HEARING BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

June 9, 2021

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

I. Introduction

Chairman Thompson, Ranking Member Katko, and Members of the Committee: My name is Joe Blount, and since late 2017, I have served as the President and Chief Executive Officer of Colonial Pipeline Company. Thank you for the opportunity to testify before the Committee today.

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

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

Just 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.