COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Joint Hearing Statement of Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Chairwoman Yvette Clarke (D-NY)

Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack

June 15, 2021

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

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

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

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

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

As I've said before, I'm working on legislation that will require critical infrastructure to report certain cybersecurity incidents to CISA so that we're developing the muscle memory and the institutional

knowledge to improve our cyber defenses over time. But this is only half the battle. CISA also needs real-time visibility into threats on private sector networks, so they're empowered to collaborate with owners and operators before, during, and after an attack – or, prevent the attack from happening in the first place.

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

For the past few years, CISA has been piloting a program called CyberSentry that gives CISA the ability to monitor and detect cyber threats on participating critical infrastructure partner networks, and work proactively with owners and operators to address threats in real time. This is exactly the kind of operational role that Congress envisioned CISA playing on critical infrastructure cybersecurity, and I am currently working on legislation to strengthen and codify these efforts. I would be remiss if I did not mention that the Federal government can only do so much.

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

# # #

Media contact: Adam Comis at (202) 225-9978