime critical infrastructure stakeholders. Our primary mission is to more effectively share information focused on cyber threats and cybersecurity best practices within a trusted community of stakeholders to help make the maritime community more resilient to cyber attacks. Our stakeholders include port authorities, vessel owners and operators, terminal owners and operators, cruise lines, en-

ergy facilities, ferry operators, and other members of the public and private-sector maritime critical infrastructure community. On a daily basis, our stakeholders are sharing actionable, timely, and relevant cyber threat information with their public and private-sector peers. They formed the MTS–ISAC out of a need to quickly share relevant cyber threat information and have quickly shown how effective their ISAC model is working to do just that.

MTS–ISAC stakeholders exchange information every day about the attacks they are seeing. The MTS–ISAC provides anonymization of identities, which when combined with the Cybersecurity Information Sharing Act of 2015 (CISA 2015), fosters community trust and enables peer-to-peer collaboration. This peer-to-peer collaboration is extremely valuable because it allows stakeholders to better understand threats targeting the maritime sector and implement cybersecurity strategies more effectively to counter those attacks. This private-sector sharing has resulted in more maritime industry-focused cyber threat intelligence advisories being distributed to our stakeholders since our inception than those released by the more than 20 Federal Government organizations with a responsibility for maritime security [1] combined. As an example, we have produced over 80 Cybersecurity Advisories this year and to our knowledge the U.S. Coast Guard has released 5 cybersecurity threat reports. The MTS–ISAC has not received any cyber threat or incident reporting from MARAD, Department of Energy, TSA, USTRANSCOM, NOAA, ODNI's National Maritime Intelligence-Integration Office (NMIO), and or other maritime-focused Governmental organizations. We have created over 500 Indicator Bulletins sourced from stakeholder shares, which I believe is roughly on par with the whole of CISA. We do this on a nonprofit budget that runs in the low 6 figures annually.

Our stakeholders believe that cybersecurity is a core element of risk management that allows their organizations to operate in a safe and secure manner. Because of the critical intermodal connections and relationships that ports, terminals, and a variety of facilities have, some of our stakeholders are subject to a variety of regulations and security directives, including the Maritime Transportation Security Act of 2002 as well as TSA's Pipeline and soon to be finalized Rail Security Directives. This is in addition to a variety of other cybersecurity-related requirements that can include safeguarding various types of information including HIPAA, PCI, PII, and other cybersecurity frameworks and requirements. I say this not to be glib, but to say the maritime sector faces a highly complex intersection of requirements, and maritime companies understand how to operate in this environment. Cyber incidents need to be handled extremely delicately since they can have major impact across supply chains, for customers, stakeholders, and shareholders. Legal departments and auditors within an organization help work these details in closed door sessions to ensure compliance and legal issues are addressed properly. Additionally, those with cyber insurance coverage will be directed by their insurance how and with whom to share information. It would be beneficial for the Federal Government to consult with stakeholders before new cybersecurity laws, security directives, or similar facets of oversight are finalized to fully understand the implications of drafts so that the desired risk management outcomes can be met in a manner appropriate for the complexities of this industry without creating undue burdens or unintended consequences.

In addition to sharing cyber threat information, our nonprofit is also working with numerous industry stakeholders to improve industry cybersecurity guidelines. We have provided inputs to drafts for updates to the International Association of Classification Societies' *Recommendations on Cyber Resilience.* The MTS–ISAC also contributed content to the following maritime industry cybersecurity references:

- *The Guidelines on Cyber Security Onboard Ships (V4)* and
- *IAPH Cybersecurity Guidelines for Ports and Port Facilities (Version 1.0).*

II. CURRENT CHALLENGES WITH FEDERAL CYBERSECURITY APPROACHES

There are currently multiple cybersecurity challenges impacting critical infrastructure cyber resiliency. Of particular interest from an ISAC perspective are the following:

Overlapping Efforts

- Redundant, and sometimes conflicting cyber regulations and enforcement or interpretation differences across Government roles and responsibilities.
  - Multiple agencies are involved with duplicative efforts. Redundant tracking, outreach, reporting, and mitigation efforts are a detriment to securing critical infrastructure as the time of limited resources is spent on redundant efforts.

[1] National Maritime Cybersecurity Plan—*https://www.hsdl.org/?abstract&did=848704.*

- Inconsistent standards often impact multiple sectors and cause confusion.
- Federal Government focus on "leading", rather than partnering to support private-sector efforts. The private sector predominantly owns and operates critical infrastructure, and the Federal Government should support effective solutions rather than lead ineffective solutions.
  - Private sector understands where the challenges lie; multiple Governmental agencies try to "solve the problem" in silos rather than in partnership.

Information & Intelligence Sharing

- There is currently a Federal Government focus on cyber incident reporting, rather than exchanging timely threat information that could minimize potential impacts.
  - Lack of consistent and clear definitions for suspicious activity, incidents, etc.—this needs to be remedied and should be in partnership with industry.
- CISA should be the Federal agency hub for information sharing, and that needs to be reflected in all regulations, Security Directives, etc. Having a single touchpoint will streamline processes and should allow for more cross-sector critical infrastructure correlations to be made that are currently being missed.
- Similarly, there are concerns with USCG being both a regulator and pushing for threat intel sharing outside of the required reporting mandates. Providing non-mandatory event reporting to a regulator is a cause for concern for some in the private sector. This should be voluntary (and based on trust), but again it would be better to have a single point of contact for all critical infrastructure sector reporting, which for maritime can then be provided to the 20+ Federal Government organizations with a responsibility for maritime security.
- Repeated misinformation that private sector does not share information with each other or with Governmental agencies.
- Greater Federal resource emphasis on granting security clearances to private-sector stakeholders, who remain constrained on acting on Classified information.
- Agency and media inaccurate claims that certain sectors are better or worse in cybersecurity protections pit private industry as competitors, not collaborators.

Cybersecurity Resourcing

- Experienced cybersecurity specialists are in short supply in all sectors and across the public and private sectors.
- Federal funding of cybersecurity efforts remains inconsistent across sectors and sometimes competes with private-sector cybersecurity efforts, which confuses and frustrates maritime stakeholders.

In addition to these, there are numerous other cybersecurity challenges that also need addressing, but others that are notable include:

- Risks related to foreign investment and/or reliance within U.S. marine critical infrastructure;
- A heavy focus on check-box style types of regulation;
- Recent TSA Pipeline Security Directive did not include a mechanism for review and feedback from the stakeholders this will impact. As a result, some challenges may be arising that could have been avoided if some language was changed. For example, requiring to inform the Government within 7 days of personnel that will be designated to be available 24/7 to the Government for any reason. There are several H.R. implications for this, including the potential need to reclassify positions, renegotiate contracts, etc. for the personnel in those roles; and
- Lack of funding for voluntary CISA cybersecurity programs, including CISA Risk and Vulnerability Assessments (RVA), Validated Architecture Design Reviews (VADR), and similar efforts within the Coast Guard, such as their outstanding Cyber Protection Team.

III. Recent Example of Post-Incident Response

A recent incident at a critical port is an example of a post incident response that highlights some of the above challenges and how the Federal Government is currently handling critical infrastructure cybersecurity.

Summary

A port quickly identified and responded to a cyber attack exploiting a zero-day vulnerability. The port confirmed the incident with their security vendor, who was able to identify other clients in other critical infrastructure sectors also experiencing the same attack. The port notified CISA, USCG, FBI and MTS–ISAC. The MTS–ISAC shared information with stakeholders and with other members of the National Council of ISACs the same day.

The Federal agencies worked with the vendor on a patch but stated they did not want vulnerability information shared broadly across critical infrastructure sectors until the patch was made available. Rather than engage in public-private partnership, these Federal agencies unilaterally decided to leave U.S. critical infrastructure owners and operators with limited visibility and awareness to on-going, active attacks exploiting a 0-day vulnerability. However, indicators that could have helped cyber defenders (for example hashes of files related to the attack) could have aided critical infrastructure to identify if they were under attack and take response actions. This could be done without leaking sensitive information that could lead to additional threat actors exploiting the vulnerability. Critical infrastructure protection and resiliency did not appear to be the priority for these agencies.

Finally, almost 3 weeks later, vulnerability and patch information was released as TLP:WHITE information along with a TLP:AMBER Joint Cybersecurity Advisory with information related to the attack. Then over a week later, similar information was released as TLP:WHITE. Then after another week went by, without coordinating or notifying the victim organization ahead of time, CISA personnel named the victim in a public Senate hearing and a USCG TLP:AMBER Technical Report was leaked to the press. During this time no Federal agency contacted or collaborated with the MTS–ISAC or other National Council of ISAC members. However, the MTS–ISAC regularly shares Cybersecurity Advisories with personnel at all 3 agencies and is a member of CISA's Cyber Information Sharing and Collaboration Program (CISCP).

Trust is critical when fostering collaboration and information sharing, which we absolutely need to create a more cyber resilient critical infrastructure community. The maritime community's trust in Federal agencies was shaken following this incident because:

1. Immediately following the incident, the Federal Government delayed information sharing for 3 weeks while the critical infrastructure community was ready to share this information immediately.
2. CISA released the name of the victim which may have been in violation of the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and perhaps the Federal Government should research whether this should lead to sanctions. "Section 1504(a)(3)(C)(ii) requires that procedures ensure there are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under CISA 2015 in an unauthorized manner."[2]
3. A USCG For Official Use Only Technical Report with details surrounding the incident was leaked to the press. The MTS–ISAC did not receive this report nor did other maritime stakeholders. If the report was intended solely for the victim, then how did the press receive it? Some industry stakeholders are wondering if this was "leaked" as part of a political agenda. No matter how or why, several stakeholders have expressed concerns with reporting incidents to the government as a result.

To be honest, the most common refrain I hear from private-sector stakeholders when it comes to information sharing with the Federal Government can be boiled down to a lack of trust in how the Government will handle the information. I hate to hear this having served on active duty and as a Federal Government civilian, but there are some legitimate concerns that should be recognized. I thought about whether to bring this challenge up in my testimony, but nothing will improve by not bringing this up. At some point conversations about how Federal Government actions are undermining the trust of the critical infrastructure community would be healthy, in my opinion.

IV. OPPORTUNITIES FOR IMPROVEMENT

There are opportunities for the Federal Government to effectively partner with the MTS–ISAC and public and private-sector maritime stakeholders:

Improve Efficiencies

- Leverage ISACs and other forums to reduce redundant efforts and join private-sector stakeholders in their chosen collaboration mechanisms. The MTS–ISAC has non-voting seats for CISA, Coast Guard, and the Department of Energy representatives which remain unfilled by these agencies.
- Support private-sector stakeholder solutions that already address Federal Governmental needs and have proven effective for critical infrastructure.

[2] *https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf.*

- A great example is also the Information Exchanges being created that include port authorities, USCG, CISA, other agencies and public and private local Maritime stakeholders working with the MTS–ISAC at a community level to define and foster trust while sharing actionable, relevant, and timely threat information.

Information & Intelligence Sharing

- CISA 2015 remains significantly underutilized. Although it has been implemented, there remains resistance to fully trusting and using the provisions of the legislation by both Federal and private partnership programs.
- Prioritize on-going bi-directional exchange of unclassified threat information between the public and private sectors, not just incident reporting.
  - Holistic sharing of threat information, best practices, and lessons learned is more beneficial for improving cyber resilience than focused incident reporting.
- Improve training of Government personnel on proper information classification procedures and how to more effectively mark information to allow for sharing.
- Focus additional Federal resources toward information declassification efforts.

Resource Investments

- Ensure requirements are in place to raise awareness of Federal employees of cybersecurity funding opportunities that align with agency mission sets.[3]
- Review opportunities for partnering with ISACs for hands-on cybersecurity training, internships, and educational opportunities.
- CISA should consider funding ISAC analyst positions at CISA Central to better facilitate the bi-directional flow of information across critical infrastructure.
- Multiple maritime stakeholders are partnering with Computer Science, Cybersecurity or other closely-related college programs to provide students with real-world experiences that they might not otherwise have exposure to for several years. These programs would benefit from further support and resourcing.
- Increase funding for voluntary programs such as RVAs, VADR, and CPTs; wait lists and backlogs for these efforts should not be reaching 18+ months as they have in the past. The Coast Guard has an outstanding Cyber Protection Team, but there is a need for regional cyber incident response teams. There are not enough to adequately provide assistance should there be even a mild demand. CISA was not able to respond in a timely manner to produce meaningful input to a recent attack on a port authority.

V. CONCLUSION

The MTS–ISAC is hopeful that the maritime critical infrastructure community and the Federal Government can more effectively partner with each other to safeguard our National interests. Sharing cyber threat information is a key element to improving our resiliency, and that will work best if industry and ISACs are engaged as envisioned by CISA 2015. Whether it is related to incident response or proactive threat information sharing, we need true collaboration between the Federal Government and other public and private-sector organizations. Currently this is not an effective system of public-private partnership and collaboration. It feels like industry is being threatened with additional regulation and security directives rather than being treated as the partners who own and operate the vast majority of critical infrastructure. I kindly request you consider the beneficial role that ISACs play daily in facilitating trusted, anonymous, information sharing for the improved resiliency of critical infrastructure across our country in the face of on-going cyber attacks. Please include, and protect the mechanisms safeguarding, the ISAC communities in legislation related to critical infrastructure cybersecurity efforts. Any bill associated with critical infrastructure cybersecurity efforts that does not reflect the positive, critical, and irreplaceable role that ISACs and industry representatives and stakeholders provide to our critical infrastructure communities, and does not include provisions requiring Federal agencies to effectively collaborate with them, should be opposed. Thank you again for the opportunity to provide this testimony.

Ms. CLARKE. I thank you, Mr. Dickerson, for your testimony here today.

I thank all of our witnesses for their testimony.

---

[3] As an example, cybersecurity was the highest stated priority for FEMA's 2020 Port Security Grant Program. Yet many stakeholder requests for cybersecurity investments were turned down by USCG Captains of the Port in favor of physical security efforts, resulting in only roughly $12 million out of the $100 million program being invested in the highest priority area.

Pursuant to today's order, the Chair declares the committees in recess, subject to the call of the Chair. Members will be given notification prior to reconvening after votes.

[Recess.]

[3:59 p.m.].

Ms. CLARKE. Let me, first of all, thank all of our witnesses for your indulgence today. Just so happened that we had one of those rare or common conflicts of having votes in the middle of our hearing. So I truly appreciate your willingness to remain tuned in, and we will move forward now with questioning.

I will remind the subcommittees that we will each have 5 minutes to question the panel.

I will now recognize myself for questions. My first question is directed to Ms. Spaulding.

Ms. Spaulding, for many years, the Federal Government has relied on voluntary partnerships and programs to improve cybersecurity for critical infrastructure. Recent cyber attacks like Colonial Pipeline have forced a new conversation about whether that voluntary partnership model is sufficient for today's threat landscape.

As the former under secretary for CISA's predecessor organization, could you talk about the limitations of the voluntary framework and the challenge of regulation in an area as dynamic as cybersecurity?

Ms. SPAULDING. Absolutely, Madam Chairwoman. Thank you. Both your points are very well taken. We are in a situation now where we have both the capability—I think we have reached a level of maturity in Government and in industry in understanding some of the basic things that really must be done and can be done to significantly raise the level of cybersecurity. So we are in a better position than we have been in the past in knowing what kinds of mandates to put in place. So that is one thing.

Then we do have a threat environment that continues to grow more and more grave with each passing day, and there is lots of evidence of this. We don't have access to the intelligence that the Government or TSA may have, although I think that TSA has briefed some of the companies about the intelligence that they are seeing that gives them that sense of urgency.

But even with what we see in open source in the media every day, it is very clear that our adversaries are very focused on our industrial control systems, on operational technology, and understanding that so that they can be in a position to disrupt it, and that criminal gangs are getting increasingly brazen in their targets with respect to ransomware, for example. But you can see it is grave.

Ms. CLARKE. So in your testimony—yes. So in your testimony, you mention that you are thinking it changed about the need to move from a voluntary to regulatory framework. What role do you see CISA playing as the long-time voluntary partner and civilian hub for cyber expertise in this shift?

Ms. SPAULDING. Yes. So CISA is thought to be, for example, the repository of mandatory reporting information that comes in. We need to have a place in Government that takes that information and adds value to it and makes sure that it is anonymous, but that it is analyzed, put in context, and then shared broadly, very quick-

ly, so that everyone can use that information to better defend their networks.

CISA brings a couple decades now of expertise on cybersecurity and on these infrastructure sectors, and work in close collaboration with sector-specific agencies like TSA can really leverage that cybersecurity expertise to help the sector experts to find the right path forward in close collaboration and partnership with industry.

Ms. CLARKE. So this is to all of our witnesses, and I only have a minute and some change left, so if I don't get to you, if you would just submit something to us in writing, that will be helpful as well. But many of you mentioned the importance of mandatory cyber incident reporting as a way to grow visibility around cyber threats and improve the quality of bidirectional information sharing with the private sector. As you know, this is a top priority of mine.

Ms. Spaulding, if a mandatory cyber incident reporting regime had been in place at CISA since you were under secretary, what security gains might have been made since that time?

Ms. SPAULDING. So two things I would point to. That information can be shared more broadly so that all network defenders have a better sense of the tactics, techniques, and procedures they are defending against. No. 2, it would help to calculate a return on security investment so that CISOs at companies all across the country can make the case more effectively for that investment. So I do believe it would have raised our cybersecurity posture.

Ms. CLARKE. Ms. Cogswell, can you elaborate on how cyber incident reporting could be used to improve security for industrial control systems across sectors?

Ms. COGSWELL. One of the most important things I have seen is that ability to bring information, like mandatory cyber reporting information, with your industry experts and to be able to use and engage with that information in a way that helps you propose a next level of solutions. The additional reporting, the ability to see how it operates in one area, how therefore it might appear in another area in advance of that area being a target can be really quite powerful. I have seen a lot of really great work when you have Government and industry sitting together engaging with that type of data.

Ms. CLARKE. Thank you very much.

I now recognize the Ranking Member, Mr. Garbarino, of the Subcommittee on Cybersecurity, Infrastructure, and Innovation, the gentleman from New York, for questions at this time.

Mr. GARBARINO. Thank you, Chairwoman. Thank you to the people testifying today, the witnesses.

My first question is for Mr. Dickerson. Can you please discuss the unique complications of the maritime environment and how ports must often comply with multiple regulations and requirements from the Coast Guard, TSA, and others? Can you describe some of the specific challenges when it comes to securing ports?

Mr. DICKERSON. Thank you, Congressman Garbarino, for that question. It is highly complex environment where, because of the intermodal aspects of the maritime sector, you will have port authorities, for example, owning the last mile of rail. So then they need to comply with TSA's upcoming rail security directive.

Similarly, they will also own pipelines. So now it becomes a question of, OK, are we reporting this information to TSA, to the U.S. Coast Guard, CISA? Do we need to involve FBI? Some of these might require CBP reporting due to goods coming into the ports. It becomes a mesh of Federal agencies that then need that required reporting.

Again, as I mentioned earlier in my testimony, that can lead to a lot of redundant efforts and really pulling the cyber defenders away from incident response to now answering multiple questions from multiple agencies at a time when they really need to be focused on those response actions.

Mr. GARBARINO. OK. So maybe for you and the—all the panelists. So what recommendations in detail do you have to better harmonize these requirements?

Mr. DICKERSON. I think one of the things——

Mr. GARBARINO. I mean, one—so it is not so—not just so that it works with industry, so it is not a high burden on industry, but also—but still sets a high cybersecurity standard.

Mr. DICKERSON. Right. So I think part of the question is, is there a centralized point, belly button, for that reporting? If that is formally the NCIC on the SIOC, CISA central, and you have representatives from those agencies there, or if you have CISA representatives at those agencies, I think there is options for either way to then correlate some of that information, make sure it gets to all of the right agencies and partners, but that then you are not having to report the same information, answer the same questions over and over, if that helps, sir.

Mr. GARBARINO. Nope, that does.

Anything else from any other panelists, or I can go to my next question? Anybody want to add anything?

All right. If nothing, this is pretty much for everybody, so jump in when you want. As the Federal Government sets the standards for industrial control systems' cybersecurity in collaboration with the critical infrastructure community, there will inevitably be requirements for companies to validate the controls in place, as we saw in the TSA security directive.

What is the most effective way to, in a scalable manner, have these validations take place? Should TSA conduct them, CISA? Or can DHS, TSA, and the industry agree on what comprises a cybersecurity validation and have private companies do it?

That is—and whoever wants to jump in first if you have——

Ms. COGSWELL. I will be happy to start. I will say that I think this is an environment where there are a number of opportunities to engage across the board. As you noted, there are existing protocols by which TSA and CISA partner for the validated architecture reviews, but at the same time, there are models under which regulatorily you can create the opportunity for third-party entities who are off an improved list, clearly qualified and found to be—to meet various standards who can also perform those types of services.

As I noted in my opening statement, one such model that TSA has actually used before is the third-party canine program, where they create an approved list of canine operators who can be used in screening operations. They therefore can regulate both the entity

that is providing the service as well as the entity who is using it, to make sure that the goals and outcomes are reaching everybody's desired end-state.

This is an area I think that should be explored. I think there is huge opportunity, frankly, to expand the number of entities who can participate, which helps all of us, so that you are not worried so much about necessarily limited resources at any one point, or, frankly, you know, every company not having to come up to speed on every nuance of cyber, which may be more difficult given the difficulties in hiring cyber talent these days in particular.

Mr. GARBARINO. Yes. Difficulties and expense.

OK. I appreciate it. So we would be better off doing a third party. I appreciate your answer.

If nobody else has anything else back, I do yield—has anything else to say, I do yield back to the Chairwoman.

Ms. CLARKE. I thank you, Ranking Member Garbarino.

I now recognize the Chairwoman of the Subcommittee on Transportation and Maritime Security, the gentlelady from New Jersey, Mrs. Watson Coleman, for her questions at this time.

Mrs. WATSON COLEMAN. Thank you, Chairwoman. Thank you to all of our witnesses.

In 2001, terrorists needed to make it onto the planes and into the cockpit in order to execute the 9/11 attack. However, in 2021, we must also consider the possibility that a terrorist or hostile nation could hijack a flight by hacking it, without ever passing through TSA checkpoints or stepping foot on that plane.

Mr. Troy, Ms. Spaulding, and Ms. Cogswell, would you comment on this: As aircraft become increasingly connected and automated, how do we prevent hackers from hijacking planes and, in worst-case scenario, if a hijacker obtained operational control, what redundancies should we have in place to ensure that a real pilot can regain control? What role do you see TSA and CISA, in concert with FAA, ensuring the security of aircraft operational control and navigational systems?

I will start with you, Mr. Troy, Ms. Spaulding, and then Ms. Cogswell, please.

Mr. TROY. Thank you. Excellent question. So the aviation industry has an incredible safety record based on strong engineering design and continuous enhancement, and the aviation industry does recognize cybersecurity as a critical part of aviation safety. So the industry has an incredible safety record, and it is the result of careful incorporation of functionality and strong secure system design. The airplane design is based on careful system integration and system isolation as appropriate and redundancy for critical systems.

So safety critical systems are highly protected and hardened against attacks, but we are continuously evaluating the changing cyber threat space and trying to incorporate then improvements to anticipate threats. So the systems are separated from cyber and system engineering reasons as well.

With respect to your question about a hacker obtaining operational control. As I stated above, the planes are designed with redundant systems such that if a system is not operating as designed, another system can be engaged to perform the function. Pilots are trained as well to address system failures and, ultimately,

pilots are a critical layer of protection for continued safe flight and landing.

With respect to the question on TSA and CISA and their roles, as well as FAA, they are all stakeholders in the safety of aircraft, as are airlines, and, you know, being operators of the aircraft. These Government agencies should be working with the manufacturers to obtain assurance that the aircraft, as designed, are periodically assessed against threats. These Government agencies are also incredibly helpful in sharing threat intelligence information.

Mrs. WATSON COLEMAN. Thank you.

Ms. Spaulding.

Ms. SPAULDING. Yes. I can vouch for my days at DHS that the industry takes this threat very seriously and that there is close interagency cooperation. Of course, DHS and FAA and DOD are all members of the Aviation Cybersecurity Initiative working closely with industry.

I do think it is something that requires constant reassessment, constant monitoring, to make sure that the design basis that Jeff talks about is up-to-date, is keeping up with everything that we know about the nature of the threat, and that that industry-Government collaboration continue to be very strong. This is a very dynamic field.

Mrs. WATSON COLEMAN. Thank you.

Ms. Cogswell.

Ms. COGSWELL. Thank you very much. As you know, the Transportation Security Administration actually started as part of the Department of Transportation. As such, we have very close, strong ties with the FAA and other sister entities within the Department of Transportation that continue to this day. On any given day, talk 12, 15 times, conduct regular exercises, share information on threats.

I will say one of the things that I want to highlight that Suzanne noted is that continuing focus on looking at what is next on the horizon and how do we best make sure that we use our compatible authorities, safety and security, to take the best action with these threats.

I will say, during my time at TSA, we also worked very closely together and then with industry on those problems where we saw a nexus crossing over between the agencies.

Similarly, CISA, given their membership in DHS as a strong partner from that front, proved valuable in a number of these conversations to help articulate and describe different angles against which we should be looking at that threat. I feel confident these conversations continue.

Mrs. WATSON COLEMAN. Thank you.

Madam Chairwoman, I yield back.

Ms. CLARKE. The Chair now recognizes the Ranking Member of the Subcommittee on Transportation, Maritime—and Maritime Subcommittee, the gentleman from Florida, Mr. Gimenez.

Let me just state that, going forward, Mrs. Watson Coleman will be presiding on the balance of our hearing this afternoon. Thank you very much.

I yield to the gentleman from Florida.

I assume that the gentleman from Florida has not returned as of yet, so I am going to turn the meeting over—the hearing over to my colleague, if she is ready at this time.

Mrs. WATSON COLEMAN [presiding.] Thank you, Madam Chairwoman.

I am trying to see who is next. I believe it is Representative Jackson Lee from Texas. I am sorry, I am getting this information in live time.

Ms. CLARKE. OK.

Mrs. WATSON COLEMAN. Representative Jackson Lee.

Ms. CLARKE. She is—I think she is trying to unmute.

Ms. JACKSON LEE. Thank you. The staff has to do so. Thank you, Madam Chair. We can't self—under the Webex Cisco, we cannot self-unmute ourselves.

But let me thank both of you and the Ranking Member for these important messages that we have been gathering today, and I am going to ask a question of all.

I think it was, Mr. Troy, your testimony, I think, suggested there was a lot of layering with respect to Governmental regulation and addition, and your point would be that we need to find a way to be more specific and pointed.

Am I correct, Mr. Troy? Was that your testimony, or Mr. Dickerson?

Mr. DICKERSON. Congresswoman Jackson Lee, I had some comments on those lines. This is Mr. Dickerson.

Ms. JACKSON LEE. OK. So would you expand on how we can be more effective regulators first? Then I have one or two other questions. But can you quickly respond to how we can be more effective in our work? This is important work and important infrastructure that needs to be secured. So, Mr. Troy?

Mr. TROY. So I believe that one of the things that is really important as we look at putting out mandatory reporting and regulations on the industry is that we use a phased approach. A phased approach basically is one that ensures that all of the people who are going to fall under these requirements can achieve the success of getting these requirements in place.

When we look at what they have done, for example, on the Department of Defense with the defense contractors, there has been, you know, a ramp-up of increased cybersecurity maturity requirements of all the defense contractors. I think a lot of great lessons have been learned from that process, and by establishing baseline controls and then continuing to evaluate the ability of industry to meet those and then challenge them and bring them up higher is an effective process.

Ms. JACKSON LEE. Let me ask—thank you so very much. Let me ask further witnesses.

Ms. Spaulding, I want to focus on trains—trains in the Eastern Corridor, trains that go really into neighborhoods. I really think that we have been on the edge of good luck, in all honesty, in terms of dealing with trains that—purposefully so, they were meant to go almost up to your front door. They go behind homes. These are interstate trains. Homes are built right on the back side of trains. They are in mountains, they are in valleys, they are in dangerous places, and they are Amtrak.

What are special efforts that specifically look at trains and the cyber system dealing with ultimately—if I could use the terminology—the massive train wreck that could come from a cyber failure on our train systems? There is interstate train system and then obviously the computer—excuse me—the commuter train. Would you care to comment on that?

Ms. SPAULDING. Absolutely, Congresswoman. Your points about the potential risks that come with our rail system across the country is exactly right. The good news is that the rail industry has worked closely with DHS for many years. When I was the under secretary at DHS, the Rail Sector Coordinating Council was very active, and they have done a lot, both in the physical safety arena and security arena, and cybersecurity.

But as you point out, it is a complex system, and we now know what are the basic things that really need to be done across the board to protect and defend and make more resilient these critical assets and systems. Sometimes you have got to issue a mandate in order to make sure that everyone, not just those who are actively involved, but that everyone that is controlling, owning, and operating sensitive assets comes up to at least that basic standard of care, and then, very importantly, has plans in place to deal with any incident that might arise to reduce the impact and the harm to the American public and to our economy.

Ms. JACKSON LEE. Thank you.

Let me just quickly, on the—combine pipeline and planes together and just say, one of the things that we have looked at over the years is the apron, the back side of the airport, which, at that time, there was intrusion by uninvited guests, potential terrorists, because it was so vulnerable in the back.

But there are also the apron of a cybersecurity system as relates to flights, maybe even as it relates to the air traffic arena, but also the airlines that sort of run their own systems, and they have a cyber system now far different than this——

Mrs. WATSON COLEMAN. The gentlelady's time has expired. I will let you finish your comment, though. Thank you.

Ms. JACKSON LEE. Thank you. Thank you so very much.

So, in the future, if you could answer the question about that back side of the airport, and then as well, to tie the pipeline question into my rail question, which is pipelines are everywhere as well and do we have the adequate cyber protection for pipelines that wind up in our backyards?

I would yield back. If Madam Chair—I don't know if someone can answer it in very short period. I don't know. I would welcome that. Thank you. If anyone can answer those.

Mr. TROY. Yes. Very quickly, when you mention a back side of the airport, it makes me think so, really, the operational technologies that help an airport run.

Ms. JACKSON LEE. Right.

Mr. TROY. That is a very big focus of the airlines and the airports right now as they look at both the common suppliers to those particular types of technologies and the potential vulnerabilities as well.

Mrs. WATSON COLEMAN. Thank you, Mr. Troy.

Thank you, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much.

Mrs. WATSON COLEMAN. I now recognize Mr. Clyde of Georgia.

Mr. CLYDE. Thank you, Madam Chairwoman. I appreciate that.

My question is for Mr. Troy. As you well know, if the aviation sector were to experience a cyber attack, it could very well have a devastating impact on the security of our Nation and our economy. So, in your opinion, what is the greatest area of cyber threat in aviation? If I could have your opinion on that.

Is it the airport itself? Is it the—I mean, you talked a little bit about the planes. I think Madam Chairwoman discussed that. Then you also have the airlines themselves with, indeed, their own systems. You know, any part of that could shut down air travel across the United States in various different sectors.

What is your opinion, what is our greatest cyber threat when it comes to the aviation side?

Mr. TROY. That is a great question, and it is very difficult to answer because of the interconnectivity of the aviation system. It is really an ecosystem.

So if I am running an airline, I am very concerned that if I land my planes into my hub airport and that airport can't function, that creates a problem for me. If I am that airport, and I have the same problem if all those airlines are parked at my gates and they can't move because of some function that they are unable to perform.

So I am not trying to cop out on your question, but I really think it speaks exactly to why our industry needs to work so well together, because of this shared risk within supply chain and the industry segments that make up the aviation ecosystem.

Mr. CLYDE. OK. That is kind-of the area I am going to here because, looking at aviation, I just see that as a—you know, such a low-hanging fruit, because, as of yet, I have not really heard of a cyber attack on aviation that really had any effect. You know, it is a fantastic thing, and that is wonderful, but that means it just hasn't showed up yet.

So would any of our other witnesses want to chime in on what the aviation industry is doing or what the greatest vulnerability might be and how we could assist in mitigating that vulnerability?

Ms. COGSWELL. I am happy to sort-of build on the answer that was presented, which I completely agree with. I think one of the most undervalued points that has come from all of this is understanding how an impact to one part of a system can ripple across and affect the system as a whole. Taking that information and going back into the various individual company systems and those interconnected systems and better assessing what would that look like, and how do we make sure that we are quickly able to contain it and mitigate it should we see that start to occur.

Not the same at all, but I will draw a comparison to when Gatwick was actually shut down for several days because of unmanned aerial systems flying overhead. As you recall, they didn't actually harm anything, but they had periodic events where they just kept coming into the area. That clearly made it unsafe to fly, right? So they grounded all of the planes in the airport. It shut down that airport. It shut down flow to connecting airport.

Exactly as my colleague just said, big ripple effects, even for something that was not actually a kinetic, physical accident or dis-

ruption that they might think of seeing otherwise. Truly important for us as a model to understand that kind of interconnected model and how we can collectively work to defend our systems.

Mr. CLYDE. Well, thank you. Thank you very much. I appreciate your comments, Ms. Cogswell.

That is my great concern, and I appreciate each of you bringing your ideas to light.

With that, Madam Chairwoman, I yield back.

Mrs. WATSON COLEMAN. Thank you very much.

The gentlelady from New York, Miss Rice, is recognized for 5 minutes.

Miss RICE. Thank you so much, Madam Chair. I am so grateful for this hearing.

You know, listening to this conversation brings me back to 9/11. As a New Yorker, we felt the pain of that attack very intimately. I remember, in the days and weeks and months after 9/11, you know, which basically shut down the aviation industry for some time, and I remember wondering whether we are ever going to come back. Are people ever going to feel comfortable flying again?

Of course they did. But during that interim period, there was thoughts in, you know, law enforcement that what is going to be next? Like, what—the terrorists showed how they could attack us here on American soil and do it in a way that shut down an entire industry that had an enormous economic impact on our country for a long time.

And I remember, you know, talking to my friends in law enforcement in New York at that time, and they were thinking, gosh, do we have to worry about someone just walking into a mall, 3 or 4 different malls across this country? You want to talk about shutting down day-to-day economic activity. Make people afraid to even leave their homes.

I think what we are—the subject matter of today's hearing brings me to that—again to that issue of how we get people around safely and efficiently and all those things that our economy can hum, but we also do it in a way that keeps people safe.

So, Ms. Spaulding, I mean, I think it is pretty obvious why a mass transit system would be of interest to a foreign adversary. Up to this point, we haven't seen one that has had a massive safety impact, you know, but I guess my question is: How do we—you know, I worry about these transportation systems, because some of them are run by Governmental agencies and others are privately-run.

So when you are looking to come up with a system of protocols to keep us safe and prevent, whether it is cyber attacks or any other kind of attack, on our transportation system, how do we set up a system that can apply equally and effectively—as effectively to both the public and private sector?

Ms. SPAULDING. Yes, it is a great question. Your point about, you know, the aviation industry in the wake of 9/11, you know, is a reminder that—of the way in which an incident one place, in one part of an industry can destroy public trust in the entire industry. Again, one of the reasons that, you know, it is in these sectors' best interests to ensure that all of the players owning and operating key

assets are brought up to a baseline level of cybersecurity to protect the public trust in that entire industry.

In terms of Government, you know, are you—our critical infrastructure is, we always say, owned 85 percent by the private sector. Nobody knows what the exact percentage is, but that means that other percent is publicly-owned. There are a number of ways in which industry and Government come together. There are—for Government-owned utilities as well as private sector.

There is a multi-State ISAC that is for the States to come together to share best practices, including around operational technology they own. There is a Government coordinating council that includes State and local and territorial and Tribal government for governments to come together to talk about the things that they own. All of the various sectors that have coordinating committees have a Government counterpart.

So the mechanisms are there. You are absolutely right; as with every other area, we need to make sure we are harmonizing the requirements and that we are looking across these industries regardless of who owns them, because our adversaries are doing exactly that.

Miss RICE. Absolutely. You know, I know this is going to sound like a political pitch. It really is not meant to be, but, you know, our transportation security, there is a cyber—certainly a very profound cybersecurity aspect to it, but there is also an infrastructure aspect to it as well.

Do we have the—are our transportation systems as up-to-date and resilient and safe as they need to be? I know my Republican colleagues on this call feel the same way that I do, that, you know, major investment in our infrastructure shows not just Americans that they should be able to travel safely and feel confident in the way that they travel around this country and around the world, but it sends a very clear message to our adversaries that we are investing in our infrastructure and so they should beware.

So thank you all so much for coming today. It is a great conversation.

I yield back the balance of my time.

Mrs. WATSON COLEMAN. I thank the gentlelady.

I now recognize the gentleman and Ranking Member from Florida, Mr. Gimenez, for 5 minutes.

Mr. GIMENEZ. Thank you, Madam Chair.

I am going to kind-of focus in on an area that has got me concerned.

Mr. Dickerson, do you have, off the top of your head, either the correct number or maybe a guesstimate of the percentage of cranes that are utilized by U.S. ports that are made in China?

Mr. DICKERSON. Thank you, Congressman Gimenez. I do not have that, but it is a pretty significant number for those ship-to-shore gantry cranes that we rely on to move the goods from ships to shore and vice versa.

Mr. GIMENEZ. I have two concerns about that. No. 1, I know that in the Port of Miami, we do have some Chinese cranes, and we know that we had concerns about embedded in the software that came with the cranes was malware that was meant to penetrate

the port systems and do whatever it was that the Chinese wanted to do with our port operating systems. That is one concern.

The other concern that I have is that, whenever the Chinese want, they can cut off our supply of spare parts, which means that a significant portion of our ability to load and offload ships will be compromised if that were the case.

Do you know—do you have any thoughts on how we can mitigate the risk of infiltration into our port systems via these cranes and other either new or existing, you know, technologies at ports and infrastructure that ports need?

Mr. DICKERSON. Thank you again, sir. I think there is a few things, and those are very valid concerns. One is the ability to be able to conduct risk assessments immediately on that equipment. So CISA has the vulnerability architecture designer's views, data, program. But, quite honestly, often that is perhaps a 12- to 18-month waiting list period before you can actually conduct that review. In those cases, we need that equipment operational immediately upon arrival. There is not necessarily that time to waste.

So then it is an opportunity to perhaps engage in, as was mentioned earlier, some prequalified private-sector vendors that might be able to help augment CISA's functionality to conduct those reviews so that they can be done in a timely manner, and we can then identify if there is any vulnerabilities that need to be addressed.

Mr. GIMENEZ. Well, do you think that maybe we need to wean ourselves off of this dependence on Chinese technology that, again, comes from a sole source that could be our adversary?

I actually believe that it is the biggest threat that we have, is the ascendancy of China, that they could basically cut off our supply of spare parts and grind this country to a halt in terms of its import and export capabilities. So, in light of that, I am going to be introducing some legislation about that. We need other sources that are either allies or friendly nations and not so much of it coming from one source with China.

I understand what China did. They undercut everybody else in the world, and basically they are the sole provider of cranes around the world, which makes them a—I think it is a very, very dangerous practice and a very, very dangerous situation we have in the United States.

Would you agree with that?

Mr. DICKERSON. Yes, sir. I think there is some undercutting of the market taking place, and so having alternative sources and then being able to augment that with perhaps some grant programs that could allow then the private sector to make those investments reasonably would be helpful.

Mr. GIMENEZ. OK. Like I said, I will be introducing some legislation to try and wean us off of these Chinese cranes and other infrastructure needs at our ports that may be coming from adversary nations.

With that, my time is up, and thank you, Madam Chairwoman. I yield back.

Mrs. WATSON COLEMAN. Thank you.

I now recognize the gentlelady from Las Vegas, Ms. Titus.

Ms. TITUS. Thank you, Madam Chairman. A very interesting——

Mrs. WATSON COLEMAN. From Nevada. I am sorry. Nevada.

Ms. TITUS. Nevada.

Mrs. WATSON COLEMAN. I shouldn't be so myopic.

Ms. TITUS. That is all right. We answer to just about anything.

I wanted to address this question to Ms. Spaulding. You know, McCarran Airport in my district, Las Vegas, sees just thousands of passengers every year. We are probably the only airport that has got slot machines, so a lot of them are playing slot machines. But a lot of them are working on their computers while they are waiting for their flights.

I just wonder if you would address the need for security on those airport WiFis, because a lot of personal data is being floated around that we don't know if that is safe or not. Furthermore, when they get on the plane, they use the plane's WiFi. One of the biggest complaints is when the flight attendant says, "Our WiFi is down," you can hear all the groans and the Candy Crush players and all of that.

But could you address the issue of securing that kind of WiFi, either in the airport or on the planes where people are connecting to it and exposing a lot of personal data?

Ms. SPAULDING. Yes. Congresswoman, you are exactly right. We have all known that those public WiFi—free public WiFi availability in places like airports is completely insecure, and certainly have advised the public as best we can to be aware of that and not to use those.

But, realistically, they are going to continue to take advantage of the connectivity that is available to them. I think it is a very good point that those systems ought to be more secured. It is very difficult to have something that is open to a very transient population, right, coming and going, where you cannot use the security protocols that you can with a work force that is more stationary. So I don't mean to minimize the challenge, but I think it is something that we should be moving toward.

In the mean time, I hope that the public is watching and hearing how, at the moment, how unsecure those networks are.

Ms. TITUS. Well, thank you. I hope so too. I wish people were just reading books instead of playing computer games, but that is just my practice.

Along those same lines, a number of the airports have vendors that take your very personal data, and we see a lot of that at McCarran, like with the prevetting of customers. They take eyes—you know, you look in and you see your eyes and biometric data, and so I would think they would need some pretty high standards of cybersecurity.

I don't know if they are doing that. If you can comment on that, you and Ms. Cogswell, and how TSA is dealing with that.

Ms. SPAULDING. So I know that Patricia will have some insights on this as well. I am familiar with some of those vendors that are providing some of that vetting before you board the plane, for example, to speed you through the lines. They know that—how absolutely vital it is that they keep that information secure. That is very personal information. So my sense is they take cybersecurity very seriously. But I will see if Patricia has more to add.

Ms. TITUS. Thank you.

Ms. COGSWELL. Thank you very much for the question. I have actually been spending quite a bit of time on this since my departure from Government, working with—across the industry—airlines, airports, technology vendors, associations, and others about how we can encourage, frankly, an environment that holistically supports innovation for aviation passenger experience, making it, frankly, from couch to gate, a more pleasant experience, one that offers many different opportunities.

You are exactly right that there is a strong recognition that we need to embed several key things along the way, one of which is that cybersecurity protection so that people feel confident and comfortable about what is happening with their data. Along with that is the press also to make sure that there is a better recognition and a better way to have these vendors tell people what are they collecting, who are they sending it to, are they storing it, and how is it being used?

So all of these, I think, will form a core that we are hoping to continue to look to progress in this environment. There are standards that are used today. CBP has published a standard that is used by CBP and TSA for a number of those pilots that you are talking about where the biometric is collected and transmitted to use either for access to a lounge or to board the plane or go through security.

There are also additional new emerging standards, such as the mobile driver's license recently announced by TSA and Apple that also are coming through in these areas.

Across the board, you are seeing an emphasis on that cybersecurity. I expect that to continue to evolve.

Your earlier point, given that all of these are operating in that WiFi-connected area, that also matters, that they need to look at it as a zero-trust environment where the network itself is not secure and, therefore, the information needs to be secure while it is in transmission.

Ms. TITUS. Well, thank you so much.

Thank you, Madam Chairman. Maybe we can look into this.

Mrs. WATSON COLEMAN. Thank you very much.

I now recognize the gentleman from New Jersey, Mr. Van Drew.

Mr. VAN DREW. Thank you, Madam Chair. It is good to see you.

This is a question for Mr. Dickerson. Mr. Dickerson, as you may know, roughly 5.4 trillion flows through the Maritime Transportation System each and every year, which compromises about 25—comprises, rather, about 25 percent of the United States' gross domestic product.

The MTS consists of an intricate network of waterways, ships, ports, and terminals, and intermodal landline connections, which allow various modes of transportation to move goods and to move people. The Coast Guard is the lead Federal agency for regulation of the MTS, and it currently has the relationships, the regulatory authority, and the response capabilities to prevent and respond to threats throughout the system.

So my first question for you is: How can we best use the Coast Guard's existing relationships at the port level to improve our ability to manage cyber risk with the MTS?

Mr. DICKERSON. Thank you, Congressman Van Drew. There is a couple of things that can be done. We already have the Area Maritime Security Committees that are active in almost all the captain of the port areas with a cybersecurity subcommittee that addresses risks. Currently, those are supported by a variety of folks with different skill levels when it comes to cybersecurity and knowledge levels at the Coast Guard level. But they are trying to hire more MTS cyber specialists into each captain of the port area which could then support those Area Maritime Security Committees.

With those committees, you have both public and private-sector stakeholders that are engaged, and they can be involved in risk planning, exercises, et cetera. One of the things the MTS–ISAC is doing, we have formed a number of information exchanges with those local stakeholders to make sure the public and private sectors are really aware of the day-to-day cyber threat activity that is targeting them.

So that helps bridge that gap between the AMSC, which might be more at a strategic level than the actual operational and tactical levels of cybersecurity that go on day-to-day. But that is definitely an area of focus that can be improved.

Thank you so much.

Mr. VAN DREW. Good. I think the Coast Guard can be very essential in this entire process, and as we move on and times change and things change, so does their role, and I think this is an area we really should focus on as well. I appreciate your answer.

I have another question for you. Members of the committee have received feedback that public-private partnerships are, unfortunately, sometimes turning into situations in which companies do give their information, as they should, to the Government, but they are not receiving anything meaningful in return. In other words, that collaboration that we want to see back and forth, I have heard, does not always exist. It should, because this is a very larger-than-life foe that we have to deal with here, and we all need to work together.

I was wondering what your thoughts on that were and how we can do better with that.

Mr. DICKERSON. Thank you, Congressman, again. Public-private partnerships are absolutely critical. This is—cyber is a team sport, and we all need to work together, absolutely. We need to work together cross-sector-wise as well, which is why the MTS–ISAC is part of the National Council of ISACs.

But when it comes to partnering with the Coast Guard, yes, we have received that feedback many times. Coast Guard receives the information, but then it might be months before any information is released from the Coast Guard back to the industry community.

I think closer partnerships—and I am in multiple conversations with a number of Coast Guard leaders, and we are working on improving that public-private partnership, making sure that we can mature those procedures that are in place, to analyze the information, enrich it, and get it back from the Government in a more timely manner.

Mr. VAN DREW. I think they want to do that. I think there is really unexplored areas there that we can really do great things together. Coast Guard is a great agency, as you know, and I think

they really can offer a great deal if we are working in tandem, if we are working in partnership. I thank you for your answers.

I yield back, Madam Chair.

Mr. DICKERSON. I completely agree. Thank you, sir.

Mrs. WATSON COLEMAN. Thank you, Mr. Van Drew. Thank you.

I now recognize the gentleman from New York, Mr. Torres, for 5 minutes.

Mr. TORRES. Thank you, Madam Chair.

You know, I have concerns that the United States for far too long has been complacent about cybersecurity instead of proactively securing critical infrastructure from cyber threats. The Federal Government is largely reacting to events. Colonial Pipeline is exhibit A. Before the breach of Colonial Pipeline, there were virtually no rules mandating pipeline cybersecurity. Only after the Colonial breach did the TSA finally issue security directives.

So as far as I am concerned, the breach of Colonial Pipeline demonstrates the laissez-faire approach to cybersecurity that the Federal Government has taken has been an abject failure.

My first question is for Ms. Spaulding about TSA. Instead of only issuing a security directive for each mode of transportation, should the TSA promulgate universal cybersecurity standards for all modes of critical transportation?

Ms. SPAULDING. It is a good question, Congressman. First of all, I think the security directives are a first step from TSA, and DHS has indicated that it is very likely to move to regulations. The security directives have a limited life span, and within a year or so, they have to be replaced. DHS has indicated it is likely to move to regulations.

That will allow for a formal notice and comment period. I think it is really important that there be some harmonization across sectors, as a number of the witnesses have noted. That is really important, particularly for companies that have assets that cross sectors. But I think there should be room—there may be need for some specialized requirements depending on the nature of the operations.

Mr. TORRES. I don't mean to—if I can interject for a moment. Obviously, there is a need for sector-specific standards, but there are best practices in cybersecurity that all individuals and institutions should adopt in both the public and private sector, whether it is the appointment of a CISO or multifactorial authentication or software updates or password updates or contingency planning.

So if we all—if those are universally agreed-upon best practices in cybersecurity, why not mandate them for all operators and owners of critical transportation infrastructure?

Ms. SPAULDING. Yes. You are absolutely right, Congressman. There is some basic cyber hygiene, we call it, that should be universal. I think the admonition that one of the witnesses made earlier, to do this in a phased approach makes sense. I think identifying what DHS has indicated is they are going to start with the most critical assets. I think that makes a lot of sense, to get the Government and industry to learn lessons about how to do this in terms of mandatory compliance with directives, how to monitor that, how to enforce that mandatory reporting.

But, yes, you are absolutely right, there is a baseline of cybersecurity that ought to be universal.

Mr. TORRES. You mentioned reporting. The policy of cyber incident reporting raises the question, what exactly qualifies as a significant cyber incident, and there is a lack of clarity about the definition.

So take as an example the Colonial Pipeline. As you know, the breach of the pipeline led to the shutdown for a 5,500-mile pipeline that made up nearly half of the fuel supplies of the East Coast. It had economic effects that were felt on the ground: The closing of gas stations, panic buying, long lines.

Despite those effects, the Federal Government did not designate the Colonial breach as a significant cyber incident. Like, in what universe does that make sense? It seems strange to me.

Ms. SPAULDING. So the designation of a significant cyber incident is more of a signal to the Government about the need for an interagency, White House-led meeting to deal with the response, right? I think there is a legitimate question about what—where you should set the threshold, for example, for mandatory reporting, but ransomware, it seems to me, is an easy threshold to set.

Mr. TORRES. So do you agree with the Federal Government's decision not to designate the Colonial breach as a significant cyber incident? Because, I mean, that situation, I mean, did implicate a number of agencies. It even reached the attention of the President himself. So it would seem to have all the hallmarks of a significant cyber incident.

Ms. SPAULDING. You know, Congressman, I am inclined to agree with you, is that the level of interagency meeting that was probably happening at the White House, it strikes me as probably very much the same as a significant cyber incident. I do think that should be separated from the thresholds that are set for mandatory reporting.

Mr. TORRES. I just feel like we need a greater sense of urgency and more common sense when it comes to cybersecurity policy in the Federal Government. So I will leave it at that.

Thank you.

Mrs. WATSON COLEMAN. Thank you, Mr. Torres.

I would like to recognize Mr. Langevin from Rhode Island for 5 minutes.

Mr. LANGEVIN. Thank you, Madam Chair. I have been on and off the hearing, so in between the meeting, so I thank you and the other Members for hosting the hearing. I really want to thank our witnesses for their testimony.

If I could start with Ms. Spaulding. First of all, Ms. Spaulding, I greatly appreciate your contributions to cyber and our National security writ large, both in your role at DHS and, of course, as one of our fellow commissioners on the Cyberspace Solarium Commission.

But let me just start with this. On October 19, several of the Senators sent a letter to TSA Administrator Pekoske encouraging him to reconsider using emergency authority for new transportation cybersecurity regulations in—and I quote, "the absence of an immediate threat."

So I am not sure if my colleagues were watching the news in May, but the Colonial Pipeline incident obviously disrupted the delivery of approximately half of the East Coast's fuel supply. Ransomware or other cyber intrusion against an air traffic control station or a mass transit system could be equally debilitating.

So I wanted to ask, if I could, do you believe TSA's new cybersecurity requirements on the rail—rail transit and aviation industries was warranted given the imminent threats that we face?

Ms. SPAULDING. Congressman, first, thank you for your kind words. Most importantly, thank you for your leadership over many years in cybersecurity, and it has been an honor to serve with you on the Cyberspace Solarium Commission.

I do believe that there is an emergency here, a sense of urgency. We are fortunate that TSA has this authority to be able to move quickly and that it has exercised that authority.

I think it is probably fair to say that, on May 6, Colonial Pipeline was not thinking that this was an urgent threat. In fact, there are reports that they had been putting off their vulnerability architecture design review. They just weren't getting around to it. That is the kind-of, you know, September 10 mindset that we are trying to avoid here.

We have so much evidence of this emergency, between the attacks in 2017 on safety systems that were clearly designed to be ready to inflict physical harm on people by disabling safety systems and operations. The Florida water treatment—the attack on the Florida water treatment facility, putting toxic levels of chemicals—trying to put toxic levels of chemicals into water. I think the sense of urgency should be palpable and felt by everyone by now.

Mr. LANGEVIN. Thank you. I would agree.

Let me turn to another line of questioning on third-party auditing. So again to you, the TSA pipeline security directives require baseline cybersecurity procedures such as reporting incidents, implementing multifactorial authentication, and developing and testing cyber contingency response plans. So in my view, these requirements are a good start, but more, candidly, should be done. I also believe that TSA should implement auditing of the cybersecurity controls covered entities have put in place.

So an impartial third-party auditor, such as a certified private-sector company or even CISA, would have both the impartiality and the on-network testing personnel necessary to ensure covered entities properly implement cybersecurity controls.

So from your experience and your perspective, do you believe TSA should incorporate third-party auditing into future cybersecurity requirements and why, if you could?

Ms. SPAULDING. I do, Congressman. As you point out, we have numerous other places throughout the Government where third parties help to scale an effort that is put in place by the Government. My colleague here today, Patricia Cogswell, has made that comparison to the third party—the role of third parties in canine certification, for example.

So there is precedent for this, and I think it is an important way to scale. Our industry witnesses have talked about the need for speed in some of these certifications and for the Government to do

the things it needs to do, and we know that CISA's resources are stretched.

Mr. LANGEVIN. Thank you very much.

I see my time has expired, so I am not going to add to my other two questions. But maybe I can submit them for the record, one on exploiting TSA regulations in other—to other sectors. The other one was on Government-sponsored testing of critical technologies. So I will submit those for the record, Madam Chair. Thank you. I yield back.

Thank you for your answers too, Suzanne, and to all our witnesses too. Thank you.

Madam Chair, you are on mute.

Mrs. WATSON COLEMAN. Thank you, Mr. Langevin. Thank you very much.

I want to thank the witnesses, not only for your very important expert testimony, but your forbearance during our delay. Thank you. We appreciate it.

Thank the Members for all of their questions today.

The Members of the subcommittees may have additional questions—as Mr. Langevin has noted he will—for you, and we ask that you respond expeditiously in writing to those questions. The Chair reminds the Members of the subcommittees that the committee's records will remain open for 10 days.

And so, with that, without objection, the subcommittees stand adjourned. Good day.

[Whereupon, at 5:01 p.m., the subcommittees were adjourned.]

○