CYBER THREATS IN THE PIPELINE: LESSONS FROM THE FEDERAL RESPONSE TO THE COLONIAL PIPELINE RANSOMWARE ATTACK

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

AND THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY HOUSE OF REPRESENTATIVES

OF THE

COMMITTEE ON HOMELAND SECURITY

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JUNE 15, 2021

Serial No. 117–18

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

45–310 PDF WASHINGTON : 2021

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

CYBER THREATS IN THE PIPELINE: LESSONS FROM THE FEDERAL RESPONSE TO THE COLONIAL PIPELINE RANSOMWARE ATTACK

Tuesday, June 15, 2021

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

The subcommittee met, pursuant to notice, at 2:37 p.m., via Webex, Hon. Bonnie Watson Coleman [Chairwoman of the Subcommittee on Transportation & Maritime Security] presiding.

Present: Representatives Clarke, Watson Coleman, Langevin, Titus, Slotkin, Gottheimer, Rice, Luria, Thompson (ex officio), Garbarino, Gimenez, Van Drew, Harshbarger, Miller-Meeks, Clyde, and LaTurner.

Mrs. WATSON COLEMAN. The Subcommittee on Transportation & Maritime Security and the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will come to order for today's hearing titled "Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack."

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

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

The impacts of the May 7 ransomware attack on Colonial Pipeline were far-reaching. As we all know now, nearly half of the East Coast's fuel is supplied by the Colonial Pipeline. When the pipeline was shut down, Americans struggled to fill up their gas tanks, and the incident threatened to cause major disruptions to the economy and well-being of our country. That is why it is so important for us to have a conversation today about the Federal Government's response to the Colonial incident and its role in ensuring the cybersecurity of our critical infrastructure.

Last week, we heard from the CEO of Colonial Pipeline about how his company responded to the ransomware attack against it. I also asked him why his company, prior to the attack, appears to have resisted TSA's efforts to assess its pipeline security prior to the attack.

Today, we will hear from TSA and CISA, the DHS components that are charged with ensuring the cybersecurity of our Nation's pipelines and responding to cyber incidents. I am looking forward to learning, not only about TSA and CISA's engagement with Colonial before and after this incident, but also about their plans to ensure we are better prepared next time. Unfortunately, we know that there will be a next time.

In recent weeks, we have seen 2 transportation systems fall victim to ransomware attacks in New York City and in Massachusetts. Hospitals have been brought to a halt. Even one of our Nation's largest meat-packers was shut down.

We must ask ourselves what is next. Our power grid? Our aviation system? Maybe the next time it won't be foreign hackers looking for a quick payday but, rather, a nation-state looking to cripple our economy. Given the magnitude of these threats, we need to ensure CISA and sector-specific agencies like TSA have the tools and the authorities that they need to take action and that they use them.

In the pipeline context, since TSA's establishment nearly 20 years ago, it has been the principal Federal entity responsible for pipeline security. To this end, TSA publishes pipeline security guidance and conducts pipeline security assessments and inspections, including assessments that focus specifically on cybersecurity. To date, these assessments have been voluntary and, unfortunately, voluntary standards have proven insufficient.

According to TSA, prior to the attack, TSA had asked Colonial Pipeline on no less than 13 occasions to participate in physical and cyber pipeline security assessments. Citing COVID–19, Colonial repeatedly delayed and chose not to participate. On multiple occasions Colonial didn't even bother responding to TSA's emails. In fact, Colonial still has not agreed to participate in a physical assessment, and only agreed to cooperate with TSA's cybersecurity assessment 3 weeks after the ransomware attack occurred.

What's more, when a Member of this committee asked Colonial's CEO whether he would accept CISA's assistance, he politely but firmly declined. If this is at all indicative of how pipeline owners and operators view their regulators and their Federal partners, we have a problem. Although many of these systems may be owned by private companies, when you operate infrastructure that we all depend on, you have a responsibility to the public.

The good news is that the TSA administrator has existing authority—statutory authority—to address this. Just a few weeks ago, TSA used this authority to impose the first mandatory cybersecurity requirements on pipeline owners and operators. Specifically, now they must report breaches, designate cybersecurity coordinators, and self-assess their compliance with TSA security guidance.

This is an important first step, but there is clearly more that needs to be done. We must resource and empower TSA and CISA to act boldly and swiftly to ensure operators of pipelines and all other forms of transportation harden their systems. Meanwhile, it is similarly important that other agencies in the Federal Government respect TSA and CISA's experience and expertise on these matters.

The cybersecurity of our critical infrastructure is too serious for us to reinvent the wheel by providing duplicative authorities to the Department of Energy. DHS has the existing statutory authority and technical talent that we need to tackle this challenge.

Finally, before I conclude, I must note my disappointment that the FBI declined an invitation to attend this hearing. It is critical that Members fully understand the FBI's role and efforts to counter cyber threats, and I look forward to their participation in future events on these topics.

That said, I am looking forward to hearing from today's witnesses about how the attack on Colonial Pipeline will inform their approaches going forward.

[The statement of Chairwoman Watson Coleman follows:]

STATEMENT OF CHAIRWOMAN BONNIE WATSON COLEMAN

JUNE 15, 2021

The impacts of the May 7 ransomware attack on Colonial Pipeline were far-reaching. As we all know now, nearly half of the East Coast's fuel is supplied by the Colonial Pipeline. When the pipeline was shut down, Americans struggled to fill up their gas tanks, and the incident threatened to cause major disruptions to the economy and well-being of our country. That's why it's so important for us to have a conversation today about the Federal Government's response to the Colonial incident and its role in ensuring the cybersecurity of our critical infrastructure.

Last week, we heard from the CEO of Colonial Pipeline about how his company responded to the ransomware attack against it. I also asked him why his company, prior to the attack, appears to have resisted TSA's efforts to assess the pipeline's security prior to the attack. Today, we will hear from TSA and CISA—the DHS components charged with ensuring the cybersecurity of our Nation's pipelines and responding to cyber incidents. I am looking forward to learning not only about TSA and CISA's engagement with Colonial before and after this incident, but also about their plans to ensure we are better prepared next time. Unfortunately, we know there will be a next time.

In recent weeks, we've seen 2 transportation systems fall victim to ransomware attacks in New York City and Massachusetts. Hospitals have been brought to a halt. Even one of our Nation's largest meatpackers was shut down. We must ask ourselves: What's next? Our power grid? Our aviation system? Maybe next time it won't be foreign hackers looking for a quick pay day, but rather a nation-state looking to cripple our economy. Given the magnitude of these threats, we need to ensure CISA and sector-specific agencies like TSA have the tools and authorities they need to take action—and that they use them.

In the pipeline context, since TSA's establishment nearly 20 years ago, it has been the principal Federal entity responsible for pipeline security. To this end, TSA publishes pipeline security guidance and conducts pipeline security assessments and inspections—including assessments that focus specifically on cybersecurity. To date, these assessments have been voluntary—and unfortunately, voluntary standards have proven insufficient.

According to TSA, prior to the attack TSA asked Colonial Pipeline on no less than 13 occasions to participate in physical and cyber pipeline security assessments. Citing COVID–19, Colonial repeatedly delayed and chose not to participate. On multiple occasions, Colonial didn't even bother responding to TSA's emails. In fact, Colonial still has not agreed to participate in the physical assessment, and only agreed to cooperate with TSA's cybersecurity assessment 3 weeks after the ransomware attack occurred. What's more, when a Member of this committee asked Colonial's CEO whether he'd accept CISA's assistance, he politely but firmly declined. If this is at all indicative of how pipeline owners and operators view their regulators, we have a problem.

Although many of these systems may be owned by private companies, when you operate infrastructure that we all depend on, you have a responsibility to the public. The good news is that the TSA administrator has existing statutory authority to address this. Just a few weeks ago, TSA used this authority to impose the first mandatory cybersecurity requirements on pipeline owners and operators. Specifically, now they must report breaches, designate cybersecurity coordinators, and self-assess

their compliance with TSA's security guidance. This is an important first step, but there is clearly more that needs to be done.

We must resource and empower TSA and CISA to act boldly and swiftly to ensure operators of pipelines and all other forms of transportation harden their systems. Meanwhile, it is similarly important that other agencies in the Federal Government respect TSA and CISA's experience and expertise on these matters. The cybersecurity of our critical infrastructure is too serious for us to reinvent the wheel by providing duplicative authorities to the Department of Energy. DHS has the existing statutory authority and technical talent we need to tackle this challenge.

Finally, before I conclude, I must note my disappointment that the FBI declined an invitation to attend this hearing. It is critical that Members fully understand the FBI's role and efforts in countering cyber threats, and I look forward to their participation in future events on these topics.

Mrs. WATSON COLEMAN. The Chair now recognizes the Ranking Member of the Subcommittee on Transportation & Maritime Security, the gentleman from Florida, for an opening statement.

Mr. GIMENEZ. Thank you, Chairwoman Watson Coleman, Chairwoman Clarke, and Ranking Member Garbarino.

I am pleased that the CIPI and TMS subcommittees are holding this joint hearing today on cyber threats to pipelines. As we saw with the recent ransomware attack on the Colonial Pipeline, securing our Nation's 2.7 million miles of pipeline is of utmost importance.

I look forward to hearing today from Mr. Eric Goldstein of CISA and Ms. Sonya Proctor of TSA on how CISA and TSA work together to ensure pipelines are secure from cyber threats. I thank the witnesses for their time today.

I am interested to hear from TSA on the pipeline industry's compliance with the security directive that TSA issued last month. I look forward to Ms. Proctor detailing what plans TSA has for additional directives in the near future.

I am concerned with the approach to move pipeline security oversight from the Department of Homeland Security and into the Department of Energy. I wholeheartedly agree that there is more that TSA can do in terms of increasing its resources and expertise, but I believe TSA or the Department of Homeland Security is the appropriate agency to oversee pipeline security.

TSA's close corroboration with CISA serves to ensure that there is a strong DHS effort in securing all transportation modes against cyber threats. As a committee, we need to continue to strengthen our Nation's cybersecurity by strengthening CISA and giving them all the tools and responsibilities needed to keep all of our cyber infrastructure safe and secure.

I look forward to the discussion today of finding ways to improve security of our Nation's pipelines against continued threats of cyber attacks and, frankly, all of our Nation's security threats and how we can protect the United States of America from cyber threats in the future.

Madam Chairwoman, I also share your displeasure that the FBI did not participate today.

Thank you, Madam Chairwoman. I yield back the balance of my time.

[The statement of Ranking Member Gimenez follows:]

STATEMENT OF RANKING MEMBER CARLOS A. GIMENEZ

Thank you, Chairwoman Watson Coleman, Chairwoman Clarke, and Ranking Member Garbarino. I am pleased that the CIPI and TMS subcommittees are holding

this joint hearing today on cyber threats to pipelines. As we saw with the recent ransomware attack on Colonial Pipeline, securing our Nation's 2.7 million miles of pipeline is of utmost importance.

I look forward to hearing today from Mr. Eric Goldstein of CISA and Ms. Sonya Proctor of TSA on how CISA and TSA work together to ensure pipelines are secure from cyber threats. I thank the witnesses for their time today.

I am interested to hear from TSA on the pipeline industry's compliance with the Security Directive that TSA issued last month. I look forward to Ms. Proctor detailing what plans TSA has for additional directives in the near future.

I am concerned with the push to move pipeline security oversight from the Department of Homeland Security and into the Department of Energy. I wholeheartedly agree that there is more that TSA can do in terms of increasing its resources and expertise, but I believe TSA or the Department of Homeland Security are the appropriate agency to oversee pipeline security.

TSA's close collaboration with CISA serves to ensure that there is a strong DHS effort in securing all transportation modes against cyber threats. As a committee we need to continue to strengthen our Nation's cybersecurity by strengthening CISA and giving them all the tools and responsibilities needed to keep all of our cyber infrastructure safe and secure.

I look forward to the discussion today and finding ways to improve the security of our Nation's pipeline against the continued threat of cyber attacks and frankly, all of our Nation's security threats and how we can protect the United States from cyber attacks in the future. Madam Chairwoman, I also share your displeasure that the FBI did not participate today. Thank you, Madam Chairwoman, and I yield back the balance of my time.

Mrs. WATSON COLEMAN. Thank you, Ranking Member.

The Chair now recognizes the Chairwoman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, the gentlelady from New York, for an opening statement.

Ms. CLARKE. I thank you, Madam Chairwoman, Bonnie Watson Coleman. To Ranking Members Gimenez and Garbarino, I thank you for working with me on today's hearing, and to our witnesses for joining us today.

The ransomware attack on Colonial Pipeline was a reminder to us all that cyber attacks can do more than compromise our data. We have seen ransomware attacks cripple hospitals, manufacturers, municipalities, and meat packers. We have seen ransom demands skyrocket, operations brought to a standstill, and organizations left without many viable options aside from paying an unknown group of criminals who may or may not be subject to U.S. sanctions.

Unfortunately, the takeaway for many of our criminals behind these attacks is ransomware is easy money. These attacks are not the stuff of SolarWinds. They are simple, unsophisticated, and rely on common cybersecurity missteps present in most organizations.

I say this not to be fatalistic but to acknowledge the tremendous challenge we face. These attacks are not going to slow down, and adversaries have learned that the higher the stakes for the victim, the higher the payout they will likely get.

If there is one message I hope to drive home today it is that this administration needs to have a plan for responding to cyber incidents and be ready to execute that plan at a moment's notice, specifically the National Cyber Incident Response Plan, which lays out clear roles for CISA, FBI, and other parts of the Federal Government that play a role in responding to cyber attacks on critical infrastructure.

We also have long-standing directives, like PPD–21 and PPD–41, that makes CISA responsible for coordinating Federal efforts to secure critical infrastructure and doing so hand-in-hand with Sector

Risk Management agencies like TSA, which oversees security for the pipeline sector.

It appears the administration deviated from that plan in a number of ways, and I want to understand why that happened and what is being done to fix it. I want to see this administration become a well-oiled machine when it comes to responding to these attacks because that is what will be demanded moving forward.

The second point I hope to make today is this: Although CISA has come a long way in a short amount of time, there is still parts of its mission that we need to clarify, and there are parts of its mission that we need to authorize and resource commensurate to the enormous job we are asking this new agency to do.

Right now, CISA is tasked with leading asset response activities during a significant cyber incident, but what if the victim organization hires FireEye instead? What if they decline CISA's offer to provide technical assistance and delay or refuse to share information about the incident with CISA? What if they never report the incident to the Federal Government in the first place?

This undermines our National security. CISA needs access to information it can use to understand the threat landscape and develop technical indicators that will help other entities prepare for similar attacks.

As I have said before, I am working on legislation that will require critical infrastructure to report certain cybersecurity incidents to CISA, so that we are developing the muscle memory and the institutional knowledge to improve our cyber defenses over time. But this is only half of the battle. CISA also needs real-time visibility into threats on private-sector networks, so they are empowered to collaborate with owners and operators before, during, and after an attack, or prevent the attack from happening in the first place.

This is especially true for the industrial control systems that power pipeline operations, energy generation, and countless other industrial functions we rely on each and every day. These systems are increasingly connected to business and IT networks, which makes them vulnerable, and simply severing those connections is not always feasible.

For the past few years, CISA has been piloting a program called CyberSentry that gives CISA the ability to monitor and detect cyber threats on participating critical infrastructure partner networks and work proactively with owners and operators to address threats in real time. This is exactly the kind of operational role that Congress envisioned CISA playing on critical infrastructure cybersecurity, and I am currently working on legislation to strengthen and codify these efforts.

I would be remiss if I did not mention that the Federal Government can only do so much. We need private-sector critical infrastructure to step up, not just by investing in their own cybersecurity, but also by partnering with the Federal Government. We need the private sector to open the door to CISA and TSA, not just because it benefits them, but because it benefits our collective National security.

In conclusion, I will also echo the Chairwoman's disappointment and our Ranking Member's disappointment that the FBI declined

our invitation to participate in today's hearing. You cannot espouse the virtues of a whole-of-Government response 1 minute and then refuse to appear before the Congress with your interagency partners the next. But I, nevertheless, look forward to hearing from the DHS officials who have answered the call to testify before us today.

With that, Madam Chairwoman, I yield back.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

JUNE 15, 2021

The ransomware attack on Colonial Pipeline was a reminder to us all that cyber attacks can do more than compromise our data. We've seen ransomware attacks cripple hospitals, manufacturers, municipalities, and meatpackers. We've seen ransom demands skyrocket, operations brought to a standstill, and organizations left without many viable options aside from paying an unknown group of criminals who may or may not be subject to U.S. sanctions. Unfortunately, the takeaway for many of criminals behind these attacks is: Ransomware is easy money.

These attacks are not the stuff of SolarWinds—they're simple, unsophisticated, and rely on common cybersecurity missteps present in most organizations. I say this not to be fatalistic, but to acknowledge the tremendous challenge we face. These attacks are not going to slow down—and adversaries have learned that the higher the stakes for the victim, the higher the payout they'll likely get.

If there is one message I hope to drive home today, it's that this administration needs to have a plan for responding to cyber incidents, and be ready to execute that plan in a moment's notice. Specifically, the National Cyber Incident Response Plan—which lays out clear roles for CISA, FBI, and other parts of the Federal Government that play a role in responding to cyber attacks on critical infrastructure. We also have long-standing directives, like PPD–21 and PPD–41, that make CISA responsible for coordinating Federal efforts to secure critical infrastructure, and doing so hand-in-hand with Sector Risk Management agencies like TSA, which oversees security for the pipeline sector.

It appears the administration deviated from that plan in a number of ways—and I want to understand why that happened, and what's being done to fix it. I want to see this administration become a well-oiled machine when it comes to responding to these attacks—because that's what will be demanded moving forward. The second point I hope to make today is this: Although CISA has come a long way in a short amount of time, there are still parts of its mission that we need to clarify. And, there are parts of its mission that we need to authorize and resource commensurate to the enormous job we're asking this new agency to do.

Right now, CISA is tasked with leading asset response activities during a significant cyber incident—but what if the victim organization hires FireEye instead? What if they decline CISA's offer to provide technical assistance and delay or refuse to share information about the incident with CISA? What if they never report the incident to the Federal Government in the first place? This undermines our National security. CISA needs access to information it can use to understand the threat landscape and develop technical indicators that will help other entities prepare for similar attacks.

As I've said before, I'm working on legislation that will require critical infrastructure to report certain cybersecurity incidents to CISA so that we're developing the muscle memory and the institutional knowledge to improve our cyber defenses over time. But this is only half the battle. CISA also needs real-time visibility into threats on private-sector networks, so they're empowered to collaborate with owners and operators before, during, and after an attack—or, prevent the attack from happening in the first place.

This is especially true for the industrial control systems that power pipeline operations, energy generation, and countless other industrial functions we rely on every day. These systems are increasingly connected to business and IT networks, which makes them vulnerable—and simply severing those connections is not always feasible.

For the past few years, CISA has been piloting a program called CyberSentry that gives CISA the ability to monitor and detect cyber threats on participating critical infrastructure partner networks, and work proactively with owners and operators to address threats in real time. This is exactly the kind of operational role that Congress envisioned CISA playing on critical infrastructure cybersecurity, and I am cur-

rently working on legislation to strengthen and codify these efforts. I would be remiss if I did not mention that the Federal Government can only do so much.

We need private-sector critical infrastructure to step up—not just by investing in their own cybersecurity, but also by partnering with the Federal Government. We need the private sector to open the door to CISA and TSA—not just because it benefits them, but because it benefits our collective National security. In conclusion, I will echo the Chairwoman's disappointment that the FBI declined our invitation to participate in today's hearing. You cannot espouse the virtues of a whole-of-Government's response 1 minute, then refuse to appear before Congress with your interagency partners the next.

Mrs. WATSON COLEMAN. I thank the gentlelady from New York.

I now recognize the Ranking Member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, the gentleman from New York, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman.

First, I would like to thank you, as well as Chairwoman Clarke and Ranking Member Gimenez, for calling this important hearing. I thank our witnesses for being here today.

Last week's full committee hearing on this topic was an important opportunity to peer into the decision-making process at Colonial and to better understand the business or victim-facing side of an attack. This week's hearing affords us a unique opportunity to closer examine the Federal Government's coordination and response efforts following an attack.

While Ranking Member Katko, myself, and our partners on the other side of the aisle have all expressed concern with the White House's decision to have the Department of Energy leading the Federal response to this attack instead of CISA and TSA as the lead agencies for the pipeline sector, we should all recognize that the decision was not any of yours to make. We are very appreciative of your efforts in response to this hack and many others, but there are clearly still many questions regarding this attack that need answers, and I hope we are able to get clarity on the outstanding issues here today.

I am also interested in learning more about the value CISA is providing to industry leadership such as organization CEOs and CIOs. CISA provides a treasure trove of helpful guidance and resources for organizations to bolster their cyber posture, but it is increasingly clear that it should be hitting the desks of our Nation's CEOs and CIOs who are making the tough investment decisions.

While many of the Members of our subcommittees understand the inherent value that CISA provides to agencies and industry alike, the truth is that CISA still has a lot to prove to the Hill, and it is important that you all are able to demonstrate that value. As the newest agency with the newest department, you are going to have to be forceful in staking your claim to ensure you are all leading the charge on major cyber incidents.

The White House also shoulders some responsibility. It must empower CISA with the stature to be successful and appropriately delineate responsibilities between CISA, the Sector Risk Management agencies, and the incoming National cyber director. Cyber threats are rarely isolated to one sector, but CISA's role as the central agency that can connect the dots and share threat information across multiple sectors will help secure all critical infrastructure across our Nation.

It is also important that you all are not bashful when it comes to highlighting areas that need strengthening and areas that require additional resources, personnel, or authorities.

Thank you all for being here today. I yield back.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW R. GARBARINO

I thank our Chairs for calling this important hearing, and I thank our witnesses for being here today.

Last week's full committee hearing on this topic was an important opportunity to peer into the decision-making process at Colonial and to better understand the business or victim-facing side of an attack.

This week's hearing affords us a unique opportunity to closer examine the Federal Government's coordination and response efforts following an attack.

While Ranking Member Katko, myself, and our partners on the other side of the aisle have all expressed concern with the White House's decision to have the Department of Energy leading the Federal response to this attack, instead of CISA and TSA as the lead agencies for the pipeline sector, we should all recognize that the decision was not any of yours to make. We are very appreciative of your efforts in response to this hack, and many others.

But there are clearly still many questions regarding this attack that need answers, and I hope we're able to get clarity on the outstanding issues here today.

I'm also interested in learning more about the value CISA is providing to industry leadership, such as organization CEOs and CIOs. CISA provides a treasure trove of helpful guidance and resources for organizations to bolster their cyber posture, but it's increasingly clear that it should be hitting the desk of our Nation's CEOs and CIOs, who are making the tough investment decisions.

While many of the Members of our subcommittees understand the inherent value that CISA provides to agencies and industry alike, the truth is that CISA still has a lot to prove to the Hill, and it's important that you all are able to demonstrate that value.

As the newest agency within the newest department, you are going to have to be forceful in staking your claim to ensure you all are leading the charge on major cyber incidents. The White House also shoulders some responsibility. It must empower CISA with the stature to be successful and appropriately delineate responsibilities between CISA, the Sector Risk Management agencies, and the incoming National cyber director. Cyber threats are rarely isolated to one sector, thus CISA's role as the central agency that can connect the dots and share threat information across multiple sectors will help secure all critical infrastructure across our Nation.

It is also important that you all are not bashful when it comes to highlighting areas that need strengthening, and areas that require additional resources, personnel, or authorities.

Thank you all for being here today.

Mrs. WATSON COLEMAN. Thank you very much to the Ranking Member.

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

The Chair now recognizes the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much.

Good afternoon. I want to thank Chairwoman Watson Coleman and Chairwoman Clarke for holding this important hearing on the Federal response to the recent ransomware attack on Colonial Pipeline.

The attack on May 7 that resulted in a week-long shutdown of 5,500 miles of petroleum pipeline on the East Coast clearly represents a significant cyber attack on critical transportation infrastructure. It is clear that the future will bring more attacks like

this, whether they are by organizations like DarkSide that seek to exploit cybersecurity weaknesses for profit or foreign enemies seeking to weaken our Nation. The Federal Government must be prepared to fight off attacks and respond to successful security breaches swiftly and effectively.

The Cybersecurity and Infrastructure Security Agency is the lead Federal coordinator for securing critical infrastructure from cyber attacks, and the Transportation Security Administration is the designated Sector Risk Management agency for pipelines. Yet Colonial failed to properly engage with TSA in recent months in order to safeguard their pipeline against attacks, and repeatedly rejected technical assistance from CISA following the ransomware incident.

While I am pleased that Colonial has finally agreed to a virtual cybersecurity assessment from TSA, I am alarmed that they refused to do so until 3 weeks after an attack that resulted in the full shutdown of their pipeline. Despite authority placed within the Department of Homeland Security to respond to cyber attacks on pipelines, including through TSA's authority to issue emergency security directives, the Department of Energy was made the lead agency for response to the Colonial incident.

Additionally, the Federal Government did not deem the attack a significant cyber incident, as defined by policy, despite its substantial impact. If you don't believe me, ask those folks who were trying to find gasoline all over, everywhere, while this event was going on. It was a significant cyber event.

Cyber incident response plans have been carefully crafted to ensure proper Government response to incidents, and we must ensure they are followed appropriately. The attacks on Colonial and others provide opportunities to learn and improve the resiliency of the pipeline sector and critical infrastructure across the United States.

I was pleased to see TSA take initial action by issuing the first-ever mandatory cybersecurity requirements for pipelines. These new requirements went into effect on May 28 and will be critical to improving coordination among the pipeline industry, CISA, and TSA.

More must be done to increase protections for our pipelines and allow Federal authorities greater ability to assess weaknesses in critical transportation infrastructure. Unfortunately, cyber criminals are not going anywhere anytime soon. In fact, they are getting smarter, and cyber attacks are likely to become more common. We must ensure the Department of Homeland Security remains at the forefront of protecting our critical infrastructure from these threats.

I look forward to our testimony. I yield back, Madam Chair.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JUNE 15, 2021

The attack on May 7 that resulted in the week-long shutdown of 5,500 miles of petroleum pipeline on the East Coast clearly represents a significant cyber attack on critical transportation infrastructure. It is clear that the future will bring more attacks like this, whether from organizations like DarkSide that seek to exploit cybersecurity weaknesses for profit or foreign enemies seeking to weaken our Nation.

The Federal Government must be prepared to fight off attacks and respond to successful security breaches swiftly and effectively. The Cybersecurity and Infrastruc-

ture Security Agency is the lead Federal coordinator for securing critical infrastructure from cyber attacks, and the Transportation Security Administration is the designated Sector Risk Management agency for pipelines. Yet Colonial failed to properly engage with TSA in recent months in order to safeguard their pipelines against attack and repeatedly rejected technical assistance from CISA following the ransomware incident.

While I am pleased that Colonial has finally agreed to a virtual cybersecurity assessment from TSA, I am alarmed that they refused to do so until 3 weeks after an attack that resulted in the full shutdown of their pipeline. Despite the authority placed within the Department of Homeland Security to respond to cyber attacks on pipelines, including through TSA's authorities to issue emergency security directives, the Department of Energy was made the lead agency for response to the Colonial incident. Additionally, the Federal Government did not deem the attack a "significant cyber incident" as defined by policy, despite its substantial impact.

Cyber incident response plans have been carefully crafted to ensure proper Government response to incidents, and we must ensure they are followed appropriately. The attacks on Colonial and others provide opportunities to learn improve the resiliency of the pipeline sector and critical infrastructure across the United States. I was pleased to see TSA take initial action by issuing the first-ever mandatory cybersecurity requirements for pipelines. These new requirements went into effect on May 28 and will be critical in improving coordination among the pipeline industry, CISA, and TSA.

More must be done to increase protections for our pipelines and allow Federal authorities greater ability to assess weaknesses in critical transportation infrastructure. Unfortunately, cyber criminals are not going anywhere anytime soon. In fact, they are getting smarter, and cyber attacks are likely to become more common. We must ensure the Department of Homeland Security remains at the forefront of protecting our critical infrastructure from these threats.

Mrs. WATSON COLEMAN. Thank you very much, Chairman.

I now would like to welcome our panel of witnesses.

Ms. Sonya Proctor is the assistant administrator for surface operations at the Transportation Security Administration. In her role, she is responsible for strategic surface transportation security operations, not only agency-wide but also on a National level and scope, for all surface transportation modes, including mass transit, freight, rail, highway, motor carrier, and pipelines.

Ms. Proctor has served in several roles at TSA previously, including in leadership roles at Ronald Reagan Washington National Airport and within the Office of Law Enforcement and Federal Air Marshal Service. Prior to joining TSA, Ms. Proctor served 25 years in the Metropolitan Police Department, rising from a patrol officer to interim chief of police, and she served as the chief of police for the Amtrak police department.

Mr. Eric Goldstein serves as the executive assistant director for cybersecurity for the Cybersecurity and Infrastructure Security Agency. In his role, Mr. Goldstein leads CISA's mission to protect and strengthen Federal civilian agencies and the Nation's critical infrastructure against cyber threats.

Previously, Mr. Goldstein was the head of cybersecurity, policy strategy, and regulation at Goldman Sachs, and he served in various leadership roles at CISA's precursor agency, the National Protection and Programs Directorate. Mr. Goldstein has also practiced cybersecurity law at an international law firm, led cybersecurity research and analysis projects at a Federally-funded research and development center, and served as a fellow at the Center for Strategic and International Studies.

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

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

STATEMENT OF SONYA T. PROCTOR, ASSISTANT ADMINISTRATOR FOR SURFACE OPERATIONS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. PROCTOR. Good afternoon, Chairwomen Watson Coleman and Clarke, Ranking Members Gimenez and Garbarino, and distinguished Members of the subcommittees. I appreciate the opportunity to appear before you today to discuss TSA's role in securing our Nation's pipeline systems. I also thank you for your indulgence as I resolved my own technology issues this afternoon.

Our Nation's pipeline systems are vital to the economy, our National security, and the livelihood of our country. There are more than 2.8 million miles of natural gas and hazardous liquid pipelines owned and operated by over 3,000 private companies.

Pipelines are susceptible to physical attacks and, as recently evidenced, cyber intrusions as well. These threats have the potential to negatively impact our National security, economy, commerce, and well-being.

For these reasons, TSA remains committed to securing our Nation's pipelines against evolving and emerging risks. To support this commitment, in October 2019, TSA established the Office of Surface Operations, and expanded its pipeline security staff from 6 positions to 34 positions, working on field and headquarters operations and policy development.

TSA has had a long-established, productive private-public partnership with partners in the pipeline industry to protect the transport of hazardous liquids and natural gas.

To support pipeline owners and operators in securing their systems, TSA developed and distributed security training materials for industry employees and partners to increase domain awareness and ensure security expertise is widely shared. In conjunction with the pipeline industry and our Government partners, TSA developed the Pipeline Security Guidelines, to provide a security structure for pipeline owners and operators to use in developing their security plans and programs. While the guidelines are not mandatory, the recommended security measures for both physical and cybersecurity serve as the de facto industry standard.

TSA works with industry partners to assess and mitigate vulnerabilities and improve security through collaborative efforts, including intelligence briefings, exercises, assessments, and on-site reviews. Two key examples would be the Validated Architecture Design Reviews, to promote a secure and resilient cybersecurity posture, that TSA conducts, in coordination with CISA, to inspect a pipeline operator's critical infrastructure, including information technology and operational technology systems, and the pipeline Corporate Security Reviews and pipeline Critical Facility Security Reviews that assess the degree to which the pipeline company is adhering to the Pipeline Security Guidelines' physical and cybersecurity measures.

In response to the recent pipeline cyber intrusion, TSA used its statutory authority and issued a security directive, which has the

force of a regulation, aimed to strengthen the cybersecurity and resilience of pipeline owners and operators. TSA is committed to using its authority to implement appropriate security measures to elevate both the physical and cybersecurity of the pipeline industry.

In addition, TSA, in close coordination with the Department and CISA, continues to explore ways to mitigate threats through additional cybersecurity measures, to ensure that critical pipeline owners and operators are engaging in baseline cyber hygiene and have contingency plans in place to reduce the risk of significant disruption of operations if a breach occurs.

The pipeline system is crucial to U.S. National security, transportation, and energy supply, and that drives TSA's work to continue collaborating with our Government and private partners to expand the implementation of intelligence-driven, risk-based policies and programs.

Thank you for the opportunity to discuss TSA's pipeline security program, and I look forward to your questions today.

Thank you very much.

[The prepared statement of Ms. Proctor follows:]

PREPARED STATEMENT OF SONYA T. PROCTOR

JUNE 15, 2021

Good morning, Chairwomen Watson Coleman and Clarke, Ranking Members Gimenez and Garbarino, and distinguished Members of the subcommittees. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in securing our Nation's pipeline systems.

TSA has engaged with the pipeline industry since 2001 and has taken clear and specific actions to address cybersecurity gaps and vulnerabilities with the pipeline industry. Our Nation's pipeline systems are vital to the economy, our National security, and the livelihood of our country. There are more than 2.8 million miles of natural gas and hazardous liquid pipelines owned and operated by over 3,000 private companies. Besides the pipelines themselves, the system includes critical facilities such as compressor and pumping stations, metering and regulator stations, interconnects, main line valves, tank farms and terminals, and the automated systems used to monitor and control them. Pipelines are susceptible to physical attacks such as improvised explosive devices (IEDs) and vehicle-borne IEDs, small arms, and stand-off weapons. Additionally, as recently evidenced, cyber intrusions into pipeline computer networks have the potential to negatively impact our National security, economy, commerce, and well-being. For these reasons, TSA remains committed to securing our Nation's pipelines against evolving and emerging risks.

PIPELINE STAFFING, RESOURCING, AND EXPANDING INTERNAL CAPABILITIES

TSA has historically devoted staff to developing surface transportation policies supporting the grant process for surface transportation-related security enhancements, and conducting inspections and assessments. In support of the TSA Modernization Act of 2018 (H.R. 302), in October 2019, TSA established the office of Surface Operations under the Office of Security Operations, which reports to the executive assistant administrator for security operations. During this time TSA expanded its pipeline security staff from 6 positions to 34 positions working in field operations, headquarters operations, and policy development. These resources allow TSA to advance our pipeline and cybersecurity mission.

In fiscal year 2020, TSA created and trained a field-based 20-member Pipeline Security Assessment Team (PSAT), which is comprised of Transportation Security Inspectors (TSIs) located around the Nation. For cybersecurity efforts, we now have 8 members from the PSAT team and headquarters who successfully completed comprehensive cybersecurity training, provided by Idaho National Labs (INL) in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), and are receiving additional cybersecurity certification in support of TSA's pipeline cybersecurity mission.

TSA continues to expand its cybersecurity staffing and resourcing capabilities through establishing a Cybersecurity Operations Support Branch, which is currently in the hiring process. The branch will be staffed by 11 specialized cybersecurity personnel, 6 of which will be hired in fiscal year 2021 as part of 34 positions as previously mentioned. Five additional cyber security personnel will be hired in fiscal year 2022. This new branch within Surface Operations aims to enhance transportation systems' cybersecurity posture through a multi-layered approach, which includes conducting cybersecurity assessments and engagements; targeted stakeholder educational efforts; evaluation of cybersecurity best practices across the sector; and Government coordination and collaboration on surface cyber programs and engagements.

The TSA Surface Policy Division within the Office of Policy, Plans, and Engagement is also increasing its cybersecurity efforts and will have a total of 9 positions by the end of fiscal year 2021 to expand its Cybersecurity Section. This section will focus on the development of cybersecurity-related policy and guidance for surface transportation security.

STAKEHOLDER PARTNERSHIP

TSA's focus on pipeline security began in 2001 and through our expanding pipeline efforts, we have focused on enhancing the security preparedness of the Nation's hazardous liquid and natural gas pipeline systems. TSA has established a productive public-private partnership with Government partners and the pipeline industry to protect the transport of hazardous liquids and natural gas. This partnership includes collaboration with our Federal partners, such as Department of Homeland Security (DHS), the Department of Transportation (DOT), the Department of Energy (DOE), the Department of Justice (DOJ), and the Federal Energy Regulatory Commission (FERC) through the Energy Government Coordinating Council (EGCC), while providing input and support to the activities and initiatives of the industry-led Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and the Pipeline Working Group (PWG). Through these partnerships, TSA continues to seek input on current efforts to develop mandatory cybersecurity measures in Security Directives (SD); collaboratively develops security guidelines and training materials, and offer cybersecurity assessments for pipeline industry partners to increase security awareness and preparedness.

To support pipeline owners and operators in securing their systems, TSA developed and distributed security training materials for industry employees and partners to increase domain awareness and ensure security expertise is widely shared. Security training products include a security awareness training program highlighting signs of terrorism and each employee's role in reporting suspicious activity; an IED awareness video for employees; an introduction to pipeline security for law enforcement officers; a cybersecurity toolkit for small and midsize businesses offering guidance on how to incorporate cyber risk into their transportation system; and a pocket-sized guide for front-line employees to outline the most common types of cybersecurity threats and explain how transportation systems can protect their data, computer systems, and personal information.

Additionally, in conjunction with the pipeline industry, TSA developed the TSA Pipeline Security Guidelines (Guidelines) in 2011 to provide a security structure for pipeline owners and operators to use in developing their security plans and programs. The Guidelines are non-regulatory but recommended security measures for both physical and cyber security that serve as the de facto industry standard. The Guidelines were updated and republished in March 2018 with a significant emphasis on cybersecurity measures that are aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework. In April of this year, the criteria for identifying critical pipeline facilities in the Guidelines were further updated. The Guideline's cybersecurity measures were developed in coordination with industry and with Industrial Control System (ICS) expertise from the Cybersecurity and Infrastructure Security Agency (CISA).

Established by TSA in 2019, the Surface Transportation Security Advisory Committee (STSAC) consists of 35 industry voting members, of which 3 are pipeline subject-matter experts, and 14 Government non-voting members. This committee advises, consults with, reports to, and makes recommendations to the TSA administrator on surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

EXERCISES, ASSESSMENTS, AND SITE REVIEWS

TSA works with industry partners to assess and mitigate vulnerabilities, and improve security through collaborative efforts including intelligence briefings, exercises, assessments, and on-site reviews. Through the Intermodal Security Training and Exercise Program, TSA provides exercises, trainings, and security planning tools to the pipeline community to strengthen company security plans, policies, and procedures. Working with pipeline operators' security personnel, TSA conducts Pipeline Corporate Security Reviews, which assess the degree to which the Pipeline Security Guidelines' physical and cybersecurity measures are integrated into the operator's corporate security plan.

In addition, TSA also conducts Pipeline Critical Facility Security Reviews on critical pipeline facilities of the 100 most critical pipeline operators to collect site-specific information on facility security policies, procedures, and cyber and physical security measures. To promote a secure and resilient cybersecurity posture, through specific Congressional funding TSA works directly with CISA to collaborate with pipeline owners and operators to offer Validated Architecture Design Reviews to assess a pipeline operator's critical infrastructure including information technology (IT) and operational technology (OT) systems. This assessment is intended to determine if OT systems are designed, built, and operated in a reliable and resilient manner. This assessment examines a series of cybersecurity technical domains that goes beyond a questionnaire-type assessment and also includes traffic analysis from selected critical network segments as well as a network architecture diagram and functionality review. While these security reviews are not mandatory, they have been welcomed over the years by pipeline owners and operators who appreciate and understand the value of identifying and mitigating vulnerabilities to help better secure their physical and cyber systems.

CYBERSECURITY

On behalf of the Department of Homeland Security, TSA serves as the co-Sector Risk Management agency alongside DOT and the United States Coast Guard for the transportation systems sector and is responsible for developing, deploying, and promoting Transportation Systems Sector-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information sharing products that support the implementation of Executive Orders on cybersecurity. TSA is in close alignment with CISA and coordinates on both a tactical and strategic level to raise the cybersecurity baseline across the transportation sector. As noted earlier, TSA participates in the Energy Government Coordinating Council and regularly collaborates with the ONG SCC and its PWG on programmatic issues affecting the cybersecurity of pipeline systems.

TSA supports DHS's cybersecurity efforts in alignment with the NIST Cybersecurity Framework (Framework). The Framework is designed to provide a foundation for industry to better manage and reduce their cyber risk. TSA shares information, resources, and develops products for stakeholders to support their adoption of the Framework. TSA works closely with the pipeline industry to identify and reduce cybersecurity vulnerabilities, including facilitating classified briefings to increase industry's awareness of cyber threats.

In response to the recent pipeline cyber intrusion, TSA is using its statutory authority to strengthen the cybersecurity and resilience of pipeline owners and operators. The first security directive issued following the recent incident requires pipeline owners and operators of critical hazardous liquid and natural gas pipelines or a liquefied natural gas pipelines facility designate a cybersecurity coordinator; report cybersecurity incidents to CISA; and assess their current cybersecurity posture against a specific set of measures within the Pipeline Security Guidance. As part of this assessment, the owner/operators must identify any gaps, develop a remediation plan if necessary, and report the results to TSA.

All information reported to CISA pursuant to this directive is shared with TSA and other Federal agencies as appropriate. Similarly, all information provided to TSA is shared with CISA. By requiring the reporting of cybersecurity incidents, the Federal Government is better positioned to understand the changing threat of cyber events and the current and evolving risks to pipelines. The designation of cybersecurity coordinators will give TSA a known and consistent point of contact with critical pipeline owners and operators, allowing TSA to easily share security information and intelligence. The assessments will assist the owners and operators and TSA to better understand the current state of cybersecurity practices in individual companies and across the industry. In addition, TSA, in close coordination with the Department and CISA, is also exploring ways in which immediate threats, such as ransomware, can be mitigated through additional cybersecurity measures to ensure

that critical pipeline owners and operators are engaging in baseline cyber hygiene and have contingency plans in place to reduce the risk of significant disruption of operations, if a breach occurs.

CONCLUSION

The pipeline system is crucial to U.S. National security, transportation, and energy supply. These pipelines provide connections to other critical infrastructure upon which we depend, such as airports and power plants. TSA is dedicated to protecting our Nation's pipeline networks against evolving threats and continues to work collaboratively with our Government and private partners to expand the implementation of intelligence-driven, risk-based policies, and programs. TSA is committed to using its authority to implement the appropriate security measures to elevate both the physical and cybersecurity posture of the pipeline industry in alignment with the threat environment. Thank you for the opportunity to discuss TSA's Pipeline Security Program and I look forward to your questions.

Mrs. WATSON COLEMAN. Thank you, Ms. Proctor.

Now I will recognize Mr. Goldstein to summarize his testimony for 5 minutes.

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

Mr. GOLDSTEIN. Chairman Thompson, Chairwomen Watson Coleman and Clarke, Ranking Members Gimenez and Garbarino, Members of the committee, thank you for the chance to testify today.

As noted in the Members' opening statements, cybersecurity threats represent an urgent risk to our National security, economic security, and public health and safety. The committee is to be commended for your continued focus on this issue and for your support of CISA's essential role therein.

As the lead agency for civilian cybersecurity, CISA plays several key roles in managing the risk of ransomware and other intrusions. In particular, recognizing that most ransomware intrusions exploit known vulnerabilities and common security weaknesses, CISA develops and shares best practices to help organizations reduce the likelihood and impact of a ransomware intrusion.

To this end, in January of this year, CISA unveiled our Reduce the Risk of Ransomware Campaign. A few months later in April, Secretary Mayorkas initiated a high-profile Ransomware Sprint that included a series of National events intended to ensure that leaders across the country understand the criticality of these risks and take urgent action in response. Our work has continued as we further release updated guidance and consider novel approaches to drive risk reduction. CISA additionally serves a critical role in providing support to victims of cybersecurity incidents and sharing actionable information to protect future possible victims.

Upon learning of the Colonial Pipeline intrusion, CISA immediately began to collaborate with the FBI and other Federal partners to gather information that could be used to help protect other potential victims of these sorts of serious campaigns. Within 4 days of the intrusion, CISA and the FBI published a cybersecurity advisory, with specific mitigations to reduce the likelihood and impact of similar events. We then updated this advisory with technical indicators of compromise and amplified the alert to maximize use by network operators, including through a stakeholder call with near-

ly 9,000 participants from across critical sectors. These activities reflect CISA's role in National cybersecurity.

While CISA's expert network defenders are available to provide incident response and threat hunting, upon request, of equal importance is our role in quickly using information from intrusions to protect others.

Well before the Colonial intrusion, CISA was taking action to address cybersecurity risks facing the pipeline sector. In particular, through the Pipeline Cybersecurity Initiative, CISA works closely with TSA and pipeline companies to conduct vulnerability assessments, analyze risk to the sector, and implement a key pilot program called CyberSentry, which, as Ms. Clarke noted, leverages commercial technologies and sensitive threat information to monitor certain highly critical infrastructure networks for sophisticated threats.

But going forward, it is very clear, as a Nation, we must do more to address the risks of ransomware and other cyber intrusions affecting our Nation's critical infrastructure. To this end, CISA is urgently driving progress in several key areas.

First, we must gain increased visibility into cybersecurity risks and use this visibility to produce targeted guidance, share actionable information, and prioritize incidents that do occur. TSA's recent security directive that requires reporting of cybersecurity incidents to CISA is one key step, and we continue to evaluate potential ways to drive further reporting of incidents and cybersecurity risks to CISA in order to further enable this essential visibility.

Second, we must continue to invest in and mature our voluntary partnerships with critical entities across the country. Going forward, we are implementing our Joint Cyber Planning Office to plan, exercise, and coordinate cyber defense operations between Government and the private sector.

Third, we must leverage lessons learned and capabilities matured through our Federal cybersecurity mission, including through activities undertaken in executing the President's recent Executive Order to support our partners across critical infrastructure, including by conducting persistent hunts, ingesting, analyzing, and acting upon security data, and driving adoption of defensible network architectures. Funding provided in the American Rescue Plan Act is a critical downpayment in driving this essential change.

Additionally, the establishment of a Cyber Response and Recovery Fund, or a CRRF, will ensure that CISA has sufficient resources and capacity to respond rapidly to cyber incidents. Recommended by the Cyberspace Solarium Commission and recently passed by the Senate, we do hope that the CRRF will be considered soon by the House and provide CISA with additional resources to conduct our rapidly-evolving and essential mission.

In conclusion, our Nation is facing unprecedented cybersecurity risk, and the list of significant incidents in recent months is long and growing. Now is the time to act, and CISA is leading our National call to action. We will deepen our partnerships, enhance our visibility into National cybersecurity risk, and drive targeted action. In collaboration with our partners in the public and private sectors, our international allies, and with Congress, we will make

progress in addressing this risk and maintaining the availability of critical services to the American people.

Thank you again for the chance to appear today, and I very much look forward to your questions.

[The prepared statement of Mr. Goldstein follows:]

PREPARED STATEMENT OF ERIC GOLDSTEIN

JUNE 15, 2021

Chairwoman Clarke, Chairwoman Coleman, Ranking Member Garbarino, Ranking Member Gimenez, and Members of the committees, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding the Federal response to the Darkside ransomware incident against the Colonial Pipeline company and the broader cyber threat facing our Nation's critical infrastructure.

CISA leads the Nation's efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. In particular, CISA serves as the Nation's "cybersecurity quarterback" and acts as the focal point to exchange cyber defense information and enable operational collaboration among the Federal Government, State, local, Tribal, and territorial (SLTT) governments, the private sector, and international partners. In this role, we are particularly focused on reducing cybersecurity risks to entities that provide or support National Critical Functions, including companies like Colonial Pipeline.

To accomplish this mission, CISA leads a collaborative effort to identify and drive reduction of the most significant cyber risks to critical infrastructure. This requires first identifying cyber risks through robust multi-directional information sharing, conducting risk and vulnerability assessments, and deploying threat detection technologies to critical assets. We work to prioritize identified risks, including by leveraging the capabilities of our National Risk Management Center to understand relative criticality of critical infrastructure assets and working with our partners across Government to understand our adversaries' potential intent and capabilities. Finally, we drive collective action to reduce cybersecurity risks, including by providing incident response and threat-hunting services, issuing alerts and guidance, and coordinating joint cyber defense operations that bring together capabilities from Government and private-sector partners.

Cyber intrusions over the past several months have further reflected the fact that our country is facing an immediate threat to our National security, economic prosperity, and public health and safety. Nation-state actors and criminal groups continue to increase in their sophistication and in their willingness to target organizations across all sectors of the economy. The impacts of these malicious activities continue to increase, impacting the provision of critical functions from health care to energy to agriculture. This hearing provides a timely opportunity to emphasize the urgency of this challenge, discuss CISA's critical role in helping our Nation manage this risk, and consider necessary steps to drive further progress.

RANSOMWARE: A GROWING THREAT

Ransomware is an ever-evolving form of malware that encrypts files on a device, rendering the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption, and often threaten to sell or leak the victim's data if the ransom is not paid. Malicious actors continue to evolve their ransomware tactics over time, and CISA remains vigilant of ransomware intrusions and associated tactics, techniques, and procedures across the country and around the world.

Recently, ransomware directed at SLTT governments and critical infrastructure organizations has surged. In fact, it is estimated that over 100 Federal, State, and municipal agencies, over 500 medical centers, and 1,680 educational institutions in the United States were hit by ransomware in 2020 and ransom demands exceeded $1 billion dollars.[1] This epidemic is now affecting our Nation's most critical infrastructure: Municipal governments, police departments, hospitals, schools, manufacturing facilities, and of course, pipelines.

---

[1] Emisoft, *The State of Ransomware in the US: Report and Statistics 2020, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/;* Emisoft, *The Cost of Ransomware in 2020: A Country-by-Country Analysis, https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/.*

CISA, and the broader Department of Homeland Security, has acted urgently to catalyze National action around this risk. In January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and combat this ongoing and evolving threat. The campaign is a focused, coordinated, and sustained effort to encourage public and private-sector organizations to implement best practices, tools, and resources that mitigate ransomware risk. Additionally, in coordination with the Multi-State Information Sharing and Analysis Center (MS–ISAC), CISA released a joint Ransomware Guide that details industry best practices and a response checklist that can serve as a ransomware-specific addendum to State and local government's cyber incident response plans.

In February, during his first remarks dedicated to cybersecurity, Secretary Mayorkas issued a call for action to tackle ransomware more effectively. To further drive a call to action, Secretary Mayorkas initiated a Ransomware Sprint in April 2021 that has included a series of high-profile National events intended to ensure that leaders across all sectors of the economy understand the criticality of this risk and take urgent action in response.

Ransomware is a critical challenge and the risks posed to our Nation's critical infrastructure are severe. But the challenge is not insurmountable. Ransomware intrusions generally do not use zero-day vulnerabilities or exquisite tradecraft, but rather exploit known security weaknesses or a failure to adopt generally accepted best practices. By investing in improved cybersecurity as recommended in CISA guidance, organizations can reduce the risk of a ransomware intrusion and limit the potential impacts.

AN EXAMPLE OF A BROADER RISK: COLONIAL PIPELINE RANSOMWARE INTRUSION

The ransomware that impacted Colonial Pipeline was one of the first cyber intrusions in our Nation to have a direct effect on many Americans' daily lives. But the intrusion itself was not unique: The Darkside ransomware-as-a-service group has been associated with hundreds of intrusions in recent months and ransomware intrusions have impacted essential services on a smaller scale, from elementary schools to hospitals. Upon learning of the intrusion, CISA immediately began to collaborate with the Federal Bureau of Investigation (FBI) and other interagency partners to gather information that could be used to help protect other potential victims. Within 4 days of the intrusion, CISA and the FBI published a cybersecurity advisory on the incident, which included detailed information on how to reduce risk across critical infrastructure. This advisory contained specific mitigation measures to reduce the likelihood of a ransomware intrusion and, critically, steps to reduce the consequences. This latter element cannot be overstated: All critical infrastructure organizations should assume that they can be compromised by a ransomware intrusion and take steps to reduce impacts, including by ensuring that their essential functions can remain operable even if their primary business network is unavailable. CISA and the FBI subsequently enriched this advisory with specific indicators of compromise associated with the Darkside ransomware group and the Colonial Pipeline intrusion.

In order to further amplify the importance of these mitigation steps, CISA convened a broad stakeholder call with over 8,000 attendees from across U.S. critical infrastructure to provide an overview of the incident, threat actor, and impacts. CISA also convened a meeting under its Critical Infrastructure Partnership Advisory Council with leadership from the 16 critical infrastructure sectors to discuss potential operational impacts for critical infrastructure due to the ransomware intrusion. This contributed to CISA's ability to assess potential impact to the 55 National Critical Functions from a sustained shutdown, and anticipate cross-sectoral impacts, including from transportation slow-downs and impacts to chemical facilities. Finally, CISA leveraged our regional personnel deployed across the country, and particularly in areas impacted by the Colonial Pipeline outage, to provide focused guidance to other critical infrastructure organizations and provide the U.S. Government with detailed information on cascading impacts across sectors.

MANAGING A BROADER RISK: CISA'S ROLE IN PIPELINE CYBERSECURITY

Well before the Colonial Pipeline intrusion, CISA was addressing cybersecurity risks to pipelines. Over the past several years, CISA and the Transportation Security Agency (TSA), in conjunction with the Department of Energy, National Laboratories, and private industry, have been focused on addressing cybersecurity risks to the Nation's 2.7 million miles of pipeline infrastructure through the Pipeline Cybersecurity Initiative (PCI). The PCI was formed in response to increasing dependence on automation within the oil and natural gas (ONG) pipeline industry and the growing attack surfaces of assets using connected technology.

As part of PCI, CISA collects, aggregates, and analyzes data to inform a holistic view of vulnerabilities, threats, and consequences to the ONG pipeline industry. Importantly, CISA also provides incident response and intelligence support for pipeline activities with a focus on industrial control systems and coordinates activities related to the PCI. In February 2021, CISA released a Pipeline Cybersecurity Resources Library to provide pipeline facilities, companies, and stakeholders with a set of free, voluntary resources to strengthen their cybersecurity posture.

To inform CISA's analysis of pipeline risk, CISA routinely partners with the TSA and pipeline companies to conduct in-depth vulnerability assessments, or Validated Architecture Design Review (VADR) assessments, on their infrastructure. Importantly, VADRs assess pipeline critical infrastructure information technology (IT) and operational technology (OT) systems to determine if they are designed, built, and operated in a reliable and resilient manner. These assessments, which are free to participating companies, help identify gaps across infrastructure operators. TSA and CISA are on track to complete 52 VADRs on pipeline entities by the end of this fiscal year. To build on the VADR assessment recommendations, CISA and TSA are working with the ONG Subsector Coordinating Council (SCC) to analyze VADR findings, conduct follow-on analysis, and develop recommendations for pipeline owners to voluntarily implement.

Given the criticality of certain pipeline entities and certain other critical infrastructure assets, CISA offers a pilot program called CyberSentry, which deploys technologies and analytic capabilities to monitor an organization's business (IT) and operational technology/industrial control system (OT/ICS) network for sophisticated threats. CyberSentry is a voluntary partnership with private-sector critical infrastructure companies using CISA's unique statutory authorities, policy and privacy solutions. This capability is not a replacement for commercial solutions; rather, the capability complements such solutions by allowing CISA to leverage sensitive threat information. CyberSentry has shown significant benefit in practice and has been used to drive urgent remediation of threats and vulnerabilities.

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

MITIGATING FUTURE RISKS

The Colonial Pipeline intrusion and the more recent intrusion into JBS Foods must serve as an urgent call to action to address our Nation's cybersecurity risks. We must collectively and with great urgency strengthen our Nation's cyber defenses, invest in new capabilities, and change how we think about cybersecurity, recognizing that all organizations are at risk, and we must focus on assuring the resilience of essential services. To that end, CISA is acting with the utmost resolve to drive reduction of cyber risk across the National Critical Functions. Achieving the progress we seek will require consideration of several key areas.

First, CISA is currently investing in, and growing capabilities to increase visibility into cybersecurity risks across Federal agencies and across non-Federal entities. This necessitates a fundamental change, in which CISA must gain the ability to conduct persistent hunts for threat activity, ingest and analyze security data at all levels of the network, and conduct rapid analysis to identify and act upon identified threats. At the same time, CISA is driving adoption of defensible network architectures, including implementation of zero-trust environments in which the perimeter is presumed compromised and security must focus on protecting the most critical accounts and data. President Biden's Executive Order on Improving the Nation's Cybersecurity will drive critical progress in advancing cybersecurity across the Federal Government. Going forward, we must take lessons learned from our investments in Federal cybersecurity to support organizations across sectors in driving similar change.

Second, CISA must work with all possible partners to gain increased visibility into National risks. With increased visibility, we are able to better identify adversary activity across sectors, which allows us to produce more targeted guidance, and identify particular incidents requiring a specialized CISA response team. Our support to TSA to develop a recent Security Directive requiring reporting of cybersecurity incidents to CISA is an important step and an example of such collaboration. We look forward to working with Congress to further encourage reporting of cybersecurity incidents to CISA in order to further enable this essential visibility.

Third, CISA must continue to invest in and mature our voluntary partnerships with critical infrastructure entities. For example, our Cyber Information Sharing and Collaboration Program (CISCP) serves as a bi-directional forum in which CISA and private industry are collaborating on significant risks, developing sector- and threat-focused products, and providing briefings on new trends, threats, and capabilities across the sectors. With information-sharing protections available through the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information Act, the program enables trusted sharing between CISA and a network of high-impact companies, Information Sharing and Analysis Centers (ISACs), and service providers. Within CISCP, the Mutual Interest Initiative brings together cyber threat companies and internet service providers to work with CISA and the broader Government community to exchange analysis and collaboratively work on threat actor-focused products. Furthermore, CISCP enables CISA to work in close coordination with software vendors and endpoint detection companies to both assess impact and mitigate risk of critical vulnerabilities. From a technical standpoint, these partnerships with industry enable us to better understand the nature of vulnerabilities pre- and post-disclosure and in turn provided timely and thorough mitigation guidance to Government agencies and critical infrastructure. Going forward, CISA is establishing a Joint Cyber Planning Office, as required by the Fiscal Year 2021 National Defense Authorization Act, to further mature our capabilities to plan, exercise, and coordinate cyber defense operations with partners across the government and private sector.

Last, recognizing that we cannot prevent all intrusions, we must drive a focus on resilience and functional continuity even as we drive improvements in security. We must advance business continuity exercises even as we catalyze adoption of cybersecurity best practices; we must ensure that operational technologies are segmented from, and can run independently of business networks, even as we advance our ability to detect threats in both environments; and, we must reduce single points of failure across our National Critical Functions as we identify and harden identified nodes of systemic risk.

CONCLUSION

Our Nation is facing unprecedented risk from malicious cyber activities undertaken by both nation-state adversaries and criminals. The list of significant incidents in recent months is long and growing. Now is the time to act—and CISA is leading our National call to action. We will deepen our partnerships with critical infrastructure partners, enhance our visibility into National cybersecurity, and drive targeted action to reduce vulnerabilities and detect our adversaries. In collaboration with our Government partners, critical infrastructure entities, our international allies, and with the support of Congress, we will make progress in addressing this risk and maintain the availability of critical services to the American people under all conditions.

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

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

I want to thank both of the witnesses for their testimony. I will remind Members of each subcommittee that we will each have 5 minutes to question the panel.

I will now recognize—oh, I am sorry. I will now recognize myself for questions.

The TSA pipeline security assessments are currently voluntary. Although a new security directive does require operators to self-assess their compliance with TSA's cybersecurity security guidance, this security directive also requires critical pipeline operators to report cyber incidents and designate a cybersecurity coordinator who will be available 24/7.

So, Ms. Proctor, I would like to ask you first, would you please discuss the process that led up to this security directive? How did TSA determine the directive was needed? How did you decide to include these specific elements?

You have to unmute yourself, Ms. Proctor.

Ms. Proctor.

Ms. PROCTOR. Madam Chairwoman, I am sorry if that was directed to me. I am having some connection problems again. I beg your indulgence again.

Mrs. WATSON COLEMAN. OK.

Ms. PROCTOR. I am requesting some assistance.

Mrs. WATSON COLEMAN. Can you hear me now? Can you hear me?

I don't have any questions for Mr.—why don't we skip me and——

Ms. PROCTOR. Madam Chair, can you hear me?

Mrs. WATSON COLEMAN. I can.

Ms. PROCTOR. OK. I am having some technical problems again. The voice is going in and out. I am requesting some assistance, so I beg your indulgence one more time here.

Mrs. WATSON COLEMAN. Thank you.

Mr. Goldstein, then, may I ask you a question?

Mr. GOLDSTEIN. Yes, ma'am.

Mrs. WATSON COLEMAN. Beyond pipelines, have you considered promulgating cybersecurity standards for other surface transportation modes and like mass transit and airports?

Mr. GOLDSTEIN. Thank you, ma'am, for that question. In general, CISA's goal is to be a source of cybersecurity expertise across all sectors. Where a given sector is subject to regulations by a regulator with particular jurisdiction, we certainly engage in discussions with regulators like TSA to ensure that they are benefiting from CISA's cybersecurity expertise when they are developing regulations that are applicable to entities within their given jurisdiction. We have a robust collaboration with TSA along those lines, and certainly look forward to similar conversations with other regulators based upon their own unique authorities.

Mrs. WATSON COLEMAN. So I am going to take that as a yes? I took that as a yes.

Mr. GOLDSTEIN. We totally support strong cybersecurity across all sectors, ma'am, that is correct.

Mrs. WATSON COLEMAN. Thank you, thank you.

I did have some questions for Ms. Proctor but, unfortunately, she is not able to answer those questions. So if we clear this up in the next few minutes, I will ask her her questions.

But now I will go to the Ranking Member, Mr. Gimenez, for his 5 minutes.

Mr. GIMENEZ. Thank you, Madam Chairwoman. I really appreciate it.

This is for Mr. Goldstein. Mr. Goldstein, is there any real difference—you know, I understand that, you know, TSA has jurisdiction, I guess, over pipeline security, but I look at cybersecurity a little bit different than, say, physical security over the physical aspect, the pipeline itself. We know that there are threats to the

pipelines, somebody does sabotage, et cetera. Those are things that we need to protect, and TSA needs to do that.

But in terms of cybersecurity, is there really a difference between the control systems for the computer network, the thing that is going to be hacked, for a pipeline and, say, an airport or a bank or any such thing? Isn't ransomware really attacking the computer systems themselves and it really doesn't matter what industry that computer system is controlling?

Mr. GOLDSTEIN. Sir, thank you for that question. I think there are 2 ways to answer it. The first is, I think your last statement is absolutely correct. Ransomware is a threat that can impact any organization in any sector big or small—financial, energy, hospitality, across the board—which is why CISA has been so focused on promulgating these cross-cutting best practices and guidance, including our advisory promulgated after the Colonial intrusion, that is equally applicable to any organization because, as you imply, these sorts of cybersecurity best practices are generalizable across sectors.

Now, it is also the case that different sectors may use different specific technologies. They may have different network architectures or different ways to use devices to achieve their operational needs. But when it comes to these cybersecurity practices that we want to see—things like making sure that your software is patched, making sure that you are using multifactor authentication, leveraging off-line backups—those are practices that are generalizable across sectors and regardless of the size of company.

Mr. GIMENEZ. So when CISA makes a recommendation, do you make a recommendation to the agencies across the Federal, you know, spectrum and say, these are the things we recommend that you then recommend or write a regulation for your specific sector? Is that the way it works here in the Federal Government?

Mr. GOLDSTEIN. So, in general, CISA puts out guidance and best practices, and in the case of Federal agencies, directives that are generally applicable. Occasionally, we will put out guidance that is specific to control systems, or certainly if we know about a given threat or incident that is affecting a particular sector, we may produce a targeted alert or warning focused on a nuanced risk to a given sector or even a given device where we have information that a certain device is being exploited.

Regarding our interaction with regulators, generally regulators, including TSA, may seek CISA's expert advice and consultation on how to produce cybersecurity regulations that actually drive improved security and can be expected to reduce the likelihood of damaging incidents affecting that sector. But given the unique authorities and independence of many regulators, CISA is generally a source of expertise for those regulators to exercise their authorities in this space most effectively.

Mr. GIMENEZ. That is where I have a problem. OK. That would be, the problem that I have is that it appears to me that CISA is there to protect, basically, the thing that we are communicating with right now. OK. That is the control systems—the control systems that are controlling most of America now, energy, the electricity, the pipelines, banks, is coming out of the computer, and the computers are being hacked, and that is where vulnerability lies.

My concern is that different agencies may put different emphasis on the vulnerability that we have for cyber attacks and that it is really not focused. You know, TSA's focus for the most part, I see as, the real focus is airport security, port security, and all that, physical security, and then cyber attacks, yes, OK, but that may not be our core mission, whereas your core mission is cyber attacks.

So wouldn't it be better for the Federal Government to kind-of gel that into, you know, your agency and you become the voice on what needs to be done on cybersecurity? That is an opinion I am asking from you, and I know that it is a loaded question. So if you can answer it, please do.

Mr. GOLDSTEIN. Without question, CISA's key role today is being the Federal civilian Government lead voice on cybersecurity, and our goal is to use every single platform to make sure that business leaders, that Federal agencies, that regulators, understand the criticality of this risk and act on it with urgency and immediacy.

Certainly under current law, our goal is to work with agencies that have unique authorities to drive change, to help them use those authorities to maximize security improvement within their sector. But to your point, we strongly agree that cybersecurity needs to be a top-of-mind issue in every boardroom, in every C-suite, and in every Federal agency.

Mr. GIMENEZ. Thank you. I see that my time is up.

Thank you, Madam Chairwoman.

Mrs. WATSON COLEMAN. Thank you, Ranking Member.

I now recognize the Chairlady from—the gentlelady from New York for her 5 minutes.

Ms. CLARKE. I thank you, Madam Chairwoman.

Mr. Goldstein, as I said in my opening remarks, I believe that for CISA to carry out its broad cyber mission effectively it needs, No. 1, greater access to information about major cyber incidents and, No. 2, greater visibility into threats targeting private-sector networks in real time.

That is why I am working on 2 pieces of legislation. One would require critical infrastructure owners to report cyber incidents to CISA, and the other would authorize the capability CISA has built through the CyberSentry pilot. I see these efforts as complementary, giving CISA the ability to monitor threats today and also learn how and why they are successful, so we can prevent them from happening tomorrow.

Can you talk about how CyberSentry works and some of the ways that it helps CISA partner more effectively with the private sector?

Mr. GOLDSTEIN. Yes, ma'am, absolutely. To begin, thank you for your on-going support of CISA. It is deeply appreciated.

You know, as you noted, one of the challenges that CISA and, frankly, our country faces is a lack of visibility into cybersecurity risks facing our Nation's critical infrastructure. When we say "cybersecurity risks," we should be precise about what we are speaking about. What we are talking about is the possibility of criminal groups or nation-states breaking into our critical infrastructure with the intent to do harm.

Without that visibility, CISA is unable to fully conduct 2 of our core functions. The first is to understand systemic risk across our

country and provide actionable information that can protect others, so they can either detect and block these threats before break-ins occur or they can evict adversaries from their networks once the intrusion happens.

We are also not able to fully understand those entities that may need our voluntary assistance in order to help understand the intrusion, remediate, and recover.

CyberSentry provides a unique capability to help protect the most critical infrastructure in this country. What we have learned from a long history of cybersecurity intrusions is that many intrusions impacting critical infrastructure and particularly control systems actually begin on business networks. So CyberSentry provides commercial off-the-shelf technology that helps detect cybersecurity threats that are attempting to move from business networks to the operational technology or control systems network and provides coverage of both, and allows CISA to use sensitive information about particular adversaries or threats to help understand and rapidly identify those kind of threats manifesting across the most critical networks.

Now, CyberSentry is only a pilot today. It is deployed across a limited number of highly critical entities, but we have seen significant success with this program thus far. It both provides CISA with the added visibility, ma'am, that you mentioned and also provides real concrete benefits to the owner-operators that are using CyberSentry in the first instance, and we look forward to further maturing the pilot as we go forward.

Ms. CLARKE. [Inaudible] today as part of our—as part of your pilot so that it can be instructive as we are drafting this authorization. So thank you so very much for your work in this space.

I know Ms. Proctor has joined us again. Can you hear us, Ms. Proctor?

You may be muted.

Ms. PROCTOR. Yes, and please accept my apologies.

Ms. CLARKE. No, no. Understood. You know, everything is not perfected yet. So we are just happy you are able to join us.

I would like to ask just a quick question about PPD–41, the National Cybersecurity Incident Response Plan. Is that something that you are familiar with?

Ms. PROCTOR. Yes, ma'am, I am.

Ms. CLARKE. OK. There is a little delay, I guess, in your audio.

On this committee, we spend a lot of time talking about the need for all organizations—large, small, public, and private—to have incident response plans in place before an emergency, whether it is a flood, a fire, or a ransomware attack. It is important that in a crisis, there is a framework to guide decision making and everyone knows what role they are supposed to play.

The PPD–41 National Cyber Incident Response Plan lays out the Federal roles and responsibilities or lines of effort.

Would you agree with me that the Colonial Pipeline cyber incident was likely to result in demonstrable harm to National security interests or the economy of the United States as defined under PPD–41?

Mrs. WATSON COLEMAN. Ms. Proctor, you may answer this question.

Ms. CLARKE. She is delayed on her audio.

Mrs. WATSON COLEMAN. Yes. I just wanted to let you know that your time has expired, but she certainly may respond to your question, ma'am.

Ms. CLARKE. Appreciate that.

Ms. PROCTOR. Yes, ma'am, I would agree with you on that, that it was a significant incident.

Ms. CLARKE. Very well.

Madam Chair, I yield back.

Mrs. WATSON COLEMAN. Thank you, Madam Chairlady.

I now recognize Mr. Garbarino.

Mr. GARBARINO. Thank you, Madam Chair.

Mr. Goldstein, the committee has concerns with the White House's decision to place the Department of Energy at the helm of the Federal Government's response to the ransomware attack on Colonial Pipeline. In this case, DOE is not the Sector Risk Management agency, nor does it have a lead role in the cyber incident response in this case.

DHS, via TSA, is the co-lead Sector Risk Management agency for pipeline sector, along with the Department of Transportation. Additionally, the National Cyber Incident Response Plan designates DHS, via CISA, as the lead agency for the response.

What rationale were you and Acting Director Wells given for DOE being given the lead response to this incident? Did you or any of CISA's leadership raise concerns with the White House about that, about DOE being put in charge?

Mr. GOLDSTEIN. Certainly. Congressman, I think it is useful to separate the various elements of this incident, because it is one of the first incidents that we have seen in this country where a cyber event led to a decision to disrupt a physical function upon which Americans depend.

There really were, I think, 3 distinct aspects to the incident. The first was the cyber intrusion itself. The cyber intrusion, insofar as the Federal response went, was managed in accordance with PPD–41. The FBI, of course, led the threat response, and CISA led the asset response.

Now, it happened to be in this circumstance, as Colonial CEO testified last week, that Colonial chose to engage a third-party incident response firm rather than accepting CISA's offer of incident response assistance. Under current law, that is certainly the prerogative of a company to do.

Not providing on-the-ground incident response assistance, CISA focused on our broader asset response role of protecting others. As mentioned in my opening statement, we shared urgent alerts, warnings, and advisories with detailed information to protect other organizations from this specific ransomware group and the broader ransomware threat.

The second element of this incident is the broad coordination of the National response. Of course, under PPD–21, the Secretary of Homeland Security plays a critical role in coordinating the response to cyber or physical incidents affecting critical infrastructure. Here, Secretary Mayorkas certainly played that role, in close coordination with the White House and with our partners in the interagency and, of course, our Secretary was at the White House

podium and was one of the key National figures communicating about their response.

The third aspect, of course, was the fuel supply issue, assuring that Americans actually had fuel available to fill their tanks and that businesses were able to keep operating. That is an issue within the remit of DOE and was one of the core focuses of the Government's interaction with Colonial, recognizing that, as advised by the company, the cyber incident was being managed by a well-regarded third party.

So DOE's role in this incident, and part of the reason for their centrality, was the justifiable National focus on the fuel supply issue and DOE's unique expertise and equities in assuring appropriate provision of fuel across the eastern seaboard during the duration of this incident.

Mr. GARBARINO. I get that, but this was the team—they were put in charge of the team, the Government's response to the ransomware attack. You know, this right now is a pipeline. Next time we don't know what it is. So don't you think that—or do you feel that further clarification is needed on the Federal level as to who is—you know, should CISA be the lead on all of these? Or, you know, because with the ransomware, it is always going to be ransomware. We just don't know what other industry it is going to hit. So I don't know if that makes sense that, you know, having DOE in charge of this one but then somebody else in charge of another one.

Do you think there should be more—that clarification is needed on the Federal level of who is actually in charge or at the top, you know, when there is a cyber incident?

Mr. GOLDSTEIN. So in this case, certainly, CISA did undertake our asset response role. Of course, the advisories and communications that we put out were joint with the FBI, consistent with PPD–41 and not with other agencies outside of that construct. But, certainly, we are deeply conscious that as we see the potential for these sort of incidents that bring together cyber intrusions and very real functional impacts that affect Americans lives, it is deeply important for the U.S. Government to communicate clearly and concretely about how we approach these incidents and how we manage them as a whole-of-Government effort to both reduce their prevalence and minimize impacts to the American people.

Mr. GARBARINO. I get that. Under PPD–41—I know my time is about to end—but why was this not a significant cyber incident under PPD? This seems pretty significant. Why was this not?

Mr. GOLDSTEIN. This was absolutely a significant event. Any time when we have Americans worried about cessation of an essential function like fuel, it is absolutely a significant event. Here, however, based upon information received from Colonial, the cyber incident aspects of this event were well-managed by a trusted third party. So based upon that information, the event itself was unequivocally significant and certainly dealt with as such at the highest levels of the U.S. Government. But the cyber incident aspect of it was well-managed by a third party and was a very well-known type of ransomware that likely didn't reach the cyber-specific threshold of significance that would usually trigger that designation under PPD–41.

Mrs. WATSON COLEMAN. Thank you.

Mr. GARBARINO. I yield back.

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

Mr. Thompson, I recognize you.

Mr. THOMPSON. Thank you very much. Let me thank the witnesses for their testimony.

Mr. Goldstein, it is always good to see you as a witness. You are good.

I want you to tell me what authorities you think CISA lacks at this point in time that this committee could help you with.

Mr. GOLDSTEIN. Thank you, sir. It is always good to see you as well. I would like to harken back to Ms. Clarke's eloquent statement, which is, we need the ability to get visibility into National cybersecurity risks. We need to understand where adversaries are intruding into networks across this country. We need to understand the techniques that they are using to break in. We need to understand what they are doing or trying to do. The more of that kind of information that we get, we can then protect others, and we can work as a whole of Government to reduce the risk facing our country.

Mr. THOMPSON. So how do we codify that authority that you are describing?

Mr. GOLDSTEIN. Yes, sir. So, certainly, the more that we as a country can do to drive reporting on cybersecurity incidents to CISA, as TSA recently did with their security directive, and certainly as several of your colleagues have suggested via the other avenues, that will help drive that change.

The second part, sir, is, you know, we need the ability to address resource gaps across far too many entities in this country, particularly, our State, local, Tribal, and territorial partners. The more that we can do to help organizations that may be underresourced to invest in core cybersecurity, build cybersecurity programs, including in the context of incident response through the Cyber Response and Recovery Fund, or through other mechanisms that allow SLTT partners to get the funding they need, that will all help raise the bar.

Mr. THOMPSON. Well, thank you. So, do we need voluntary compliance on the part of companies? Or do you see something down the road where we will have to require companies to take a test for their systems?

Mr. GOLDSTEIN. Certainly, sir. CISA right now is urgently focused on making best use of the voluntary partnership model where we are encouraging companies and giving companies help and resources to drive security across their systems and manage National risks. They are absolutely——

Mr. THOMPSON. Well——

Mr. GOLDSTEIN [continuing]. Please, sir.

Mr. THOMPSON [continuing]. OK. I don't want to go over my time, but that is a good point. So what did Colonial do?

Mr. GOLDSTEIN. Sir, I don't have deep visibility into Colonial's security posture at the time of the intrusion. It is certainly the case today that there are many organizations in this company that—pardon me, in this country, for a variety of reasons, are unable to invest in the security they need. The U.S. Government must take

urgent steps to incentivize, drive, and require those companies to make the investments that they need to make.

Mr. THOMPSON. OK. Well, thank you. Now Ms. Proctor, what is your knowledge of what TSA did on the security side?

Ms. PROCTOR. Thank you so much for that question, sir. TSA has had a long relationship, security relationship, with Colonial. That goes back to the beginning of our Pipeline Security Guidelines. We have conducted Corporate Security Reviews with Colonial in the past. We have had—as you are aware, we have done Critical Facility Security Reviews with them. Last year, during the pandemic, we approached Colonial to engage in a Validated Architecture Design Review. That conversation was on-going over a period of time. They recently submitted their approval to participate in the VADR. It is now scheduled for the last week of July of this year. So we have conducted——

Mr. THOMPSON. So——

Ms. PROCTOR [continuing]. OK.

Mr. THOMPSON [continuing]. Thank you. My concern is that if there is no regulatory requirement for companies to allow TSA or whomever to look at their security protocols, they will tell you to come back next month, they will tell you to come back in 6 months. I am just concerned that given the expansion of ransomware attacks, a voluntary system without some compliance mandated puts us at risk. You don't have to comment. That is, you know, my thoughts on it.

Ms. PROCTOR. Sure.

Mr. THOMPSON. You know, you can have relationships with companies, but if that company knows that they don't have to, at the end of the day, comply, then I just don't see us working to a threshold for security. So, Madam Chair, I yield back.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman. I now recognize Representative Harshbarger for 5 minutes.

Mrs. HARSHBARGER. Thank you, Madam Chair, and Ranking Members, and witnesses. I have a question for Mr. Goldstein. You know, CISA needs to engage directly with our Nation's business leaders, and, my goodness, receiving a voluntary program where they will assess their vulnerabilities.

But most of these companies, you know, they won't do it. I totally understand why they are afraid that their customer base may see that they have vulnerabilities. They may not want them to know that they somehow would have their information compromised. There are things like their stock prices may drop. They may be afraid that they will be hauled in front of Congress if this vulnerability is shown. So I do understand that.

I guess my question is, what is CISA's position on whether a victim of ransomware should pay the ransom or not? Who decides that?

Mr. GOLDSTEIN. Thank you for that question, ma'am. It is the position of the U.S. Government to strongly discourage the payment of ransoms. This is the case for 2 reasons. First of all, paying a ransom offers no assurance that the victim organization will actually have their data restored or have stolen data returned. We have seen many instances of ransomware gangs either failing to decrypt

the data, or providing a decryption tool that only decrypts part of the data and still leaves a lot of the data locked up and unusable.

But, of course, the second reason is that these ransomware campaigns and these criminal gangs are fueled by ransom payments. The more the organizations pay ransom, the more that we can expect these criminal gangs to be incentivized to continue the scourge of attacks against U.S. critical infrastructure. The decision to pay remains with the impacted company, and certainly, for many companies, this is a hard decision, particularly, if they provide some critical service. But these payments, again, provide no assurance of restoration, and what is driving these campaigns and these really damaging attacks to continue.

Mrs. HARSHBARGER. Do you know how many private companies have paid ransomware because they were hacked in—you know, a lot of companies, even in my district, they don't even report it, because of those reasons I gave you initially. You know, you can't really track and get an accurate number of how many people have been hacked or paid the ransom, because they don't want you to know. They have cyber insurance because of these ransomware attacks. This is—I mean, it is has gotten out of control when our own Government, you have 9 different agencies hacked, and they don't really know how it happened. It was an outside entity that had to tell us.

So, there is a lot of reasons, I understand, why private businesses won't voluntarily be assessed, even to find out what their own vulnerabilities are. Maybe they just don't trust the Government. I don't know. But what percentage of companies do you have numbers on that report that they have had to pay ransomware, or they have been compromised? Do you have a number?

Mr. GOLDSTEIN. So, ma'am, we don't have a good number today. It gets back to the question that the Chairman raised, which is today, you know, it is largely voluntary whether a victim of a cybersecurity intrusion, including ransomware attacks, does report to either CISA or Federal law enforcement.

I do want to comment briefly though, ma'am, on your last point, which is well-taken, on disincentives for sharing information with the Government. Because Congress has already acted to largely address many of those concerns, both in the Cybersecurity Act of 2015, and in the Critical Infrastructure Information Act, both of which provide strong protections for information shared by the private sector with CISA, including protections from regimes like FOIA, regulatory use, civil litigation, et cetera. So, certainly, one of our goals at CISA is to ensure broad understanding of these protections and ensure companies take advantage of them by reporting both their cybersecurity risks and incidents to CISA.

Mrs. HARSHBARGER. Yes. This is big business right now, and we have got to get a handle on it, and that is why we are having these hearings.

I do have another question. Why—and this is just your opinion—why do you think the FBI did not take this committee up on our invitation, I guess you could say?

Mr. GOLDSTEIN. Ma'am, I have not discussed that question with my colleagues at the FBI, and I wouldn't be able to comment.

Mrs. HARSHBARGER. Well, that is your opinion. I appreciate that. I don't know. How much time do I have left?

Mrs. WATSON COLEMAN. You have 20 seconds.

Mrs. HARSHBARGER. Twenty seconds. Well, I will just yield back. Thank, you ma'am.

Mrs. WATSON COLEMAN. Well, thank you very much. I will now recognize Representative Titus.

Ms. TITUS. Thank you, Madam Chairman. Thank you for holding this hearing. We certainly realized that we have put this off for too long. We need to get on top of it, and the testimony has been excellent. We focused on the Colonial Pipeline, but I would like to be sure that other kinds of energy infrastructure are protected like generating stations.

I represent Las Vegas, and we have a lot of lights there, and we need a lot of sources of energy that are consistent, that are persistent that we can count on to serve our residents, and also 40 million visitors.

Now, Nevada Energy is our primary provider of energy, and they are doing a lot of investing in renewable energy resources. They are developing throughout the State, mostly solar, but some wind, which I think is a great thing. But I want to be sure that the Government is adequately protecting those sources, too, from these kinds of threats.

I wonder if y'all would comment on what CISA and TSA are doing in anticipation of maybe some needs in this area?

Mr. GOLDSTEIN. Yes, ma'am. So, certainly, CISA is deeply focused on cybersecurity risks facing the energy sector and iteration entities in particular. Of particular note, the White House recently announced a 100-day industrial control system Cybersecurity Sprint. The first sprint focused precisely on this sector recognizing the centrality of the energy grid, of course, to our Nation's economy and National security, and the potential for a cybersecurity event to cause significant disruption.

You know, certainly, many entities across the electric subsector are well-resourced and mature in this space. This is a sector that recognizes the risk and has invested accordingly. But, certainly, CISA and our colleagues at DOE are deeply focused on providing tools, resources, and guidance to this sector, recognizing the risks and the need to make further investments to stay ahead of our adversaries.

Ms. TITUS. So do you work directly with the utilities? You would be working directly with Nevada Energy to help them to be sure they are up to speed?

Mr. GOLDSTEIN. Yes, ma'am. I can take back to see if we have worked with Nevada Energy recently. But, certainly, we work very consistently with individual operators to assess their security and make sure they have what they need to be secure.

Ms. TITUS. Oh, I am glad to hear that. Any other comment? Well, the second question that I have is that I know one of the problems that we often have is trying to recruit and train and have in the field cyber professionals. I understand that there is a program—it is a scholarship program—called CyberCore. Now, my district is home to several minority-serving institutions. I just wonder how much outreach you are doing, or how much work you are doing

with those institutions to try to attract and train people who are—well have the skills to enter into this field that is going to be needed increasingly as we go forward?

Mr. GOLDSTEIN. Ma'am, thanks so much for that question. You are absolutely correct. Building a deep, diverse cybersecurity work force is absolutely essential for us not only getting our arms around this risk, but managing it going forward. CISA is deeply focused on working with institutions across the country, but particularly minority-serving institutions, HBCUs, and community colleges, to make sure that those schools have curriculum, have training, have resources, and assistance so that they can train the next generation of cybersecurity professionals.

Certainly, we are focusing in that regard, not only training that work force so that they can join Federal service, including through the programs like Scholarship for Service, but, also, ensuring that we are driving and catalyzing a robust educational community around the cybersecurity work force at all levels of education to ensure that we are educating people today, so that they can be well-equipped for the jobs of tomorrow.

Ms. TITUS. I am going to reach out to the campuses in my district about this CyberCore program and see what they are doing. Then can I have them get in touch with your office or somebody there to find out how they might enhance that, and maybe get the word out more and be sure people—students in there know that they can apply for this kind of program.

Mr. GOLDSTEIN. Yes, ma'am. Most certainly.

Ms. TITUS. Thank you. Thank you, Madam Chairman, I yield back.

Mrs. WATSON COLEMAN. I want to take this opportunity to ask Ms. Proctor a question that I tried to ask when our system went down. Ms. Proctor, are you there?

Ms. PROCTOR. Yes, ma'am, I am.

Mrs. WATSON COLEMAN. Oh, thank you very much. You know, given that operators will only be required to self-assess their compliance with TSA guidelines, how would TSA verify the information provided, and what will the consequences be if the pipeline operator misrepresents their cybersecurity practices to the TSA?

Ms. PROCTOR. Thank you so much for that question, because I think it is important to know that in the first security directive we have issued, there is a requirement for companies to conduct a self-assessment as part of those requirements that security directors want. However, we are continuing to develop additional measures for pipeline companies. We are developing now a second security directive, which will have the force of a regulation. That one will require more specific mitigation measures, and it will ultimately include more specific requirements with regard to assessments.

The second security directive is going to be an SSI directive, because of the nature of the mitigating measures that are going to be required within there. But these are also subject to inspection by TSI inspectors. We have a cadre of service inspectors that we have trained that underwent training at PHMSA Training Academy for pipeline operations. We have a subset of them who have also undergone cybersecurity training. They just recently completed

an in-residence course at Idaho National Lab. So they have both pipeline operations training and cyber training.

Ms. TITUS. Thank you.

Ms. PROCTOR. Those will be the individuals who will be ensuring that the pipeline companies are adhering to what is required in those security directives.

Mrs. WATSON COLEMAN. Thank you. Yes or no, do you all have the resources and personnel that you need to be able to ensure the accountability measures that we think are important?

Ms. PROCTOR. Yes, ma'am, we do have those resources now.

Mrs. WATSON COLEMAN. OK. Thank you. Thank you very much.

Now, I would like to recognize Mr. Van Drew from New Jersey.

Mr. VAN DREW. Thank you, Madam Chair. I have just some questions, and some of them may seem a little repetitive, but I really want to tack this down.

For Sonya Proctor from the TSA, I understand there are growing concerns that the TSA [inaudible].

Mrs. WATSON COLEMAN. Congressman, Congressman, can you unmute? I guess while we are trying to work this out, I will recognize Representative Clyde.

Mr. CLYDE. Thank you, Madam Chair, for holding this hearing. This question is for Eric Goldstein. Mr. Goldstein, the subcommittee held a hearing last month on the ransomware crisis with experts from the private sector, and former Director Krebs responded to a question of mine about how CISA gets word out about its great services. He said that marketing is not an area of strength for the agency.

Considering the recent attacks where CISA has not been directly involved, I think it is important that business leaders, critical infrastructure companies, and State and local governments are aware of CISA and its great services. So, my question to you is how many dedicated marketing professionals does CISA have? If I may, sir.

Mr. GOLDSTEIN. Thank you, sir. So I don't have an exact number on the size of our relative external affairs team. I am happy to get that back for you. What I would say is fully agree with the general point. It is absolutely critical for CISA to make sure that every company in this country, as well as every SLTT government partner understands the services that we are offering and understand how our services can help them drive down cybersecurity risks and the investments that they need to make. So, certainly, we need to do more to convey that message to every corner of this country, and part of doing that is by having, as you frame it, sir, marketing campaigns that make sure that the word gets out effectively. So that is an area of urgent investment for us. The point, sir, is very well-taken.

Mr. CLYDE. OK. Well, because the more I learn about you, the more I like you. OK. So I want to make sure that the entire Nation knows just what outstanding services you provide. So, I strongly encourage you to have a very good media campaign, because I think our business is needed. OK? We need to know that CISA is there really to help. Tell me, does CISA have a position on whether the victim of ransomware attack should pay ransom?

Mr. GOLDSTEIN. Sir, we do. We advocate that victims—we strongly discourage victims from paying ransom. As noted, I think, from

a prior question, that is for 2 reasons. First, because there is no guarantee that victims will have their data restored. Second, of course, because paying ransoms is exactly what these criminal gangs want. Paying ransoms only further incentivizes these sort of damaging attacks to continue.

Mr. CLYDE. OK. Does CISA have an offensive capability?

Mr. GOLDSTEIN. We do not, sir. We are purely a cyber defensive organization.

Mr. CLYDE. OK. Last week, I asked FireEye senior VP Charles Carmichael if his company would be willing to work with the Federal Government in helping secure a network. He stated that he would certainly be interested in the opportunity. Mr. Carmichael also stated that he believes the attacks on the Colonial Pipeline and JBS Foods originated overseas. Does CISA work with the private sector regarding any intelligence sharing or threat assessments to safeguard private or public networks?

Mr. GOLDSTEIN. We do, sir. We have deep relationships with many, if not the vast majority of the Nation's leading cybersecurity companies, internet companies, cloud providers to do just the work you describe. Sharing and exchanging of information that these companies are learning about cybersecurity risks affecting their customers, fusing that together with what CISA is learning from Federal networks, and what we are learning from our partners elsewhere in government, and developing that common operating picture of cybersecurity risks.

We have made real investments there, but there is certainly more work to do to ensure that we have that deep visibility we need to understand risks that are impacting our country.

Mr. CLYDE. OK. Would you agree with his assessment that these attacks were perpetrated from overseas, all of them, or any of them from this country that you know of?

Mr. GOLDSTEIN. Sir, as a general matter, many of these ransomware gangs are domiciled overseas. I am not able to speak about any particular act in this committee, sir.

Mr. CLYDE. OK. Do you have any evidence that would suggest that they are sponsored by a foreign state?

Mr. GOLDSTEIN. Sir, in general terms, these criminal groups are seeking financial gain, and are generally not seeking any sorts of strategic ends sought by nation-states.

Mr. CLYDE. OK. If CISA doesn't have an offensive capability, do you know does one exist in our country somewhere?

Mr. GOLDSTEIN. Sir, there are various other Federal agencies that do exercise under their own authorities the ability to disrupt adversaries using cyber means, including within the Defense Department. I would, of course, defer to the departments for further detail in their committees.

Mr. CLYDE. OK. Do you coordinate with any of those to assist them?

Mr. GOLDSTEIN. Yes, sir. We work very deeply across the interagency, with Federal law enforcement, with the Defense Department, and other partners to ensure that we are sharing information, and that all of our activities across the Government are well-coordinated and aligned.

Mr. CLYDE. OK. All right. Well, thank you very much, sir, I appreciate your responses in that. With that, I yield back.

Mr. GOLDSTEIN. Yes, sir.

Mrs. WATSON COLEMAN. Thank you, Representative Clyde, for raising that issue because I was just talking about that myself. I think the capacity to be able to be on the defense is something we really do have to drill down a little bit better on.

Mr. Langevin.

Mr. LANGEVIN. Very good, Madam Chair, can you hear me OK?

Mrs. WATSON COLEMAN. Yes.

Mr. LANGEVIN. Very good. Madam Chair, thank you holding this joint hearing. I want to thank our witnesses for their testimony today and for the important work that they are doing.

Mr. Goldstein, let me start with you if I could. Last week, in front of this committee, I was so bold as to offer CISA's service to the CEO of Colonial Pipeline, and he refused them. So, I urged him certainly to reconsider, as he says, he is acting for the good of the country. So that being said, I just want to confirm that the offer is still on the table. So, Mr. Goldstein, just to confirm, CISA stands ready to offer assistance on the networks of the Colonial Pipeline if your services are requested, correct?

Mr. GOLDSTEIN. Yes, sir, we stand ready to support any entity providing critical services in this country, including, of course, Colonial.

Mr. LANGEVIN. Thank you. Thank you. So Mr. Goldstein, now I know that CISA is a relatively new agency, and not everyone is familiar with the services that you offer. Can you help the committee understand what value you bring to entities when they invite you onto their networks following a breach? Furthermore, what benefits to other critical infrastructure owners and operators across various sectors can CISA bring to the table by having on-network presence? I hope that the CEO of Colonial is watching. Maybe this will encourage him to invite you in once and for all.

Mr. GOLDSTEIN. Indeed. Thank you for that question. Sir. The way you framed it is exactly right. First and foremost, it bears noting that we do encourage organizations that are victimized by cybersecurity incidents to bring on a third-party private response provider if they are so inclined. We work very frequently closely in tandem with private incident response firms to conduct a joint response.

So CISA's role is not replacing the extraordinary talent in the private cybersecurity market, but is, instead, additive there, too. That is the case really in 2 ways. The first is in supporting a victim of a cybersecurity intrusion, we are able to bring to bear information from other Federal agencies, and from what we have learned across incidents affecting the Federal Government, and our other partners, and enrich the incident response that may be already undertaken by the victim itself or their third-party provider. So, we can complement and add to the incident response, bringing some unique information, and in the case of incidents, that impact control systems, some unique expertise and capability. In fact, our team that is focused on control system cybersecurity is actually one of the oldest and most expert teams doing that kind of work.

So, in the first instance, we can be deeply complementary to and additive to the work already going on by an organization. Of course, if a victim chooses not to bring on a third party and seek CISA's help, foundationally, we can certainly provide the primary incident response role as well.

But as you note, sir, our role extends far more broadly, and we are focused on managing National risks and ensuring that a cybersecurity intrusion that impacts one entity doesn't spread across others. Certainly, organizations should think of this as even if you are not a victim today, you may be one tomorrow. If you are one today, that doesn't mean that you will not have an intrusion again in the future.

So, organizations should certainly see this as an issue of National interest where the more information that CISA can receive in the early days of an incident by being part of the incident response and part of that initial assessment, that lets us move more quickly to glean information, glean those technical indicators that we can then share either in a focused way with organizations that may be directly impacted based upon their sector, their technology footprint, their geography, or broadly and nationally, and even internationally, to raise the cost for adversaries and ensure that they are not using these same tactics, these same indicators over and over again.

Mr. LANGEVIN. Thank you for that. Before my time expires, Mr. Goldstein, we have seen press reports that third-party incident responders suggested not bringing the Government in. Do you find that outside cyber consultants tend to work cooperatively with CISA in emergency situations like this one with Colonial, for example, or do they bring their clients' reservations about Government involvement?

Mr. GOLDSTEIN. So we do find in general, sir, that certainly, most of the major cybersecurity providers in this country work collaboratively with CISA. We have deep relationships with many of them and have on-going operational collaboration around significant campaigns and significant threats, and, certainly, would discourage any company or third party from deciding not to share information with the Government.

As noted throughout this hearing, this really at this point is both an issue of National security and public health and safety. The more that U.S. Government can understand this risk and take urgent action and mitigate it, the more we can drive down this trend over time and protect our people.

Mr. LANGEVIN. Thank you.

Mrs. WATSON COLEMAN. Thank you for the question. The gentleman is out of time. Thank you.

I understand Mr. Van Drew is now available to be recognized for 5 minutes. Mr. Van Drew.

Mr. VAN DREW. Thank you. I will give this a shot again. We had some technical issues. So, although, Congress gave the TSA authority [inaudible] over pipeline [inaudible] in 2001 have recently been efforts to transfer its authority to the Department of Energy [inaudible]——

Mrs. WATSON COLEMAN. Mr. Van Drew is having technical problems again. We cannot hear you. So I will recognize Representative LaTurner.

Mr. LATURNER. Thank you, Madam Chair. My question is for Mr. Goldstein. Mr. Goldstein, how are you doing today?

Mr. GOLDSTEIN. Doing well, sir. Thank you.

Mr. LATURNER. Good. Thanks for being with us. Could you help us understand how many, just the scope, in the Federal Government, of how many different Government agencies are dealing with cybersecurity ransomware, either on an offensive or defensive nature?

Mr. GOLDSTEIN. Certainly, sir. So the existing model for Federal Government cybersecurity is—in the first instance, there are 2 agencies that are focused on cybersecurity incident response, and that is CISA, as they lead for asset response, which are efforts to understand and mitigate the immediate impacts of an incident, and then help to protect others. Then our colleagues at the FBI, who are the leads for threat response and focused on understanding the adversary, and then, of course, taking actions to disrupt or impose costs.

Apart from CISA and the FBI, there are a number of Sector Risk Management agencies that bring to bear specialized authorities in their sectors that may support CISA and the FBI for a cybersecurity incident affecting their sector. Then, of course, apart from these civilian space, both the Department of Defense and our Nation's intelligence community have unique authorities to either gather information about adversaries who are seeking to damage our country through cyber means, or, of course, take other measures to impose costs on our adversaries wherever they may be.

Mr. LATURNER. The Colonial Pipeline CEO recommended that there be designated a single point of contact to coordinate the response to cyber attacks and incidents at large. What is your reaction to that?

Mr. GOLDSTEIN. So sir, our goal as a U.S. Government is to make this as easy as possible for victims on cybersecurity incidents. Certainly, today if an organization calls CISA, if they call the FBI, if they even call their Sector Risk Management agency, they should get the same response.

So, we have worked deeply within the Federal Government to ensure that we are providing victims of cybersecurity incidents with all of the resources that the Federal Government can bring to bear. I think that this actually worked fairly well in the context of the Colonial intrusion where, you know, there was a wide breadth of Federal agencies based upon the unique attributes of this incident. But those agencies collaborated well together behind the scenes. Colonial was able to interact with a handful of agencies, and not, frankly, the full breadth of agencies with some authority to manage an incident of this complexity.

But certainly to your point, we can always do more to make this clearer in the private sector, and make sure that the activity of reporting an incident in the Federal Government, and engage in our health is as frictionless as possible and as simple as possible.

Mr. LATURNER. I talked to people in the private sector in my State that this has happened to, and it has happened to a lot, and

the number seems to be growing. So, it is a great concern to me that the Federal response to this can be kind-of clunky. It has been described, or suggested by some, that we have one person that coordinates this and have the ability to control the budgets of all of these other entities. Do you have a response to that?

Mr. GOLDSTEIN. So, sir, I think the answer is——

Mr. LATURNER. There is some precedence for it in the past as well. I am sorry. Go ahead, Mr. Goldstein.

Mr. GOLDSTEIN. Sure. Certainly, sir. So, certainly, the various agencies involved here, and certainly CISA and FBI have been the lead for cyber asset response, have unique authorities and unique capabilities to bring to bear. But you said it had the opportunity to hear testimony from our nominee for National cyber director just last week. That role, I think, will also help further codify the structure and the engagement model, and further streamline the manner in which the Federal Government engages with all manner of entities.

So we are looking forward both to the speedy confirmation of the National cyber director, as well as director for CISA. Both of those individuals, I think, will help the Government further mature our processes to simplifying engagement with the private sector.

Mr. LATURNER. Do you think that that solves the problem, though? Because, I think, from my perspective, it can still put us in the exact position that we are in right now. Maybe improve it, right? But at the end of the day, it is concerning to me that we don't have one point of contact who controls the budgets who can force these different bureaucracies to come together and make sure that our response in the United States is clear and concise and efficient. Do you think that those confirmations fix that problem?

Mr. GOLDSTEIN. I think that we are making progress over time in significant ways. I will say, sir, I was in this agency 5 years ago. Having recently come back in, we have made significant progress in the intervening time. I think the confirmation of both the new CISA director and the National cyber director will make another significant step forward in our ability to offer these sort-of simplified, cohesive engagement model that you described. But, assuredly, we will have more work to do because this is a deeply evolving space, and as the U.S. Government, we will have to evolve the pace.

Mr. LATURNER. Thank you for your——

Mrs. WATSON COLEMAN. Mr. LaTurner, your time has expired. Thank you. The Chair recognizes Representative Slotkin.

Ms. SLOTKIN. Thank you, Madam Chair. Thanks for our witnesses for being here. Two very different questions. So, you know, after the Colonial Pipeline was attacked, I went to all of the CEOs of the pipelines that criss-cross through Michigan, both over land and over sea, or under our inland seas, and asked them, like, what they were doing in the wake of the Colonial attack to improve their own cybersecurity, learning from the painful example that Colonial was offering us.

I know that we put in these new procedures at the end of May. So, I just want to understand, in a very concrete way, what actually happened? Let's say, Enbridge, which is a big pipeline company that goes under the Straits of Mackinac, a very sensitive

place in Michigan's Great Lakes. Let's say they are attacked. What is the actual procedure? Tell me the 9–1–1 process from the moment they are attacked in terms of engaging with Federal agencies? Whoever is the responsible party should take that one.

Mr. GOLDSTEIN. Sorry, ma'am. I will take it first, then I will yield to my colleague. Under—and I will defer to my colleague if this pipeline is in scope for the TSA directive. But the TSA directive does require a certain set of pipeline entities to report cybersecurity intrusions centrally to CISA. Upon receiving such a report, CISA triages the report based upon a standard methodology to assess the criticality of the incident, based upon risk to the country, the nature of the entity, the nature of the intrusion, and then certainly for an incident affecting an entity of the criticality that you note we would likely offer some measure of incident response or threat hunting assistance.

Now, I will note in this case it would still remain voluntary for this pipeline entity to accept our assistance. This entity could say, they have chosen to engage a third party, and that is how they want to engage their response. Now, even in that model, we would still encourage them to share information with us urgently so we can help them with the response and protect others. I am sorry, ma'am. Go ahead.

Ms. SLOTKIN. As a requirement, just so I understand, is it true that within 12 hours now, they must contact CISA? Is that the sort of requirement with the new rules that were put in place at the end of May?

Mr. GOLDSTEIN. Ma'am——

Ms. PROCTOR. Yes, ma'am.

Ms. SLOTKIN. OK. Perfect. So just so I understand, that is the 9–1–1 call they must make within 12 hours if they detect some sort of cyber intrusion. OK. I know it depends on the type of pipeline, but I understand.

Then a completely different question on sort-of the eve of a big meeting between President Biden and Vladimir Putin, where Putin had suggested that there be some sort of trade for groups that are conducting ransomware attacks, you know, from Russia, and groups that are allegedly conducting ransomware attacks from the United States.

Can you confirm for me—I know you are defensive and not offensive in nature, I know that you are not law enforcement—but, Mr. Goldstein, can you confirm in one sort-of yes or no, the United States of America has the ability to go after any criminal actors who are conducting ransomware attacks, here or abroad?

Mr. GOLDSTEIN. Ma'am, that question will get into the authorities vested in Federal law enforcement, which I am not able to answer.

Ms. SLOTKIN. OK. Have you seen the Russians do anything to try and clamp down on ransomware actors emanating from their soil?

Mr. GOLDSTEIN. Ma'am, I think, what I can say, generally, there is, you know, we strongly encourage all countries to take urgent action against ransomware actors operating within any country. The trend that we have seen of ransomware attacks over the past year suggest that such acts across the board is not being taken.

Ms. SLOTKIN. Right. So it is more—I understand it is not your jurisdiction. I guess I just want to make the point that a trade between Vladimir Putin and Joe Biden makes zero sense. Because we actually go after our criminals. We actually would take action if we had a ransomware group that were threatening other countries, that were attacking Russia, or attacking a European ally, or attacking China, that we would go after them, unlike the Russians, who have taken, at best, limited action against those, who we know, who we have said publicly, are attacking United States infrastructure.

So it is more of a statement. I just feel like this—until we get to the root of the problem that no action is being taken often by the Russians and the Chinese against actors emanating from their soil, we are going to keep having this conversation over and over again. I know I am out of time. I will leave it at that. Thanks very much.

Mrs. WATSON COLEMAN. Thank you. We will now recognize Representative Luria for 5 minutes. Thank you.

Mrs. LURIA. Thank you, Madam Chair, and the Chairs and Ranking Members of both committees for having this important hearing. I was reviewing one report, and I saw that there were over 304 million ransomware attacks world-wide in 2020. That was a 62 percent increase from 2019.

So the recent Colonial Pipeline ransomware attack was, obviously, not the first we have seen against critical infrastructure, but it spurred the fuel shortages across the Eastern Seaboard for several days. At the local level, I was seeing impacts like this as well in my district. For example, the Hampton Road Sanitation district suffered a ransomware attack last November that disrupted billing across the service region for several weeks.

I think that we can all agree that ransomware attacks are a National security crisis. As Chairman Thompson noted last week, the Colonial Pipeline ransomware attack raised serious questions about the cybersecurity practices of our critical infrastructure owners and operators, and whether the voluntary cybersecurity standards are sufficient to defend ourselves against these types of cyber threats.

So I wanted to the ask the question of our witnesses today. With regards to our critical infrastructure owners and operators, such as those that operate pipelines, what evidence do you and other agencies have that the organizations you oversee actually understand the extent of their cybersecurity risk?

Ms. PROCTOR. We offer briefings to owners and operators of critical infrastructure. Based on the threat that has been made clear over the last several years, we have arranged Classified briefings for owners and operators of infrastructure to ensure that they understand the nature of the threat. We also have provided assessments, vulnerability assessments, so that they can identify and then close those cybersecurity gaps to make themselves less likely to be a successful target for those who would be likely to launch those kinds of intrusions.

We also work with owners and operators to conduct exercises, so that they can actually exercise their plans. It is one thing to have plans on paper. It is another thing to be able to exercise those both

within your company, and within the region or with others in your industry.

So, we have a layered approach, both in terms of providing education, assessments, exercises to exercise those plans, and to be able to continue to inform of emerging threats, and to keep the cycle of both informing, exercising, and updating plans to keep that process under way.

Mrs. LURIA. Well, thank you. I mean that does sounds like a good resource, and a good way for them to understand the potential threats, the emerging threats that helped developing plans. But can you clarify—am I understanding that this is still all voluntary on behalf of the company?

Ms. PROCTOR. Well, currently, we certainly started out with the Pipeline Security Guidelines which were not mandatory. But as of May 28, we issued our first security directive, which has the power of regulation. We are in the process now of developing our second security directive, again, which will be mandatory, which will have more specific mandatory mitigating measures that will be required by owners and operators. That directive is going to be very specific. So there is going to be marked as an SSI document, security—excuse me, Security Sensitive Information. So that one will have a lot more detail and will be rather prescriptive in terms of the mitigation measures required.

Mrs. LURIA. Well, thank you. Just in the last couple of seconds remaining, do you have a good assessment for all of the operators of the major pipelines? Do you know where they are on a scale that shows both their awareness and preparedness, their plans, their training that they have completed in order to execute plans, and is that something you are tracking so that kind-of within the network of pipelines around the country, you know where the biggest vulnerabilities exist?

Ms. PROCTOR. Within the network of critical pipelines, we have conducted Corporate Security Reviews and Critical Facility Security Reviews with most of them. So we do have a good baseline for them in terms of where they are with regard to their corporate plans, their cybersecurity plans, and also, with their critical facilities in the field. So both are assessments that we continually perform with owners and operators in the pipeline community.

Mrs. LURIA. OK. Well, thank you very much. Ma'am, my time has expired. I yield back.

Mrs. WATSON COLEMAN. Thank you very much. The Chair recognizes Representative Rice.

Miss RICE. Thank you so much. Mr. Goldstein, I know that Chairman Thompson had asked you some questions about, you know, additional resources and such. I mean, it is clear that, you know, your agency has issued extensive ransomware guidance and led efforts such as the Reduce the Risk of Ransomware Campaign to help owners and operators of critical infrastructure prepare for ransomware threats. But we also know that, you know, the Colonial hack demonstrates that even when companies are willing to self-report and engage with law enforcement after a ransomware attack, they may not report to, or engage directly with CISA. I think that is one of the issues we need to address here.

So, is this something that, you know, CISA is not being clear enough to owners and operators about the value added that you could bring to their protection of their, you know, critical infrastructure? Or is it just that they are saying thanks, but no thanks.

Mr. GOLDSTEIN. There is certainly more that we can do to make sure that companies across sectors understand the unique value proposition, which we discussed in response to Congressman Langevin's question, about engaging CISA and the way that that value is unique and additive to engaging a third-party response firm, and additive to engaging with Federal law enforcement. We worked very closely with our partners in law enforcement and often conduct joint responses, because we are achieving different mission objectives where we support a victim organization. So, certainly continuing to clarify the value proposition that CISA brings to the table, and differentiating that and showing that it is complementary to engaging other partners, I do think is a critical area for the work for the agency.

Miss RICE. What percentage of ransomware attacks would you say get reported to CISA?

Mr. GOLDSTEIN. So, ma'am, as noted, due to the real challenge we have here with visibility, we don't have a good number there. What I would say is after recent intrusions of Colonial, JBS Foods, et cetera, we are seeing a real increase, both in organizations that are reporting incidents, and also in organizations that are availing themselves of CISA's guidance and best practices. As just one example, in the week after the Colonial intrusion, I think we saw increased views of our ransomware guide, I think, something like 400 percent for that week after.

So, we are seeing organizations across the country recognize this risk and recognizing that CISA is a source of support and expertise. We just need to make sure that that continues, and that we reach again into every corner of the country going forward.

Miss RICE. Well, I agree with that, Mr. Goldstein, but I also think it is also really important for whatever Federal agency it is that gets contacted by an operator of a critical piece of infrastructure in this country, that whether they take it to the FBI—if the FBI brings in CISA, and whatever other agency, Federal agency we need to partner with to address this as comprehensively as possible. I hope that that is what the practices is—or if it isn't, will be, going forward.

Ms. Proctor, just in the past few weeks, a ransomware attack against a Massachusetts ferry operator shut down travel between the State and its islands. It was revealed that hackers had breached the networks of New York's MTA on whose trains my constituents work and ride every day.

Now, neither of those hacks posed a risk for passenger safety, but, you know, cyber attacks targeting mass transit, railways, aviation, they have the potential to put travelers at risk, and would be massively disruptive to society writ large. So can you, specifically, discuss the recent ransomware attack against the MTA?

Ms. PROCTOR. Yes, ma'am. As a matter of fact, I can. After that incident, I actually did speak with New York's MTA's CISO. I did learn from speaking with him that the attack was not considered to be successful. They did not actually access information in the

system. They did not make a demand for ransom. They did not acquire information from the MTA. The example that the CISO used would be that the ransomware intrusion opened the screen door, but did not get in the front door.

Miss RICE. OK. So thank you.

Ms. PROCTOR. That was the example that they used. They did not acquire anything in that attack.

Miss RICE. Thank you for that clarification. I think it is really important for TSA to engage with MTA and other public transit agencies on security measures, and cybersecurity, in particular, not just private-sector companies who are running pieces of critical infrastructure. Thank you both so much, and I yield back the balance of my time.

Mrs. WATSON COLEMAN. Thank you. I recognize Mr. Gottheimer from New Jersey.

Mr. GOTTHEIMER. Thank you, Chairwoman Watson Coleman also from New Jersey, and Chairwoman Clarke for recognizing me and arranging today's important hearing on cyber threats to pipelines.

The recent ransomware attack on the United States' largest fuel pipeline, Colonial Pipeline, I think many Americans across these East Coast experience a rush on gas and long lines at the pump because of the collective failure to secure our critical infrastructure from hackers, as we have heard time and time again today and before.

I think it is fair to say that Colonial had serious security flaws, including an outdated VPN system which permitted ransomware hackers to breach Colonial systems that required dual-factor authentication. But I am also concerned that Colonial's spotty record of engagement with TSA, which since 9/11, has been tasked with securing our pipelines by conducting voluntary assessments of private operators.

If I can ask Assistant Administrator Proctor, we may know that on multiple occasions prior to the attack on May 7, TSA requested cybersecurity assessment of Colonial's system, but Colonial repeatedly punted, and has yet to participate in these assessments. Can you please compare TSA's experience with Colonial to the cooperation you received from other pipeline operators?

Ms. PROCTOR. Yes, sir. I would speak to that in that the experience we have had with Colonial is—it is for the request that they have made to reschedule, not unusual during the pandemic. During the pandemic, there were a number of companies that had limited personnel on-site. They considered their personnel on-site to be essential personnel. They did restrict them from a lot of interaction with outsiders. So Colonial had postponed a discussion to get a scheduled date for their VADR assessment.

The postponement was not unusual for other companies. Other companies did go through. We did pivot, and we did manage to find a way to conduct the VADR virtually. So we were able to schedule those in other cases.

The Colonial discussion was postponed because they were installing some new software. At one point, they were doing some other updates, and we had a focus in March. They had asked for about 6 weeks to complete some cyber updates. The 6 weeks was actually a week after the incident with Colonial. We have since focused on

getting that date in place. They are now scheduled for the last week of July for their Validated Architecture Design Review.

Mr. GOTTHEIMER. Got it. Has a pipeline ever flat-out refused to cooperate with an inspection or assessment, or tried to limit the scope of what you are assessing?

Ms. PROCTOR. No, it wasn't a refusal, it was rescheduling the discussion so that they could deal with personnel issues. At one point, we had a conversation set with them, and they had several employees that were COVID-impacted. So they delayed that.

Mr. GOTTHEIMER. I am sorry to interrupt. I was just going to ask, is that similar in terms of others' ever having done the same thing where they have delayed? Have others refused? Other pipelines? Is this consistent, with the last little extra time?

Ms. PROCTOR. We have had other delays, but we have gotten to the point where we have done those assessments. We had worked out a way to do them virtually, so it made this more manageable for the company, even though they were trying to protect their essential employees from engaging with outsiders.

Mr. GOTTHEIMER. Got it. Thank you so much.

Mr. Goldstein, you recently witnessed a series of attacks, not just against pipelines, but also against mass transportation infrastructure. Clearly, we need robust cybersecurity standards for the transportation sector writ large. What additional measures can we take to protect this sector not just from ransomware hackers, but, also, determined nation-state adversaries like China, Iran, or North Korea?

Mr. GOLDSTEIN. Thank you, sir. The good news here is that there is nothing particularly unique about ransomware intrusions. The sorts of cybersecurity advisories and best practices that are promulgated by CISA and the sorts of cybersecurity directives that we impose upon Federal civilian agencies are effective against ransomware actors, nation-states, and really any adversaries.

In addition, as we think through the more sophisticated types of adversaries that may want to cause more lasting damage or gain more persistence, that is where a program like CyberSentry really comes into play. Our ability to gain persistent visibility into cybersecurity risks affecting our most critical infrastructure. By broadening and maturing that pilot program, we will be able to get more visibility and drive targeted action to drive out those risks of intrusions as soon as they are identified.

Mr. GOTTHEIMER. Thank you. I yield back. Thank you so much, gentleman.

Mrs. WATSON COLEMAN. Thank you very much. With that, I want to thank the witnesses. Your testimony has been invaluable, enlightening, and thank you so much.

The Members of the subcommittee may have additional questions for you all, the witnesses, and we ask that you respond expeditiously in writing to those questions. The Chair reminds Members of the subcommittee that the committee's record will remain open for 10 days. Without objection, the subcommittee stands adjourned. Thank you so much.

[Whereupon, at 4:33 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTION FROM HONORABLE JEFFERSON VAN DREW FOR SONYA T. PROCTOR

Question. I understand there are growing concerns that the TSA's performance in pipeline security has been inadequate. Given the recent attack on Colonial, I am inclined to share those concerns.

Although Congress gave the TSA authority over pipeline security in 2001, there have recently been efforts to transfer its authority to the Department of Energy. Do you believe that the TSA should retain its authority, and what assurance can you provide us that the TSA will expand and improve on its Pipeline Security Guidelines?

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

QUESTION FROM HONORABLE JEFFERSON VAN DREW FOR ERIC GOLDSTEIN

Question. During last week's hearing, Colonial Pipeline CEO Joseph Blount stated that he did not feel like including CISA at this state of their response would add much value. Moreover, Colonial chose to hire private firms to assist with their recovery efforts from the ransomware attack last month instead of working with CISA.

Does Colonial's decision to hire private companies instead of working with CISA concern you?

Do you feel that CISA maintains a competitive edge in the cyber realm? What can CISA improve upon to incentivize organizations who are victims of cyber attacks to collaborate with the agency?

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