CYBER THREATS IN THE PIPELINE: USING LESSONS FROM THE COLONIAL RANSOMWARE ATTACK TO DEFEND CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JUNE 9, 2021

Serial No. 117–15

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
45–085 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*

CONTENTS

CYBER THREATS IN THE PIPELINE: USING LESSONS FROM THE COLONIAL RANSOMWARE ATTACK TO DEFEND CRITICAL INFRASTRUCTURE

Wednesday, June 9, 2021

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

The committee met, pursuant to notice, at 12 p.m., via Webex, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Payne, Correa, Slotkin, Cleaver, Clarke, Titus, Watson Coleman, Rice, Demings, Gottheimer, Torres, Katko, McCaul, Bishop, Van Drew, Norman, Miller-Meeks, Harshbarger, Clyde, Meijer, Cammack, Pfluger, and Garbarino.

Chairman THOMPSON. The Committee on Homeland Security will come to order. The committee is meeting today to receive testimony on "Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure." Without objection, the Chair is authorized to declare the committee in recess at any point. The gentlelady from New Jersey, Mrs. Watson Coleman, shall assume the duties of the Chair, should I have technical difficulty. I now recognize myself for an opening statement.

Last month, malicious hackers infiltrated Colonial Pipeline's network and infected its IT systems with ransomware. For nearly a week, 5,500 miles of pipeline supplying 45 percent of the fuel on the East Coast was shut down, and panic buying resulted in fuel shortages in the Southeast. Since pipeline service was restored, we have learned more about what happened. We know hackers exploited an unprotected VPN account that was no longer in use to gain access to Colonial Pipeline's network. We know Colonial Pipeline paid the ransom demand and the FBI has since recovered most of it. We know Colonial Pipeline is hardly alone.

This spring, ransomware attacks hit the world's largest meat processor, transportation systems in New York City and Martha's Vineyard, and Scripps Health in San Diego. But the potential impact of a long-term shutdown of the country's biggest pipeline crystalized the devastating consequences of ransomware. More importantly, it raised serious questions about the cybersecurity practices of critical infrastructure owners and operators and whether voluntary cybersecurity standards are sufficient to defend ourselves against today's cyber threats.

I was glad to see the Transportation Security Administration issue a security directive to mandate some security requirements for the pipeline industry, but more requirements may still be needed to drive the policies necessary to defend against and mitigate the impacts of future ransomware attacks. We need a complete understanding of the circumstances surrounding the ransomware attack against Colonial and the decisions it made during the incident response.

Today, our goal is to examine the cybersecurity practices in place at Colonial prior to the May 2021 ransomware attack, and assess whether other critical infrastructure operators might be similarly situated and vulnerable. We need to understand the degree to which Colonial utilized the full range of security resources made available by TSA, Colonial's Sector Risk Management Agency, and Cybersecurity Infrastructure Agency. I am troubled by reports that Colonial declined repeated offers by TSA over the past year to assess its security defenses.

We also need to understand whether Colonial had a ransomware incident response and continually of operation plan—continuity of operation plan and whether it had been practiced and tested. Government officials and cybersecurity experts have been warning about the growing threat of ransomware for years. We need to know how private-sector entities, like Colonial, acted on these warnings. I am concerned that too few have robust cyber incident response and continuity of operation plans in place.

Finally, we need to understand the threat actor, how it targets victims, what tools it utilizes to infiltrate networks, and how we can deter this kind of behavior.

Before I close, I would like to commend the FBI for its work recovering Colonial's ransomware payment and depriving the hackers of the financial benefit of their malicious cyber activity. I hope the FBI success serves as an incentive for future ransomware victims to engage with law enforcement early. I hope Colonial will use the recouped money to make necessary improvements in its cybersecurity.

I look forward to a productive discussion, and I thank the witnesses for being here today. With that, I recognize the Ranking Member, the gentleman from New York, Mr. Katko, for an opening statement.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JUNE 9, 2021

Last month, malicious hackers infiltrated Colonial Pipeline's network and infected its IT systems with ransomware. For nearly a week, 5,500 miles of pipeline supplying 45 percent of the fuel on the East Coast were shut down, and panic buying resulted in fuel shortages in the Southeast. Since pipeline service was restored, we have learned more about what happened.

We know hackers exploited an unprotected VPN account that was no longer in use to gain access to Colonial Pipeline's networks. We know Colonial Pipeline paid the ransom demand—and the FBI has since recovered most of it. And we know Colonial Pipeline is hardly alone—this spring, ransomware attacks hit the world's largest meat processor, transportation systems in New York City and Martha's Vineyard, and Scripps Health in San Diego.

But the potential impact of a long-term shut-down of the country's biggest pipeline crystalized the devastating consequences of ransomware. More importantly, it

raised serious questions about the cybersecurity practices of critical infrastructure owners and operators and whether voluntary cybersecurity standards are sufficient to defend ourselves against today's cyber threats.

I was glad to see the Transportation Security Administration issue a security directive to mandate some security requirements for the pipeline industry—but more requirements may still be needed. To drive the policies necessary to defend against and mitigate the impacts of future ransomware attacks, we need a complete understanding of the circumstances surrounding the ransomware attack against Colonial and the decisions it made during incident response.

Today, our goal is to examine the cybersecurity practices in place at Colonial prior to the May 2021 ransomware attack, and assess whether other critical infrastructure operators might be similarly situated and vulnerable. We need to understand the degree to which Colonial utilized the full range of security resources made available by TSA—Colonial's sector risk management agency—and the Cybersecurity and Infrastructure Security Agency (CISA). I am troubled by reports that Colonial declined repeated offers by TSA over the past year to assess its security defenses. We also need to understand whether Colonial had a ransomware incident response and continuity of operations plan and whether it had been practiced and tested.

Government officials and cybersecurity experts have been warning about the growing threat of ransomware for years. We need to know how private-sector entities like Colonial acted on those warnings. Finally, we need to understand the threat actor—how it targets victims, what tools it utilizes to infiltrate networks, and how we can deter this kind of behavior.

Before I close, I would like to commend the FBI for its work recovering Colonial's ransomware payment and depriving the hackers of the financial benefit of their malicious cyber activity. I hope the FBI's success serves as an incentive for future ransomware victims to engage with law enforcement early. And, I hope Colonial will use the recouped money to make necessary improvements to its cybersecurity.

Mr. KATKO. Thank you, Mr. Chairman, and I thank you for calling this most timely and important hearing today. I thank you for your continued partnership in the joint effort to increase American cybersecurity resilience. From the added integrity on Federal systems to pipelines, to meat processing, to e-transportation assets, the connected systems that underpin our way of life are constantly under attack by cyber adversaries. It has been getting worse and it must stop. This isn't hypothetical or the plot of a Hollywood film. These attacks on our critical infrastructure are happening right in front of our eyes.

The next steps we take are of vital importance. They should be a mix of short-term tactical and longer-term foundational policy shifts. The next step, the Government will need to take the lead in certain areas. For other responsibilities, the onus will be on industries.

Throughout all of this, however, we must work together. Foundational to the work of this committee must be maximizing the role of CISA. We must mature the relationship between CISA and the Nation's lead civilian cybersecurity agency with centralized capacity and tools, and the Sector Risk Management Agencies, who have the sector-specific relationships and expertise. Optimizing, not eroding, these relationships between CISA and the various SRMAs will be critical going forward. Now is not the time to relitigate previous turf battles.

I am hopeful that the recent TSA security directive is an important first step forward in strengthening both TSA and CISA's ability to respond to these rapidly evolving cyber threats, although there is a valid question of why it took so long for TSA to finally leverage this authority. It is vital that TSA be relentless in its focuses going forward to secure the Nation's 2.7 million miles of pipe-

lines. TSA needs to continue to involve industry in the implementation of this security directive and future ones.

As we continue to provide clarity and confidence in Federal roles and responsibilities, we also must keep on the full court press to provide CISA with the resources it needs to help the critical infrastructure community. I recently introduced H.R. 1833, the DHS Industrial Control Systems Capabilities Enhancement Act of 2021, a bill with bipartisan support that is designed to protect critical infrastructure from cyber attacks and further bolster the deployable and scalable pool of resources CISA offers to assess—to assist stakeholders. I am pleased that this bill passed out of committee unanimously, and I am hopeful for its prompt consideration on the floor of the House.

Make no mistake about it, the Federal Government has some significant execution challenges on the horizon where it cannot afford to fumble. I recently worked with the Chairman to sound the alarm on the implementation time line of continuity of the economy planning as mandated by last year's NDAA. This is a provision we supported that was designed exactly for moments like this. Where is it? We need it now, and we need it the most.

Following the devastating SolarWinds attack in December 2020, I created a 5-pillar plan to enhance American cybersecurity. I am encouraged to see that the software-heavy provisions of the administration's new cyber Executive Order tread very closely to my suggestions, but, again, we must hold the administration's feet to the fire to ensure the aggressive but necessary deadlines are met.

The Federal Government also faces a moment of reckoning when it comes to deterrents. While many of the recent hacks have come from so-called apolitical organizations, certain countries, in particular Russia, are creating safe havens for these bad actors. The President is meeting with Putin next week. I hope to see the President send a clear message: Turning a blind eye to cyber criminals who attacked our critical infrastructure is completely unacceptable. He must make it abundantly clear what the continued harboring of these groups will mean. Ultimately, strength only respects strength, and that is what we need to project now.

As we learned from incidents, from like the Colonial Pipeline ransomware attack, I do believe the private sector also must look hard in the mirror. While I don't think a culture of blaming the victim is ultimately constructive, clearly, and I mean clearly, we can all do better to protect our critical infrastructure networks.

I appreciate Colonial Pipeline's identification of places where they are now hardening systems in response to the devastating ransomware attack in May, but this begs an obvious question: If your pipeline provides fuel to 45 percent of the East Coast, why are you only hardening your systems after an attack has occurred? Why wasn't it done beforehand? Again, I am not interested in blaming the victim here, but we must all learn from these incidents to prevent future destruction.

As we painfully witnessed a string of even more ransomware attacks since Colonial, it is clear to all of us that we must break the ransomware business model once and for all. We cannot accept default to accepting extortion. As an industry leader, there is certainly heavy pressure to get your own systems up and running

when facing a frightening cyber attack. But these the effects of today only fund some ransomware attacks of tomorrow.

Everything should be on the table here with know your customer and cryptocurrency reporting requirements being the low-hanging fruit. While it is encouraging that the FBI was able to recover the majority of the bitcoin ransom in this instant, and I, along with the Chairman, applaud them for that, we can't rest on the capability of this happening going forward.

Finally, this string of devastating cyber incidents with real-world impacts has reinforced that we need a codified process of identifying systematically important critical infrastructure. I look forward to working with a wide range of stakeholders to get this right. I anticipate that much of today's hearing will highlight just how much time is of the essence. I am heartened to see that tomorrow the Senate will hold confirmation hearings for the CISA and National cyber directors. Let us keep our foot on the gas pedal. Let us work together. There is no other option.

I yield back, Mr. Chairman.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

I thank the Chairman for calling this timely and important discussion, and I thank him for his continued partnership in the joint effort to increase American cybersecurity resilience. From data integrity on Federal systems, to pipelines, to meat processing, to key transportation assets—the connected systems that underpin our very way of life are under constant attack by cyber adversaries. It's been getting worse, and it must stop. This isn't hypothetical or the plot of a Hollywood film. These attacks on our critical infrastructure are happening right in front of our eyes.

The next steps we take are of vital importance. They should be a mix of short-term tactical and longer-term foundational policy shifts. The Government will need to take the lead in certain areas. For other responsibilities, the onus will be on industry. Throughout all of this, however, we must work together.

Foundational to the work of this committee must be maximizing the role of CISA. We must mature the relationship between CISA—as the Nation's lead civilian cybersecurity agency with centralized capacity and tools—and the Sector Risk Management Agencies, who have the sector-specific relationships and expertise. Optimizing, not eroding, these relationships between CISA and the various SRMAs will be critical going forward. Now is not the time to relitigate previous turf battles.

I am hopeful that the recent TSA security directive is an important step forward in strengthening both TSA and CISA's ability to respond to these rapidly-evolving cyber threats, although there's a valid question of why it took so long for TSA to finally leverage this authority. It's vital that TSA be relentless in its focus going forward to secure the Nation's 2.7 million miles of pipelines. TSA needs to continue to involve industry in the implementation of this security directive and future ones.

As we continue to provide clarity and confidence in Federal roles and responsibilities, we also must keep on the full court press to provide CISA with the resources it needs to help the critical infrastructure community. I recently introduced H.R. 1833, the DHS Industrial Control Systems Capabilities Enhancement Act of 2021, a bill with bipartisan support that is designed to protect critical infrastructure from cyber attacks and further bolster the deployable and scalable pool of resources CISA offers to assist stakeholders. I am pleased that this bill passed out of committee unanimously and look forward to its prompt consideration on the floor of the House.

Make no mistake—the Federal Government has some significant execution challenges on the horizon where it cannot afford to fumble. I recently worked with the Chairman to sound the alarm on the implementation time line of Continuity of the Economy planning as mandated by last year's NDAA. This is a provision we supported that was designed exactly for moments like this. Where is it now when we need it the most?

Following the devastating SolarWinds hack in December 2020, I created a 5-pillar plan to enhance American cybersecurity. I am encouraged to see that the software-heavy provisions of the administration's new Cyber Executive Order track very

closely to my suggestions. But again, we must hold the administration's feet to the fire to ensure the aggressive, but necessary, deadlines are met.

The Federal Government also faces a moment of reckoning when it comes to deterrence. While many of the recent hacks have come from so-called "apolitical" organizations, certain countries, in particular Russia, are creating safe havens for these bad actors. The President has a meeting with Putin next week. I hope to see the President send a clear message that turning a blind eye to cyber criminals who attack our critical infrastructure is completely unacceptable. He must make it abundantly clear what the continued harboring of these groups will mean. Ultimately, strength only respects strength, and that's what we need to project now.

As we learn from incidents like the Colonial Pipeline ransomware attack, I do believe the private sector also must look hard in the mirror. While I don't think a culture of blaming the victim is ultimately constructive, clearly we can all do better to protect our critical networks. I appreciate Colonial Pipeline's identification of places where they are now hardening systems in response to the devastating ransomware attack in May, but this begs an obvious question. If your pipeline provides fuel to 45 percent of the East Coast, why are you only hardening systems after an attack? Again, I'm not interested in blaming the victim here, but we all must learn from these incidents to prevent future destruction.

As we've painfully witnessed a string of even more ransomware attacks since Colonial, it's clear to all of us that we must break the ransomware business model once and for all. We cannot default to accepting extortion. As an industry leader there is certainly heavy pressure to get your own systems up and running when facing a frightening cyber attack, but the easy fix of today only funds the ransomware attacks of tomorrow. Everything should be on the table here, with Know Your Customer and cryptocurrency reporting requirements being the low-hanging fruit. While it is encouraging that the FBI was able to recover the majority of the Bitcoin ransom in this instance, we can't rest on this capability as free pass going forward.

Finally, this string of devastating cyber incidents with real-world impacts has reinforced that we need a codified process of identifying Systemically Important Critical Infrastructure. I look forward to working with a wide range of stakeholders to get this right.

I anticipate that much of today's hearing will highlight just how much time is of the essence. I'm heartened to see that tomorrow the Senate will hold confirmation hearings for the CISA and National cyber directors. Let's keep our foot on the gas pedal. There is no other option.

Chairman THOMPSON. Thank you very much, Mr. Ranking Member. Other Members of the committee are reminded that under committee rules, opening statements may be submitted for the record.

[The statement of Honorable Sheila Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

JUNE 9, 2021

Chairman Thompson, and Ranking Member Katko thank you for holding today's hearing on "Cyber Threats in the Pipeline: Using Lessons Learned from the Colonial Ransomware Attack to Defend Critical Infrastructure."

I look forward to the questions that will follow the testimony of:

- Mr. Joseph A. Blount, Jr., president & CEO, Colonial Pipeline Company; and
- Mr. Charles Carmakal, senior vice president for strategic services & CTO, FireEye.

I thank today's witnesses for agreeing to testify before the House Homeland Security Committee.

The private sector has 85 percent of the Nation's critical infrastructure and much of it has some connectivity to the internet—they can no longer go it alone.

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

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

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

The market and regulatory forces that should have forced security and safety improvements on computing technology never developed due to interference from Congress and the courts that excused or deflected culpability for known computing tech-

nology errors or omissions in product development or manufacturing that left systems open to attack.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This is especially critical to the protection of large complex information systems that run on applications and hardware that may be decades old, which is the case with some supervisory control and data acquisition (SCADA) control system archi-

tectures that are pervasive in the provision of essential services provided critical infrastructure owner and operators.

H.R. 2890 bolsters the efforts to engage critical infrastructure owners and operators in communicating cybersecurity threats; and lays the foundation for greater transparency on the real threats posed by cyber terrorist to private and Government sector critical infrastructure and information systems.

The legislation allows the Science and Technology Directorate in consultation with CISA to establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities to information systems and industrial control systems including supervisory control and data acquisition systems.

This bill when it becomes law would put our Nation's best minds to work on closing the vulnerabilities that cyber thieves and terrorists to use them to access, disrupt, corrupt or take control of critical infrastructure and information systems.

In addition to these changes, the bill requires a report to Congress that may contain a Classified annex.

NEED FOR THE REPORT'S CLASSIFIED ANNEX

Congress needs to know how prevalent and persistent cybersecurity threats targeting critical infrastructure and information systems might be, especially if those threats result in a payment of ransom.

As the Chair of the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security, I can assure you that the best way to keep criminals at your door is to give them what they want.

The initial post event news report said that Colonial Pipeline may have paid a ransom to regain control of its pipeline is particularly troubling because of what this, if true, might mean for the entire oil and gas industry at every level.

Paying a ransom for ransomware emboldens and encourages cyber bad actors and places everyone at greater risk for the financial and societal costs of increases in threats as other seek payouts.

As long as there is silence about cyber attacks like ransomware the criminals and terrorists will remain out of reach and continue to feel safe in carrying out these attacks often from the soil of our enemies or peer competitors.

A company cannot stand up to Russia or China, but the United States can and has done so to protect our National interest.

I applaud and thank the Biden administration for its quick action to respond to the attack against Colonial Pipeline in issuing a new Executive Order.

It is troubling that some news accounts report that Colonial Pipeline did not respond to the administration when contacted about the attack against its pipeline.

If true, the cyber terrorist may have been aided in their attack by this lack of cooperation and engagement by the target with authorities that could provide aid and unbounded access to know how to address the crisis created by the attack.

Today, our Nation is in a cybersecurity crisis.

My concern regarding the security of information networks began in 2015 when the Office of Personnel Management's data breach resulted in the theft of millions of sensitive personnel records on Federal employees.

What few understood in 2015 was that the attack on the OPM may have actually begun in 2013 when cyber criminals breached the computer network and stole the operation manuals for the agency's information system.

The on-going attacks against Federal, State, local, territorial, and Tribal governments, as well as threats posed to private information systems, and critical infrastructure systems makes this bill necessary.

On May 13, 2021 it was reported that the DC Metropolitan Police Department had experienced the worst reported cyber attack against a police department in the United States.

The gang, known as the Babuk group, released thousands of the Metropolitan Police Department's sensitive documents on the dark web.

A review by The Associated Press found hundreds of police officer disciplinary files and intelligence reports that include feeds from other agencies, including the FBI and Secret Service.

This type of attack has the potential to undermine trust within the ranks regarding the security of personal information in the department's information network as well as reduce cooperation of other Federal law enforcement agencies with the DC Police Department out of cybersecurity concerns.

These problems are not limited information related to Government employees.

In February 2021, a cyber attack on an Oldsmar, Florida water treatment facility involved increasing the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million in drinking water.

At low levels sodium hydroxide is used in the treatment of drinking water to raise the pH of the water to a level that minimizes the corrosion.

Raising the pH remains one of the most effective methods for reducing lead corrosion and minimizing lead levels in drinking water.

However, the levels of this chemical in the water produced by Oldsmar, Florida was increased to levels that would cause harm to people if they drank or used it.

This is just one example of how terrorists can attack critical infrastructure and cause threats to health, safety, and life.

Cyber terrorists and cyber criminals are also motivated to attack information networks in exchange for money.

This was the case with the DC Metropolitan Police Department who were threatened if they did not pay the thieves.

The sources of revenue from cyber attacks has moved from demands of payment for thieves not to release information—to the sale of stolen information on the dark web and now to a sophisticated denial of service attack in the form of ransomware that locks a system using encryption until the victim pays.

RANSOMWARE

Ransomware is becoming the tool of choice for those seeking a payout because it can be carried out against anyone or any entity by perpetrators who are far from U.S. shores.

The ill-gotten gain reaped from ransomware can be used to fuel terrorist networks, drug cartels, attacks against the homeland, human trafficking, or other efforts to undermine homeland security.

The Colonial Pipeline incident is just one in a long line of successful attacks or infiltrations carried out against domestic information systems and critical infrastructure with increasing consequences for the life, health, safety, and economic security of our citizens.

There is no way of knowing how many attacks resulted in payouts to criminals, who would use the funds to fuel additional attacks that target business, Government, or other entities in the United States.

There are few concrete details on how the cyber attack took place, and it is likely that this will not change until Colonial Pipeline and the third-party company brought in to investigate have concluded their analysis of the incident.

However, what did occur was a ransomware outbreak, linked to the DarkSide group, that struck Colonial Pipeline's networks.

The initial attack entry point into Colonial Pipeline's network is not known, but it may have been an old, unpatched vulnerability in a system; an email that got passed its firewall to an employee who opened it unknowingly; the use of a legitimate employee's computer access credentials that were purchased or obtained by the thieves that were leaked previously, or any other number of tactics employed by cyber criminals to infiltrate a company's network.

There would be no need for the Cybersecurity Vulnerability Remediation Act if owners and operators were succeeding in meeting the cybersecurity needs of critical infrastructure.

I know that there is more that should and ought to be done to address the issue of cyber crime and I will be pursuing this avenue under the jurisdiction of the House Judiciary Committee, as the Chair of the Subcommittee on Crime, Terrorism, and Homeland Security.

Thank you.

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

I welcome our witnesses. Our first witness, Mr. Joseph Blount, is the president and CEO of Colonial Pipeline. Mr. Blount joined Colonial in 2017, with more than 3 decades of experience in the energy industry. Our second witness, Mr. Charles Carmakal, is senior vice president and chief technology officer at FireEye Mandiant. In that role, he oversees a team of security professionals that assist organizations in responding to security breaches by foreign govern-

ments and organized criminals. Without objection, the witnesses' full statements will be inserted in the record.

I now ask Mr. Blount to summarize his statement for 5 minutes.

STATEMENT OF JOSEPH BLOUNT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, COLONIAL PIPELINE

Mr. BLOUNT. Chairman Thompson, Ranking Member Katko, and Members of the committee, my name is Joe Blount, and since 2017, I have served as president and CEO of the Colonial Pipeline Company. Thank you for the opportunity to testify before the committee today.

Since 1962, we have been shipping and transporting refined products to market. Our pipeline system spans over 5,500 miles. It is one of the most complex pieces of energy infrastructure in America, if not the world. On any given day, we transport more than 100 million gallons of gasoline, diesels, jet fuel, and other refined products. Shipping that product safely and securely is what we do. The product we transport accounts for nearly half of the fuel consumed on the East Coast, providing energy for more than 50 million Americans, the Americans who rely on us to get the fuel to the pump, but so do cities and local governments. We supply fuel for critical operations, such as airports, ambulances, and first responders.

The safety and security of our pipeline system is something we take very seriously, and we always operate with the interest of our customers, shippers, and the country first in mind. Just 1 month ago, we were the victims of a ransomware attack by a cyber criminal group, and that attack encrypted our IT systems. Although the investigation is still on-going, we believe the attacker exploited the legacy VPN profile that was not intended to be in use. DarkSide demanded a financial payment in exchange for a key to unlock the impacted systems. We had cyber defenses in place, but the unfortunate reality is those defenses were compromised. This attack forced us to make difficult decisions, choices in real-time, that no company ever wants to face. But I am proud of the way our people reacted quickly to isolate and contain the attack, so we could get the pipeline back up and running safely.

I am also very grateful for the immediate and sustained support of law enforcement, CISA, and other Federal authorities, including the White House. We reached out to Federal authorities within hours of the attack, and they have continued to be true allies as we worked so quickly and safely to restore our operations. I especially want to thank the Department of Justice and the FBI for their leadership and the progress they announced in this matter earlier this week.

I also want to express my gratitude to the employees of Colonial Pipeline and the American people for your actions and support as we responded to the attack and dealt with the disruption that it caused. We are deeply sorry for the impact that this attack had, but we are also heartened by the resilience of our country and of our company.

Finally, I want to address 2 additional issues that I know are on your minds, and I am going to address them in the only way I know how to, directly and honestly.

First, the ransom payment. I made the decision to pay and I made the decision to keep the information about the payment as confidential as possible. It was the hardest decision I have ever made in my 39 years in the energy industry. I know how critical our pipeline is to the country, and I put the interest of the country first. I kept the information closely held because we were concerned about operational security and we wanted to stay focused on getting the pipeline back up and running. I believe with all my heart that it was the right choice to make. I also want to now state publicly that we quietly and quickly worked with law enforcement in this matter from the start, which may have helped lead to the substantial recovery of funds announced by the DOJ this week.

Second, we are further hardening our cyber defenses. We have rebuilt and restored our critical IT systems and are continuing to enhance our safeguards, but we are not yet where I want us to be. If our CIO needs resources, she will get them. We also have brought in several of the world's leading experts to help us fully understand what happened and how we can continue, in partnership with you, to add defenses and resiliency to our networks.

I especially want to thank Mandiant, Dragos, and Black Hills on the consultant side, and the White House and all the Government agencies who assisted us, both with the criminal investigation and with the restart of the pipeline. We are already working to implement the recent guidance and directives on cybersecurity. Our forensic work continues and we will learn more in the months ahead. I appreciate your support and I look forward to our discussion today.

[The prepared statement of Mr. Blount follows:]

PREPARED STATEMENT OF JOSEPH BLOUNT

JUNE 9, 2021

I. INTRODUCTION

Chairman Thompson, Ranking Member Katko, and Members of the committee: My name is Joe Blount, and since late 2017, I have served as the president and chief executive officer of Colonial Pipeline Company. Thank you for the opportunity to testify before the committee today.

The Colonial Pipeline Company was founded in 1962 and is proud of its long history of connecting refineries with customers throughout the Southern and Eastern United States. Today, we have about 950 employees across the United States. Colonial Pipeline is the largest refined products pipeline by volume in the country and transports many products, such as gasoline, diesel, aviation fuels, and home heating oil. Our pipeline system is one of the most complex pieces of infrastructure in America, if not the world. On any given day, we may transport more than 100 million gallons of product. Shipping that product is what we do. We do not own the fuel, the refineries, the marketers, or gas stations. Rather, we transport it from 29 refineries in the Gulf Coast all the way up to the New York Harbor.

Colonial Pipeline is cognizant of the important role we play as critical infrastructure. We recognize our significance to the economic and National security of the United States and know that disruptions in our operations can have serious consequences. Our pipeline system spans more than 5,500 miles. The product we transport accounts for nearly half of the fuel consumed on the East Coast, providing energy for more than 50 million Americans. Not only do everyday Americans rely on our pipeline operations to get fuel at the pump, but so do cities and local governments, to whom we supply fuel for critical operations, such as airports, ambulances, and first responders. The safety and security of our pipeline system is something we take very seriously, and we operate with the interests of our customers, shippers, and country top of mind.

Just 1 month ago, we were the victims of a ransomware attack by the cyber criminal group DarkSide. At this time, we believe the criminal attack encrypted our IT systems, and DarkSide demanded a financial payment in exchange for a key to unlock those systems. We responded swiftly to the attack itself and to the disruption that the attack caused. We were in a harrowing situation and had to make difficult choices that no company ever wants to face, but I am proud of the fact that our people reacted quickly to get the pipeline back up and running safely. I am also extraordinarily grateful for the immediate and sustained support of Federal law enforcement and Governmental authorities, including the White House. We reached out to Federal authorities within hours of the attack and since that time we have found them to be true allies as we've worked to quickly and safely restore and secure our operations. We also look forward to their support as the United States enhances its response to the increasing challenges private companies must address in light of the proliferation of ransomware attacks and the actions of these cyber criminal groups. I appreciate your interest in this incident and our response, and I welcome the opportunity to discuss it with you. Our hope is that we will all learn from what happened and, through sharing, develop even more robust tools and intelligence to address this threat moving forward.

I also want to express my gratitude to the employees of Colonial Pipeline, our numerous partners, and the American people for their actions and support as we responded to the attack and dealt with the disruption that it caused. We are deeply sorry for the impact that this attack had, but are heartened by the resilience of our country and of our company.

II. TIME LINE OF THE MORNING OF THE RANSOMWARE ATTACK

We identified the ransomware attack just before 5 o'clock AM Eastern Daylight Time (EDT) on Friday, May 7, when one of our employees identified the ransom note on a system in the IT network. Shortly after learning of the attack, the employee notified the Operations Supervisor at our Control Center who put in the stop work order to halt operations throughout the pipeline. This decision was driven by the imperative to isolate and contain the attack to help ensure the malware did not spread to the Operational Technology (OT) network, which controls our pipeline operations, if it had not already. At approximately 5:55 AM EDT, employees began the shutdown process. By 6:10 AM EDT, they confirmed that all 5,500 miles of pipelines had been shut down. Overall, it took us approximately 15 minutes to close down the conduit, which has about 260 delivery points across 13 States and Washington, DC.

On May 7, our employees activated our company-wide incident response process and executed the steps they were trained to carry out. Shutting down the pipeline was absolutely the right decision, and I stand by our employees' decision to do what they were trained to do.

We have an incident response process that follows the same framework used by some Federal agencies. Everyone in the company—from me to the operators in the field—has stop work authority if they believe that the safety of our systems is at risk, and that is a critical part of our incident response process.

I recognize that the attackers were able to access our systems. While that never should have happened, it is a sobering fact that we cannot change. That being said, I am proud and grateful to report that our response worked: We were able to quickly identify, isolate, and respond to the attack and stop the malware from spreading and causing even more damage. We then turned to remediating the problem and safely restoring service. We retained a leading forensic firm, Mandiant, and with their help, within hours, we were able to return some of our local lines to manual operation. Within days, we returned all of our lines to operation. We are well under way, with the assistance of leading outside experts and our own team, with efforts to further strengthen our defenses against future attacks.

III. COMMUNICATION WITH FEDERAL LAW ENFORCEMENT AND GOVERNMENT AUTHORITIES

We are grateful for the constructive relationship and cooperation of our Federal regulators in our efforts to respond to the attack and get the pipeline restarted as quickly as possible.

On the morning of the attack, we proactively reached out to the Federal Bureau of Investigation (FBI) to inform them that cyber criminals had attacked Colonial Pipeline. We also scheduled a call within hours to debrief both the FBI and the Cybersecurity & Infrastructure Security Agency (CISA) with information about the attack, and we remained in regular communication with law enforcement. We proactively shared Indicators of Compromise (IOCs) with law enforcement as well

as other valuable threat intelligence in an effort to help thwart these kinds of attacks in the future, and assist the Federal Government with its endeavor to bring the criminals to justice.

We also have worked closely with the White House and National Security Council, the Department of Energy, which was designated as the lead Federal agency, as well as with the Department of Homeland Security, the Pipeline and Hazardous Materials Safety Administration (PHMSA), the Federal Energy Regulatory Commission (FERC), the Energy Information Administration, and the Environmental Protection Agency (EPA).

Our cooperation with Federal agencies continues to this day, which is why I am grateful for your invitation to be here today and am pleased to support your efforts in determining how Government can play a role in helping private companies better defend themselves against similar threats.

Our engagement with those Federal authorities helped us achieve meaningful milestones in our response process to address the attack and restore pipeline operations as quickly as possible. In particular, we are appreciative for the cooperative way that Federal agencies worked with us. Their focused collaboration made it easier to restart the pipelines and improved the speed with which we could transport fuels to their destinations.

IV. POST-ATTACK RESPONSE

We take our role in the United States infrastructure system very seriously. We recognize the gravity of the disruption that followed the shutdown, including panic-buying and shortages on the East Coast, and we express our sincerest regret to everyone who was impacted by this attack. The interests of our customers, shippers and the country are our top priorities and have been guiding our response.

I want to emphasize that the importance of protecting critical infrastructure drove the decision to halt operations of the pipeline to help ensure that the malware was not able to spread to our OT network. When we learned of the attack, we did not know the point of origination of the attack nor the scope of it, so bringing the entire system down was the surest way—and the right way—to contain any potential damage.

After halting operations, we took steps to continue to move product manually where we could, while working systematically and methodically to scan all of our systems for any potential malware or indicators of compromise. Once we knew we could safely restart the pipeline, we worked as quickly as possible to get our pipeline back up and running. Bringing our pipeline back on-line is not as easy as "flicking a switch on," as President Biden correctly stated. It is an extraordinarily intricate and complex system, and this process required diligence and a Herculean, around-the-clock effort to restore our full OT network and begin returning all pipelines to service on Wednesday evening, May 12.

While working through the restart process, we increased air surveillance, drove over 29,000 miles while inspecting our pipeline, and worked with local law enforcement agencies to secure our physical pipeline. Employees manually collected and real-time reported key pipeline information along our entire system to ensure the integrity of the system while our OT was not visible. We worked tirelessly to restore system integrity and bring the pipeline back in service as soon as we could do so safely.

Being extorted by criminals is not a position any company wants to be in. As I have stated publicly, I made the decision that Colonial Pipeline would pay the ransom to have every tool available to us to swiftly get the pipeline back up and running. It was one of the toughest decisions I have had to make in my life. At the time, I kept this information close hold because we were concerned about operational security and minimizing publicity for the threat actor. But I believe that restoring critical infrastructure as quickly as possible, in this situation, was the right thing to do for the country. We took steps in advance of making the ransom payment to follow regulatory guidance and we have explained our course of dealings with the attackers to law enforcement so that they can pursue enforcement options that may be available to them.

V. ON-GOING INVESTIGATION INTO HOW THIS HAPPENED AND WHAT WE CAN DO TO FURTHER STRENGTHEN OUR DEFENSES

Colonial Pipeline is an accountable organization, and that starts with taking proactive steps to prevent an attack like this from happening again. To further strengthen our defenses against future threats and cybersecurity attacks, we need to get to the bottom of how this one occurred. Over the past 4 weeks, we have learned a great deal. But forensic investigations, as many of you know, take time.

Our experts are reviewing massive amounts of evidence and indicators of compromise and devoting ample resources to retracing the attackers' footsteps so we know, if possible, exactly where they got in, how they were able to move within our systems and what they may have been able to access. That investigation is on-going, and while we may not have all of the answers today to the questions that you have, we are working hard to get them.

Although the investigation is on-going, we believe the attacker exploited a legacy virtual private network (VPN) profile that was not intended to be in use. We are still trying to determine how the attackers gained the needed credentials to exploit it.

We have worked with our third-party experts to resolve and remediate this issue; we have shut down the legacy VPN profile, and we have implemented additional layers of protection across our enterprise. We also recently engaged Dragos' Rob Lee, one of the world's leading industrial and critical infrastructure and OT security specialists to work alongside Mandiant and assist with the strengthening of our other cyber defenses. We have also retained John Strand from Black Hills Information Security, another leader in the cybersecurity space, who will provide additional support to strengthen our cybersecurity program.

It will take time to review all the evidence to make sure we get the most accurate answers possible, and we will continue to look for ways to further enhance our cybersecurity. We're committed to sharing lessons learned with the Government and our industry peers. As painful as this experience has been for us and those that rely on our pipeline, it is also an opportunity to learn more about how these criminals operate so that we and others can better protect ourselves moving forward. Once we complete our investigation into this event, we plan to partner with the Government and law enforcement and share those learnings with our peers in the infrastructure space, and more broadly across other sectors, so that they too learn from this event.

VI. FEDERAL GOVERNMENT RESPONSE GOING FORWARD

I recognize that Congress and Federal agencies have been discussing what additional regulations may be appropriate in the wake of this ransomware attack. As the leader of Colonial Pipeline, I have been focused on restoring our normal operations and further strengthening our cyber defenses. One recommendation I have is to designate a single point of contact to coordinate the Federal response to these types of events. Having a single point of contact was helpful and constructive as Colonial Pipeline worked around the clock to respond to the ransomware attack and restore operations, and I believe that would be valuable in the event of future cyber attacks.

There are also limits to what any one company can do. Colonial Pipeline can—and we will—continue investing in cybersecurity and strengthening our systems. But criminal gangs and nation-states are always evolving, sharpening their tactics, and working to find new ways to infiltrate the systems of American companies and the American Government. These attacks will continue to happen, and critical infrastructure will continue to be a target. Whichever organization may be designated as the single point of contact, Congress must ensure it is adequately staffed and resourced to support industry, facilitate information sharing, and respond appropriately. We will also need the continued support of law enforcement to disrupt cyber crime networks and to bring attackers like DarkSide to justice.

VII. CONCLUSION

In closing, I want to reiterate that we were the victims of a ransomware attack by criminals. I am proud of the way we were able to react and respond. We quickly took measures to secure critical infrastructure, to notify the appropriate authorities, and to work to safely restore operations. I appreciate Congress' interest in this attack and the lessons it may have for Government and industry, and I welcome the opportunity to answer your questions.

Chairman THOMPSON. Thank you very much. I now ask Mr. Carmakal to summarize his statement for 5 minutes.

STATEMENT OF CHARLES CARMAKAL, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, FIREEYE MANDIANT

Mr. CARMAKAL. Thank you for this opportunity to share our observations and experiences regarding this important topic, as well

as for your leadership on cybersecurity issues. My name is Charles Carmakal and I am a senior vice president and CTO at FireEye Mandiant. We commend the committee for holding this hearing to further examine the recent ransomware attack against Colonial Pipeline. Both Governmental and corporate responses to this attack continue to evolve and the committee plays an important role in overseeing these efforts.

As requested, I am going to share our observations of the threat actor associated with the ransomware attack against Colonial Pipeline and discuss cybersecurity threats to organizations in the United States.

In my role at Mandiant, I oversee a team of incident responders that help organizations respond to complex cybersecurity incidents. My team and I have had the opportunity to help organizations across the globe deal with some of the most significant cybersecurity incidents in history. Mandiant is on the front lines of the cyber battle, actively responding to computer intrusions at some of the largest organizations on a global scale. We employ over 1,000 cybersecurity experts in over 25 countries, with skills in digital forensics, malware analysis, intelligence collections, threat actor attribution, and security strategy and transformation.

Over the last 17 years, we have responded to tens of thousands of security incidents. It is unfortunate, but, unfortunately, every day we get calls from organizations that are dealing with a cybersecurity breach. On the early morning of May 7, 2021, Mandiant was engaged to help Colonial Pipeline respond to the ransomware incident earlier that day. Prior to that date, Mandiant had not provided cybersecurity consulting services to Colonial Pipeline. Shortly after being called by Colonial Pipeline in the morning, we mobilized a team of experienced incident responders to help Colonial Pipeline investigate and contain the incident, eradicate the threat actor, and further enhance the security posture of the network to facilitate a safe restart to the pipeline.

Additionally, Mandiant is advising Colonial Pipeline on ways to become more resilient to cyber attacks. Cyber intrusions have become more increasingly disruptive over the past decade. Every year, Mandiant publishes an annual security report, where we summarize the trends that we have observed in the past year. In 2015, Mandiant observed a notable surge in disruptive intrusions in which the threat actors deliberately destroy data, leak confidential data, taunt business executives, and extort victim organizations. We anticipated that these intrusions would become more disruptive over time given the high impact to victim organizations and the low cost to threat actors.

In late 2019, a hacking group by the name of Maze changed the way the threat actors would conduct their intrusions. Prior to deploying ransomware, they would steal data from victim organizations in a way to conduct multifaceted extortion. They launched a website in which they would shame victim organizations by amplifying the message that they have hacked into those organizations and published tranches of data from those victim organizations.

Last October, the threat to the United States had reached an unprecedented level. Hospitals across the United States dealt with an acute threat from Eastern European criminals that wanted to de-

liberately disrupt operations. Hospital technology systems were taken off-line, and medical professionals and administrative staff had to rely on paper-based mechanisms to document procedures and medicine.

The impact of cyber intrusions to human lives had never been more dire. The majority of today's intrusions by financially motivated threat actors involve multifaceted extortion. Threat actors will apply immense pressure to coerce victims to pay substantial extortion demands, often in the 7- to 8-figure range. Some threat actors will convince news and media organizations to write embarrassing stories about the victims, they may call or harass employees, and they may also conduct security service attacks against those organizations.

I want to spend a moment talking about the DarkSide threat group. DarkSide is a ransomware service that enables a network of different groups to conduct cyber intrusions under the name DarkSide. Like many financially motivated threat actors, the criminals affiliated with the DarkSide service conduct multifaceted extortion schemes to coerce victims into paying large extortion demands. The exfiltrate victim data, deploy DarkSide ransomware encryptors, and threaten to publish the stolen data to victim-shaming sites. They have launched a global crime spree affecting organizations in more than 15 countries and multiple industry verticals since initially surfacing in August 2020. Following the security incident at Colonial Pipeline and the FBI's public attribution to DarkSide, the group claimed to have lost access to the infrastructure, including their blog, payment, and content distribution network servers, and they said they would be closing down their service.

Operational technology and industrial control systems are responsible for managing and monitoring the industrial equipment, machines, and processes across the world. They facilitate the generation and distribution of power, operations of manufacturing plants, and transportation of people and products.

To mitigate the risks associated with OT environments, organizations often segment their IT environments from their OT environments. There have been relatively fewer publicly disclosed intrusions of OT environments, but, certainly, the impact is incredible.

On behalf of Mandiant, I thank you for the opportunity to testify before the committee. We stand ready to work with you to devise effective solutions to deter malicious behavior in cyber space and to build better resiliency into our networks.

[The prepared statement of Mr. Carmakal follows:]

PREPARED STATEMENT OF CHARLES CARMAKAL

JUNE 9, 2021

INTRODUCTION

Chairman Thompson, Ranking Member Katko, and Members of the House Homeland Security Committee, thank you for the opportunity to share our observations and experiences regarding this important topic, as well as for your leadership on cybersecurity issues. My name is Charles Carmakal and I am a senior vice president and chief technology officer at FireEye-Mandiant ("Mandiant").

We commend the committee for holding this hearing to further examine the recent ransomware attack against Colonial Pipeline. Both governmental and corporate

responses to the attacks continue to evolve, and the committee plays an important role in overseeing these efforts.

As requested, I am going to share our observations of the threat actor associated with the ransomware attack against Colonial Pipeline and discuss the cybersecurity threats to organizations in the United States.

BACKGROUND

In my role at Mandiant, I oversee a team of security professionals that help organizations respond to complex security breaches orchestrated by foreign governments and organized criminals. My team and I have had the opportunity to help organizations across the globe deal with some of the most significant and catastrophic cybersecurity incidents in history.

Mandiant employees are on the front lines of the cyber battle, actively responding to computer intrusions at some of the largest organizations on a global scale. We employ over 1,000 cybersecurity experts in over 25 countries, with skills in digital forensics, malware analysis, intelligence collections, threat actor attribution, and security strategy and transformation. Over the last 17 years, we have responded to tens of thousands of security incidents. It is unfortunate, but we receive calls almost every single day from organizations that have suffered a cybersecurity breach. For every security incident we respond to, our mission is to help our clients investigate the attack, contain the incident, eradicate the attackers, guide our clients through the recovery of their environments, and help them become more resilient to future attacks.

THE CYBER INTRUSION INTO COLONIAL PIPELINE

On the early morning of May 7, 2021, Mandiant was engaged by Hunton Andrews Kurth LLP, on behalf of Colonial Pipeline, to help respond to the ransomware event that was discovered earlier that day. Prior to that date, Mandiant had not provided cybersecurity consulting services to Colonial Pipeline. Shortly after being called on the morning of May 7, we mobilized a team of experienced incident responders and information technology and operational technology security experts to help Colonial Pipeline investigate and contain the incident, eradicate the threat actor, and further enhance the security posture of the network to facilitate the safe restart of the pipeline. Additionally, Mandiant is advising Colonial Pipeline on ways to become more resilient to cyber attacks in the future.

The earliest evidence of compromise that we have identified to date occurred on April 29, 2021. On that date, the threat actor had logged into a virtual private network (VPN) appliance using a legacy VPN profile and an employee's username and password. The legacy VPN profile did not require a one-time passcode to be provided. The legacy VPN profile has since been disabled as part of Colonial Pipeline's remediation process.

THE EVOLUTION OF DISRUPTIVE INTRUSIONS: RANSOMWARE TO MULTIFACETED EXTORTION

Cyber intrusions have become increasingly disruptive over the past decade. Every year, Mandiant publishes an annual report, M–Trends, which covers the cybersecurity trends we observed from our breach investigations.[1] In 2015, Mandiant observed a notable surge in disruptive intrusions in which threat actors deliberately destroyed critical business systems, leaked confidential data, taunted executives, and extorted organizations. We anticipated that intrusions would become more disruptive over time given the high impact and low cost to threat actors.

Over the next few years, financially motivated threat actors began shifting away from stealing payment card information to deploying malicious software that encrypts data on systems, commonly referred to as ransomware. Threat actors asked for ransom payments in exchange for the software that would enable victim organizations to recover their encrypted data.

In late 2019, a hacking group by the name of Maze changed the way threat actors would conduct their intrusions. Prior to deploying ransomware across victim environments, they would look for and steal sensitive corporate information. They launched a website where they would publicly shame the victim organizations that they compromised and publish the data that they stole. They would demand money in exchange for tools to recover the data that they encrypted, a promise to not publish the data they stole, and details of how they compromised the organization. Ex-

[1] M–Trends, *https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html*.

tortion demands were often in the 6- and 7-figure ranges, but sometimes went up to 8 figures.

Last October, the cyber threat in the United States reached an unprecedented level. Hospitals across the United States were disrupted by a group of eastern European threat actors. Hospital technology systems were taken off-line and medical professional and administrative staff had to rely on paper and pen to record data. Many hospitals had to divert patients and ambulances to emergency departments at other hospitals. The impact of cyber intrusions to human lives has never been more dire.

The majority of today's intrusions by financially motivated threat actors involve multifaceted extortion. Threat actors will apply immense pressure to coerce victims to pay substantial extortion demands—often in the 7- to 8-figure range. Some threat actors will convince news and media organizations to write embarrassing stories about victims. They may call and harass employees. They may notify business partners that their data was stolen due to a breach of their partner, creating friction in business relationships. They may also conduct denial-of-service attacks to create further chaos and disruption.

Ransomware and multifaceted extortion events have reached an intolerable level and we must come together as a community to help organizations defend their networks.

THE DARKSIDE THREAT GROUP

DarkSide is a ransomware service that enables a network of different groups to conduct cyber intrusions under the name "DarkSide." Like many other financially motivated threat actors, the criminals affiliated with the DarkSide service conduct multifaceted extortion schemes to coerce victims into paying large extortion demands. They exfiltrate victim data, deploy DarkSide ransomware encryptors, and threaten to publish stolen data to their victim-shaming website. Since initially surfacing in August 2020, they have launched a global crime spree affecting organizations in more than 15 countries and multiple industry verticals.

DarkSide operates as a ransomware-as-a-service (RaaS) wherein profit is shared between its owners and partners, or affiliates, who provide access to organizations, steal sensitive victim data, and deploy the ransomware encryptors. Mandiant currently tracks multiple threat groups that have conducted these intrusions, some of whom have also worked on behalf of ransomware services besides DarkSide. These groups demonstrate varying levels of technical sophistication throughout intrusions.

Mandiant has identified multiple DarkSide victims through our incident response engagements and from reports on the DarkSide victim-shaming website. Most of the victim organizations were based in the United States and span across multiple sectors, including financial services, legal, manufacturing, professional services, retail, and technology.

Following the security incident at Colonial Pipeline and the FBI's public attribution to DarkSide, Mandiant has observed multiple actors cite a May 13, 2021 announcement that appeared to be shared with DarkSide RaaS affiliates by the operators of the service. This announcement stated that they lost access to their infrastructure, including their blog, payment, and content distribution network (CDN) servers, and would be closing their service. The post cited law enforcement pressure and pressure from the United States for this decision. Multiple users on underground forums have since come forward claiming to be unpaid DarkSide affiliates, and in some cases privately provided evidence to forum administrators who confirmed that their claims were legitimate. We have not seen evidence suggesting that the operators of the DarkSide service have resumed operations.

OPERATIONAL TECHNOLOGY (OT) AND INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY

Operational Technology (OT) and Industrial Control Systems (ICS) are responsible for managing and monitoring the industrial equipment, machines, and processes. They facilitate the generation and distribution of power, operations of manufacturing plants, and transportation of people and products. To mitigate the risks associated with OT environments, organizations segment their OT environments from IT environments (i.e., the environment that supports email, web browsing, and other business processes).

There have been relatively fewer publicly disclosed intrusions of OT environments as compared to IT environments, but the impact can be exponentially more significant. Some of the most notable incidents include the disruption of power distribution in Ukraine in 2015 and 2016, the development of malware that could manipulate safety control systems that was used against an organization in the Middle East in 2017, and an attack on a Florida water treatment plant in 2021.

CONCLUSION

On behalf of Mandiant, I thank you for this opportunity to testify before the committee. We stand ready to work with you and other interested parties to devise effective solutions to deter malicious behavior in cyber space and to build better resiliency into our networks.

Chairman THOMPSON. Yes, I thank the witnesses for their testimony. I will remind each Member that he or she will have 5 minutes to question the witnesses. I now recognize myself for questions.

Mr. Blount, I want to clarify the time line of certain events following the ransomware attack. Would you please walk the committee through the 24 hours or so after Colonial learned of the attack? In that, would you include the approximate time you reached out to Mandiant, when you reached out to and met with various offices, with the FBI, when you reached out to and met with CISA, when you reached out to the Department of Energy, when you reached out to TSA, and exactly when did you pay the ransom?

Mr. BLOUNT. Mr. Chairman, I will be glad to answer your questions. I may have to ask you to repeat a few of them along the way but let me start with what I gathered here.

The attack, the ransom note, showed up on a system in our control room at approximately around 5 a.m. on May 7. The controller that saw the ransomware note immediately took it to a supervisor and they consulted quickly with our IT group. The decision was made right before 6 a.m., as a result of that threat and in order to contain that threat, to shut down the pipeline system and all the IT associated with that.

Shortly thereafter, within an hour or so, and I will be glad to get the exact time for you because I don't have it, we contacted Mandiant to come in and determine exactly what we had and to start the investigative process and, obviously, to start the restoration process. So, that is the conversation there.

Shortly thereafter, and still early in the morning, we contacted the local office, the Atlanta office, of the FBI. We have a relationship there. Told them what we had seen on our computer systems and our concern regarding that. The agent in charge there agreed that we needed more conversation, and they volunteered that they would call CISA and bring them into the conversation, which the FBI scheduled for slightly after 12 noon of that day.

While all that was going on, we had various employees responsible for making contact to any number of other Governmental entities. So, again, I can give you a more detailed time line, but I will tell you over the course of that day, in the early morning hours following, we contacted the White House, we contacted the National Security Council, we contacted DOE, we contacted PHMSA, we contacted FERC, we contacted DHS, and we contacted EIA. In addition to that, to help to start sharing what we knew with our industry counterparts, we also contacted the API and the AOPL, as well, of which we are members, in order to make sure they were aware of what was going on and if they had any opportunity to keep a closer eye on their systems, in case there was a similar threat attack to them as a result of that.

Chairman THOMPSON. Thank you. We will send a specific request on the time line following, but I appreciate what you have done. What time and what day did you pay the ransom?

Mr. BLOUNT. Mr. Chairman, we had a discussion about the ransom in the late, late afternoon of May 7, consulting with legal—outside legal representatives who have been involved in cyber attacks in the past, and we made the decision that afternoon to proceed forward with negotiations with the criminal on the possibility of paying the ransom. The actual payment of the ransom was not made until sometime on Saturday, and, again, it—if you need that exact time, I can get that for you, sir, but I don't have that here.

Chairman THOMPSON. But it would be helpful. The other thing, did you talk to the FBI or any other Government official about paying the ransom?

Mr. BLOUNT. We are having additional discussions with the FBI or any other Governmental agency regarding the ransom.

Chairman THOMPSON. I did not get the first part of your question—your answer.

Mr. BLOUNT. My apologies, Mr. Chairman. We did not have any discussion with the FBI or any other Governmental entity about the actual negotiation or the payment of the ransom at that time.

Chairman THOMPSON. Thank you very much. Now, I understand you have received about $2.3 million. In my opening statements, I talked about are you committed to investing some, if not all, of that money toward hardening your systems, so that something like this might not happen again?

Mr. BLOUNT. Mr. Chairman, I am glad you asked me that question, and, you know, I will go back to what I heard from Ranking Member Katko, as well. We are always in the process of hardening our systems and making investments in IT and cybersecurity at Colonial. So, to your request today of putting an additional $2.2 million into hardening our systems further is not a difficult one to address and agree to. In my opening statement, I already explained that we, not only in addition to Mandiant, have also brought in Dragos to take a very close look at our OT system and further strengthen whatever needs to be done there. They are a world-known expert in that, as well as to bring in Black Hills to also look at the entire process. We are making a substantial investment, and part of the reason for that is we have been compromised, we have had criminals within our system now, and we need to change a lot of things that we already had because they would be familiar with them from having been in the system over the course of those days.

Chairman THOMPSON. Thank you very much. Mr. Carmakal, just 2 quick questions. Would an open VPN system with a normal security or IT security system have been picked up?

Mr. CARMAKAL. Yes, so, let me just provide a little bit of context into what is now believed to be the earliest evidence of compromise. As we conduct investigations, we try to figure out what is the earliest evidence of what the attacker has done within the environment. Based on our investigation, the earliest evidence was a login to the Colonial Pipeline VPN. We do know that an employee's credentials were used. So, a username and a password was used to do that. We did not figure out exactly how the attacker was able to get access to the username, but it is a possibility that the

attacker was able to leverage credentials that the employee may have used on another website that was compromised prior to this date. So, it is certainly possible that that is how the attacker got in. Whether or not the vulnerability or the misconfiguration—and let me, you know, clarify it as a misconfiguration—whether it would have been picked up by a vulnerability assessment is hard to tell. But I just want to clarify that what actually occurred was there was a legacy VPN profile that was in place that wasn't believed to be active, and that enabled an attacker to leverage both the user and the password to login.

Chairman THOMPSON. So, how would one correct that problem?

Mr. CARMAKAL. Yes, so, the problem has been corrected at this point in time. The legacy VPN profile has been completely removed. So, a user, whether an attacker or an employee, would not be able to attempt to login to the system without requiring multifactor authentication. So, in addition to a password, you would need a one-time code in order to be able to login to the Colonial Pipeline VPN at this point in time.

Chairman THOMPSON. All right. Do, you just said it was a common password that allowed the breach to occur?

Mr. CARMAKAL. Yes. So, I want to clarify, the password that the account was set to was not a common password, it was not a easily guessable password. In fact, it was a relatively complex password in terms of length, special characters, and case set. It wasn't something that somebody would be able to easily guess or predict. However, it was a password that had been used on a different website at some point in time.

I just wanted the group and the audience to understand that it is actually really common for everyday people to use similar passwords or the same exact passwords across different websites, across social media accounts, or email accounts or financial accounts, and this is a very common problem. So, unfortunately, what happened here is a password for an account that wasn't believed to be in use anymore had the same password as what was used for that employee on a different website that had, unfortunately, been compromised.

Chairman THOMPSON. I mean, I understand, but, you know, we are not talking about ordinary people. We are talking about a pipeline that controls 55 percent of the energy resources in the Northeast. So, you would expect a more robust system than just an ordinary system.

Mr. CARMAKAL. Understood.

Chairman THOMPSON. Thank you. The Chair recognizes the Ranking Member for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman, and thank you to Mr. Blount and Mr. Carmakal for being here today. This is a very, very important hearing, and not just for what happened at Colonial Pipeline, but what we can do going forward to protect our critical infrastructure and our computer systems Nation-wide. This is an issue that is getting more ubiquitous, unfortunately, and we are going to have to deal with it.

So, Mr. Blount, I appreciate your candor, and I appreciate your professionalism in testifying. I am not interested in playing doctor, but I do want to clear up something from yesterday. You were

asked a question, by I believe it was Senator Hawley, about the money you spent to secure your systems. I think you said over the past decade it was over $200 million, and I think that includes for your entire IT system all together, correct? That is not just for the hardening of that system?

Mr. BLOUNT. Ranking Member Katko, that is a correct statement. Yes, sir.

Mr. KATKO. OK. OK. Thank you for that clarification. I appreciate it. You talked about hardening the system now, right, and, again, and we are not trying to play got you, I know you have—you referenced a little bit about the hardening of the system before. What are you doing now that you weren't doing before to harden your system?

Mr. BLOUNT. I thought that was a good point you made before, because I think a lot of people are hearing about hardening of the system right now and they think that that means that operators haven't been doing that all along. As we all know, these threat actors evolve very quickly. They have very sophisticated tools. So, all responsible operators are continuing to assess their investment and where they need to go next. So, from a Colonial perspective, as I stated previously, we have had a bad actor, we have had a criminal inside our system. So, we are making a lot of changes in our system with the help of Mandiant as they go about restoring our systems, as well as mitigating the damage done. Again, with Dragos and Black Hills involved, we will be doing a lot of things differently that we certainly could share with you probably more one-on-one because we don't want to give a road map to the outside criminal characters that they could come in and have a successful attack again. But we have got a lot of things in progress right now, and we will continue to make those investments.

We take cybersecurity as well as physical security extremely serious at Colonial, so that is where we are headed. We are heading toward a lot more hardening and a lot different architecture than we had before, mainly because we have been compromised and we need to change the architecture, so that it is not as easily known by previous perpetrators.

Mr. KATKO. You know, and I understand that. I appreciate your candidness there. My concern in you—you are learning from the attack, right? The next question is how do we get other critical infrastructure into entities that have not been subject to attack yet? I hope they never do, but if they happen in a subsequent attack, how do we get them to take those similar additional steps that you are now taking out of necessity? How do we get them to pay attention to this issue?

You have competing interests all the time from your budgets, but there is no question this is going to cost money, but there is no question that the critical infrastructures across this country have to do it. I am quite confident that they are not all doing it. So, what would you say to them or how would you—what would—what do you think we should be doing to help them, basically, see the light? You are muted, sir, I am sorry.

Mr. BLOUNT. I knew I would get that wrong at some point. I apologize. Thank you.

Ranking Member, I share your concern. You know, as a large operator who has been making investments in this area, I think that we need to work together and find a way to work together to share those best practices and what makes sense, and perhaps what made sense yesterday that no longer makes sense today as the threat actor continues to evolve. You know, we participate, all of us responsible operators participate, in a lot of tabletop exercises, and we have standards that we follow, like API security standards for SCADA and things like that. But I think we need to continue to communicate, communicate, and communicate.

You know, the one fortunate thing about this unfortunate event, it certainly highlighted the risk to all the operators in the United States and it certainly has heighted the Government's focus on the issue. Again, as private operators, we can continue to make the investments and do the things that we should do to be accountable and responsible, but there is certainly things that the Federal Government can do, like approach the host of these bad actors in these foreign countries and things like that, and put political pressure on them, so that we can stop it before it even starts.

Mr. KATKO. Well, the President certainly has an opportunity to do that this week when he meets with President Putin, that is for sure. Yesterday, in your hearing you mentioned that the free services offered by CISA generally weren't considered to be value-adds to what you are already doing. Is there something more that CISA could be providing that would further enhance your engagement with them? Because we want to make CISA more proactive in this area.

Mr. BLOUNT. Ranking Member Portman, you know, as I look at lessons learned along the way, I think one of the things I saw pretty early on was the involvement of all the Federal agencies, which we greatly appreciated. If I look at it from a CISA-alone perspective, some of the things that I saw them doing was participating in the FBI calls, learning about, you know, indications and compromised evidence that they could sort through and then figure out how to share with others in the industry on a real-time basis.

You know, the new mandates that they have right now are designed to do the same thing. If you are being attacked or being—someone is knocking on that door every day, you know, is there a random pattern there or is there an actual pattern of threat there that they can share with all the industry? I think those are the things that, you know, we should see policies around and focus on, on the part of CISA, that would be helpful to all operators of critical infrastructure in the United States today.

Mr. KATKO. Mr. Chairman, I don't know how much time I have left. I just want to check with you real quick.

Chairman THOMPSON. One more question.

Mr. KATKO. Pardon me?

Chairman THOMPSON. One more question.

Mr. KATKO. Oh, OK. Thank you very much. Dr. Carmakal, I wanted to give you an opportunity to comment. What can we do to make sure that the other critical infrastructure entities across the spectrum take the cybersecurity and the hardening actions that they need to take that a lot of them just aren't taking?

Mr. CARMAKAL. Yes.

Mr. KATKO. So, what can we do other than what Mr. Blount has stated?

Mr. CARMAKAL. Yes. Thank you for the question. I really think what we need to do is share as much information as we possibly can about the threat actor, the threats, and really what—some of the learnings at Colonial Pipeline, as well as other organizations, that are dealing with cyber attacks on a day-to-day basis are learning from their investigations and their response. So, if we can get information out to other organizations more quickly, I think it will help enable them to better defend their environments.

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

Chairman THOMPSON. Thank you very much. The gentleman yields back. The Chair recognizes the gentlelady from Texas for 5 minutes, Ms. Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, Mr. Ranking Member, thank you so very much for this hearing. Let me express the urgency that I feel about this particular crisis that we are in the midst of. To both gentlemen, we know that the private sector over the years has had 85 percent of the Nation's critical infrastructure, including cyber. I would make the point at this time, 2021, that because of this major crux of calamity that we face, that the private sector can no longer go it alone. Mr. Blount, do you agree with that, that the private sector can no longer go it alone with respect to its infrastructure that it possesses versus the Federal Government?

Mr. BLOUNT. Thank you, Representative Lee, for your question. I think there is no question that these threat actors are extremely capable. They are housed in countries other than the United States. We are responsible, as operators, for our own internal security and our cybersecurity, but we need the Government's help to put pressure on the host countries, so that we can stop these attacks before they start.

Ms. JACKSON LEE. Thank you. Can you explain, again, why, when you were requested to provide information as to whether or not you paid ransom, that you hesitated and took, really, a considerable length of time to the extent that it was reported that the White House was not getting a direct answer regarding whether you paid ransom?

Mr. BLOUNT. Representative Lee, as far as the White House goes, they never asked whether we—they never talked about the ransom at all, period. Never had a question about it from anybody that I talked to. Never had a question about it from any of my employees that talked to Federal agencies. So, that is the reason why the White House,they weren't—they never asked about it.

Ms. JACKSON LEE. Who was the first Governmental entity that you reported to that indicated that you paid ransom?

Mr. BLOUNT. The first entity that we reported to that we paid ransom would have been the FBI.

Ms. JACKSON LEE. What was the gap between the time that you paid it and the time that you spoke to the FBI? The time.

Mr. BLOUNT. Representative Lee, I would say that was approximately 48 hours. I could give you the more definitive number, but that would be my guesstimate.

Ms. JACKSON LEE. Thank you so very much. So, it was 2 days—there was a 2-day gap between the time you paid it and the time you spoke to the FBI.

Mr. BLOUNT. Representative Lee, I would share with you that, obviously, we communicated with the FBI throughout the course of the week, shared a lot of evidence with them, and we made ourselves as open——

Ms. JACKSON LEE. Thanks.

Mr. BLOUNT. [continuing]. As we possibly could.

Ms. JACKSON LEE. Thank you very much. Let me, again, compliment the FBI for being able to secure dollars. This may be your question, I think, Mr. Carmakal. Why wasn't a multifactor authentication used on that VPN? I am going to give you a series of questions, if you want to take quick notes, because my time is running out. Who had a legitimate access to that password? Where else was the password used? Was the password listed in any of the company's on-line documentation?

So, it is authentication, legitimate access to that password. So, do you want to start with the authentication?

Mr. CARMAKAL. Sure.

Ms. JACKSON LEE. If you can be concise and as quickly as possible.

Mr. CARMAKAL. Yes, thanks, ma'am. In terms of multifactor authentication, it was not required for the specific VPN profile that was used for this specific account. It is because the account and the VPN profile wasn't believed to actually be enabled.

Ms. JACKSON LEE. OK. Can I move to——

Mr. CARMAKAL. So, it was known at the time. Yes?

Ms. JACKSON LEE. Can I move to the next question?

Mr. CARMAKAL. Yes, ma'am.

Ms. JACKSON LEE. Who had a legitimate access to the password, sir?

Mr. CARMAKAL. One person, as far as we know.

Ms. JACKSON LEE. Is that person vetted, from your perspective?

Mr. CARMAKAL. Yes, it was an employee's account.

Ms. JACKSON LEE. Where else was the password used?

Mr. CARMAKAL. We do not know the exact source of the website that it was used, but presumably it was used on at least one other website because there are passwords that are readily available on the internet, and we did find that it was one of the passwords that was stolen from another website. But we don't know exactly where it came from.

Ms. JACKSON LEE. Was the password listed in any of the company's on-line documentation?

Mr. CARMAKAL. Not that I am aware of.

Ms. JACKSON LEE. You started out by saying you can't go it alone. We are ready to help you. I introduced H.R. 2980, which deals with Cybersecurity Vulnerability Mediation Act. The committee was kind enough to pass it out of the committee. Hopefully, it will go to the floor.

But the crux of this is that part of it is a reporting feature that really requires companies to the DHS to secure a report that indicates what kind of mitigation companies are engaged in. Do you think that if a company crosses into the public domain, and when

I say that Colonial Pipeline impacts, as you well know, massive energy streams that literally shut down the East Coast, that the Government should come in more quickly than it obviously did because it has moved into the public domain? Do you believe that that would be an appropriate approach in terms of assessing how the Government comes in to help those who have been attacked?

Mr. CARMAKAL. I think private corporations would welcome any support they could get from the Government dealing with cybersecurity incidents.

Ms. JACKSON LEE. OK. Thank you, Mr. Chairman.

Chairman THOMPSON. The gentlelady's time has expired. Yes, ma'am.

Ms. JACKSON LEE. Thank you very much.

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

Mr. MCCAUL. Thank you, Mr. Chairman. Mr. Blount, this was the fourth recent attack by either Russia as a nation-state or organized——

Mr. BLOUNT. The what?

Mr. MCCAUL [continuing]. Russian Mafia. You know, this is the kind of thing that keeps us up at night, a pipeline shutting down in the Nation from New York to Houston. The problem, as I see, the Chairman and I stood up to CISA, which is on the defensive side, but the problem, as I see it, is we continue to see hundreds of these attacks, billions of dollars in ransomware, and yet there is no consequence to bad behavior. They get away with this every day.

I introduced and marked up on the Foreign Affairs Committee the Cyber Diplomacy Act, which sets up an ambassador-at-large at the State Department to set up international norms and standards. So, Mr. Blount, my question to you is, as the President now is going to sit down with Mr. Putin, and certainly I hope the President is going to raise these attacks, the recent attacks by Russia, either as a nation-state or by organized crime. I believe that we need it to start thinking about going on the offensive and hitting them back, and there should be consequences.

In a recent statement, you have stated, ultimately, the Government needs to focus on the actors themselves. As a private company, we don't have a political capability of shutting down the host countries that have had these bad actors in them. Do you agree with my bill? But, more importantly, that we need to start—stop just taking it. We need to respond and we need to start hitting them back. Do you agree with that assessment?

Mr. BLOUNT. Representative, I appreciate your leadership in this particular issue. That does, very much, address what you read in the press statement that I made. We have a responsibility, obviously, as operators to continue to strengthen our systems and protect our asset base, but we have to stop the threat actor themselves. We have to stop the criminals, and that is something private industry can't do without a partnership with the public sector.

So, I think your proposal is dead on and we certainly support it, and I think every other operator in the United States would love to see us stand up and push back and not allow this to continue. It is unfortunate you had to take a hit on a, you know, critical in-

frastructure asset to get the focus that it is getting now. But I think it is very important and, again, I appreciate your leadership on it.

Mr. MCCAUL. Thank you, Mr. Blount. Mr. Carmakal, you know, FireEye has been a leader in this issue and, you know, we, Congressman Langevin and I, introduced a mandatory breach notification law. You know, CISA is only as good as the information it gets and the private sector has the majority of the threat information. I think Colonial Pipeline did a good job notifying CISA, but other companies don't. Would you agree with the assessment or the tone of this bill that we need to start looking at, instead of 50 different States, a Federal law, instead of patchwork in 50 States, that would require a mandatory breach notification if the identifiers can be taken out, that it can be sanitized and scrubbed, like we do with the Classified information, so that the producer is not compromised in any way. But the threat information is mandatorily shared with CISA, so it can better protect the Nation from these attacks.

Mr. CARMAKAL. Yes, Congressman, I certainly agree that right now the data breach disclosure laws are highly complex. Every State has their own nuanced requirements, and it would certainly be a welcome change to have one standard data breach disclosure requirement. It will be much more simple for the organizations that are trying to figure out the complexity around notification requirements.

In terms of getting information out to help other organizations defend themselves, absolutely. We agree with the spirit and the intent of that. We welcome the opportunity for CISA to take that information and disseminate it as best as they can, but they certainly need victim organizations to come forward and provide that, the threat information, to them, so they have something to share. I think one of the challenges that organizations deal with today is the fear or the repercussions and the scrutiny around data breaches. So, if there is a way to get information out to the Government, to CISA, and to the broader community in a way where it doesn't feel like the victim organizations are going to face a penalty, I think that would be a welcome change.

Mr. MCCAUL. The last question to you, sir, would be, you know, we don't allow private companies to hack back, right? That is still illegal and it would create a Wild West scenario. But what is your opinion of the Federal Government protecting itself and responding in kind to nation-state actors when they perpetrate these acts of cyber warfare, for lack of a better term, because they are destructive and it shut down, you know, the energy supply for days on the East Coast? What would be the best way to show them that there are consequences to their bad actions?

Mr. CARMAKAL. Yes, so, I certainly agree that private organizations shouldn't hack back, but from a Government perspective, and perhaps, you know, certain select private organizations that maybe have the capability and the operational security to be able to conduct these offensive operations, I certainly think there is a way and an opportunity to disrupt the aggressive threat actors that continue to cause havoc in the United States. So, I do believe that there is an opportunity for us to get more aggressive, but we certainly need to define what are the rules of engagement.

Mr. MCCAUL. OK, thank you, Mr. Chairman. I think the time to act is now and that the international norms and standards need to be set with our allies and across the globe. With that, I yield back.

Chairman THOMPSON. Thank you. The gentleman's time has expired. The Chair recognizes the gentleman from Rhode Island for 5 minutes, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Good afternoon. I want to thank Mr. Blount and Mr. Carmakal for your testimony here today and helping us to understand this. I have a list of questions I want to get through, and if you can be as brief and direct as possible, it would be appreciated.

So, if I could start with Mr. Blount. So, I understand that Colonial has cyber insurance. So, do you expect your insurers to cover—will cover the $4.4 million ransom payment?

Mr. BLOUNT. Congressman, thank you for that question. We do have cyber insurance. We have had cyber insurance for quite some time. We have submitted a claim for that ransom payment, and I haven't had that confirmed to me yet, but I suspect that it will be covered.

Mr. LANGEVIN. OK, thank you. Did you have discussions about whether your insurers would cover the ransom payment before you made the decision to pay?

Mr. BLOUNT. I think there were consultations going on through my CFO at the time, but that wasn't my focus. Again, my focus was to get access to that de-encryptor, to have all the options that I could get available to me in an effort to try to restart that pipeline as quickly and safely as possible. So, from my perspective, the insurance wasn't even in the forefront of my mind.

Mr. LANGEVIN. OK, thank you. Mr. Blount, yesterday you testified that you recommended to other companies that they be, "extremely transparent in their contact with the authorities who indeed do have resources that potentially could help move through a very difficult process." So, in talking with CISA, my understanding is that regional representatives offered Colonial assistance, including assistance ensuring that the incident was contained and validate the integrity of your OT network. Allowing CISA to help on your network could also allow them to provide better information to other critical infrastructure entities. You know, I am not interested in litigating the past month of what services were offered when, but will you commit today to take CISA up on their offer of direct assistance on your network?

Mr. BLOUNT. Thank you, Representative, for that question. Just for clarity, we reached out almost immediately to Mandiant that morning to basically do the same thing, which was to come in, investigate, and help restore our systems. By the time that the conversation with CISA took place, with the FBI, they were well engaged and in the process of doing that. I think CISA offers great services for companies that perhaps don't have the resources we have, to bring in the best in class with regard to people like Mandiant, Dragos, and Black Hills. So, I think that is a good service. But in this particular case, we were already engaged.

Mr. LANGEVIN. All right, yes, let me stop you there, if I could. You know, you have testified that you will—if there was a 1 percent chance that OT could be affected, it is worth shutting it down.

So, you know, in that light, you know, isn't it—if there is a 1 percent chance that Mandiant had missed something, isn't it worth bringing CISA in? Aren't 2 sets of eyes better than one?

Mr. BLOUNT. Representative, with all due respect, I have 3 sets of eyes in already with the parties that I have explained we have engaged with.

Mr. LANGEVIN. OK.

Mr. BLOUNT. So, from my perspective, I don't think having a fourth, a fifth, and a sixth gets productive.

I think that CISA has been very, very helpful in the process of sharing information that they have learned through us——

Mr. LANGEVIN. Yes.

Mr. BLOUNT. [continuing]. Indications and compromise and things like that to other operators.

Mr. LANGEVIN. So, you are not going to take them up on their offer of direct assistance on your networks at this time?

Mr. BLOUNT. Again, Representative, we have 3 world-class experts in there right now.

Mr. LANGEVIN. Yes, OK. Mr. Blount, what outside firms did Colonial contact before Mandiant?

Mr. BLOUNT. Representative, as I said earlier, we contacted the FBI and Mandiant.

Mr. LANGEVIN. Yes.

Mr. BLOUNT. It was almost simultaneously.

Mr. LANGEVIN. Did you contact outside legal counsel, though, before you had hired Mandiant, and the legal counsel hired Mandiant?

Mr. BLOUNT. We have retained outside legal counsel, and, yes, probably did talk to them before Mandiant. I would have to give you the time line on that. I am not as familiar with it.

Mr. LANGEVIN. OK, thank you. Mr. Carmakal had testified that Mandiant was retained by an outside legal firm. Are you contending that—so, you contacted Mandiant before Hunton Andrews Kurth LLP, or was it the other way around? I am just curious as to why you did——

Mr. BLOUNT. Representative, I am sorry, Representative, is that question for me? I thought you were addressing Mr. Carmakal.

Mr. LANGEVIN. Yes, no, that was for you. I am sorry. Mr. Carmakal had testified that Mandiant was retained by outside legal counsel.

Mr. BLOUNT. That is a correct statement, yes, sir.

Mr. LANGEVIN. OK, and why did you retain Mandiant's services through outside counsel?

Mr. BLOUNT. Representative, I don't know the answer to that. I would have to ask my general counsel why we went down that avenue.

Mr. LANGEVIN. OK. I see my time is expired, but I had a bunch of other questions. Hopefully, we can submit those for the record. Thank you for your time here today, Mr. Blount. Thank you, Mr. Chairman, I yield back.

Chairman THOMPSON. Mr. Garbarino for 5 minutes.

Mr. GARBARINO. Thank you very much, Mr. Chairman. Just some questions for Mr. Blount. As you may know, the Information Sharing and Analysis Centers, or ISACs, can provide member owners

and operators useful services and insight into the current threats facing their sectors. This can include information sharing, actionable intelligence, Federal and private-sector information, and more. Yesterday, you, in front of the Senate, you said you weren't sure if Colonial was a member of an ISAC. Have you tracked down that answer yet? Is Colonial a member of the Oil and Natural Gas ISAC?

Mr. BLOUNT. Thank you for asking for that clarification because I actually did do that, and, indeed, we are. It is the acronym that threw me off. I have heard it through the long name, not through the acronym. So, I wanted to be careful yesterday that I stated it correctly.

Mr. GABARINO. OK, so, you are a member. So, can you provide in detail your engagement with them? How do you leverage their services? What do you provide back to the group?

Mr. BLOUNT. We are a learning organization and it is in our DNA to share. We participate in a lot of industry collaborative processes like that. I would have to call upon my CIO to really explain in detail exactly what they share with regard to our systems and how we approach cyber risk and all those things. But, again, we belong to a lot of organizations like that, that have—also have a lot of acronyms, and they may differ from cyber all the way to pipeline integrity and things like that.

Mr. GABARINO. OK, so, your CIO is the one who deals directly with the Oil and Natural Gas ISAC?

Mr. BLOUNT. That is correct, Representative, or someone on her staff.

Mr. GABARINO. OK. How often do you—would you say you meet with your CIO?

Mr. BLOUNT. Thank you for that question. I meet with my staff every day. We have a staff meeting every day. So, I meet with each one of my executives every morning and typically, throughout the day, I will have one-on-ones with them. Certainly at least twice a month I meet with each one, on one-on-one, to talk about things in general, so, constant contact. It is a small team. It is a very close-knit team.

Mr. GABARINO. So, you, in the past year, you have met with your CIO every day. For how long is that meeting? Is it just a morning meeting? Is it just updates? What is discussed when you—or, and, you know, you meet every day, but are there more in-depth discussions about cyber risk and whatnot, and how many times do you have those meetings?

Mr. BLOUNT. Yes, Representative, the meetings that we have in the morning revolve around a lot of topics. So, with the entire team, they can last anywhere from 1 hour to upwards of 3 hours. Then, as I said, I, you know, in the COVID environment, I have to kind-of do a virtual walkaround. I don't have the ability to knock on doors in the office anymore, but it is not unusual for me to talk to any of the executives that work for me once or twice a day, in addition to the morning meeting. Then, if we have things that we want to talk about in-depth, we make appointments and we spend whatever time we need to on those critical matters.

Mr. GABARINO. OK. So, following the breach, how many meetings have you had with your CIO specifically about the breach and what you are going to do to better protect your—the pipeline?

Mr. BLOUNT. Well, thank you for that question. That is a really good question. We, again, we meet every day as a management team. My CIO has been very engaged in the restoration process with Mandiant, and certainly, if you go back to the first week of it, fully engaged 24/7, every day, until we got the pipeline system back up. So, there might have been a few touch-bases during that week, but for the most part, we let her run with the Mandiant team to make sure that we brought this critical infrastructure up.

Since that time, both her time and my time has been used in forums like this, which are helpful to get the word out about what happened to us, so that it might prevent this from happening to other people. I still talk to her every day, but the length of those discussions varies, depending upon both our schedules. But, again, we are both focused on this particular issue and, quite frankly, that is all we have been focused on for the last month.

Mr. GABARINO. I appreciate that. Now, you just answered the previous Member's question about, you know, you—when he asked about allowing CISA in to help with your systems, it sounded like that was not something you were interested in. TSA had offered its assistance prior to attack, I believe once last year during COVID, then again back in March, and you turned them down last year. I don't believe there was an answer yet as to allowing them in in March. Do you intend on allowing them to come in and do a diagnostic check or at least run a program on your system, like they had offered twice before the attack?

Mr. BLOUNT. Representative, let me address that question. The word "turn down" I have heard as well. I have also heard the word "refusal". Neither one of those is the case. We have worked with TSA for a long time. They have done a lot of physical security audits with us, worked collaboratively with them. In fact, they actually filled in for PHMSA last year on a virtual audit that took place on one of our facilities.

With regard to the VADR program, we never denied wanting to do it. It is a voluntary program, as you know. It was a function of scheduling. We were getting ready and still getting ready to move into a new facility as our lease expired, and so, I think the conversation, again, between my CIO and the director of security over there was a function of when it would be best to do it. I do know that that has been scheduled at the end of July.

Mr. GABARINO. Thank you very much. My time has expired. I yield back. Thank you, Mr. Blount.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from New Jersey, Mr. Payne, for 5 minutes.

Mr. PAYNE. Thank you, Mr. Chairman, and thank you for, once again, having this timely hearing. See, Mr. Blount, since March 2020, your company has been contacted at least 9 times by TSA to schedule, you know, the CFSR. On at least 3 occasions, including April 16, 2020, this was for a ransomware attack. Colonial did not bother to respond to TSA's request for a security assessment. To this date, even after the attack, I guess we are going over the

same—hashing over the same thing. Could you just clarify for me why you opt not to participate in TSA's CFSR security assessment?

Mr. BLOUNT. Representative, I would be glad to answer your question on that. Again, we think the VADR program is a good program. We have a good working relationship with TSA. It has been a function of timing, and, again, we have never refused or denied the part of wanting to participate in that program as a volunteer, and that is why it is scheduled here at the end of July.

Mr. PAYNE. OK. I understand the typical TSA pipeline security assessment involves 3 to 4 TSA employees. Given your company's COVID–19 concerns, were any small groups of individuals not employed by Colonial Pipeline allowed into your facility since the beginning of the pandemic? If so, for what purpose?

Mr. BLOUNT. Representative, you can appreciate that we have essential employees in our operation, just like all pipeline companies do, just like all utilities do. So, in our Alpharetta office, our headquarters in Georgia, we have a rotating shift of controllers in a control room, and our concern and all operators' concerns that the outbreak of COVID was how do we protect these essential workers? They are not people that can be replaced by just anybody. They are kind-of like air traffic controllers. They are highly trained. They are certified. So, we almost immediately, with the breakout of COVID, went to remote work for all our employees and all our vendors in order to protect those essential workers that work in that office. So, there has been no one in that office that I am aware of other than some, potentially, critical repair that needed to be done on something, and I am not even sure about that, highly protected workspace.

Mr. PAYNE. Yes. Well, I appreciate that, sir. You know, we are, you know, just concerned with respect to what has happened to you, to make sure that, you know, TSA is able to help with respect to these issues. You know, we just want to know will you commit to participating in TSA's CFSR inspection as soon as TSA can conduct one or as soon as you can work it out?

Mr. BLOUNT. Yes. Representative, we have already committed to a date. Again, I think it is the last—one of the last days in July.

Mr. PAYNE. OK. Thank you. Mr. Chairman, with that, I will yield back.

Mr. BLOUNT. Mr. Chairman, could I take a minute to make a statement, please?

Chairman THOMPSON. The gentleman is recognized.

Mr. BLOUNT. Thank you, sir. Mr. Chairman, I would like to make a clarification on a statement that I made to Representative Jackson Lee. We shared information with the FBI about the digital wallet on Sunday and discussed the specific ransom payment on Wednesday. The Justice Department, in its announcement a few days ago, commended us for the quick communication with authorities. Thank you, sir.

Chairman THOMPSON. Thank you. The Chair recognizes Mr. Van Drew for 5 minutes.

Mr. VAN DREW. Hi, Chairman, and thank you, Chairman Thompson, for having this meeting. I want to thank you and, of course, Member Katko and Members of the committee. You know that we have a serious problem on our hands. Hackers, who are primarily

located in Russia, have developed sophisticated methods of infiltrating the Federal Government, State and local governments, and private-sector entities in the United States. As we saw just about a month ago, with the ransomware attack on Colonial Pipeline, America is very vulnerable, frankly, too vulnerable to these attacks. They can have crippling ramifications, like gas shortages throughout the entire country.

The attack on Colonial demonstrates the need to shore up our cyber defenses through initiatives such as public-private partnerships and more communication and more accountability in both the public and the private sector. It is of extreme importance. I find it deeply concerning that Russian hackers, through a compromised password on a virtual proxy network, were able to essentially shut down a 5,500-mile pipeline that supplied roughly 45 percent of the fuel consumed by the East Coast of the United States of America.

Shortly after the attack on Colonial, meatpacker JBS was the victim of ransomware attack that caused major disruptions in the United States meat supply, and it also expected that the perpetration of this attack are Russian-based, as well. The FBI Director Christopher Wray recently said that the current levels of ransomware attacks can be compared to the challenges proposed by the September 11, 2001 attacks, that they could be compared to that, and that there are a lot of parallels.

Obviously, if the FBI director is comparing anything to the level of September 11, Congress and the Federal Government need to pay attention. I commend the Biden administration for its recent Executive Order on improving the Nation's cybersecurity and encouraging the administration to work with the Members of the committee on practical, effective solutions on protecting America and our critical infrastructure.

So, I have a few questions. Mr. Joseph Blount, I understand the Transportation Secretary—I am sorry, the Transportation Security Administration contacted Colonial multiple times to conduct a Validated Architecture Design Review, VADR, to evaluate your company's cyber posture, but you refused to move forward with the evaluation. Can you help me and my colleagues on the committee understand why you declined?

Chairman THOMPSON. The gentleman is muted. Unmute yourself.

Mr. BLOUNT. Sorry, Mr. Chairman. Representative, I will be glad to address that. I have heard that word "refusal" over the course of the past month. I don't know where it emanates from. We have had an on-going discussion with TSA about that VADR program. We think the VADR program is a good program. We have a historically good working relationship with TSA. We have participated in any number of security audits with them throughout the years. They have been in our headquarters in Alpharetta, Texas. I have met the administrator on multiple occasions. It has been simply a function of timing on when to do the assessment. There has never been a refusal, and we have that planned at the end of July to have that assessment done. It is a good program.

Mr. VAN DREW. Thank you. I am glad it is a good program. Didn't it seem to you that it could be done in a more timely way

rather than, you know, this period of time, and we are still waiting until the end of July, and here we are in the beginning of June?

Mr. BLOUNT. Representative, I think the issue has been we have been getting ready to move into a new facility. Our lease has expired. The discussion between my CIO and the director of the security group of the TSA has been more around what is the best date for them, as well as the best date for us. Again, I don't know where the word "refusal" comes from. We have never refused anything like that with the TSA.

Mr. VAN DREW. You state that categorically, OK, there is no time that you absolutely——

Mr. BLOUNT. I mean, no question about that, Representative, no, sir.

Mr. VAN DREW. OK, thank you. You state that you paid the ransom demanded by the DarkSide, but also admitted, too, that the decryption tool that they provided you did not entirely work. What made you decide to pay the ransom? Did you agree that paying ransom is, in one important sense, is rewarding bad behavior?

Mr. BLOUNT. Representative, I would love to address that. If I go back to May 7, 6 a.m. in morning, when I found out about the attack, I automatically started focusing on how do we contain the threat, how do we restart our systems now that we are taking them down? Like all good operators, I have to avail myself of every available option that I have, and the—paying the ransom allowed me access not only to the de-encryption tool, but also additional services that DarkSide offers those to systems they have corrupted. When you are moving 100 million gallons of fuel to the American public every day, 50 million Americans, and you think you can potentially get there quicker, bring that system on quicker, by having that tool, then you avail yourself with that tool. A tough decision to make. I did not like handing that money over to criminals, but it was a decision that I made in order to support the country.

Mr. VAN DREW. OK, and I——

Chairman THOMPSON. The gentleman from New Jersey's time has expired.

Mr. VAN DREW. All right, I yield.

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

Ms. SLOTKIN. Thank you, Mr. Chairman, and welcome to our guests. I appreciate your professionalism in showing up and answering what I cannot imagine to be fun questions about what I am sure will be a dark day in your professional experience. I can't imagine that this is easy.

After the attack, I wrote a letter to a bunch of the pipeline companies that go through the State of Michigan, just to ask, you know, what were they doing, what were they learning? I am more interested, at this point, in trying to understand how we learn from your experience because I can't imagine any company in the world wants to go through what you are going through.

If the attack wasn't bad enough, then the hearing, I am sure, will prove to them that they should not want this to happen to them. But, you know, I am concerned, we have the deputy attorney general calling it a clear and present danger. Are these cyber attacks? We have a former Secretary of Defense saying he is just waiting

for our cyber 9/11 to happen. If it hasn't happened, then this incident, I think, with your company, is the USS Cole attack before 9/11. It is the warning that we should all see before an attack that really debilitates us in a much more profound way.

So, I guess you have answered lots of questions about what you are doing differently. You know, you mentioned a bunch of tabletop exercises and things that you did, but, obviously, they did not work, right? I guess my question is, are you allowing researchers, kind-of the white hat hackers, to try and get into your system? Are you using kind-of that approach where you are allowing people to try and attack you, not just doing a tabletop exercise on what you would do, but actually trying to let them into your system? Have you done that before?

Mr. BLOUNT. Representative, first let me thank you for your kind words. I appreciate those. Very nice of you to do that.

Yes, we participate in penetration tests. We participate in audits and that is by design, to try to find weaknesses. If you find weaknesses, then determine how you best remedy them. Of course, if you consider how fast the criminal element is growing and their skills are growing, you have to continually stress test your system in order to stay ahead of the curve. It is like all technology, it changes constantly. That is why you are continually hardening your systems and making those investments.

So I appreciate——

Ms. SLOTKIN. You have invited outsiders to do this, not just folks inside your own system, but outside organizations, outside groups that do this for a living?

Mr. BLOUNT. Representative, absolutely, because you run the risk of being myopic if you were to do it yourself. You have to have outside experts. You know, similar to the reason we brought Mandiant in to help us restore our systems and to determine what happened to us and run an investigation. That is the absolute right thing to do and I think all responsible operators are doing that.

Ms. SLOTKIN. Yes. I think, you know, beyond the pipeline companies that go through Michigan and through our Great Lakes, you know, the average company doesn't have nearly the resources that you have, doesn't have nearly the staff that you have. I think a lot of us are looking at, you know, if you can't and other companies like you can't protect against these attacks, what are the little guys supposed to do who are even less in touch with some of the latest and greatest in cybersecurity?

I have tried to get at this problem by requiring DHS to help State and locals figure this out and do more tabletop exercises. But if you could give a message to the CEOs of those companies and what you wish you would have done differently ahead of time, what would that message be?

Mr. BLOUNT. Well, I think the message is that I would like to share, Representative, is we need to be aware of what is going on. We have gotten a lot more press about it here in the last month as a result of this particular incident, but we can't be complacent in our defenses.

Just as importantly to preventing the attack is we really need to work hard, and most operators are capable of doing it, and we certainly have demonstrated that, we must respond immediately to

contain that threat, recognize the threat, contain that threat, remediate, and then be able to restore our systems. I think a lot of pipeline operators, for the most part, know how to do that. It is inherent. We all have those emergency response processes.

Then the other thing that is most important, and we talked about it earlier today in this forum, is the willingness to be very transparent and come forward extremely quickly. I think we have seen in the United States over the course of the last month a lot of companies admitting that they were hacked and paid ransom 3 or 4 months ago. That is not helping defend any of the other companies that are being attacked let alone critical infrastructure.

Ms. SLOTKIN. I couldn't agree more. Being able to be transparent with the public has to be the first step.

I also just want to associate myself with the comments of a peer who talked about the absolute lack of deterrence, the absolute lack of punishment and consequences for the people who conduct these attacks. Until we get at that, we are going to have more CEOs in front of our committee.

Thank you. With that, I yield back.

Chairman THOMPSON. The gentlelady yields back. The Chair recognizes Mr. Norman for 5 minutes.

Mr. NORMAN. Thank you. Mr. Carmakal, the DarkSide, the Russian hackers that caused the Colonial Pipeline attack, really seemed to enjoy the approval of the Russian government and Putin. Is this one of the roles, I think Congressman McCaul asked this, that Government can use to prevent Russia from approving this? Do you agree with this? Mr. Carmakal.

Chairman THOMPSON. The gentleman needs to unmute himself.

Mr. CARMAKAL. Can you hear me now? OK, thank you. So, the DarkSide group is——

Mr. NORMAN. I can hear you now.

Mr. CARMAKAL [continuing]. A network of different operators that conduct intrusions on behalf of the DarkSide name. So, while there is a requirement to be affiliated with the DarkSide Group that you have to speak the Russian language, it doesn't mean that every single operator is located within Russia. We assess that the majority of the operators are Eastern European criminals, and so, you know, we certainly would request the U.S. Government to help with encouraging the Russian government and other governments that harbor these criminals to try and apprehend them and discourage them and stop them from conducting these operations.

Mr. NORMAN. Would you not think it would make sense, this administration has removed the sanctions for the Nord Stream 2 pipeline, would you not think this would play into putting the sanctions back on to have leverage against Russia? Just asking them, I don't think that is going to get the job done, but we need leverage. Wouldn't that be one of the tools that Mr. Biden could suggest when he meets with Putin this week?

Mr. CARMAKAL. Congressman, I would certainly defer to the Government to make decisions like that. You know, I want to focus on cybersecurity and, you know, that would be outside of my expertise.

Mr. NORMAN. OK. Mr. Blount, yesterday in the hearing you said that the decryption tool that you purchased from the DarkSide was not a perfect tool. Can you elaborate on that?

Mr. BLOUNT. Yes, Mr. Representative. I will do that and then——

Mr. NORMAN. Mr. Blount.

Mr. BLOUNT. Are we on mute again?

Chairman THOMPSON. You are unmuted.

Mr. BLOUNT. Am I on? Mr. Representative——

Chairman THOMPSON. Yes, you are.

Mr. BLOUNT. Can you hear me now?

Chairman THOMPSON. Yes, we can.

Mr. BLOUNT. Sorry. To respond to your question, Mr. Representative, I did make the statement yesterday that the tool is not perfect and I heard that is often the case. The tool has been used, and Mandiant probably could speak further to that. But, again, for me, not knowing in those critical hours in the morning what I had and my capability to bring that pipeline system back on as soon as possible, I had to run the risk that the tool perhaps wasn't perfect, but, indeed, it was a tool that was advertised as being able to decrypt a massive amount of material on my system that had been encrypted.

Mr. NORMAN. So if you rewound the clock, knowing what you know now, Mr. Blount, what is your opinion of the type of things Colonial needs to do moving forward to prevent this from happening again?

Mr. BLOUNT. Yes, if I rewound the clock I would say that, you know, we need to continue to do what we have been doing, which is continue to invest in defense. But, you know, granted, we have talked today in this forum today that nobody is immune to an attack. We, like any operator, get hit millions of times a day by people trying to do the same thing that we saw DarkSide do. Fortunately, we have the defenses to stop that.

Certainly, if we started to pull all these reports that the operators have been filing every 12 hours, you are going to see that that is not unique to us. That goes on at every operator in every State in this country right now. It is a maximum amount of volume of attacks that we are dealing with.

So, again——

Mr. NORMAN. I was just going to say I agree with you. You have got 4,000 ransomware attacks every day. So, a lot of companies, because of their name and don't want it out, how would you incentivize other companies to come forward, share what they have learned, and work with you to prevent this from happening?

Mr. BLOUNT. I encourage it. I think——

Mr. NORMAN. Mr. Blount, can you hear me?

Mr. BLOUNT. Yes, sir. Mr. Chairman, can you hear me?

Chairman THOMPSON. Yes, I can. We are hearing you.

Mr. BLOUNT. Very good. I encourage all CEOs who have been hacked and subject to a cyber attack could be very transparent about it. It is the only we are going to learn that these attacks continue to change. There is variance to these attacks. Any information we can get in a timely basis is helpful to everybody in this country to help avoid and help deal with after the fact responding to these types of hacks.

I am sure there is any number of reasons why people are hesitant to it, perhaps they are embarrassed, perhaps they have a

brand name they are trying to protect. But I think in the long run transparency and honesty with regard to this particular topic is extremely important to all American citizens in our effort to try to stop what we are seeing become more and more a daily event.

Chairman THOMPSON. The gentleman's time has expired. The Chair recognizes the gentlelady from New York for 5 minutes.

Ms. CLARKE. I thank you very much, Mr. Chairman, and thank the Ranking Member. This is a very important hearing and I am so glad that we have the witnesses before us today.

Mr. Blount, I just wanted to circle back to a question that was raised by my colleague, Mr. Langevin. We know that you hired Mandiant through our outside counsel. My question to you is, did you or your legal team have any discussions about retaining Mandiant through counsel in order to place any of the findings that you have been able to obtain under attorney-client privilege?

Mr. BLOUNT. Representative, I wasn't involved in the hiring of Mandiant. We would have to talk to my general counsel about why we went about taking that route.

Ms. CLARKE. Very well. Would you get back to us after you speak with them? That would be very interesting for us to know.

Over the past several years, ransomware attacks have become more frequent and consequential. Did Colonial Pipeline have a ransomware continuity of operations plan to ensure that operations could continue in the event of a network disruption?

Mr. BLOUNT. Representative, thank you for asking that question. We have what we call an emergency response process. We use it for every threat that we identify throughout our pipeline system. So, in this particular case, it was a cyber threat, came through our control room in the form of a ransomware note. We identified it. We continued it by shutting down the pipeline system. Then, obviously, we went on to the process of remediating and restoring our operation back into service as quickly and safely as we possibly could.

We also——

Ms. CLARKE. But that was part of your planning. My next question is, with that consideration in mind, is ransom part of that planning that you do?

Mr. BLOUNT. Well, thank you for that question. Of course, ransom is part of the threat, so the answer to that question would be yes. Each threat is unique, right? Not all of them, obviously, come from the standpoint of a criminal element. It could be something that we see in one of our yards that is not a safe event that we want to identify and contain and figure out how to remediate. So ransomware is part of our emergency response process. It is just another variable that we would deal with.

Ms. CLARKE. Very well. Last week, Deputy National Security Advisor Anne Neuberger circulated a memo to corporate leaders urging them to take immediate action to defend against ransomware, mitigating the impacts of an attack. It recommends practices like backing up data, patch management, developing and testing incident response plans, working with penetration testers, and network segmentation, among other things. Before this incident, to what degree had Colonial backed up this critical data and systems? Did you keep back-ups off-line?

Mr. BLOUNT. Great question, Representative. In fact, if you look how quickly we brought our system back on and our response, a good portion of that was the result of the fact that we wound up having very quality back-up systems. As I understand and as I have learned a lot over the course of the last month, that is not always the case, which is why you want to make as many options available to you. When you see that threat, you contain that threat, and you start to remediate.

But in our case, we apparently had some very quality back-up systems that allowed us to bring the pipeline on sooner than later.

Ms. CLARKE. So, my next question is, before this incident, when was the last time you tested your incident response plan and what corrective actions did you take afterward?

Mr. BLOUNT. The incident response process is part of our DNA. We do tabletop exercises. If you talk about it from a physical standpoint, we work with local law enforcement in regions throughout the United States on an annual basis to prepare for emergencies that might take place across our pipeline system.

Ms. CLARKE. Also, do you recall when the last time was or is that something your CIO would have the answer?

Mr. BLOUNT. Representative, again, ours is an emergency response process, so it might not even have been a cyber issue tabletop-type exercise. It could have been any number of things, like a pipeline physical attack and things like that. I will be glad to share those dates with you. We do it continually. Again, it is part of our DNA as a safe organization.

Ms. CLARKE. I am sure having experienced this incident there will be a closer look at the cybersecurity concerns of your organization. Let me just say that I think this is certainly a case study for cyber hygiene because it was through an unsecure password that the Nation's largest pipeline was disrupted. I want that to be a lesson to everyone who is listening to this hearing that we must, must do better with our cyber hygiene.

With that, Mr. Chairman, I yield back. I thank you, Mr. Blount, for your candor and your participation today.

Chairman THOMPSON. The lady's time has expired. The Chair recognizes Mrs. Miller-Meeks for 5 minutes.

Mrs. MILLER-MEEKS. Thank you, Chair Thompson, and thank you, Ranking Member Katko and our witnesses today.

Cyber attacks are certainly becoming more and more commonplace in the ever-evolving digital age. In fact, we have had those to our local governments here in Iowa, and I have a JBS meat processing plant in my Congressional district, as we know, was recently involved. From public schools and local libraries to critical infrastructure companies, like Colonial Pipeline, no one is immune and all require prevention tools. Systemically important companies, such as Colonial, should be particular wary of attack, as you indicated that you were, due to the unique source of the risk that you represent.

You mentioned yesterday, Mr. Blount, that ransomware was not mentioned in your cyber incident response plan and so I have 2 questions. Due to the high risk of attack, have you given consideration to the risk of ransomware affecting your company? What resiliency do you have in place to digitally communicate with the

internet of things, devices, and OT, or operational technology, industrial controls that would protect your enterprise from future attacks knowing that they are coming? This is also to help other companies as well.

Mr. BLOUNT. Well, thank you for your question and let me try to address them because I think you had a couple of those—a couple questions embedded in there. You know, certainly, as the investigation goes on and we continue to allow Mandiant to do what they have been brought in to do, we see no indications of compromise in the OT system. I was asked that question earlier as to, well, then why did you shut down the system? The response to that would be if you even think there is a 1 percent chance that that criminal got into your OT system, it could potentially take over control of a 5,500-mile pipeline moving 100 million gallons a day, then you shut that pipeline down.

That is what we did that morning. We used our stop-work authority. That control room employee made the right decision and shut the pipeline down. I am very proud of what he did there because it helped protect all of us not only as United States citizens, but also potentially protecting the environment and the communities in which we serve.

Now, I think you had 1 other question embedded in there.

Mrs. MILLER-MEEKS. It was had you given consideration to ransomware?

Mr. BLOUNT. You know, when we look at, you know, our response, I am very pleased with our response. When we look at our emergency response process, certainly there won't be a definitive way to handle ransom in the future because I think each case is unique. In this case, obviously, it was the concern that we really had no vision into our IT or OT systems to understand the degree of corruption and encryption. It really took us days, even with the help of a world-class expert by Mandiant to get there. So, again, that is why that decision was made.

So, again, I think for operators it is probably better not to have a strict policy because you may need that option. There are a lot of entities. In some cases, like hospitals, that would be their only option potentially, to pay the ransom. Again, I am not saying that is a morally right or wrong decision, but it may be a decision you have to make like I did that day, which was extremely difficult.

Mrs. MILLER-MEEKS. So, thank you. Certainly we know I don't disagree with Representatives McCaul or Slotkin that, you know, we need to punish bad actors. In this case, there could be State or country entities involved. Even though the OT system was not involved in this instance, we know that OT systems with access to the internet and emerging 5G technology bring further digital problems and opportunities for bad actors.

Mr. Carmakal, are there other technologies, i.e., mobile high-frequency technologies, that are safer, not on the internet, and more cost-effective that perhaps we should be recommending to companies that are critical points of our infrastructure?

Mr. CARMAKAL. This has to do with the interaction between the IT environments and the OT environments. So we would, you know, continue to encourage organizations to not only segment their operational technology environments, but continue to get bet-

ter visibility and to the assets that exist within the operational technology environment and mitigate some of the risks associated with vulnerabilities that exist out there.

Mrs. MILLER-MEEKS. Thank you so much. Certainly, I think both of you have emphasized the need to have a single source point for reference to interact with the Federal Government, some things we need to work on. Is there a regulation that either of you think that Congress should enact for companies for transparency, for immediate reporting, and, you know, before negotiating to pay ransom?

I am running out of time, so thank you, Chair Thompson, if they could answer the question. I will yield back.

Chairman THOMPSON. Either one of the witnesses can answer the question.

Mr. BLOUNT. Representative, I would say that I think the new TSA standards are a great start on the part of the Government. You know, the timely reporting, the 12-hour reporting, I think that is extremely valuable.

Chairman THOMPSON. The gentlelady's time has expired. The gentleman recognizes Mr. Correa for 5 minutes.

Mr. CORREA. Thank you, Mr. Chairman, again for this most important hearing. I can't think of any issue that is more important to our country and to our Nation throughout society than cybersecurity. Gentlemen, thank you for being here today with us.

As I listened to your testimony, Mr. Blount, I am reminded of a case I had here in my district about a year ago. Just a local tax preparer with about 4,000 clients one day calls me and says I have got a problem, Lou. I said, what is it? It sounded just like a Colonial Pipeline, you know, the good old days, which is small-scale. This guy had his 4,000 customers essentially held hostage and he was in trouble. Now we have Colonial that shows that this is not random and it is going to continue to get worse.

So, my question is really to Mr. Carmakal. If you can go back and envision a situation that we have had [inaudible].

Chairman THOMPSON. I believe the gentleman is having some technical difficulties. While Mr. Correa is getting corrected, Mrs. Harshbarger, we will recognize you for 5 minutes.

Mrs. HARSHBARGER. Thank you, Mr. Chairman and Ranking Member Katko and the witnesses. Mr. Blount, you know, I feel for you being in front of Congress, going in front of the Senate, now in front of us. Private companies, a lot of them, don't even report that they have been ransomed in a lot of ways. I have talked to my companies in my district, the First District of Tennessee, and they don't do it because they don't want their customer base to feel that they are vulnerable or that they can't protect their information, the stock value goes down, or the fact that they might be hauled in front of Congress. Those things would prohibit a lot of companies from even telling us that they have been hacked, basically.

Let me ask you a simple question. Did you have confidence that the Government, if you reported a cyber breach, that the Government could help you with that breach before this ever happened?

Mr. BLOUNT. Thank you for that question. That is an interesting question. I haven't heard that one in the last few days, so thank you.

Mrs. HARSHBARGER. Well, that is just a straight-up yes or no.

Mr. BLOUNT. Well, you know, we have a 57-year history——

Mrs. HARSHBARGER. Listen, I came from the private sector to the public sector, so I understand exactly how you feel right now.

Mr. BLOUNT. Yes, ma'am. Well, we have a 57-year history of dealing with the American Government, both on a regulated side as well as the other entities that we have relationships with. So, never in my mind did I think that, No. 1, I would have to make those calls, but when I was making them or my team was making them, because it was an all-hands effort that day, we knew that if there was things that we needed done that they would get done. We saw that and I will just give you one example because I don't want to eat up your time.

We knew that trucks would have to be able to move fuel and we knew that drivers have limited number of hours and we know currently in our COVID environment there aren't as many truck drivers. So, again, reaching out early allowed some regulation to be waived, which helped, you know, to some degree, get fuel into the market.

Mrs. HARSHBARGER. Absolutely. You put in your testimony that you would recommend designating a single point of contact to coordinate these Federal responses to types of events just like this. In other words, you are recommending establishing reciprocity across these Federal agencies. Who did you—when all this happened within that first 24, 48 hours, what agency did you primarily work with?

Mr. BLOUNT. Just to give you some context, Representative, I want to give you a list because you weren't on the call earlier, but we contacted within 24 hours the White House, the NSC, the DOE, PHMSA, FERC, DHS, CISA with the FBI, EIA.

Mrs. HARSHBARGER. Yes, good.

Mr. BLOUNT. If you think about that, if we had to make daily calls or intraday calls with each one of those throughout the restoration process, we probably would have come on a whole lot later.

So, we were fortunate in that in this particular case, the White House designated the DOE as our conduit for everybody but the FBI. The FBI and CISA kind of handled the investigative side and then DOE was our conduit to all the other entities that I named. That was extremely valuable to us. I am not stating that one entity over the other should have that role, but I think if you look at the 24/7 effort that my team had to make, we needed that ability communicate, in this case through DOE, about what was going on in the market, what we were doing to restore our IT systems, while we also had the same conversations with the FBI, giving them data and evidence and things like that that we were finding as Mandiant went about doing what they needed to do throughout the course of the beginning of the event.

Mrs. HARSHBARGER. Fantastic. I see where you recommended, too, to be adequately staffed, have adequate resources, and I totally agree with every bit of that.

Mr. Carmakal, you explained in your testimony the definition of "operational technology" and "industrial control systems". You state that there are relatively fewer disclosed intrusions of OT environ-

ments as compared to the IT environments. My question is, why do you think that is?

Mr. CARMAKAL. Congresswoman, I think one of the reasons for that is because there are probably fewer intrusions into operational technology environments given the general segmentation that exists between IT environments and operational technology environments.

I also think that many of the threat actors out there that conduct intrusions, while they might be very skilled from an IT intrusion perspective, many of them don't actually know and they are not familiar with the operational technology vendors and other infrastructure that exists within those environments. So, they may not actually even know how to conduct substantial intrusions.

But with that said, although there are fewer publicly reported incidents, the incidents that have been reported are quite substantial. When you think about a power outage in a certain part of a country or potentially the modification of software that controls safety control systems at a petrochemical facility in the Middle East, obviously the consequences are quite substantial.

Mrs. HARSHBARGER. OK. Thank you so much and I yield back.

Chairman THOMPSON. The gentlelady's time has expired. The Chair recognizes again the gentleman from California, Mr. Correa. The gentleman needs to unmute.

Mr. CORREA. Can you hear me now?

Chairman THOMPSON. We got you now.

Mr. CORREA. Mr. Chairman, thank you very much. Just to expose these bad guys when I got cut off. I guess that is the way technology works.

Mr. Carmakal, my question to you, sir, if you had a moment to pull back and look at the big picture, what should we be doing now to prepare for the next 5 years in terms of defending our system? Defense, offense, what is it—what would your top 2 or 3 things that you would ask us to do on your wish list to make sure that we are better prepared for these attacks moving forward?

Mr. CARMAKAL. Congressman, unfortunately, we are dealing with cyber intrusions every single day and what occurred over the past few months, it has been happening for the past several years. So I think we all need to come together from both a Government perspective, commercial organizations, as well as the security community to not only help organizations better defend themselves, but we would certainly look for help from the Government to create some repercussions to the threat actors that are conducting these intrusions.

So we would certainly like to see individuals become identified that are conducting intrusions. We would love to see arrests to the extent that is possible. We would love to see sanctions. We would love to see indictments where it is possible. We certainly would like Government support to come in more from an offence perspective and help disrupt some of the operations that these criminals continue to conduct in.

So I do believe that we all need to come together and not only defend——

Mr. CORREA. Let me ask you, Mr. Carmakal, if I may interrupt you in the couple of minutes that I have left.

Mr. CARMAKAL. Please.

Mr. CORREA. What about us here? You are talking about the offense, but what about us here at home? What can we do to better coordinate the private and public sector? We keep hearing this issue of, you know, hygiene, cyber hygiene, and the fact that not everybody seems to buy into the threats that are out there, and people are just not doing the right thing. How do we get the private sector to better coordinate with us and make sure they do the right thing?

Mr. CARMAKAL. Yes. Maybe 2 things. No. 1, I would certainly encourage organizations to conduct Red Team Exercises or ethical hacks against their environment to test their defenses, to test their controls. I think a lot of organizations are under the assumption that they have all these security hygiene things in place, but unless you actually test your defenses, it is sometimes hard to identify when those defenses and those controls don't exist.

We also want to continue to encourage organizations to share information about active threats. Again, we talked about this before, but we would certainly love for CISA to get more information about active intrusions and we would love for them to be able to disseminate that information as quickly as they can.

Mr. CORREA. Do you think the private sector right now on a voluntary basis is doing enough in terms of sharing their information with CISA when it comes to intrusions?

Mr. CARMAKAL. I think it depends on the organization. Some certainly are; others may not be. But, you know, one thing I would love to commend Colonial Pipeline on is very shortly after their incident we had talked to them about publishing information about the DarkSide network and some of the indicators of compromise that they use and a description of the techniques that they use to not just help the Government, but also help other organizations that are trying to defend themselves. So, you know, we are trying to do our part as well to get information out to help the community to defend themselves.

Mr. CORREA. Thank you very much. I also want to thank Colonial Pipeline for their work and their cooperation with the Federal Government. I just hope there are some lessons learned here and that we can apply them and distribute them on a National to make sure we are all working, Mr. Carmakal, your words, sharing and working together in a coordinated fashion. Thank you very much.

Mr. Chairman, I yield.

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

Ms. TITUS. Thank you, Mr. Chairman. Many of my questions have been asked and answered and asked again, but I would like to expand on what was just discussed about better coordination here between public and private and among the different agencies throughout the country.

We have to realize that this is an international problem. Not only is the enemy international, but some of our friends are subject to the same kind of attacks. That is especially true among our NATO allies. They are probably experiencing some similar kinds of things, being hacked from people in Russia. So, I wonder what we are doing or what we could be doing to better develop best practices

or share information with our international allies and companies abroad. Anybody?

Mr. CARMAKAL. Congresswoman, that is a great point. I certainly want to recognize that there are cyber threats that occur all over the world. In fact, when you look at, you know, the geopolitical climate and you look at certain countries that are considered to be hot zones for cyber attacks, Ukraine is certainly one of them, the Kingdom of Saudi Arabia is another one of them. A lot of time we see intrusion activity occurring in that part of the world sometimes before that occur in the United States, possibly for—you know, for a number of different reasons. I think it certainly helps to share information with the community, the broader community, to apply some of the learnings that have occurred with respect to some of the intrusions in Ukraine and Saudi Arabia.

For example, I mentioned that there were operational technology security incidents in both Ukraine and Saudi Arabia. There are learnings that we have all been able to gather from that and make—you know, and apply them within the United States. Again, we certainly welcome collaboration.

Ms. TITUS. Well, OK. Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you very much. The gentlelady yields back. The Chair recognizes Mr. Clyde for 5 minutes.

Mr. CLYDE. Thank you, Mr. Chairman and Ranking Member Katko, for holding this very important hearing.

You know, Mr. Blount, my district, Georgia 9, certainly felt the impact of the pipeline shutdown and I saw many gas stations with no fuel. But I certainly commend you and the Colonial Pipeline workers for how quickly they worked with both private assets and Federal agencies to get the pipeline back up and running in as reasonably short time as possible. I know the decisions that you made were very difficult, especially the decision about the ransom, and that you made them in the best interests of your customers and our country in mind, and personally, I appreciate that.

I also commend the Department of Justice and the FBI for recovering the $2.3 million in ransom that was paid. By the way, Mr. Blount, have they given you that money back yet?

Mr. BLOUNT. Thank you for your kind words. I don't know the answer to that. I suspect we haven't seen those bitcoins back yet, but that is the first question I have heard along those lines in the last 2 days as well, so thank you.

Mr. CLYDE. Well, I just want to make sure you get it back, OK?

Mr. BLOUNT. Sounds good to me. Thank you, sir.

Mr. CLYDE. All right. In your testimony, you mentioned your desire that our Government put pressure on host countries. Now having gone through this very difficult experience do you have any thoughts on how we could do that and how our President could send a strong message to our adversaries?

Mr. BLOUNT. Well, thank you for that question. You know, from our standpoint as a private operator, you know, we don't play in the geopolitical scene, of course. The President has a lot of capability in that regard and certainly that is what we ask that he consider, the Government consider, putting pressure on these host countries that are allowing this to happen behind their boundaries. But as far as our recommendations, it is really not our backyard.

We just think it is necessary in order to, you know, thwart as many of these attempts and to eliminate as many of these criminals as we possibly can so that no one does have to make the critical decision that I made on May 7 and to work 24/7 like my employees did in the great State of Georgia to bring that pipeline system back on.

Mr. CLYDE. OK. So, you just want to hear that he is doing it?

Mr. BLOUNT. I have got no problem with hearing that, yes, sir.

Mr. CLYDE. All right, great. For Mr. Carmakal, I have a couple questions for you. I have always believed that the best defense is a good offense, and I am a big proponent of making the bad actors pay, especially those who extort others. In all of your work, do you have any information that would lead you to believe the ransomware attacks on Colonial Pipeline and JBS Foods were foreign state-sponsored? If——

Mr. CARMAKAL. Sorry. Congressman, we do not have any information indicating that the attacks against both those organizations were directed by the Russian government.

Mr. CLYDE. Well, not just the Russian government, but any other state.

Mr. CARMAKAL. Congressman, we do not have any direct evidence suggesting that.

Mr. CLYDE. OK, all right. Well, the same question that I had for Mr. Blount. How do you think our Government could do a better job with putting pressure on host countries, I think, to basically root out and eliminate these criminals like DarkSide? How could we do that? I think you are on mute, sir.

Mr. CARMAKAL. Congressman, I certainly welcome a number of things. From a diplomacy perspective and foreign policy perspective, I would welcome any support that our President and Government can apply to Russia and other neighboring countries that host criminals. We certainly don't want that, you know, ransomware and destructive attacks to continue.

We would certainly also welcome more of an offensive capability to disrupt some of the criminal operations. We have seen successes over the past few weeks and certainly the past few months. We would love to see continued support to make it more difficult for these criminals to conduct these operations.

Mr. CLYDE. OK. I am sure the people in your company are very talented. Would your company have the ability or desire to assist the Government if offered the right rules of engagement?

Mr. CARMAKAL. Congressman, it is a great question. It is something that I would need to talk to my team about.

Mr. CLYDE. OK, all right. Thank you. I have one more and this is for Mr. Blount. Between CISA, the FBI, TSA, and other agencies, there is a wealth of information and helpful guidance that is pushed to all companies across all sectors. Has any of that ever made it to your desk or to that of your CIOs? If it did, were there any that you found specifically helpful?

Mr. BLOUNT. During the the event, we found all the resources available to us to be extremely helpful. You know, those phone calls that we had every day with DOE, everybody on those phone calls was expressing support and offering to help to the extent that they could. Again, we saw a lot of that. We saw, you know, regu-

latory things waived in order to move fuel quicker, move more fuel on the same truck and things like that.

So, again, as I have said previously, I have got nothing but good things to say about the response from the Federal Government and all those entities that we dealt with over the course of those days and continue to deal with, as you can expect.

Mr. CLYDE. OK. Well, thank you very much. With that, Mr. Chairman, I yield back.

Chairman THOMPSON. The gentleman yields back. The Chair recognizes the gentlelady from New Jersey, Mrs. Watson Coleman, for 5 minutes.

Mrs. WATSON COLEMAN. Thank you, Chairman. There has been some confusion on the topic of TSA assessments. There are 2 types of TSA assessments: The Critical Facility Security Review, CFSR, which looks at the physical security; and the Validated Architectural Design Review, which looks at cybersecurity.

Mr. Blount, you said that Colonial never declined these assessments. But according to TSA, Colonial has repeatedly postponed participating in a CFSR since March 2020 and has repeatedly postponed participating in a VADR assessment since October 2020. Delaying these assessments for so long amounts to declining them, sir.

I understand a VADR assessment is now planned for late July, but that a CFSR assessment still has not been scheduled. Given Colonial's recent track record of stonewalling TSA's requests for 2 separate types of pipeline security assessment, it raises serious questions about your company's perspective on regulation.

Does Colonial have a policy regarding requests for its regulators? Who decides whether Colonial cooperates or does not cooperate with a TSA security assessment? To your knowledge, did any of those requests that have been declined by your company to TSA ever get to your desk?

Mr. BLOUNT. Thank you for the question because I appreciate the opportunity to clarify that. I am not aware that we have ever denied TSA or refused the TSA to do any assessments. We have had a long-standing, great relationship with TSA. I will share with you that my CIO is extremely frustrated with this continual question that we have refused. Her contacts at TSA don't understand why the word "refusal" has been used.

We have asked for some exceptions as related to COVID–19. We are not going to expose our control room personnel to outside people prior to the large majority of the United States being vaccinated. As far as——

Mrs. WATSON COLEMAN. Mr. Blount.

Mr. BLOUNT [continuing]. VADR——

Mrs. WATSON COLEMAN. I am sorry. Thank you. I understand that TSA offered to do one of the assessments virtually and even that was declined. So, I am going to say that I think that your perspective on your relationship with TSA is one thing. Their perspective on the relationship from the information we are getting is something other than that. So, do you think there is a value in having a written policy that says that Colonial will respond to requests coming from a regulator such as TSA and that that policy could be forthcoming as early as July 1?

Mr. BLOUNT. Representative, with all due respect, we always respond to any regulatory agency where we are responsible to. Again, we have had a good working relationship with TSA. Next week, when I get back to the office, I will be calling the head of TSA to have a discussion regarding this word "refusal". It is not consistent with the relationship that this company has had.

Mrs. WATSON COLEMAN. Thank you. Let me ask you a totally different—I look forward to hearing from you as to the advances moving forward with regard to your relationship and the mutual understanding between TSA and Colonial. I think TSA has a very important role in this space.

I have a real quick question, I think. You paid $4 million for an encryption key and then you said that it was insufficient. Can you tell us where the insufficiencies existed? What was problematic, how you overcame those deficiencies to get things up on-line?

Mr. BLOUNT. Representative, great question. I am not a technical person, so I couldn't explain deficiency as far as the tool. I know that all these tools are not perfect, but they have—I have been told that Mandiant has used the tool. So, whether they have had to manipulate it in order to make it perfect, so to speak, that would be a great question for them. I don't have the technical expertise to define that further for you.

Mrs. WATSON COLEMAN. Then in the little bit of time I have left could I ask Mandiant to respond to that question? Because I want to reiterate, you spent $4 million to get it. Other folks who have a malware hacking, they need to understand that they could go on and pay the ransom and still not get what they need to get up and running again.

So, can I have Mr. Carmakal respond to that for the remainder of my time?

Mr. CARMAKAL. Congresswoman, the decrypter that was provided by the threat actor, it did work. It was effective. There were bugs in it, certainly, but it didn't actually—it wasn't actually needed to be able to recover systems and data within the Colonial Pipeline environment. They leveraged their back-up processes and their restoration processes to be able to effectively come back on-line. So while the tool did work, it just wasn't needed at the time.

Mrs. WATSON COLEMAN. Thank you. That begs the question then, since they already had the capacity to get back up on-line: (A) Should they have ever paid the ransom; and (B) should they have ever cut the supply of resources off to those who were waiting for it along the Northeast corridor? Thank you and I yield back.

Chairman THOMPSON. The gentlelady yields back. The Chair recognizes the gentleman from Michigan, Mr. Meijer, for 5 minutes.

Mr. MEIJER. Thank you, Mr. Chairman. Thank you to those who are here today, our experts, Mr. Blount and Mr. Carmakal.

You know, Mr. Blount, I really appreciate you coming before this committee. I know this has obviously been challenging and Colonial Pipeline has been the focus just given the wide-spread economic impact that has been felt throughout the region. But part of our committee's role here is to determine how we can make this Federal engagement and critical infrastructure stakeholder relationship as efficient and effective as possible to prevent and also mitigate any other future attacks.

So I just wanted to say I appreciate your willingness to talk to us on this end. I do not want this to be viewed or felt as too much of an inquisition. But we obviously need to make sure that we are learning the right lessons from what happened.

You mentioned in your testimony that you were in contact with the FBI and CISA within hours of discovering the attack and that you have stayed in contact throughout the process. You went through in prior questioning of what that time line was like. Just as a brief yes or no from that experience, is it clear to you how the U.S. Government shares information internally on cybersecurity?

Mr. BLOUNT. I would say the answer to that, Congressman, is no.

Mr. MEIJER. OK. That is certainly an area where I think our Federal Government needs to clarify that given the vast array of actors on the Governmental side at play here. Then you offered the recommendation of creating that single point of contact. You know, with the Colonial Pipeline attack we had DOE leading the Federal Government's response, we had entities like CISA and TSA that had more explicit responsibilities that were obviously involved in that, and then obviously the FBI as well. So, within the internal processes we obviously need to work to streamline as best as we can.

I guess another yes or no, would you support a mandatory reporting requirement to CISA and the FBI in the event of a cyber attack on an institution?

Mr. BLOUNT. Representative, I guess the way I look at that is, you know, that is exactly what we did, so that is the right choice for Colonial. You know, I would hate to say that I think that is the right choice for another party, but for us that transparency is extremely important and we would do it again just like we did it last time. No issues with that at all.

Mr. MEIJER. Then, again, I think we have seen with the naming of former attacks, and I am thinking Solar Winds comes to mind, the stigma that is associated can create a set of incentives that cause companies to hide that, to not report it or to just stay in the shadows, and how that can have a compounding effect in terms of being able to identify, deal with the risks, and then root it out.

Mr. Carmakal, we have spoken about this earlier and I want to strongly associate myself with the remarks of Mr. McCaul, Mrs. Miller-Meeks, and Ms. Slotkin on this front. The asymmetric nature of this threat and dealing with asymmetric threats as a nation-state, as a superpower is perennially challenging.

I am frustrated to no end that lawmakers and corporate executives and others in Government and in the private sector in the United States are staying awake at night concerned about the cybersecurity threat. Meanwhile, the DarkSides, the advanced persistent threat actors overseas, especially those who are not officially supported by a nation-state, but certainly offered safe harbor or otherwise not being—not upholding any sort of rule of law, those actors are not staying awake at night. They don't have the same fear that we have.

I firmly believe that the U.S. Government needs to engage in this in a serious way. We need to have those actors understand the consequences before we have an incident that takes American lives. We certainly saw wide-spread economic disruption with the Colo-

nial Pipeline, but the asymmetry here is palpable and it is something that we need to work strongly to address. We need to be able to put that fear into those who seek to attack the United States, but they cannot operate with impunity. We will be the ones who knock and that there will be consequences.

So, I know that you have addressed that prior, but I just wanted to give you a brief moment to address any further thoughts you have on that offensive capability. Thank you.

Mr. CARMAKAL. Congressman, I certainly agree that we need to make it more difficult for these threat actors to conduct their operations. I am really proud of some of the successes that we have had over the past few weeks and the past few months, and Government coming together with commercial organizations to disrupt some of the capabilities of threat actors.

When we look back at what occurred back in October 2020 with respect to the acute threat to health care organizations, a lot of folks came together to help curb the ransomware problem that was occurring that was directly impacting health care organizations. When you look at the disruption of the TrickBot network and the Emotet botnet, you know, there has been a number of successes, but I think there is a lot of opportunity for us to do more, to go more offensive. But I think we need to define what the rules of engagement are and what is accepted and what is acceptable.

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

Chairman THOMPSON. Thank you. The Chair recognizes the gentleman from Missouri for 5 minutes, Mr. Cleaver.

Mr. CLEAVER. Let me, first of all, thank you, Mr. Chairman, for giving me the opportunity to introduce and the committee passed the Pipeline Security Act, which codifies TSA's Pipeline Security Division and it increases engagements between the pipeline operators, TSA, and CISA. As I said, it came out of the committee last month.

But, Mr. Carmakal, based on your experience working with critical infrastructure owners and operators who have experienced and even suffered from this ransomware or other types of cyber attacks, do you have any observation about how the Federal Government can improve its response and better coordinate its efforts, particularly for private-sector critical infrastructure such as pipelines? Give us what you think we ought to be doing.

Mr. CARMAKAL. Congressman, I certainly think that we need to take the learnings from these attacks, these other intrusions, and perhaps some of the things that organizations thought they were doing well from a security perspective and share that with other organizations out there. I think it is a missed opportunity if we don't take these learnings from both an intrusion perspective and, you know, security control failures perspective, and share that with other organizations. I certainly welcome other—more Red Team Exercises or penetration testing for organizations, again, to test the defenses and to maybe test some of their assumptions with respect to controls that they believe that they have.

Mr. CLEAVER. Do you feel vulnerable? I mean, do you still feel like you are vulnerable?

Mr. CARMAKAL. Congressman, unfortunately, we deal with cybersecurity incidents every single day. As the days progress, I feel

more direct impact by some of these intrusions. I do feel unless we actually come together and do something, we will continue to feel this on a day-to-day basis from a personal perspective.

Mr. CLEAVER. Now, the Colonial attack, you know, actually has brought cybersecurity to the front of the line in terms of international issues and security issues. But this impacts the pipeline sector into, you know, trying to figure out, you know, what we can—what you can do and other people in your same business are trying to figure out what challenges they have and what they can do.

Given FireEye Mandiant's role as a leading cybersecurity provider, you surely have a front row seat into the vulnerabilities. Does FireEye have other clients in the pipeline space? In your experience how would you generally describe cybersecurity preparedness in your sector, the pipeline sector?

Mr. CARMAKAL. Congressman, we have got clients across all sectors. I will tell you, the skills and sophistication and security maturity of those organizations certainly vary. It is sometimes hard to summarize a certain capability for a particular sector. What I will say is that any time there is a major security incident and it becomes public, organizations within the same sector, they try to take learnings from those organizations and they try to apply some of the best practices and, you know, some of the learnings from those organizations.

I will certainly say that there are a number of organizations that are taking note right now and they are trying to do whatever they can to improve their security defenses. I think, unfortunately, a lot of our organizations are in a similar position.

Mr. CLEAVER. I should have added I am extremely concerned about the transportation sector, you know, compared to other forms of critical infrastructure. I mean, how would you, you know, generally assess the vulnerability of the transportation sector?

Mr. CARMAKAL. Congressman, I think that there are opportunities for transportation sector organizations to continue to improve their security posture and apply the learnings from this.

Mr. CLEAVER. Yes, OK. I yield, Madam Chair—Mr. Chairman.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from Texas for 5 minutes, Mr. Pfluger.

Mr. PFLUGER. Mr. Chairman, thank you, Ranking Member Katko. What an opportunity to talk about something that is so important. Mr. Blount and Mr. Carmakal, thank you for your expertise here. I have got one question for each of you. I will start with Mr. Blount.

The district I represent includes the Permian Basin. We produce 40 percent of the country's oil. Energy security is National security. I am very worried about making sure that we ensure that we protect this industry that keeps our homes, runs our businesses, obviously lets our economy continue to flourish. So, you know, beyond the ones and the zeroes, Mr. Blount, what do you see as another aspect of resiliency? Because it is obvious that the Colonial Pipeline is a very significant piece of critical infrastructure for our country. I hope that we can take these lessons and truly learn them and apply them. So what other types of resiliency can we look to in this sector, in this industry?

Mr. BLOUNT. As you know, I have spent 35 years of my career in Houston, Texas, and I can tell you that though I haven't really had the opportunity to return a lot of phone calls here in the last month, that is a major concern on the part of all the energy sector right now.

I think a lot of what we talked about today with regard to the private-public partnership is extremely important. I think Mandiant added a really valuable equation today, which is the security sector has a lot to add in that conversation so it is a 3-way partnership.

We need to find a way to communicate all the learnings that we take away from the Colonial incident and combine that with the just the amazing amount of other incidents that have happened that, No. 1, we aren't aware of, that Mandiant might be, and learn from those to create the resiliency we need to compete against a very sophisticated criminal element that continues to get more sophisticated. That is a great question.

Mr. PFLUGER. Well, thank you for what you do, for what Colonial does to provide the energy that the, specifically, East Coast needs, such an important piece of our infrastructure. I think we all need to look at it and continue to diversify in this country when it comes to providing those sources of gasoline and natural gas and other fuels to the coast lines.

For Mr. Carmakal, I also represent Angelo State University, a minority-serving institution, an Hispanic-serving institution in the middle of rural America. It is a cyber center of excellence. I am very interested in understanding what we can do at the university level to ensure that we are building the next generation of cyber experts that can come to your company, FireEye, appreciate what you do, and can go throughout the rest of the United States, quite frankly, to bolster against the threat that we are talking about today. Can you specifically talk about at the university level what we should be doing to help that effort?

Mr. CARMAKAL. There is a need for educating more university students and individuals at a much younger level about cybersecurity. There is a desperate need for more cybersecurity professionals out there. Really, anything that we could do to create more cybersecurity curriculum within universities and encourage more young individuals to take on careers in cybersecurity would certainly help us improve and the defense and overall security posture of the Nation.

At FireEye and Mandiant we do a number of things with respect to recruiting talent from universities. We do a lot of presentations at universities. We try to inspire young professionals and students to become cybersecurity professionals once they graduate from college. So, I really do appreciate the question.

Mr. PFLUGER. Well, thank you for that. We are going to continue to push on this because in rural America we need to make sure that our folks understand this is an option for them, this is a job that they can do. You know, whether it is farming, ranching, or the oil and gas sector, or any other sector in the United States, we need people who understand this and it needs to start earlier and earlier. I think a whole-of-Government approach is called for.

Again, I am going to reiterate in my last 45 seconds here that energy security is National security. Our country exports more than we import. We are dominant in the world. In countries that are buffered up against Russia—Latvia, Lithuania, Estonia, the Ukraine, Poland, and others—their leaders wake up every single day and they are trying to figure out how to deliver energy to their citizens. We in the United States are blessed with a bountiful source of energy. The winter storm in Texas is another example of just how fragile our infrastructure can be.

So as part of the Homeland Security Committee I think it is incumbent upon all of us to look at the cyber aspects of defense and to make sure that any other vulnerability is considered, that we can continue to provide affordable, reliable energy for the country.

With that, Mr. Chairman, thank you for this and I yield back.

Chairman THOMPSON. The gentleman yields back. The Chair recognizes the gentlelady from Florida, Mrs. Demings, for 5 minutes.

Mrs. DEMINGS. Well, thank you so much, Mr. Chairman, and thank you as well to our Ranking Member and also to our witnesses. Thank you for your testimony today. We certainly cannot get to the point where we need to without you and your participation.

You know, this hearing is extremely timely for a lot of reasons, but we have known for decades now that the new weapon of choice certainly for the criminal element is a cyber attack. I think the question is, what are we willing to do about it to certainly prevent further attacks in the future?

Mr. Blount, I want to thank you so much for your candor earlier as we were talking about, you know, the time line; the Chairman started out with that. I was particularly interested in the time line of notification and decision to pay the ransom. You very clearly said that, you know, you made that decision to pay the ransom and keep it confidential, you know, because of operational security concerns. So while we certainly appreciate that, I just want to make sure I understand.

In terms of you notified the FBI, which certainly I am glad you did that in a timely manner because you were a victim certainly of an attack, but I don't believe you consulted with the FBI before you made the decision to pay the ransom. If that is correct, since it is an investigation and certainly getting direction from law enforcement is so very important, if that is correct why didn't you make the decision to consult with the FBI, the lead investigatory agency, if you will, in a sense, before agreeing to pay the ransom?

Mr. BLOUNT. Representative, thank you so much for asking that particular question. That is true that I made the decision to pay the ransom. It is true that we called the FBI immediately on May 7 to report what we saw as an intrusion into our system. We have been extremely cooperative with the FBI throughout the process and including on Sunday, that Sunday, sharing with them information about the digital wallet.

As far as actually going to them and having a conversation about we are going to pay the ransom, it is very clearly if you go to their website, as you probably know, that they don't encourage that. So, unfortunately, the decision winds up on the part of the private industry player to make that decision, which, of course, I have taken

all of the accountability for doing that. But, again, extremely cooperative with them.

Then from an operational security standpoint we needed to keep the conversation with the perpetrator going in order to preserve that optionality of getting the de-encryption tool and anything else we might need in those early days before we even understood whether our back-up systems could be de-encrypted on our own and actually help us bring that pipeline back on by Wednesday, starting Wednesday of that following week.

Mrs. DEMINGS. Mr. Blount, thank you so much for that. You are absolutely correct, the FBI does not encourage that and there certainly is a reason for that. It, obviously, has turned out better than it could have, but still—I am still just trying to understand because I am thinking about, you know, one of the questions that was asked earlier is, you know, how are you working with other organizations, other corporations to make sure that they aren't attacked? You know, lessons learned from your attack. I am just a little curious about why you chose to not take the recommendation of the FBI in this particular case.

You ultimately made the decision anyway and I think you knew you could always do that. But why did you decide not to take the recommendation of the FBI in the first place in this particular attack?

Mr. BLOUNT. Thank you, again, for asking that question. The FBI never recommended that we not pay. We know that their guidelines suggest that they don't encourage you to pay. Again, when you are responsible for moving 100 million gallons of fuel into the market every day and suddenly that stops, and you consider the potential dire consequences that I prefer not to get into publicly of not bringing—able to bring that pipeline on as quickly and safely as we did, think about what we would look like if we had not brought that pipeline on until the following weekend. Right? We serve a lot of airports. Obviously, we serve a lot of critical services like ambulances and things like that with those fuels.

So, in those early hours of the morning, not knowing how quickly we could de-encrypt our own servers and things like that on our own, that was an option I had to avail myself of. Again, I——

Mrs. DEMINGS. Mr. Blount, thank you so much. Thank you so much for that. I just need to get this last question in and then you can answer.

You know, it has been said, and I am a former law enforcement officer, and I have heard it said and kind-of witnessed it, that the private sector is not the partners in terms of cooperating with investigations involving law enforcement in situations like this. What role would you say Colonial played in the attack that occurred? How do you learn from that moving forward? In other words, what could you have done better to prevent this attack?

Mr. BLOUNT. Again, thank you for that question, Congresswoman. I think that, you know, if you look in hindsight we responded extremely well to what happened to us. You know, we heard the word out of the DOJ this week that we were an innocent victim. We continue to invest in IT, in cyber, and have and taken that seriously because we do understand the importance of our

pipeline system when it comes to the American security and lifestyle and growth of the country. Right?

In hindsight, I am extremely pleased with the transparency we have exhibited as a corporation, but, of course, it is not a surprise to me because that is the way I am and that is the way this company has been. We are very straightforward. We are going to tell you what is going on. We are going to share information along the way and you have seen a lot of press releases by me in the last month. Not anything I really like to do, but I want to share the information as it becomes available, including, you know, the statement we made about the VPN and the issue that we had with the VPN. A lot of companies wouldn't have admitted to that. Right? They would have just moved on, especially private companies.

But, again, our role here is critical to the Nation and we are going to be very clear about what happened to us, so that it doesn't happen to someone else in the future.

Mrs. DEMINGS. Thank you, Mr. Blount. So, Chairman, I yield back. Thank you.

Chairman THOMPSON. Thank you very much. The Chair recognizes the Vice Chair of the full committee, the gentleman from New York, Mr. Torres.

Mr. TORRES. Thank you, Mr. Chair. My first question is directed toward Mr. Carmakal. How would you rate the cybersecurity preparedness of the pipeline sector? Give me a letter grade.

Mr. CARMAKAL. Congressman, again, sir, it is hard to make an assessment right now, but I would say, you know, there are certainly opportunities for improvement.

Mr. TORRES. Do you feel like it is satisfactory?

Mr. CARMAKAL. I do believe that [inaudible] for the security of the sector.

Mr. TORRES. Do you advise your clients to pay a ransom?

Mr. CARMAKAL. Look, Congressman, we don't tell our clients to pay or not to pay, but we do encourage them to have a very robust conversation about whether or not a payment should be made. We look at a number of different criteria, such as does the threat actor still have access to the environment? Could they potentially escalate their attacks? Have they stolen data from the organization? What is the actual impact to perhaps human lives or environmental conditions? Things like that.

So, we encourage our clients to have a robust conversation, but we don't tell them one way or the other. It is up to them to make the decision to do it.

Mr. TORRES. Mr. Blount, what was the overall cost of the ransomware attack? By cost I am referring not only to the ransomware cost of disrupted service, the loss of revenue——

Mr. BLOUNT. Representative, we haven't been focused on the cost of the incident. We have been focused on the remediation of what took place. We were very focused on bringing the pipeline back as quickly as we could to help support the economy of the United States. Cost doesn't play into this. It is the reaction, the containing the threat, remediating, and restoring the pipeline system. The cost will play out over the next couple of years.

Mr. TORRES. You have no cost estimate?

Mr. BLOUNT. Excuse me, I didn't hear that. There was some interference.

Mr. TORRES. You have no cost estimate at all?

Mr. BLOUNT. Hasn't been our focus, Representative, no, sir.

Mr. TORRES. The decision to shut down the pipeline, the decision to pay the ransom, was that your decision or was it made pursuant to a company policy?

Mr. BLOUNT. Representative, at Colonial we have what is called stop work authority. It exists in a lot of companies around the world, certainly pipeline companies. Any employee that sees a risk and a threat has the ability to shut down the pipeline system. That is what occurred that morning. A controller saw the threat come in the form of the ransomware, communicated it to his supervisor, and the supervisor made a call to shut the pipeline down. It was the absolute right move to make. If the OT system had been compromised you potentially had a foreign actor having access to critical infrastructure. Absolutely right decision to make.

Mr. TORRES. So, my question is, if your operational systems were compromised, what are the nightmare scenarios that keep you up at night?

Mr. BLOUNT. Representative, that is every operator's worst-case nightmare is having a third-party criminal element come into their system and take over their operation. We have seen that in some recent events, some waterworks that I heard, where they had the ability to change the chemical content of the water and things like that.

Mr. TORRES. I am asking in your opinion what is the nightmare scenario that keeps you up at night?

Mr. BLOUNT. Representative, I can't hear you. There is some glitch in the system.

Mr. TORRES. I am asking if your system had been compromised, your operational system, what would happen in the worst-case scenario that keeps you up at night?

Mr. BLOUNT. Representative, with all due respect, I don't think you want to play that out in the [inaudible] right now. Right? I think you could have some very dire consequences.

Mr. CLEAVER. Mr. Chairman? Mr. Chairman, I hate to interrupt, but at some point someone has to have a microphone on.

Chairman THOMPSON. Yes. I think they heard you and perhaps they muted themselves.

Mr. TORRES. Should I proceed or——

Chairman THOMPSON. Excuse me, Mr. Torres. Excuse me.

Mr. TORRES. Can I—OK, thank you. What sorts of issues should TSA consider with respect to [inaudible] you believe would help improve critical infrastructure [inaudible]?

Chairman THOMPSON. The gentleman—excuse me for just a minute. We are really having some interference and I am not certain exactly what it is. Let me try one more time, Mr. Torres. OK, it might have been the gentleman from New York.

Mr. Torres, we are going to let you try one more time.

Mr. TORRES. Can you hear me clearly or——

Chairman THOMPSON. Much clearer.

Mr. TORRES. OK. Mr. Blount, did Colonial make the ransom payment or did an insurance provider do so on your behalf?

Mr. BLOUNT. A third-party negotiator made that payment.

Mr. TORRES. My understanding is that a company can seek a tax deduction for a ransom payment. Does your company intend to seek a tax deduction for the ransom payment?

Mr. BLOUNT. Senator, great question. I have no idea about that. I am not aware of that at all.

Mr. TORRES. What sorts of issues should TSA consider addressing in follow-on requirements beyond the security directive? Are there specific statutory or regulatory reforms you believe would help prevent a shutdown of critical infrastructure from occurring in the future?

Mr. BLOUNT. Representative, I think anything any Governmental entity can do in the form of communication and what they have available and how they can collaborate with private industry, including critical infrastructure, would be extremely important.

Mr. TORRES. Mr. Chair, if I can ask one more question or——

Chairman THOMPSON. One more question. The gentleman is recognized.

Mr. TORRES. TSA's new security directive does require pipeline operators to assess their own compliance with TSA guidance and report back to TSA and CISA. However, it does not require pipeline operators to submit to inspections conducted by TSA itself. Would you support such a requirement? That will be my final question.

Mr. BLOUNT. Great question, Representative. We have cooperated with TSA in the past and there is no reason why we wouldn't cooperate with them now or in the future.

Chairman THOMPSON. The gentleman's time has expired. Let me thank the witnesses for their testimony today. There are 2 items I would like to make sure we get additional clarification on.

Mr. Blount, a number of Members have questioned how much the FBI actually knew about the ransom payment. Could you indicate whether or not they have any involvement with the company on advising them one way or the other on the payment?

Mr. BLOUNT. Mr. Chairman, I would be glad to clarify that. No, they were not involved in that decision nor were they consulted about that decision. As far as how much they knew, they are the FBI. They could have known a lot more than they learned from us, but we did not have those conversations.

Chairman THOMPSON. Well, no question about it. All right. Thank you very much.

Second, Mr. Carmakal said that you did not need the decryption tool to reopen the pipeline, but you said you paid the ransom so you could get the pipeline back on-line. So, which is it?

Mr. BLOUNT. Mr. Chairman, it is actually both. I would suggest that Mr. Carmakal chime in on this after I finish.

When you are there in the early hours of having your system and your servers and computers encrypted, you don't know what you have in front of you. You don't know how good your back-up systems are. What I have learned over the course of the last month is a lot of companies have back-up systems that don't help them at the end of the day.

So, again, not knowing what the answer to that was for days, whether we could use our back-up systems to restore the Colonial Pipeline system back to service or not, we had to avail ourselves

of any and every option that we had, one of which was the de-encryption tool. So, therefore, the ransom payment was made in order to get the tool.

The tool was then brought in-house; Mandiant had the tool. While Mandiant was also working with the tool, they were working with our back-up systems, which, in this case, allowed us to bring the pipeline system back on.

If our back-up systems had been corrupted and were never capable of being used, there was the potential that we would have to rebuild the entire system, which could have taken us a lot longer to bringing the pipeline back on before Wednesday of the following week. Again, critical, critical dire consequences could have come out of that.

So, again, I availed myself of an option that in hindsight we didn't necessary need, but we wouldn't have known it for days, which would have just delayed our ability to start the system back up and bring 100 million gallons of fuel back into our country.

Chairman THOMPSON. Thank you very much. Mr. Carmakal, is there anything you would like to add to that?

Mr. CARMAKAL. Mr. Chairman, I agree with Mr. Blount that, you know, in the early days there were a lot that was unknown. You know, Mr. Blount wanted to have any option available to recover and to be able to turn the pipeline back on. So, I do believe that there were a number of options and, you know, having those options available certainly helped with the more expedited recovery of the pipeline.

Chairman THOMPSON. Thank you very much. Let me thank the witnesses for their testimony and the Members for their questions.

Members of the committee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions. The Chair reminds Members that the committee record will remain open for 10 business days.

Without objection, the committee stands adjourned.

[Whereupon, at 2:36 p.m., the committee was adjourned.]

○