COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

A Whole-of-Government Approach to Combatting Ransomware: Examining DHS's Role

November 17, 2021

Earlier this year, as chair of the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee, I held our first hearing of this Congress on the ransomware epidemic because I recognize what a serious challenge it poses to our national security. At that hearing, we heard from members of the Ransomware Task Force, the president of the National Association of State Chief Information Officers, and former CISA Director Chris Krebs about what actions the federal government must take to address this cybersecurity crisis. Just two days later, Colonial Pipeline reported it was shutting down 5,500 miles of pipeline as a precaution after being hit by a ransomware attack.

Reports about ransomware attacks had been simmering for years, but they reached a boiling point overnight as gas shortages occurred across much of the East Coast. As spring wore on, we learned about ransomware attacks against JBS Foods, Kaseya, Brenntag, and others. Fortunately, President Biden has made combatting ransomware a top priority since taking office. At DHS, Secretary Mayorkas announced that ransomware would be the first of the Department's 60-day cybersecurity sprints. And CISA has continued to lead the way in raising awareness about how to protect against ransomware, including by supporting StopRansomware.gov, a website with resources for businesses and individuals with steps they can take to reduce their risk.

But, these actions are not limited to DHS. President Biden has committed to a whole-of-government approach that includes the Departments of State, Commerce, Justice, and Treasury and the Intelligence Community, and the issue of ransomware has been a topic at high-level international meetings both with our allies and with our adversaries, including Russia. I look forward to hearing from our witnesses today about how DHS is leveraging the authorities and capabilities of its components to contribute to the Administration's broader ransomware efforts.

I am also pleased that Congress is stepping up to provide the authorities and resources necessary to combat ransomware. In particular, the Infrastructure Investment and Jobs Act signed into law by President Biden on Monday includes my legislation, the State and Local Cybersecurity Improvement Act, providing $1 billion in cybersecurity preparedness grants to State, local, Tribal, and territorial governments. Additionally, the package includes $100 million for a new Cybersecurity Response and Recovery Fund that will complement cybersecurity preparedness grants by providing state and local government victims with alternatives to making ransom payments. Together, these new resources will help make ransomware a higher-cost and lower-reward endeavor.

While I wish we had taken steps to enhance state and local cybersecurity earlier, I am glad that with the support of President Biden and the Senate this year, we have finally stepped up as a partner with all levels of government to secure our critical public networks. Furthermore, after many years of debate in Congress, I am confident that we will finally enact mandatory cyber incident reporting legislation as part

of the National Defense Authorization Act. As I work with my colleagues on both sides of the aisle on this Committee and in the Senate to finalize an agreement, I am eager to hear our witnesses' perspective on how greater information on cyber incidents and ransom payments would strengthen the Administration's counter-ransomware efforts.

It is my hope that greater information sharing in support of the Administration's whole-of-government approach to combatting ransomware will help improve our visibility into the ransomware epidemic and enhance our ability to respond appropriately.

# # #

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