COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis

May 5, 2021

I first chaired this subcommittee over ten years ago. While ransomware is not a new problem, the number of cases and the financial impact has skyrocketed since then. That's why I wanted to focus on ransomware at our first subcommittee hearing of the year. We must understand the problem we're facing and learn more about how the federal government should respond.

Estimates show that ransomware victims paid $350 million in ransom payments last year. Among those victims were 2,400 US-based governments, healthcare facilities, and schools. As the COVID-19 pandemic forced governments and businesses to shift to remote work, thousands found themselves locked out of their networks as cybercriminals demanded ransom payments. These attacks are more than a mere inconvenience – they are a national security threat. It is time for bold action rooted in robust partnerships between the federal government and its state, local, and private sector partners.

In the coming days, I will introduce the State and Local Cybersecurity Improvement Act, which would authorize $500 million in annual grants to state, local, territorial, and Tribal governments to strengthen their cybersecurity. As the ever-increasing number of ransomware attacks on state and local governments demonstrates, adequate investment in cybersecurity has been lacking, and more resources are needed. Just last week, we saw ransomware attacks that released sensitive law enforcement information from police departments in Washington, DC and Presque Isle, Maine, showing that cities large and small are vulnerable to this kind of cybercrime. This legislation would ensure funding is available, while insisting state and local governments step up to prioritize cybersecurity in their own budgets.

I am proud of the bipartisan support this bill has received on this committee and look forward to working with Ranking Member Garbarino, along with Chairman Thompson and Ranking Member Katko, to get this critical bill enacted. I hope this hearing will give us an opportunity to learn more about the challenges state chief information officers face under current funding constraints and how they would be able to use additional resources to strengthen their defenses to ransomware. While state and local governments are some of the most notable victims of ransomware, this crisis affects many private businesses in the U.S. and around the world. Combatting this threat will require coordination between the public and private sector and all levels of government.

The Ransomware Task Force Report released last week provided 48 recommendations on what government and industry can do to address this crisis in the coming months and years. I am excited to have two of the co-chairs of the Task Force here today to share more information on the recommendations. As Secretary Mayorkas has made clear in announcing that addressing ransomware would be the first of DHS's 60-day sprints on pressing cybersecurity challenges, responding to ransomware is a priority for this administration. And it is definitely a priority for this Committee and many in Congress. So, I hope that this hearing will help further the conversation on how the private

sector, Congress, the executive branch, and state and local governments can collaborate to address this crisis.

In particular, I am interested to learn how other Committee priorities – including developing a cyber incident reporting framework – could improve our understanding of ransomware trends and how to defend against such attacks. Relatedly, I am interested to hear how CISA can play an important role in information sharing and coordinating this response. As the agency that works closely with governments at all levels and the private sector on cybersecurity matters, I know it will have a significant role on this issue going forward.

# # #

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