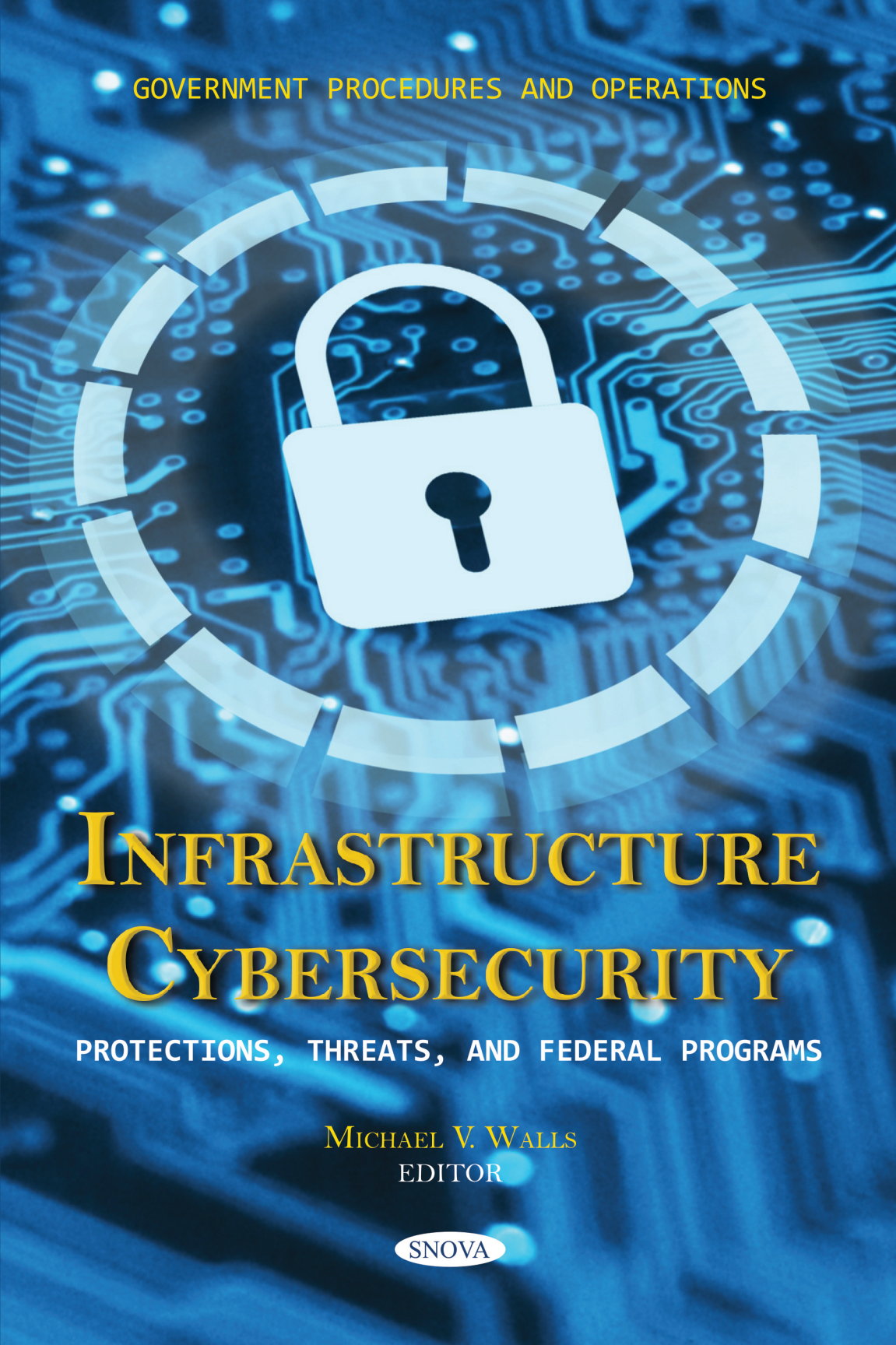
GOVERNMENT PROCEDURES AND OPERATIONS



# INFRASTRUCTURE CYBERSECURITY

## PROTECTIONS, THREATS, AND FEDERAL PROGRAMS

MICHAEL V. WALLS
EDITOR

SNOVA

# Government Procedures and Operations

# Government Procedures and Operations

**COVID-19 in Nursing Homes: Impact, Transmission and Prevention**
Fred C. Wallace (Editor)
2023. ISBN: 979-8-88697-673-1 (Hardcover)
2023. ISBN: 979-8-88697-683-0 (eBook)

**The Significance of the COVID Pandemic in Nursing Homes**
John S. Gill (Editor)
2023. ISBN: 979-8-88697-660-1 (Hardcover)
2023. ISBN: 979-8-88697-682-3 (eBook)

**Putting an End to Surprise Medical Billing**
Danial E. Tackett (Editor)
2022. ISBN: 979-8-88697-296-2 (Hardcover)
2022. ISBN: 979-8-88697-327-3 (eBook)

**Abortion Rights, Access, and Legislative Response**
Jorge P. Sandford (Editor)
2022. ISBN: 979-8-88697-258-0 (Softcover)
2022. ISBN: 979-8-88697-294-8 (eBook)

**Review of Capitol Police Procedures During the Capitol Attack**
Rafael B. Phillips (Editor)
2022. ISBN: 979-8-88697-260-3 (Hardcover)
2022. ISBN: 978-1-53617-478-6 (eBook)

More information about this series can be found at
https://novapublishers.com/product-category/series/government-procedures-and-operations/

**Michael V. Walls**
Editor

# Infrastructure Cybersecurity

## Protections, Threats, and Federal Programs

**Library of Congress Cataloging-in-Publication Data**

ISBN: 979-8-89113-052-4 (eBook)

*Published by Nova Science Publishers, Inc. † New York*

# Contents

# Preface

Private entities, especially those critical to our nation's infrastructure, are responsible for assessing their individual risk and investing in technology to prevent breaches. At the same time, the federal government must develop a comprehensive approach to not only defend against cyberattacks, but also to punish foreign adversaries who continue to perpetrate them. This book examines policies that will help secure our critical infrastructure networks.

# Chapter 1

# Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyberattack*

## Committee on Homeland Security and Governmental Affairs

Tuesday, June 8, 2021
U.S. Senate
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 cyberattack against your company, Colonial Pipeline, and how we can work together to strengthen our coordination and response to this very serious cybersecurity incident.

---

* This is an edited, reformatted and augmented version of the Hearing Before the Committee on Homeland Security and Governmental Affairs, United States Senate, Publication No. S. Hrg. 117–429, dated June 8, 2021.

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

In: Infrastructure Cybersecurity
Editor: Michael V. Walls
ISBN: 979-8-89113-039-5

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.

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 cyberattacks, 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[2]

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 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.

[2] The prepared statement of Senator Portman appears in the Appendix.

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 cyberattack 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 cyberattacks, 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,[3] 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.

[3] The prepared statement of Mr. Blount appears in the Appendix.

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 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 cyberattacks?

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 cyberattacks 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.