S. Hrg. 117–429

THREATS TO CRITICAL INFRASTRUCTURE: EXAMINING THE COLONIAL PIPELINE CYBERATTACK

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JUNE 8, 2021

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
46–569 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

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

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

David M. Weinberg, *Staff Director*
Zachary I. Schram, *Chief Counsel*
Christopher J. Mulkins, *Director of Homeland Security*
Jeffrey Rothblum, *Professional Staff Member*
Pamela Thiessen, *Minority Staff Director*
Andrew Dockham, *Minority Chief Counsel and Deputy Staff Director*
Cara Mumford, *Minority Professional Staff Member*
Patrick T. Warren, *Minority Investigative Counsel*
William H.W. McKenna, *Minority Chief Investigator*
Laura W. Kilbride, *Chief Clerk*
Thomas J. Spino, *Hearing Clerk*

CONTENTS

Page

Opening statements:

Senator Peters 1
Senator Portman 2
Senator Carper 12
Senator Johnson 14
Senator Hassan 17
Senator Lankford 19
Senator Rosen 22
Senator Hawley 24
Senator Ossoff 27

Prepared statements:

Senator Peters 33
Senator Portman 35

WITNESSES

TUESDAY, JUNE 8, 2021

Joseph Blount, President and Chief Executive Officer, Colonial Pipeline Company
Testimony 5
Prepared statement 38

APPENDIX

Responses to post-hearing questions for the Record:

Mr. Blount 43

THREATS TO CRITICAL INFRASTRUCTURE: EXAMINING THE COLONIAL PIPELINE CYBERATTACK

TUESDAY, JUNE 8, 2021

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

The Committee met, pursuant to notice, at 10:04 a.m., via Webex and in room SD–342, Dirksen Senate Office Building, Hon. Gary C. Peters, Chairman of the Committee, presiding.

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

OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. The Committee will come to order.

Mr. Blount, welcome to the Committee, and thank you for joining us for this important discussion on the harmful cyber attack against your company, Colonial Pipeline, and how we can work together to strengthen our coordination and response to this very serious cybersecurity incident.

When Colonial Pipeline was forced to shut down operations last month due to a ransomware attack, millions of Americans up and down the East Coast had their lives disrupted by gas shortages and price increases. In the weeks since your company was struck, we have seen a series of other attacks on everything from our transportation networks to meatpacking centers.

Just today we learned of additional intrusions into Internet platforms. Those private sector strikes follow especially damaging attacks on our Federal Government, including the extensive SolarWinds hack earlier this year.

While the objectives of these attacks differ, they all demonstrate that bad actors, whether criminal organizations or foreign governments, are always looking to exploit the weakest link, infiltrate networks, steal information, and disrupt American life.

Mr. Blount, I am glad your company continues to recover from this malicious attack and that the Federal Bureau of Investigation (FBI) was able to recover millions of dollars in ransom paid. But I am alarmed that this breach ever occurred in the first place and that communities from Texas to New York suffered as a result.

[1] The prepared statement of Senator Peters appear in the Appendix on page 33.

I appreciate that you have joined us today to provide answers to the Committee and the American people on how a group of criminals was able to infiltrate your networks, steal nearly 100 gigabytes (GB) of data in two hours, and then lock your systems with ransomware to demand payment. I am also looking forward to hearing an update on your progress to recover from this serious breach.

Private entities, especially those that are critical to our Nation's infrastructure, are responsible for assessing their individual risk and investing in the technology to prevent breaches and to ensure that they can continue to provide service to customers who rely on them for basic necessities like fuel.

At the same time, the Federal Government must develop a comprehensive, all-of-government approach to not only defend against cyber attacks, but punish foreign adversaries who continue to perpetrate them or harbor criminal organizations that target American systems.

This approach requires bolstering our defenses and using the full might of our diplomatic, military, and intelligence capabilities.

We must also ensure private entities like Colonial are providing the Federal Government with timely and relevant information in the event of a major incident. We need Federal agencies charged with cybersecurity like the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA)to understand the extent of these attacks and how best to support victims.

Make no mistake. If we do not step up our cybersecurity readiness, the consequences will be severe. The ransomware attack on Colonial Pipeline affected millions of Americans. The next time an incident like this happens, unfortunately, it could be even worse.

As Chairman of this Committee, I am committed to prioritizing policies that will help secure our critical infrastructure networks, including in the proposed infrastructure package Congress is now negotiating.

Protecting the American people from these sophisticated, harmful, and growing attacks will not be easy. We must learn from our past mistakes, find out what went wrong, and work together to tackle this enormous challenge. Inaction, however, is simply not an option.

With that, I will turn it over to Ranking Member Portman for your opening remarks.

OPENING STATEMENT OF SENATOR PORTMAN[1]

Senator PORTMAN. Thank you, Mr. Chairman. Mr. Blount, thank you for being here today. We are going to get into some tough questioning, and, unfortunately, what happened to your company is not an isolated incident.

We have had some good bipartisan work over the years to improve cybersecurity on this Committee with you, Senator Peters, with you, Senator Johnson, and others. Let us face it, there is a lot more to do. What happened with regard to Colonial Pipeline is one example. This is about ransomware attacks on critical infra-

[1] The prepared statement of Senator Portman appears in the Appendix on page 35.

structure, and that is the topic of the hearing broadly today. This paralyzes a company by locking its computer systems, holding its data and operations hostage until ransom paid.

Interestingly, these ransoms are not on the company itself, typically. Increasingly, the hackers also pursue a two-pronged ransom approach where they download and threaten to release sensitive victim data so individuals, say your customers, may also have been subject to ransomware.

There seems to be a new ransomware attack every week. We are going to hear today again about Colonial Pipeline and some of the details there, but no entity, public or private, is safe from these attacks. Last week, we learned that ransomware shut down the world's largest meat processor, JBS, including nine beef plants in the United States. Both the Colonial Pipeline attack and JBS attacks were attributed to a Russian criminal organization, by the way.

Just this morning, news broke that a constituent outreach services platform that nearly 60 offices in the U.S. Congress, the House of Representatives, uses was hit with a ransomware attack. As I have said before, no one is safe from these attacks, including us.

I hope that we will cover four specific areas here today. One is we have to understand that these attacks have real-world consequences. On May 7th, Colonial Pipeline learned they suffered a ransomware attack impacting their information technology (IT), systems by this Russian-based criminal group called "DarkSide." Recent news reports indicate that hackers accessed the Colonial system through a compromised password of a virtual private network (VPN) account. This account did not use multifactor authentication (MAF), which is a very basic cybersecurity best practice. We will talk more about that and why they did not. This easily allowed the hackers to gain access.

Colonial moved quickly to disconnect their operational system to prevent hackers from moving laterally and accessing those systems. That, of course, although an appropriate response to a cyber attack made Colonial's critical pipelines unusable, and that was a huge problem. So real-world consequences, 45 percent of the East Coast fuel was coming from Colonial. With operations shut down, people across the East Coast bought fuel in a panic, unsure how long the shortage would last. A lot of service stations ran out of fuel altogether, so people could not get gas, could not get to work. Of course, prices skyrocketed. Again, real-world consequences.

Second, I hope today we will talk about how this shows the difficult decision ransomware victims face. Should they pay the ransom or not? The U.S. Government has a position on this. Both CISA at the Department of Homeland Security and the FBI strongly recommend organizations do not pay ransoms. Why? Because paying ransoms rewards ransomware hackers. If no one paid ransoms, criminals would have little incentive to engage in ransomware attacks. Even if an entity pays, there is no guarantee that the hackers will give them the decryption key or not strike again, and we will talk more about that, too, in terms of this incident.

However, organizations obviously have to weigh these consequences against keeping the operations offline, in this case limiting 45 percent of the East Coast fuel supply. Colonial Pipeline paid DarkSide a ransom, we are told, of 75 bitcoins worth over $4 million at the time. Yesterday the good news is the Department of Justice (DOJ) announced the recovery of 63.7 of those bitcoins, but DOJ will not be able to recover those ransom payments in other cases. We will talk more about that and how they did it and what that means.

I appreciate Mr. Blount's transparency in acknowledging that his company paid the $4.4 million in ransom. I hope today we can explore the reasons for that decision.

Third, this attack demonstrates the gaps in information sharing between these impacted organizations and the Federal Government. Last month, Brandon Wales was before us in that very seat. He is the Acting Director of CISA. He testified in response to one of my questions that he did not think Colonial Pipeline would have contacted CISA at all if the FBI did not bring it to them. CISA's authorities allow the agency to engage on a voluntary basis when requested by an affected organization, and CISA has the Federal Government's best practices as to how to deal with these cyber attacks, and it was set up at the Department of Homeland Security for that purpose.

While I think that CISA being able to engage is the right approach, they must have relevant information to be able to share it among other critical infrastructure owners and operators who may be similarly targeted. We have to get them that information, and there is a gap now.

Finally, we have to recognize these ransomware attacks for what they are. It is a serious national security threat. Attacks against critical infrastructure are not just attacks on companies. They are attacks on our country itself. When DarkSide attacked Colonial Pipeline, it was not a company that was affected. Americans across the East Coast felt the squeeze at fuel pumps when Colonial shut off nearly 50 percent of the fuel supply.

The criminals conducting these attacks often operate with at least the tacit acceptance and approval of the foreign governments they operate out of. The U.S. Government needs to take stronger steps to hold these countries like Russia accountable. At the upcoming summit with President Putin and President Biden, one would hope that this is going to be at the top of the agenda.

Ransomware attacks will continue to plague U.S. companies and critical infrastructure. As the Committee of jurisdiction over both cybersecurity and critical infrastructure security, we need to reevaluate how we defend against ransomware and identify solutions to mitigate the consequences of these attacks.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Portman.

Mr. Blount, it is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses, so if you will stand and raise your right hand, please. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. BLOUNT. I do.

Chairman PETERS. Thank you. You may be seated.

Mr. Joseph Blount is the president and Chief Executive Officer (CEO) of Colonial Pipeline. He joined Colonial in October 2017 with more than three decades of experience in the energy industry. Mr. Blount previously served as CEO of Century Midstream LLC, a company which he co-founded. Mr. Blount has also spent 10 years with Unocal Corporation and ultimately served as president and chief operating officer (COO) of Unocal Midstream and Trade.

Mr. Blount, welcome to the Committee. We look forward to your testimony and appreciate your willingness to answer our questions. You are recognized for your seven-minute opening statement.

TESTIMONY OF JOSEPH BLOUNT,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, COLONIAL PIPELINE

Mr. BLOUNT. Chairman Peters, Ranking Member Portman, and Members of the Committee, my name is Joe Blount, and since 2017 I have served as the president and CEO of 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 the market. Our pipeline system spans over 5,500 miles and 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, diesel, jet fuel, and other refined products. Shipping that product safely and securely is what we do.

The product we transport accounts for nearly half the fuel consumed on the East Coast, providing energy for more than 50 million Americans. Americans rely on us to get 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 interests of our customers, shippers, and 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 ongoing, 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 that those defenses were compromised.

The attack forced us to make difficult 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 that we could get the pipeline back up and running safely. I am also very grateful for the immediate and sustained support of law enforcement and 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 have worked to quickly and safely restore our operations. I especially want to thank the

[1] The prepared statement of Mr. Blount appears in the Appendix on page 38.

Department of Justice and the FBI for their leadership and the progress they announced earlier this week.

I also want to express my gratitude to the employees at 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 two additional issues that I know are on your minds, and I am going to address them the only way I know how: 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 made in my 39 years in the energy industry, and I know how critical our pipeline is to the country, and I put the interests of the country first.

I kept the information closely held because we were concerned about operational safety and security, and we wanted to stay focused on getting the pipeline back up and running. I believe with all my heart it was the right choice to make, but I want to respect those who see this issue differently.

I also 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 where I want us to be. If our chief information officer (CIO) needs resources, she will get them.

We have also 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, in 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 look forward to our discussion today.

Chairman PETERS. Thank you, Mr. Blount.

Mr. Blount, Colonial is one of hundreds of victims of ransomware attacks against our Nation's critical infrastructure this year. Would you think and would you agree with the statement that the Federal Government should be doing more to help companies like yours prevent cyber attacks?

Mr. BLOUNT. Thank you for that question, Mr. Chairman. First, I would like to state that as a private entity we know we have a responsibility as well. We are accountable for our defenses and our reaction to attacks like this. But I think if we look at the number of incidents that are taking place today throughout the world, let alone here in America, private industry alone cannot do everything, cannot solve the problem totally by themselves. The partnership between private and government is very important to fight this ongoing onslaught of cyber attacks around the world.

Chairman PETERS. CISA is the main Federal domestic cybersecurity agency, and it hosts the Pipeline Sector Coordinating Council (SCC) to help bring together the private sector and government in that partnership, as you mentioned, to identify and address security issues. Do you know if Colonial ever participated in these meetings or any other exercise or events that were hosted by CISA?

Mr. BLOUNT. Thank you for that question, Mr. Chairman. I know that CISA is a good organization, and I know that we maintain a lot of communication and contact with CISA and have historically between our CIO and representatives from CISA. Actually, I was somewhat disappointed when I heard that they felt like if we had not gone in and contacted them the first day with the FBI that we would not have contacted them separately. If you go back and look at the record and look at who we contacted throughout the event, we talked to every entity that could possibly help us get through the condition that we found ourselves in that day.

Chairman PETERS. Do you know if you participated in any of those meetings?

Mr. BLOUNT. Yes, Senator, we participate in every governmental opportunity that we have to do tabletop exercise, security screens, and things like that.

Chairman PETERS. You mentioned that you did not contact CISA directly. Why did Colonial Pipeline decide to forgo contacting or notifying CISA directly? What was the rationale for that?

Mr. BLOUNT. Thank you, Mr. Chairman. We contacted the FBI almost immediately that morning once we determined that we were under attack. In that conversation with the FBI that morning, they frankly said, “We want to get on a phone call later today. We are going to bring CISA into the conversation.” At that point we already knew the contact would be made there. We had a lot of governmental entities to respond to that day and call directly, and that was the most efficient means. We knew they would be in that meeting, and they were indeed in that meeting right after noon the day of the 7th.

Chairman PETERS. As you mentioned in your opening comments and you have reiterated here in answers to these questions, you have been working closely with the FBI, and I know you allowed Mandiant, the private security firm, which you also referenced in your opening, to share information with CISA, and that is happening now.

Given those actions, I would suspect that you agree that you have a responsibility to protect other potential victims based on what you have learned. To what extent do you believe that responsibility extends?

Mr. BLOUNT. Thank you for that question, Mr. Chairman. We have been very transparent from the start. If you looked at who we contacted that day, we started with the FBI. Obviously, they included in the follow-up conversation. Then we started marching through all the ones that we normally would report to, whether it is the Federal Energy Regulatory Commission (FERC), Pipeline and Hazardous Materials Safety Administration (PHMSA), Department of Energy (DOE), et cetera, et cetera. What we found during that day was that we were allowed the conduit through DOE to talk to all these organizations on an ongoing basis, but through one central briefing.

We found that the ability to have that conduit, to work on the supply side of the equation, and on the restoration side of the equation, with any number of governmental entities was extremely helpful to us. Then, of course, on the investigative side, we had the FBI and CISA working on that.

For anybody that comes under an attack like this, what you cannot re-create is time and space and the ability to respond. The ability to have the conduit both on the investigative side as well as on the restoration and on the supply side was extremely helpful to Colonial Pipeline and our employees. It was an all-hands-on-deck situation that morning and throughout the event.

Chairman PETERS. Prior to the attack, I know you are not a technical expert, but it would have been helpful for you to get information about other potential attacks or other companies that may have been attacked with similar types of cyber incidents?

Mr. BLOUNT. Yes, Mr. Chairman. For example, we gave a lot of indications of compromise to the FBI and CISA during the days of the event, and I think what we saw as an industry is immediately that material was dispersed out, and in the case of the internet protocol (IP) addresses, I believe CISA actually posted those. And that was a means for us once again to efficiently communicate to our industry partners what was going on. In addition to that, go back to the first day when we were contacting people, we made initial contact with some of our industry trade groups to tell them what we could possibly tell them at that point in time. So we have been, once again, very open and transparent, hoping that everybody could not only be aware of the situation, but think about what they could do to help prevent that from occurring in their own company.

Chairman PETERS. That is all very encouraging to hear, and for the record, I am working on legislation right now to make sure that information is indeed being shared with CISA to get a better understanding of what is happening in ransomware, not just with your company but across the board.

Reporting indicates and you have affirmed today that you made the decision to pay the ransom of $4.4 million. We are certainly happy to see that a portion of that is being recovered by the Department of Justice now. My question to you, though, is: Prior to making the decision to pay the ransom, had you consulted with anyone in the Federal Government on whether that would be an appropriate response?

Mr. BLOUNT. Thank you for that question, Mr. Chairman. It was our understanding that the decision was solely ours as a private company to make the decision about whether to pay or not to pay. Considering the consequences of potentially not bringing the pipeline back on as quickly as I possibly could, I chose the option to make the ransom payment in order to get all the tools necessary and the optionality of those tools to bring the pipeline on as quick as we possibly could, safely as well as securely.

Chairman PETERS. After you paid the ransom and received the key to unlock your systems, did that actually fix all of the problems? Where are you today? How long do you think it will take for you to be 100 percent?

Mr. BLOUNT. That is a great question, Mr. Chairman. Thank you for asking it. I think what a lot of people do not realize about cyber attacks and the repercussions of a cyber attack is it takes months and months and months, and in some cases, what we have heard from other companies that have been impacted, years to restore your systems. Our focus that first week was to restore the critical systems that we needed on the IT side in order to safely and securely bring our pipeline system back up. So that is what we focused on.

An example would be this week we are bringing back online seven finance systems that we have not had since the morning of May 7th. Again, the remediation is ongoing, and, again, that is why you bring someone like a Mandiant in immediately, one, to help investigate the situation, but also to help restore what you have lost throughout the process.

The keys are helpful, and we have used the keys, so they have been advantageous to us. But they are not perfect.

Chairman PETERS. I think that is important to remember. You get the keys, but you still have a problem for many months and a lot of work to do.

Mr. BLOUNT. Yes, sir, that is correct.

Chairman PETERS. It really illustrates the seriousness of what we are dealing with. Thank you for your answers.

Ranking Member Portman, you are recognized for your questions.

Senator PORTMAN. Thank you, Mr. Chairman.

Mr. Blount, you are a victim, and we understand that. And yet we are trying to provide oversight and even provide some new laws potentially to try to deal with this increasing and really dramatic issue of cyber attacks, and specifically today talking about ransomware. Let us clarify the record. You made your ransomware payment to the hackers on the day you discovered it. Is that correct?

Mr. BLOUNT. Ranking Member, thank you for that question. We did not. We made the decision that evening to negotiate with——

Senator PORTMAN. So that was the evening of May 7th?

Mr. BLOUNT. Yes, sir.

Senator PORTMAN. And so you did not make the payment until when?

Mr. BLOUNT. The payment was made the following day.

Senator PORTMAN. May 8th.

Mr. BLOUNT. Yes, sir.

Senator PORTMAN. And you indicated today that the FBI was in discussions with you on May 7th. Is that correct?

Mr. BLOUNT. Ranking Member Portman, that is correct. Yes, sir.

Senator PORTMAN. What did the FBI tell you? What did they advise you to do with regard to paying the ransom?

Mr. BLOUNT. Ranking Member Portman, I was not involved in those conversations with the FBI, but in discussions with my team, I do not believe the discussion about the ransom actually took place the first day, on May 7th. The focus more was on getting to the proper centers of expertise with the FBI. In this case, I believe it was the San Francisco office. We started with the Atlanta office in our notification. And then it was a function of starting—they already started to collect data from us, indications of compromise and——

Senator PORTMAN. So their official position is you should not pay ransoms, and yet they did not communicate that to you as far as you know?

Mr. BLOUNT. Ranking Member Portman, of course, I was not in that conversation. I cannot confirm or deny that. But I do agree that their position is they do not encourage the payment of ransom. It is a company decision to make.

Senator PORTMAN. Yes, and so you knew what their advice was going to be even if they did not provide it that day?

Mr. BLOUNT. Ranking Member Portman, yes, sir, we did.

Senator PORTMAN. OK. Did you talk to the Treasury Department's Office of Foreign Assets Control (OFAC)? This is the office that is charged with sanctions, and so if you are a sanctioned individual and you make a payment, as you know, there are potential violations of law. Did you contact Treasury Department's Office of Foreign Assets Control?

Mr. BLOUNT. Ranking Member Portman, the day that we decided to negotiate, we hired experts both on the legal side as well as on the negotiation side. We did not have any direct contact with DarkSide ourselves. I can assure you that everyone involved in that process continually went and fact-checked to make sure that this was not an OFAC-listed entity.

Senator PORTMAN. So you were in touch with OFAC to ensure you were not paying the ransom to a sanctioned entity or to a sanctioned individual?

Mr. BLOUNT. Ranking Member Portman, I was not involved in those conversations, and so I cannot attest to who actually talked to who. But I do know that repeatedly throughout the process the fact of whether DarkSide was on the sanctions list or not was fact-checked repeatedly.

Senator PORTMAN. OK. We may have some follow-up questions on that just to figure out what the relationship was there. Again, this is about looking forward, how do we avoid this situation where sanctioned individuals or entities are getting a ransom payment, which would be a violation of Federal law.

The Wall Street Journal says that the decryption tool did not really work, so you paid the ransom, they give you the decryption tool to be able to undo the harm that they did. That is how it normally works. And yet the decryption tool was not effective. Is that correct?

Mr. BLOUNT. Ranking Member Portman, the encryption tool is an option that is made available to you, and when you are looking at bringing critical structure back up as quickly as you possibly can, you want to make every option available to you that you can. Mandiant can be the best one to answer about how important the encryption tool was restoring the critical options we needed within the first couple days.

Senator PORTMAN. Did the decryption tool work?

Mr. BLOUNT. It has worked, yes, sir.

Senator PORTMAN. The Wall Street Journal story was inaccurate, it was effective?

Mr. BLOUNT. Ranking Member Portman, I think that article came out pretty early on, so I would say that we know subsequently that the de-encryption tool actually does work to some degree. As I stated earlier, it is not a perfect tool.

Senator PORTMAN. OK. It was provided to you by the hackers, correct?

Mr. BLOUNT. Ranking Member Portman, yes, sir, that is correct.

Senator PORTMAN. OK. There are also news reports about how this happened. As I said in my opening statement, there was a compromised password of a virtual private network account. This account apparently did not use multifactor authentication, which, again, is kind of a basic cybersecurity hygiene item that, companies should have in place, making it harder for people to gain access. Prior to the attack, did your company require all employees to use multifactor authentication?

Mr. BLOUNT. Ranking Member Portman, in the case of this particular legacy VPN, it did only have single-factor authentication. It was a complicated password, so I want to be clear on that. It was not a "Colonial 123" type password. The investigation is ongoing by Mandiant to try to determine how that material was compromised. But in our normal operation, we use an RSA token allowance in order to create authentication difficulties for remote access.

Senator PORTMAN. Would your advice going forward be that multifactor authentication ought to be used?

Mr. BLOUNT. Ranking Member Portman, that is absolutely the correct advice.

Senator PORTMAN. The Transportation Security Administration (TSA) has given the industry a lot of leeway. Critical infrastructure and voluntary compliance has been the approach. They came out late last month, after your attack, with some new directives, and now there is a mandate that reporting cyber attacks must happen; they must go to CISA, which is, again, this group within the Department of Homeland Security, and then it will be shared with TSA. You have a designated cybersecurity coordinator within the company, and you have to review your current activities against their recommendations on cyber risks, identify gaps, and develop remediation measures. Do you support that?

Mr. BLOUNT. Ranking Member Portman, if you look at our actions starting on May 7th, we almost to the "T" duplicated what the new standards are, and we are in full compliance today as well.

Senator PORTMAN. I had mentioned earlier that, we have written legislation in this Committee over the years to try to deal with cybersecurity. Pretty much every member here today has been involved with that. As I said earlier, we obviously need to do more. The question is: With regard to critical infrastructure in particular, should there be more mandates? And now there is, and they have the authority to do this under a 2007 law, it appears. Now there is this mandate on reporting it, a mandate on having a coordinator. But, still, there is not a mandate saying that you have to do certain things in terms of best practices or good cyber hygiene. Do you think there should be additional requirements from TSA with regard to critical infrastructure?

Mr. BLOUNT. Ranking Member Portman, first I would like to thank you for your leadership on these issues in the past, but certainly on a go-forward basis, I think anything that can help industry have better security practices, standards to follow, would be extremely helpful, especially for the smaller companies that are in other industries as well as my industry, less sophisticated.

Senator PORTMAN. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Portman.

Senator Carper, you are recognized for your questions.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman.

Mr. Blount, thank you very much for joining us. The fact that you and your employees, your company, and those who have been certainly consumers that have been harmed by this, but we regret that. But if you had the opportunity to speak to other people, your counterparts in businesses around the country, maybe give them two or three words of advice to help them with this sort of thing, what would you say?

Mr. BLOUNT. Senator, that is a great question, and if I could boil it down to two or three words of advice, as you suggested, I would suggest that we certainly take a look at our defenses, and even though we felt comfortably historically that we are where we felt we needed to be to protect our assets, this threat grows every day. The sophistication of this threat grows every day. So let us make sure that we are keeping our eye on that.

And then the other side of the equation is if you wind up in a situation like we found ourselves on May 7th, have an emergency response process that allows you to respond quickly and, most importantly, to be extremely transparent and to contact the authorities who indeed do have resources that potentially could help you through a very difficult process.

Senator CARPER. Thank you. Abraham Lincoln was once asked, “What is the role of government?” And he responded, “The role of government is to do for the people what they cannot do for themselves.” With respect to one of the things—I have been on this Committee for about 20 years, and we have spent a lot of time trying to figure out what is the role of government, especially with respect to cybersecurity, but my question is: What do you believe the appropriate role for government is, should be, should have been? How do we measure up? What did we do well or what could we have done better?

Mr. BLOUNT. Senator, thank you for that question. Obviously, with the threat that we have in this country and around the world today, I think the private-public partnership is extremely important. We can do things as private industry to protect our facilities and assets and be safe cybersecurity-wise. But there are things around the world that we obviously have no ability to participate, and that is pressure on foreign governments that harbor criminals and people like this, and that is where government comes into play.

As a company that has been regulated for over 57 years, regulation is not foreign to us, and we think regulation can be healthy.

And so we support anything that helps further protect these critical assets that we all rely upon for our daily life.

Senator CARPER. As I am sure you know, there are numerous government agencies that are involved in trying to secure critical infrastructure, all kinds of infrastructure, specifically pipelines. The Transportation Security Administration is in charge of Federal programs for pipeline security, but most people think of TSA as they are going to the airport, going through airport security, but they do a lot of other things, for the most part doing them, I think, very well. But the TSA works closely with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration as well as folks at the Department of Energy and the Federal Energy Regulatory Commission. That is just a handful of government agencies that are working to secure our Nation's pipelines, and that type of coordination among agencies requires continued collaboration and communication.

I have a two-part question for you, if I could. First, how frequently are you or your counterparts, your team members, how frequently are you in contact with these government agencies I mentioned above? Second, how has interagency coordination among these agencies strengthened or weakened pipeline security?

Mr. BLOUNT. Thank you for that question, Senator. We are in contact quite often with all the agencies that you mentioned. Again, as I noted, we are a regulated entity, and we know it is important to communicate what is going on across our pipeline system and with our operations, with all our governmental partners. And then there are a lot of entities within the government that do not regulate us, like CISA, up to May 7th, that we also have had constant communications going on.

I know from my CIO's perspective, she does spend a lot of time with CISA, she does spend a lot of time with the TSA talking about what is going on in cyberspace and defenses and things like that. I will go back to May 7th, and what I saw as being most helpful for an operator that has been, subject to an attack is, again, that was critical for us to be able to have that one central conduit in the government, and in this case it was DOE, who allowed us to communicate everything that was going on at the time through one central conduit, although all the parties that you mentioned were sitting at that table—virtually, of course, because of Coronavirus Disease (COVID)—hearing material real time that could help them go about doing their job or potentially could go about helping the market resolve the issue that we saw. So we saw a lot of permitting changes allowing truck drivers to drive longer hours or allowing trucks to carry more fuel. That was the kind of coordination that we go through that central conduit that the White House gave us.

Again, I am not saying one entity over the other. I am saying that the combination of all of them through that central conduit was extremely valuable to our response, extremely valuable to the American public to get as much fuel back into the system as we possibly could, and whether that is through deviations in regulations or things that allowed us to bring our pipeline on much sooner than perhaps it would have been.

Senator CARPER. Good. Maybe one other question. How quickly did your company reach out to the FBI?

Mr. BLOUNT. Senator, great question. We reached out to the FBI within hours.

Senator CARPER. What was the response?

Mr. BLOUNT. The response, Senator, was, "We want to get you back on a phone call. We are going to bring CISA into the conversation, and we are going to start going through it." I think part of that was we called the Atlanta office, and in this particular case, they felt it was DarkSide, and the FBI has an office specifically dedicated—they call it a "Center of Excellence"—for DarkSide, so their DarkSide experts, which are California based.

Again, as early as we called in the morning—I mean, I know the FBI probably responds regardless of the hour of the day. It was pretty early in California when we made our call to the Atlanta office. But great response on the part of the FBI.

Senator CARPER. Good. How about the response from CISA? That will be my last question. How about the response from CISA?

Mr. BLOUNT. Senator, of course, I was not involved in those conversations, but what I saw as a result of CISA being involved in those conversations was the ability to take some of the forensic evidence that the FBI was comfortable seeing released to the public wind up in CISA notifications that would then help like companies and certainly a lot of pipeline companies take a look at IPS addresses and things like that that we had shared during that phone call and get that out in memo form to other operators. So great sharing of information on the part of CISA.

Senator CARPER. Good. Thanks very much for joining us. Good luck.

Mr. BLOUNT. Thank you, sir.

Chairman PETERS. Thank you, Senator Carper.

Senator Johnson, you are recognized for your questions.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman.

I want to start out by again emphasizing and pointing out that you were the victim of a crime. You are not the bad guy here, and I appreciate my colleagues pretty well acknowledged that as well. I think that has been reflected in the line of questioning.

I want to, because a lot of people do Monday morning quarterbacking and it is easy for Federal agencies to say, "No, do not pay ransoms because it just encourages more." But I just kind of want you to for the record lay out how much worse could it have been had you not made that very difficult decision to kind of bite the bullet so that you could get your pipelines back up and operational?

Mr. BLOUNT. Senator, first, thank you for your kind words, and thank you for your question as well. That is an unknown we probably do not want to know, and it may be an unknown that we do not want to play out in a public forum. But if you start to look at the fact that it took us from Friday all the way to Wednesday afternoon the following, and we already started to see pandemonium going on in the markets, people doing unsafe things, like filling garbage bags full of gasoline or people fist-fighting in line at the fuel pump. The second would be what would happen if it had stretched on beyond that amount of time, right? What would happen at the airports where we supply a lot of jet fuel, let alone what might happen at the gas pump?

My concern the first day was more to the first responders and the ambulances and the things that we count on in emergencies beyond our own current energy. That was my concern that first day. Again, our focus and our team's focus, regardless of what type of threat we see, is to identify the threat, contain the threat, remediate, and restore. And that goes beyond just an incident like that. That is about anything that we see is unsafe, and that is why the call that morning by that controller, the supervisor of the control room, to shut the pipeline down was so critical.

Senator JOHNSON. I think that is an appropriate response, and I will leave it to people's imagination, but I want people thinking about that as well.

Mr. BLOUNT. Yes, sir.

Senator JOHNSON. Cyberattacks are an ongoing problem. There is no easy solution. As you say in your testimony, the criminals are on the offense, and they have a huge advantage. And it does not take much in terms of vulnerability—no matter how strong your IT systems are, your cybersecurity systems are, there are vulnerabilities, and they get exploited, and they are becoming more and more susceptible to this.

In terms of government versus private sector, from my standpoint I think CISA is very valuable from the standpoint of sharing information preemptively, trying to stop some of these things. We have heard in testimony that 90 percent of these attacks can be prevented just by basic cyber hygiene. It certainly sounds like you had pretty sophisticated cyber hygiene, although obviously vulnerabilities.

The Federal Government can hold nation-states accountable that are allowing these cyber attackers to operate on their foreign soil and then, of course, hold them accountable when something happens, but also help in recovery and law enforcement.

I am not convinced that the Federal Government is going to be particularly effective at issuing standards and keeping them up-to-date. I really look to the private sector being far more nimble at that.

One of the processes I proposed is using a private sector model like an International Organization for Standardization (ISO) certification. I imagine you go through something like that. I did. You have six-month surveillance audits. You tie that to the insurance system as well where your rates are based on how good you achieve the standards. That is a system that will be as nimble as the private sector can be, as up-to-date, be able to employ the absolute best cybersecurity experts, which is one of the problems with the government. I am not—again, it is just a problem. Government cannot pay to retain the absolute best talent across the board.

I just kind of want your thoughts on that type of framework, public versus private.

Mr. BLOUNT. Senator, thank you, and I think those are all very good thoughts. I think, again, we have an obligation as a private entity to make sure that our systems are as capable as they possibly can be, and we have a responsibility to continue to look at those systems because, as we all know, the threat continues to evolve. The sophistication of the players continues to evolve. Their ability to compromise systems continually evolves. I think in combination with the government, together combined we have a much better ability as Americans to thwart the threat of cyber attacks, and I think that, again, we both have a responsibility. You shared the concept of private industry cannot do things to foreign governments, cannot put pressure on foreign governments. That is extremely important here if we look at where these criminals are housed, right? Something needs to be done there.

Again, I think that private-public partnership is very valuable, but we certainly know we have responsibilities and accountability as well.

Senator JOHNSON. Again, I am concerned about the government's, A, capability of establishing the standards, then, again, penalizing businesses for being victims of crime, if you do not meet their probably in many cases out-of-date standards. I would proceed down that line with caution.

Just real quick, were you a member of an Information Sharing and Analysis Center (ISAC), for your industry?

Mr. BLOUNT. Senator, I do not actually know the answer to that. If I can get back to you on——

Senator JOHNSON. OK. I would appreciate it.

Then the final question I have is: In our briefing and news reports, it was not just the shutdown, the ransomware. But prior to them shutting you down, they extracted all kinds of data that apparently they tend to reveal or not reveal. Can you describe that if possible? Because I am—"intrigued" is maybe the wrong word, but I thought that was quite interesting. Do you have any assurances—did you get that data back? Was that part of the ransom deal that that will not be disclosed? And can you tell us what kind of data they are talking about, why that would even be valuable for them or hurtful for that to be disclosed?

Mr. BLOUNT. Senator, very important question. As part of the ransomware note, they tell you that they have encrypted information, that they have exfiltrated information, so we knew that they had exfiltrated information. We worked very closely with the FBI on that, and the FBI is probably the best entity to respond to that since they are still, investigating the situation and getting closer, apparently, at least we hope, to the perpetrators themselves.

Senator JOHNSON. Would that be personal information from your employees that would be valuable or just trade secrets? I mean, you are a public company so the financial information is available. I am just kind of wondering what threat that represents to your entity or to your employees?

Mr. BLOUNT. Senator, what we know about that material right now is it was exfiltrated off the share drive, so it contains a lot of different type of material. The good news is it was retrieved very quickly. It was brought back in. Again, I think the FBI can talk a little bit more about that than I feel comfortable right now because of their investigation.

Senator JOHNSON. OK.

Mr. BLOUNT. But, again, the fact that it was retrieved very quickly is helpful. We do not fully understand everything that is in it because of where it has been held since it was retrieved. But we have people obviously involved in the combined process who have been looking very closely at that data.

Senator JOHNSON. OK. Listen, I appreciate you coming in here and being as forthright as you have become, so thank you.

Mr. BLOUNT. Thank you, Senator.

Chairman PETERS. Thank you, Senator Johnson.

Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Chair Peters, and thank you, Ranking Member Portman, for this hearing today. Thank you, Mr. Blount, for being willing to come before the Committee today.

Cybersecurity is a collaborative effort, to be sure, and we need to work together to strengthen public and private cyber defenses.

Mr. Blount, I was glad to see that U.S. authorities were able to deprive hackers of millions of dollars in expected ransom. However, I want to better understand your decision to pay the ransom, and I understand it was a difficult decision.

As you have already discussed, the FBI and other Federal agencies strongly discourage paying ransom because it incentivizes more people to become cyber criminals and to develop better ransomware tools.

When you decided to pay the ransom, did you know how much of your network was affected at the time?

Mr. BLOUNT. Thank you for that question and good morning again.

Senator HASSAN. Good morning.

Mr. BLOUNT. No, we did not, and I think that is what a lot of people do not understand in these incidents, these attacks. It takes you days, basically, to see into your system that has been corrupted as to what you have, what has potentially been exfiltrated. In the case of Colonial, we had really good backups, is what I have been told by Mandiant. But it still took them days to get through those backups. When we look at our response time and ability to bring the system back up, it was fairly good in reality. My concern was you do not have that view at all for days, and when you have a critical asset like this, you have to focus on what is the best opportunity of options you have in front of you to take avail of, and in that case it was to get the encryption tool and to get our information back.

Senator HASSAN. OK. I wanted to follow up. You mentioned the Federal agencies that you reached out to, but what, if any, outside of those agencies, non-Federal entities did you consult with? Were there private firms that you consulted with?

Mr. BLOUNT. Yes, Senator, great question. Obviously, we talked to Mandiant.

Senator HASSAN. Yes.

Mr. BLOUNT. We talked to Mandiant about that. We talked to our legal resources that have been involved in any number of cyber cases in the United States over the last couple years, people that have had real-time experience with these criminals as well as the specific science of cyber attacks and compromise. So, yes, a lot of conversation went into that decision that I made to negotiate.

Senator HASSAN. OK. Did you have a cybersecurity response plan in place prior to the attack? If so, did it include any guidance about paying a ransom?

Mr. BLOUNT. Senator, great question. What we have as a pipeline operator—and it would not be unique necessarily to us at Colonial—is we have an emergency response process.

Senator HASSAN. Right.

Mr. BLOUNT. Again, I said earlier this morning, see the threat, contain the threat, remediate the threat, and restore. So in this case, you use the same process, but you use a different set of experts. So in this case, we reached out immediately to the FBI because it was criminal.

Senator HASSAN. Right.

Mr. BLOUNT. We immediately reached out to legal resources that have dealt with this. We immediately reached out to Mandiant.

Senator HASSAN. Right, but my question is: In your planning, did you have a plan for cybersecurity response that included guidance about ransomware?

Mr. BLOUNT. Senator, specifically no discussion about ransom and action to ransom.

Senator HASSAN. Did your team do tabletop drills, for instance, to go through an actual simulated cyber attack before this happened?

Mr. BLOUNT. Senator, yes, we do participate in those with various groups, as well as do them on our own at Colonial.

Senator HASSAN. OK. Some private sector companies can focus strictly on economics and perform traditional cost-benefit analyses without having to consider national security concerns. However, owners and operators of critical infrastructure—and I appreciate your comments this morning acknowledging that Colonial oversees critical infrastructure. That carries a heightened obligation and duty to be capable of delivering goods and services to citizens in this case all up and down the East Coast.

Mr. Blount, Colonial Pipeline surely performed some number of cost-benefit analyses regarding the operation of its pipeline to determine how much to spend on pipeline hardware, personnel, and even cybersecurity. Did any of your analyses incorporate any public responsibility factors, such as the impact of a potential cyber attack on consumers or on the U.S. economy?

Mr. BLOUNT. Senator, that is a great question. I would not say that we approached it that way. We know our No. 1 goal at Colonial is to safely and securely operate that pipeline, because we have known for 57 years the importance of that pipeline to the well-being of the American citizen. So that has always been our focus. Our investment, whether it is in pipeline integrity or whether it is in cyberware and IT, is all derived around keeping safe and protecting the asset because of what its main benefit is to the United States.

Senator HASSAN. OK. I understand that, and I appreciate that answer. But, as you have had conversations with other Senators this morning, you have mentioned that you did not have two-step authentication in place. You have mentioned a legacy VPN which, in my understanding, means it was a pretty old VPN. I do not think it is acceptable to understand the critical nature of your product, but then not really have the preparation and the system in place to protect it as if it is critical infrastructure. You really do have an obligation to U.S. communities that you serve and to consumers and to our national security, so I am concerned that it does not seem to have been a formal factor in your analysis of how much to strengthen your systems.

Mr. BLOUNT. Senator, we take cybersecurity very seriously. I did reference earlier that the VPN was a legacy VPN——

Senator HASSAN. Yes.

Mr. BLOUNT [continuing]. That we could not see and it did not show up in any pen testing, that is unfortunate. But, again, the safety and the security of the system is highly critical. We have never had our board deny us any funds associated with safety and security, whether it is on the IT side or the physical side of the pipe. If my CIO wants funds, she gets them.

Senator HASSAN. OK. I would just—and this is an issue that I think we are seeing across the board on cyber. We need to start imagining what can happen and respond accordingly as opposed to always be looking at what the last problem was and really investing, and for critical infrastructure, I think it is absolutely important that we have standards that really make sure that companies are investing in the kind of infrastructure they need.

I have another question. I am running out of time, so I will submit it for the record.[1] But I really would like to get your thoughts about what kind of public-private information sharing needs to happen, between and among whom, and at what level, because I think that is another important piece to this whole issue.

Thank you very much for being here this morning.

Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hassan, for your questions.

The Chair recognizes Senator Lankford for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman.

Mr. Blount, thanks for being here. There is no CEO in America that wants to be sitting in the same chair you are sitting in right now, to be able to go through all this. You are a month past a major attack. Obviously, there is a lot of work that you are going through.

Can I back up for Colonial? When is the last time that the Colonial Pipeline was down and not providing fuel to the East Coast?

Mr. BLOUNT. Senator, that is a great question. That pipeline has never been down completely with the exception of—and I learned that just this week—over the couple hours of Y2K, and we can all appreciate going back in time that we were all concerned about the clock back then. Periodically from time to time we will have a portion of the system down during a hurricane event or something like that, but never the entire system at one time, and never for, obviously, that duration of time.

Senator LANKFORD. I think we as Americans get so used to going to the gas pump and filling up with refined products. Every one of

[1] The question of Senator Hassan appears in the Appendix on page 43.

us has landed at Charlotte airport and Jet A has been added to our plane as we change planes there. We get so used to that, we lost track of some of these things.

I want to ask a couple of things here. You had to do a physical inspection and a cyber inspection of this pipeline or just going through the digital portion of it, or physical inspection as well?

Mr. BLOUNT. Great question. So in the early hours of May 7th, we did not know exactly what we had. We had the ransomware. But, again, we are always concerned about the security of the pipeline, and you may have read in the press—and it is a factual statement. We drove over 29,000 miles of the pipeline, and, again, remember it is only a 5,500-mile pipeline. So we had constant ground surveillance. In addition, we also fly the pipeline—it is a PHMSA regulation that we fly the pipeline. We fly in excess of that regulation on a normal basis, and on top of that even doubled up our efforts during this point in time. Again, we did not know that it was just a cyber attack. We had to make sure that it was not potentially an attack on our physical structure as well.

Senator LANKFORD. So that was completed? There was no other physical damage that you could identify?

Mr. BLOUNT. That is correct, Senator. We did not see anything. We did keep an eye, obviously, on the pipeline. Just so you are aware, we kept the pipeline under pressure, and that would allow us to bring the pipeline up much quicker. So we had people manually in the field looking at gauges, the old-school way of watching pipeline pressures, to make sure that we were in compliance with all the regulations, regardless of the attack and what happened in the shutdown.

Senator LANKFORD. I said to several people that I have talked to in the last month, when we saw suddenly gas lines appearing and a pipeline go down at this point, that everyone learned the importance of pipelines. If I rewind two months before that, all the conversation was about, slowing down permitting new pipelines, maybe we are not going to do pipelines at all, make it harder to be able to do maintenance on Federal lands on pipelines. Two months ago, the conversation was, well, maybe we need fewer pipelines, and maybe we need to make this harder to be able to develop new pipelines—obviously, Keystone Pipeline was in the news—to say we are just not going to do that at all. And so products coming out of Canada and out of Montana are just going to have to find trucks and trains to be able to get there.

I am not going to ask you this same question because that is not going to be fair to you, but I have told a lot of folks what we watched happen with a sudden shutdown of a pipeline is the ghost of Christmas Future for the entire country if we do not continue to maintain our pipelines, increase capacity of pipelines, if we do not continue to expand and have duplication of pipelines in spots, to be able to make sure we have redundancy for this. Pipelines are essential to America. The 2.5 million miles of pipelines that we have scattered around the country, we lost track of how incredibly important they are.

I am grateful that your company has had such a good reputation. This is terrible to be a victim of a ransomware attack. There is something that you have that every CEO in America would like to hear, and that is, what are the lessons learned on cyber issues that you have already identified, obviously your team has taken on? The No. 1 has already come out, looking for legacy entries into your system that do not have two-factor authentication on it. What else has been identified that you need to be able to take and pass on to others?

Mr. BLOUNT. Thank you for your question. Again, I think the most important thing is to not be complacent about what you have because of the pace of change on the outside, from the criminal side. And then secondary to that, but equally as important, is the ability to have an emergency response process in place. If we had not been trained for the last 57 years to respond to any threat, whatever that threat is—it is an extension cord on the ground that has not been taped down that someone might trip over and hurt themselves—if we had not been trained like that and our employees had not been trained like that, who knows how many days it potentially could have taken to bring the asset back online? We know the importance of the asset. We are dedicated to the American public as a result of all the training and everything that we have done through the years to make sure that we have the fuel that we need.

Senator LANKFORD. Backing up systems, clearing unused accountable, guarding data in other ways. Are there other things that you would mention to say these are lessons that are going to be important for the future? Obviously, there was a gap, a single area, a single vulnerability. Other lessons you would mention?

Mr. BLOUNT. Thank you, Senator. I think from a proactive standpoint, you have seen now where we brought Mandiant in to investigate as well as to restore and start to harden our systems. But we have talked a lot about standards in this room today, and so we have also brought Dragos in and Black Hills in, and people may ask why, is that overkill? I would say I do not think so because what we want to make sure is we get the best out of each one of those experts. They all have a specific skill. Dragos is very good at operational technology (OT) systems. We want to make sure that we have the best hardening and the best segmentation we can possibly have on our OT side.

So I think, again, it is that investment in resources to get the best in class, because, again, even the best in class is still susceptible. We have heard that from each one of those experts.

Senator LANKFORD. All right. So this is not a ransomware attack. This is actually somebody that is getting into the system. Have you been able to determine going through it whether they would be able to get your operating system to be able to change pressure, to be able to change volume, to be able to change flow through the structure that actually came through?

Mr. BLOUNT. Senator, that is a great question. Obviously, that factored in largely to my decision and the employees' decision to shut the pipeline down that day. We did not know, and we probably did not know the answer to that for days. The investigation is ongoing. But up to this point, Mandiant has not confirmed any evidence that they were in the OT system, and typically that is not what DarkSide does.

Senator LANKFORD. Right, it is a different animal, but it is a vulnerability that sits out there for someone else that does mean to be able to do our Nation harm, not just your company harm, at this point, and they are not just going out for money, but they are actually going out for physical damage. Thanks for being here. Thanks for being so frank in your testimony.

Mr. BLOUNT. Thank you, Senator.

Chairman PETERS. Thank you, Senator Lankford.

Senator Rosen, you are now recognized for your questions.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chairman Peters, Ranking Member Portman. This hearing, of course, is so timely, so important. Mr. Blount, thank you so much for spending your time with us today to bring some clarity to these extremely important issues to our Nation, because you know what? It is a challenge for business owners across a variety of industries to commit the resources necessary and critical to preventing and combating cyber threats. It requires a team of dedicated staff with cyber expertise and the technologies needed actually to defend against an attack.

Mr. Blount, it would be helpful to understand the resources you have at Colonial Pipeline devoted to cybersecurity technology personnel and trainings. So can you tell us just a bit about your cyber guidelines and best practices your company follows? Do you collaborate with Federal agencies like National Institute of Standards and Technology (NIST), DOE, and CISA? If you do not, why not? And just talk about your plans, either current collaboration or collaboration going forward, if you plan to do that.

Mr. BLOUNT. Thank you, Senator, for that very important question. We are highly collaborative organization. We are highly transparent organization. We spent a lot of time in Washington, at least up until COVID, and now we spend a lot of time on the phone and in Zoom calls with all our regulators as well as other entities like CISA, like the DOE, and other people that we feel accountable to for what we do for the Nation.

Again, very communicative, very present in Washington with all the Federal agencies that we have access to, and we certainly appreciate all the collaboration that we are able to do with them. From a Colonial perspective, we have over 100 people dedicated to IT. Our CIO, when she asks for funds related to anything associated with cyber, she gets it. Our board is highly supportive of anything that protects the pipeline and protects our data. So we have never had any issue from the standpoint of getting the funding that we need in order to protect the asset and to protect our information and protect the American public.

Senator ROSEN. Thank you. I want to kind of build on this a little bit because, according to recent news reports, you have discussed scheduling a voluntary cybersecurity review with TSA. A lot of people have touched on this. But that review never took place, and so how often does your company conduct internal cybersecurity reviews or self-assessments? Do you do this on a regular schedule? And what do you do with the results? Who do you share them with, or do you share them?

Mr. BLOUNT. Senator, thank you for that question. With regard to the Validated Architecture Design Review (VADR) voluntary program that TSA has, I had also heard in the press that we had refused to participate in that, and that was quite a shock to me and quite a shock to our CIO. We maintain a lot of conversation with the TSA and specifically the Director of Security level there. We have participated in any number of things with the TSA in the past, including physical screening of our facilities. We have actually had the head of TSA in our office meeting with me and my management team.

Senator ROSEN. Do you do your own internal reviews? Do you share them with others? Do you do those on a regular basis? I guess that is also the point of my question as well.

Mr. BLOUNT. Senator, we do participate in periodic penetration tests. We do auditing, outside auditing of our cyber procedures and our IT department. And like all audits, you expect you are going to find something with the pace of change outside from the threat, and you rank the things that come back, and then you go about the business of tackling those things that are deemed deficient or weak in order to improve your defenses. So, yes, we do.

Senator ROSEN. I want to build on that because you have repeatedly said during this hearing that you were not part of conversations in the wake of the cyber attack, including the discussion with the FBI about paying a ransom. In hindsight, if you are doing this analysis, you are ranking things, doing all this, do you think you should have been part of those conversations?

Mr. BLOUNT. Senator, that is a very good question. This was an all-hands-on-deck day and week. My responsibility that week was to communicate to my board, make sure that my team was communicating where they needed to communicate. I directly handled all the discussions at the DOE level, including the daily briefings that we did with the DOE. I participated in the briefing with the Governor's offices throughout the States that were impacted. So while it would be nice to be involved in every conversation, the reality of it is I cannot be every place at once, but it was well taken care of by any number of my management team members, the people that report directly to me.

Senator ROSEN. Thank you. I appreciate that.

I want to talk a little bit about my Cyber Sense Act because we know, of course, cyber attacks, that is what has happened to you. So last Congress I introduced the Cyber Sense Act. It is bipartisan legislation that would create a voluntary cyber sense program at the Department of Energy that is going to test the cybersecurity of products and technologies intended for use in our bulk power system. This bill also directs the Energy Secretary to consider incentives to encourage the use of analysis and testing results when designing products and technologies, although I think the incentive would actually be not to be hacked.

But, Mr. Blount, while the program my bill would establish is solely for electric utilities, do you think a similar program for pipelines would be helpful for gas companies like yours across the board to collaborate and communicate and have some sense of what is going on in the industry?

Mr. BLOUNT. Senator, thank you for that question. I think that is a great program for the electric utilities, and I think anything that would help our side of the business be more secure and less susceptible to any threats is a great idea.

Senator ROSEN. Thank you. I think the last question—I have about a minute left—I just want to ask a quick question about why Colonial Pipeline did not notify CISA immediately following the ransomware attack. Mr. Wales told this Committee "there is benefit when CISA is brought in quickly, because of the information we glean, we work to share it in a broader fashion to protect other critical infrastructure."

So what is your response to Mr. Wales' statement and you not sharing your ransomware attack?

Mr. BLOUNT. I am glad you asked that question, Senator. One of the first phone calls we made that morning within hours of noticing the compromise was to the FBI office, and during that conversation with the FBI, the FBI said, "We will call you back later. We want to bring in our Center of Excellence from California into the conversation, and we will call CISA and bring them into the conversation." So at that point, based upon the number of phone calls that we had to make that day to any number of governmental entities, we knew that CISA would be notified and brought into the conversation. We had a conversation with CISA the first day as a result of that connection with the FBI. If the FBI had not called them, we would have. We called every other governmental agency we were required to and then some that day.

Again, I do not know why he made that statement, but I can tell you we would have called him. There is no reason not to. We were extremely transparent, and we wanted all the help that we could get that morning.

Senator ROSEN. Thank you very much for your testimony today. My time has expired, Mr. Chairman.

Chairman PETERS. Thank you, Senator Rosen.

Senator Hawley, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman. Thank you, Mr. Blount, for being here.

I think you mentioned this in your written testimony, but I would just like to start here. What percentage approximately of all fuel on the East Coast of the United States is transported by your company's pipeline?

Mr. BLOUNT. Thank you for that question, Senator. It is approximately 45 percent.

Senator HAWLEY. How many gallons of fuel does your company's pipeline transport on a daily basis?

Mr. BLOUNT. Normally we would move approximately 100 million gallons of fuel a day, Senator.

Senator HAWLEY. That is a lot. Is it fair to say that tens of millions of Americans do not really have any choice but to rely on your pipeline for fuel? You have enormous market power, is what I am driving at. Is that a fair statement?

Mr. BLOUNT. Senator, over time we have evolved as a big player in the fuel business, and it is because of our reliability record and, quite frankly, we are the cheapest cost of transportation for the fuel to those customers.

Senator HAWLEY. Yes, I think that the amount of fuel running through the pipeline exceeds the fuel consumption of Germany. If I am not mistaken, the closure of your pipeline facilitated nearly— or led to nearly 16,000 gas stations without fuel across the country, which is huge. You are huge, and consumers really rely on your, is my point.

I am curious as to, given this, given your market power, given the reliance of consumers, given the sheer number of consumers you serve, why didn't you take up the Transportation Security Administration's offer to do a comprehensive cybersecurity review of the pipeline?

Mr. BLOUNT. Senator, thank you for asking that question. We indeed were in contact with them about setting that up. Obviously, COVID got in the way in the early days of that. We were getting ready to move at the end of the year into a new facility, so I think the conversation was that we want to do it, the VADR program is a good program, but we will schedule that later on. We do have that scheduled at the end of July.

Senator HAWLEY. So it was a COVID issue, basically? Or it was a moving issue, you were moving to a new headquarters? I am looking at the Washington Post article here that reports that the TSA had tried to schedule a voluntary in-depth cybersecurity review but that Colonial just could not get it done. Any regret not doing that in retrospect?

Mr. BLOUNT. Senator, anything that you could do is always helpful. If we look at that test, it is a great test, but it is not dissimilar to a lot of the tests that we already do in our system. Again, we have a good working relationship with TSA. I am a little surprised by the statement that I heard about refusal, actually investigated it on my end from my CIO and their contacts on the TSA side. No one really understood why the word "refused" was used.

Senator HAWLEY. So just let me understand your last statement. Are you saying you think that the TSA review would have been redundant, not particularly helpful? You said it is duplicative of things you do on your own end internally.

Mr. BLOUNT. Senator, I think in this case it probably would not have resulted in finding that legacy VPN. Again, they do not actually go into the system. It is a questionnaire format type thing. I am not saying it would not be valuable. It very much could be. I think each one of these tests are slightly different, so if there is that one little piece that can make the difference in seeing something, that is helpful. Again, never any issue with us actually getting to the point of doing that. It was a timing issue.

Senator HAWLEY. Got you. Who owns Colonial Pipeline?

Mr. BLOUNT. Colonial Pipeline is owned by several entities.

Senator HAWLEY. Including?

Mr. BLOUNT. Including a division of Shell, Midstream actually, Caisse du Quebec, KKR, IFM, and Koch Industries.

Senator HAWLEY. Got it. I am asking that because it has been reported that over the last decade Colonial has distributed—I am looking at the article here from Bloomberg. Colonial has distributed almost all of your profits, sometimes more, actually, in the form of dividends to your investors. In 2018, for instance, Colonial Pipeline paid $670 million to its owners, which actually exceeded your net income for that year. That is a pretty good return. What do you invest in cybersecurity every year?

Mr. BLOUNT. That is a great question, Senator. We invested over $200 million over the last five years in our IT systems.

Senator HAWLEY. And that is cybersecurity? How about on an annual basis for cybersecurity? $670 million distributed in dividends in 2018 alone, give me a sense of—you are operating not unlike a public utility, right? I mean, we covered the fact you serve 45, 50 percent of customers on the East Coast; you transport 100 million gallons a day. The attack on you led to 16,000 gas stations being shut down. So just give me a sense of—given the importance of your company, the size of it, the reliance, what are you doing in terms of your investment for cybersecurity? I know you are paying your investors well.

Mr. BLOUNT. Yes, Senator, great question. Our dividend policy is not much different than any other Midstream company, so I want to state that first. Our owners have never denied us any opportunity to spend what we need to spend in order to keep the pipeline safe and secure.

Senator HAWLEY. Which is about what a year?

Mr. BLOUNT. Take the average, over $200 million in the last five years.

Senator HAWLEY. OK, I tell you what——

Mr. BLOUNT. Over $1.5 billion in system integrity every five years.

Senator HAWLEY. Got it. We will give you this as a question for the record so that we can get the actual—I know you do not have the number right in front of you, but we will give you the question for the record,[1] and you can give us the exact number on an annual basis. I think that would be interesting to know.

You talk about Federal regulations in your testimony, and you say Congress should consider designating an official point of contact at a Federal agency to better facilitate communications. That is an interesting idea. What rules do you think Congress ought to consider requiring of you and your company? So your suggestion is what the Federal Government should do itself, but given, again, your status, given the reliance on you, what do you think Congress ought to require of your company and companies like it going forward?

Mr. BLOUNT. Senator, great question. I think what Congress should require is that we have a focus on safety and security of this critical asset, and I think we have demonstrated that over the last 57 years of responsible ownership and operations.

Senator HAWLEY. Let me ask you a little bit about the attack in the IT system. I understand that the attack occurred or was first detected only in the IT network, not in the OT network. Is that right? Do I have that correct?

Mr. BLOUNT. Senator, that is correct.

Senator HAWLEY. OK.

[1] The information requested by Senator Hawley appears in the Appendix on page 49.

Mr. BLOUNT. That is what the investigation shows up to this point.

Senator HAWLEY. Got it. OK. So, to your knowledge, the OT network, the operational technology network, would not have been compromised by the attack if you had not shut down—you shut that down as a precaution, security measure?

Mr. BLOUNT. Senator, if there was one percent chance that that OT system was compromised, it was worth shutting the pipeline system down.

Senator HAWLEY. Got it. I am just trying to establish that, to your knowledge, at this time you think it was concentrated in the IT system?

Mr. BLOUNT. Senator, based upon the investigation by me——

Senator HAWLEY. Got it.

Mr. BLOUNT [continuing]. Up to this point, that would be a correct statement.

Senator HAWLEY. Yes, OK. This leads me to ask this. The pipeline is seven years old, roughly, right? There was a time, I assume—and you correct me if I am wrong, but there was a time, I assume, where you operated the pipeline without today's computer systems. What I am driving toward here is do you have the capability to manually operate the pipeline in the future in the event of an IT attack like this one? If you do not have that capability, should you, do you think, going forward?

Mr. BLOUNT. Senator, that is a great question. We actually did operate small portions of the pipeline manually in order to alleviate some of the fuel shortage, and the discussion took place with the operations team about the ability to do that systemwide. And the response to that was it would be quicker to get back up on our feet by correcting the corruption of the critical IT systems that we needed in order to get the pipeline system up and operate it manually. But I think on a go-forward basis, there is no question that we will look at that capability, and it is a really interesting question because if you look at the aging workforce now, a lot of those people that did operate Colonial Pipeline and other infrastructure in America historically manually, they are retiring or they are gone. Fortunately, we still have that last bit of that generation which allowed us to do what we did during this particular event. It is a great question.

Senator HAWLEY. Very good. Thank you for being here.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Hawley.

Senator Ossoff, you are recognized for your questions.

OPENING STATEMENT OF SENATOR OSSOFF

Senator OSSOFF. Thank you, Mr. Chairman. Thank you as well to Ranking Member Portman. Mr. Blount, thank you for being here today. Thank you for your candid testimony. I want to express my appreciation to your team based in Georgia for their diligent efforts to restore service swiftly and offer you the opportunity before the Committee now to state any lessons learned as well as reflections on potential improvements to Federal policy that we have not had a chance yet to explore on the record.

I also want to thank you for your team's continual updates of my team as you sought to restore service, as you have investigated the nature of the threat, and for the conversation that you and I have had about the matter as well. But lessons learned, recommendations for Congress.

Mr. BLOUNT. Good morning, Senator.

Senator OSSOFF. Good morning.

Mr. BLOUNT. Thank you for your kind words, too. Yes, I think there are several really important lessons learned. I think, the most important lesson learned is to respond immediately, right? We have talked about stop-work authority at Colonial, the ability to identify the threat, contain the threat, remediate the threat, and restart the system. Again, that goes toward any type of threat that we see, not just particularly a cyber threat. I think that is an important thing for any operator to remember, is contain that threat.

The other side that I would like to share with you that I think is extremely important is communication, and there has been a lot of conversation in this room about who did you talk to and who did you communicate with and at what time did you do that. I will stress again I think that what we learned was that being transparent and responding quickly and not being afraid to come forward was probably one of the most important things that we did in this particular case, not foreign to us but perhaps foreign to others.

Finally, I would add I think the ability to communicate with the Federal Government through one conduit, regardless of who it is, was extremely valuable to us because, again, as I looked at this all-hands-on-deck effort that we had to do, the ability to communicate everything that we were seeing, whether it was the market response or the things that we were trying to get done on the IT side to do the restart all the way to the investigative side of the equation, extremely helpful for a management team already stretched to be able to communicate quickly and efficiently, and then allow our government partners to do what they could do to help us, which indeed they did. They were very helpful in the process.

Senator OSSOFF. Thank you, Mr. Blount. As you and I discussed last week, your team, I believe in collaboration with Mandiant, is conducting a comprehensive review of the threat, the nature of the attack, what might have been done to mitigate the risk, the efforts to thwart the attack once it was discovered. Is that correct?

Mr. BLOUNT. Yes, Senator, that is correct.

Senator OSSOFF. What impediment would there be, if any, to sharing the results of that review and the conclusions of that investigation, including at the technical level with this Committee once it is completed?

Mr. BLOUNT. Senator, I do not think there are any issues with that. What we have been trying to do all along the way is share the information as we learn it. We have been very straightforward about the legacy VPN. Hopefully that will help out other operators who have similar type legacy assets.

We know from working with Mandiant that is not an unusual issue for companies. I think we will continue to communicate as we go through the process with Mandiant, but our ability and desire to sit down with you is ready and available when you would like that.

Senator OSSOFF. Great. So we can expect that once that review and investigation are complete, you would voluntarily share with this Committee the results of Mandiant's investigation?

Mr. BLOUNT. Yes, Senator, we will be very transparent.

Senator OSSOFF. I appreciate that. When you and I spoke last week, I believe you stated that you had not refused any requests for information from the Department of Homeland Security, the FBI, or other Federal entities. You have discussed the importance of the free flow of information between the target of an attack like this and the Federal Government.

Having now had the experience of your company being subjected to an attack such as this and the communication that you had to engage in swiftly with Federal entities, what do you think can be done to improve and make more efficient and direct the flow of information between the victim of a cyber attack and Federal law enforcement, Federal cybersecurity authorities? I want to drill down a little bit on the following: You and I also discussed last week that the criminal enforcement side of the investigation and the cybersecurity side of the investigation overlap but are also distinct. Have you found any difference in the quality of the Federal response, the nature of the communication with Federal authorities between the criminal prosecutorial investigation and the cybersecurity investigation?

Mr. BLOUNT. Senator, from my perspective, I would say the answer is no. Again, as we discussed, we had FBI, CISA, and, of course, Mandiant helping in the process. We told Mandiant from the very beginning if the FBI had questions or CISA had questions, please share information with them. Of course, as structured by the White House, we had the ability to communicate with everybody else on the restoration side and on the supply concern side through the DOE. Again, that worked wonderfully for us. Again, our time was stretched during the day when we were trying to respond to the situation and get things remediated so that we could bring the pipeline back up. From my perspective as the CEO, to sit down at least at 5 p.m. every day and sometimes more often phone calls would come, but at least have the ability to communicate, the restoration side, what we were doing to restore the IT systems, share market intelligence because we have a unique perspective as Colonial as well. That was very helpful.

So regardless of who that conduit is, the ability to communicate on the investigative side with all those parties at once and on the restoration and the market side, extremely valuable to us. As you can imagine, there is a lot going on as you head toward bringing an asset like this back up, and you have a lot of people that want to know a lot of things, and you do not have all the answers yet. But what I found is by having them all in the same room, the expert on this one particular area would say, "They would not know that yet," and that would alleviate a lot of concern that the less knowledgeable person might have, even though they were very strong in what their particular discipline or science was.

Senator OSSOFF. Thank you, Mr. Blount. Finally, circling back to the ongoing Mandiant investigation, can you commit that the product that you share with this Committee of that investigation will be the same product that you and your executive team and your board review and that it will not be a different set of conclusions that are produced for the consumption of Congress but it will be the same assessment that you receive?

Mr. BLOUNT. Senator, as I have stated previously, we will be very transparent. I think the one thing that we need to be careful about as a Nation is how do we share that information. Obviously, it would be very difficult in a public forum like this because a lot of what we will share about our strengthening and hardening of our systems will be critical to keeping those strong and defensive against attacks.

But, yes, we need to talk and figure out what is the best way to talk about what happened as well as what best practice on a go-forward basis is for an operator like ours that operates such sensitive infrastructure.

Senator OSSOFF. So recognizing that some of those conclusions, information, and plans may be sensitive and confidential, nevertheless the appropriate forum for those confidences being provided, we will be able to exchange that information freely and review in full the Mandiant report?

Mr. BLOUNT. Senator, we will gladly cooperate with you.

Senator OSSOFF. Thank you, Mr. Blount.

I yield back, Mr. Chairman.

Chairman PETERS. Thank you, Senator Ossoff.

Mr. Blount, I would like to thank you for joining us here this morning on this incredibly important matter. We are clearly experiencing relentless and unprecedented assaults against both our private and public sector information systems, and we are getting those assaults by both criminal organization as well as foreign adversaries, and this is a grave national security concern. Certainly from the questions that were posed today by all of my colleagues, I think it is clear that my colleagues believe this is something that we need to address immediately and in a comprehensive fashion.

It is clear to me that the cyber attack against Colonial highlights the need for increased cooperation and coordination between both the Federal Government and our critical infrastructure partners. We must ensure that the American people are capable of not only defending our critical infrastructure partners from attack, but also maintaining a secure information system environment to prevent those cyber attacks from occurring in the first place.

The interference that American lives depend on is increasingly connected, connected to each other and connected to the Internet. This brings a whole new meaning to the phrase "You are only as strong as your weakest link," and these weak links can be hacked accounts, inadequate passwords, or unknown vulnerabilities to the system.

More must be done in this space, and I am committed to certainly focusing my attention. I think every Member on this Committee agrees that this Committee will focus our collective attention and resources on dealing with this problem. Cyberattacks used to be merely an inconvenience. We now know that they are becoming attacks on our very way of life.

Once again, thank you for appearing here today. I look forward to your continued engagement on this important issue.

The record for this hearing will remain open for 15 days, until June 23rd at 5 p.m., for submission of statements and questions for the record.

With that, this hearing is now adjourned.

[Whereupon, at 11:33 a.m., the Committee was adjourned.]

APPENDIX

Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack
June 8, 2021

Mr. Blount, welcome to the Committee. Thank you for joining us for this important discussion on the harmful cyber-attack against your company, Colonial Pipeline, and how we can work to strengthen coordination and response to these serious cybersecurity incidents.

When Colonial Pipeline was forced to shut down operations last month due to a ransomware attack, millions of Americans up and down the East Coast had their lives disrupted by gas shortages and price increases.

In the weeks since your company was struck, we have seen a series of other attacks, on everything from our transportation networks to meat-packing centers. Those private sector strikes follow especially damaging attacks on our government, including the extensive SolarWinds hack last year.

While the objectives of these attacks differ, they all demonstrate that bad actors, whether criminal organizations or foreign governments, are always looking to exploit the weakest link, infiltrate networks, steal information, and disrupt American life.

Mr. Blount, I am glad your company continues to recover from this malicious attack and that the FBI was able to recover millions of dollars in ransom paid. But I am alarmed that this breach ever occurred, and that communities from Texas to New York suffered as a result.

I appreciate that you have joined us today, to provide answers to the Committee and the American people on how a group of criminals was able to infiltrate your networks – steal nearly 100 gigabytes of data in just two hours – and then lock your systems with ransomware to demand payment. I am also looking forward to hearing an update on your progress to recover from this serious breach.

Private entities, especially those that are critical to our nation's infrastructure, are responsible for assessing their individual risk and investing in the technology to prevent breaches and ensure they can continue providing service to customers who rely on them for basic necessities, like fuel.

At the same time, the federal government must develop a comprehensive, all of government approach to not only defend against cyber-attacks, but punish foreign adversaries who continue to perpetuate them or harbor criminal organizations that target American systems.

This approach requires bolstering our defenses, and using the full might of our diplomatic, military, and intelligence capabilities.

We must also ensure private entities, like Colonial, are providing the federal government with timely and relevant information in the event of major incidents.

We need federal agencies charged with cybersecurity – like the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency – to understand the extent of these attacks and how best to support victims.

Make no mistake – if we do not step up our cybersecurity readiness – the consequences will be severe. The ransomware attack on Colonial Pipeline affected millions of Americans. The next time an incident like this happens – it could be even worse.

As Chairman of this Committee – I am committed to prioritizing policies that will help secure our critical infrastructure networks – including in the proposed infrastructure package Congress is negotiating.

Protecting the American people from these sophisticated – harmful – and growing attacks will not be easy. We must learn from our past mistakes – find out what went wrong – and work together to tackle this enormous challenge. Inaction, however, is NOT an option.

OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
THREATS TO CRITICAL INFRASTRUCTURE: EXAMINING THE COLONIAL PIPELINE CYBERATTACK

June 8, 2021

Thank you, Chairman Peters. I've appreciated our bipartisan work over the years to improve cybersecurity and I look forward to continuing our partnership.

Today's topic is both incredibly relevant and highly concerning: ransomware attacks on critical infrastructure. Ransomware paralyzes a company by locking its computer systems and holding its data and operations hostage until the ransom is paid. Increasingly, ransomware hackers pursue a two pronged ransom approach where they also download and threaten to release sensitive victim data.

There seems to be a new ransomware attack every week. While today, we will hear from a recent ransomware victim, Colonel Pipeline, these attacks are not limited to one sector. No entity – public or private – is safe from these attacks.

Last week, we learned that ransomware shut down the world's largest meat processor, JBS, including nine beef plants in the United States. Both the Colonial Pipeline attack and the JBS attacks were attributed to Russian criminal organizations.

Just this morning, news broke that a constituent outreach services platform that nearly 60 offices in the House of Representatives use was hit with a ransomware attack. As I said before, no one is safe from these attacks.

I hope today's hearing will cover four topics:

First, we must understand that these attacks have real-world consequences.

- On May 7, Colonial Pipeline learned they suffered a ransomware attack impacting their information technology, or IT, systems by DarkSide, a Russia-based criminal group.

- Recent news reports indicate that hackers accessed Colonial's systems through a compromised password of a Virtual Private Network account.

- This account did not use multifactor authentication, a basic cybersecurity best practice, which easily allowed the hackers to gain access.

- Colonial moved quickly to disconnect their operational systems to prevent hackers from moving laterally and accessing those systems.

- This was an appropriate response to a cyberattack, but it made Colonial's critical pipelines unusable. And that is a huge problem—Colonial Pipeline provides about 45 percent of the East Coast's fuel.

- With operations shut down, people across the East Coast bought fuel in a panic, unsure how long the shortage would last.

- Colonial brought its systems back online within a week, easing what could have been a much worse situation.

Second, this shows the difficult decision ransomware victims face: should they pay the ransom or not?

- The U.S. government, including both CISA and the FBI, strongly recommend organizations do not pay ransoms.

- Paying ransoms rewards ransomware hackers—if no one paid ransoms, criminals would have little incentive to engage in ransomware attacks.

- And even if an entity pays, there is no guarantee that the hackers will give them the decryption key or not strike again.

- However, organizations must weigh these consequences against keeping their operations offline—in this case, limiting 45 percent of the East Coast's fuel supply.

- Colonial Pipeline paid DarkSide a ransom of 75 bitcoins—worth over $4 million at the time. Yesterday, the Department of Justice announced the recovery of 63.7 of those bitcoins, but DOJ won't always be able to recover those ransom payments.

- I appreciate Mr. Blount's transparency in acknowledging that his company paid the $4.4 million ransom. I hope today we can explore the reasons for that decision.

Third, this attack demonstrates the gaps in information sharing between impacted organizations and the federal government.

- Last month, Brandon Wales, the Acting Director of CISA, testified in response to one of my questions that he didn't think Colonial Pipeline would have contacted CISA at all if the FBI didn't bring them in.

- CISA's authorities allow the agency to engage on a voluntary basis, when requested by an affected organization. While I think this is the right approach, CISA must have relevant information to be able to share it among other critical infrastructure owners and operators who may be similarly targeted.

Finally, we must recognize these ransomware attacks for what they are: a severe national security threat.

- Attacks against critical infrastructure entities are not just attacks on companies; they are attacks on our country itself.

- When DarkSide attacked Colonial Pipeline, it wasn't just the company that was affected. Americans across the East Coast felt the squeeze at fuel pumps when Colonial shut off nearly 50 percent of the fuel supply.

- The criminals conducting these attacks often operate with at least the tacit acceptance of the foreign countries they operate out of. The U.S. Government needs to take stronger steps to hold those countries, like Russia, accountable.

Ransomware attacks will continue to plague U.S. companies and critical infrastructure. As the committee of jurisdiction over both cybersecurity and critical infrastructure security, we need to reevaluate how we defend against ransomware, and identify solutions to mitigate the consequences of these attacks.

HEARING BEFORE THE UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS

June 8, 2021

Testimony of Joseph Blount, President and Chief Executive Officer
Colonial Pipeline Company

I. Introduction

Chairman Peters, Ranking Member Portman, 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 one 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. Timeline of the Morning of the Ransomware Attack

We identified the ransomware attack just before 5:00 AM Eastern Daylight Time (EDT) on Friday, May 7th, 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 fifteen minutes to close down the conduit, which has about 260 delivery points across 13 states and Washington, D.C.

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 underway, 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 online 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. Ongoing 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 four 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 ongoing, 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 ongoing, 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.

Post-Hearing Questions for the Record
Submitted to Joseph A. Blount, Jr.
From Senator Maggie Hassan

"Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack"
June 8, 2021

1. Cybersecurity needs to be a team effort. Therefore, encouraging two-way information sharing and establishing effective private-public partnerships is really important. CISA can piece together a wider perspective on emerging cybersecurity threats when many individual companies share their individual, fragmented perspective. And companies can be proactive and alert when federal authorities better share threat information.

    a. What information do you believe needs to be shared, in each direction, to strengthen the public-private partnership needed to identify, mitigate, and prevent future cyberattacks?

    b. Given CISA's acknowledgement that it must protect any trade information it receives as part of an information sharing agreement, is there any good reason for not sharing information? What are the roadblocks?

Response: On the morning of the attack, we proactively contacted the Federal Bureau of Investigation (FBI) to inform them that cyber criminals had attacked Colonial Pipeline. We also scheduled another call within hours to brief both the FBI and the Cybersecurity & Infrastructure Security Agency (CISA) together with information about the attack, and we remained in regular communication with law enforcement. We proactively shared with law enforcement Indicators of Compromise (IOCs) and other threat intelligence in an effort to help thwart these kinds of attacks in the future and to assist the federal government. Additionally, given the sensitive nature of this information, maintaining the confidentiality of this data was vital.

As difficult 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 we and others can better protect ourselves moving forward. We are continuing to undertake a thorough forensic investigation into the attack and it will take time to review the evidence to make sure we get accurate answers. However, we have begun the process of sharing preliminary lessons learned with industry partners and peers, so that they too learn from this event. We look forward to continued engagement with CISA and other government entities as we work to share information in an effort to prevent attacks like this in the future. Of course given the nature of this information, maintaining the confidentiality of certain sensitive data and findings is vital to the future security of the pipeline.

2. There are a lot of federal agencies potentially involved with pipeline security.

    a. Prior to the attack, which federal agencies did Colonial usually interact with regarding cybersecurity issues?

    b. Was it usually the agencies who reached out to you, or did Colonial Pipeline proactively reach out to the agencies?

    c. In your view, how well did those interactions help you identify weaknesses and improve your cybersecurity?

Response: We are grateful for the constructive relationship and cooperation of our federal regulators both before and since the attack. In addition to our engagement with federal law enforcement authorities regarding the attack, as described in our response to Question 1, we have also worked closely with CISA, 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), and the Federal Energy Regulatory Commission (FERC). Our engagement with those federal authorities, preexisting productive relationships, and history of contact in both directions helped us achieve meaningful milestones in our response process to address the attack and restore pipeline operations quickly and safely. In particular, we appreciate the cooperation of the federal agencies that worked with us in connection with the attack. Their focused collaboration facilitated our ability to restart the pipeline, so we could transport various types of fuel to their destinations.

Post-Hearing Questions for the Record
Submitted to Joseph Blount
From Senator Kyrsten Sinema

"Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack"
June 8, 2021

1) Prior to the early May attack on Colonial Pipelines, what steps did your company take to prioritize cybersecurity? In retrospect, are there additional steps you could have taken to better prepare for an attack?
   a. **Response:** Colonial Pipeline takes cybersecurity and the integrity of our pipeline extremely seriously. Over the past few years, we have increased our level of spending on information technology (IT) over 50%. Additionally, our IT team has nearly doubled in size as we continue to make significant investments in seasoned technical talent, our infrastructure, industry partnerships, and technology to further harden our systems and strengthen our defenses. We are continually preparing for a range of cyber risks and we remain focused on enhancing our cybersecurity program by leveraging industry-leading vendors that have helped us take steps to further strengthen our cyber defenses going forward.

2) Aside from the Transportation Security Agency's May 27th Security Directive for critical pipeline operators, what additional steps does Colonial plan to take as a result of the attack? And what additional recommendations do you have for the federal government in responding to these types of attacks?
   a. **Response:** See Response to Question 1. Additionally, we are grateful for the immediate and sustained support of federal law enforcement and governmental authorities, including the White House. We proactively contacted federal authorities within hours of the attack and found them to be extremely helpful as we worked to quickly and safely restore and secure our operations. Two key takeaways from our experience were that it was critical to have a single point of contact with the federal government to ensure a swift and coordinated response, and that the coordinating entity prioritize preserving the confidentiality of sensitive data regarding the attack and the company's security infrastructure. The inter-agency approach implemented by the Biden Administration streamlined the federal government's response and was very valuable, but having a single point of contact enhanced our coordination efforts. Whichever organization may be designated as the single point of contact, Congress must ensure it is adequately staffed and resourced to support the industry, facilitate information sharing and the preservation of confidential information, and respond appropriately. It is also important that victims receive the continued support of law enforcement to disrupt cyber-crime networks and bring attackers like DarkSide to justice.

3) Throughout our country, we are increasingly reliant on interconnected devices and networks that help manage critical areas such as pipelines, healthcare, and energy. How does your company plan to address such concentrated cyber risks in your operations moving forward?
   a. **Response:** See Response to Question 1. In addition, Colonial retained some of the best experts in the industry to advise on further strengthening its defenses.

4) Shortly after the attack on Colonial Pipelines, JBS Foods, the world's largest meat processing company with a facility located in Arizona, became the victim of a similar ransomware attack. What lessons would you share with other business owners, such as JBS's incident response team, which will help them to overcome a major cyber incident?
   a. **Response:** As difficult 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 we and others can better protect ourselves moving forward. We are continuing to undertake a thorough forensic investigation into the attack and it will take time to review the evidence to make sure we get accurate answers. We have already begun the process of sharing preliminary lessons learned with industry partners and peers, so that they too learn from this event.

5) Given that many cyber incidents start with poor cybersecurity practices by just one person inside an organization, does the entire staff of Colonial Pipelines receive cyber hygiene training? If so, can you generally describe the training they receive?
   a. **Response:** We leverage a number of industry-leading vendors that have helped us take steps to strengthen our cyber defenses over the past few years and provide redundant controls and enhanced capabilities. Some of the implemented measures specific to employee training include requiring mandatory annual physical and cybersecurity training as well as conducting simulated cyberattacks. Colonial provides training for employees at least annually on cybersecurity risks and engages employees through Cybersecurity Awareness Month.

Post-Hearing Questions for the Record
Submitted to Joseph A. Blount, Jr.
From Ranking Member Rob Portman

"Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyberattack"
June 8, 2021

1. What Colonial employees or agents acting on behalf of Colonial communicated with DarkSide regarding the ransom payment?
   a. **Response:** Colonial did not communicate directly with the attackers. Rather, the communication with the attackers was handled by external negotiators, who were retained for this purpose.

2. What was DarkSide's initial ransom demand?
   a. **Response:** DarkSide's initial ransom demand that appeared on the initial notice of the attack was for "$4.8 million now or $9.6 million after doubled."

3. Did Colonial employees or any entity acting on behalf of Colonial inform the U.S. Government of their intent to pay the ransom prior to making the payment? Please specifically indicate whether Colonial employees or anyone acting on its behalf informed FBI, OFAC, or other government entity. If so, what advice or information did that entity provide in response?
   a. **Response:** Colonial called the FBI the morning of May 7, 2021, which is the day we became aware of the ransomware attack. We also had a call with the FBI and CISA together several hours later. On those calls, we did not indicate our intent to pay the ransom as we had not determined whether to do so at that time. We were aware of the FBI, OFAC, and other government entities' positions on ransom payments and our external experts checked OFAC's sanctions list to ensure that DarkSide was not on the list before we decided to pay the ransom. Additionally, during the May 7, 2021 telephone call we conducted with CISA and the FBI, the FBI indicated that the attackers were not sanctioned actors.

4. Please describe any sanctions compliance due diligence undertaken by Colonial or agents acting on behalf of Colonial prior to making the ransom payment.
   a. **Response:** See Response to Question 3.

5. Who purchased and transferred the 75 Bitcoin ransom to DarkSide? Please include the titles of any Colonial officers or senior employees and the names of any other organizations involved and their roles.
   a. **Response:** Payment was handled by third-party negotiators.

6. What steps, if any, did Colonial take while paying the ransom to facilitate the FBI's partial recovery of the ransom?
    a. **Response:** Beginning on the morning of the attack, we quickly provided the FBI with extensive information about the attack and perpetrator, including the bitcoin wallet on Saturday afternoon. We continued to cooperate and provide relevant information. We understand that this cooperation aided law enforcement in the recovery of the ransom payment.

7. Once DarkSide compromised Colonial's networks, did the attackers demonstrate a particular interest in specific sensitive information held by the company? If so, what specific sensitive information was targeted?
    a. **Response:** Our forensic investigation is ongoing and our experts continue to review the files that were exfiltrated. Based on the findings to date, we have no reason to believe that the attackers had a particular interest in specific sensitive information held by the company.

8. What sensitive information was exfiltrated by DarkSide in its attack?
    a. **Response:** Our forensic investigation is ongoing and our experts continue to review the files that were exfiltrated.

9. How did the exfiltration of this information contribute to Colonial's decision to pay the ransom?
    a. **Response:** Colonial Pipeline CEO Joe Blount stated publicly that this was one of the toughest decisions he ever had to make. Colonial's focus was to safely secure and restart the pipeline as quickly as possible. We believe this was the right thing to do for the country and our shippers.

10. During the hearing, Mr. Blount indicated Colonial had good backups. How long did it take for Colonial to bring these backups online?
    a. **Response:** We are 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, and our backups were critical in achieving that quickly. The backups allowed us to begin to bring our critical systems back online within hours of containment and restore functionality. The containment and restoration took several days to complete, and we took steps to make all tools available to complete this process safely and efficiently. We are well underway, with the assistance of leading outside experts and our own team, with efforts to further strengthen our defenses against future attacks.

Post-Hearing Questions for the Record
Submitted to Joseph A. Blount, Jr.
From Senator Josh Hawley

"Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack"
June 8, 2021

1. In the recent hearing on the Colonial Pipeline cyber-attack, you testified that your company invested approximately $200 million over the past five years in its IT system. Of that total, you did not know how much was specifically invested in cybersecurity. In addition, public reporting has suggested that in 2018, your company paid nearly $670 million to its owners in the form of dividends. Given this, please clarify the following:

    a. Of the $200 million that Colonial Pipeline invested in its IT system over five years, how much of that total was spent on cybersecurity?
    b. In 2016, how much did Colonial Pipeline invest in cybersecurity? And how much did Colonial Pipeline pay its owners in dividends?
    c. In 2017, how much did Colonial Pipeline invest in cybersecurity? And how much did Colonial Pipeline pay its owners in dividends?
    d. In 2018, how much did Colonial Pipeline invest in cybersecurity? And how much did Colonial Pipeline pay its owners in dividends?
    e. In 2019, how much did Colonial Pipeline invest in cybersecurity? And how much did Colonial Pipeline pay its owners in dividends?
    f. In 2020, how much did Colonial Pipeline invest in cybersecurity? And how much did Colonial Pipeline pay its owners in dividends?

Response: Colonial Pipeline takes cybersecurity and the integrity of our pipeline extremely seriously. Over the past five years, we have spent more than $200 million on our information technology ("IT") systems, including on multi-year improvements. The investments we have made in hardening and improving our IT systems are inextricably linked to the maintenance and performance of our systems and therefore are a critical part of our cybersecurity efforts. In addition, the benefits of our IT investments extend beyond the year when the improvement was made. Increased investment in IT has been and continues to be a priority for Colonial. Over the past few years, we have increased total spending on our IT program by more than 50 percent. Additionally, our IT team has nearly doubled in size. As part of our post-incident plan going forward, we will be assessing whether and where we may make further investments.

Information on dividend payments made by Colonial Pipeline Company for all requested years is available in the "Statement of Cash Flows" section on Colonial Pipeline Company's Form 6, which is filed on the FERC website at https://www.ferc.gov/industries-data/oil/general-information/oil-industry-forms/form-66-q-data-current-and-historical.