COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Securing the DotGov: Examining Efforts to Strengthen Federal Network Cybersecurity

May 17, 2022

Before I begin with my opening remarks, I would like to take a moment to express my condolences to the family and friends of those who were so senselessly murdered in the mass shooting at a grocery store in Buffalo over the weekend. For too long, hate-driven domestic terrorism has made the core of our communities - grocery stores, schools, and places of worship – unsafe. We cannot tolerate that any longer. I am pleased that both the Biden-Harris Administration and this Committee are confronting the threat posed by domestic extremists with such urgency and look forward to continuing those efforts.

In December 2020, we learned that the Russian intelligence services has infiltrated the networks of multiple Federal agencies by inserting malware in a SolarWinds software update. The Russians remained on Federal networks undetected for months. This intrusion highlighted that the Federal government's signature cybersecurity programs had failed to evolve and adapt to meet the threats our Nation faces today.

Fortunately, over the past year and a half, we have seen a renewed focus in Congress and the Executive Branch on taking the necessary steps to bring our Federal network security to where it must be. Immediately upon taking office in January, President Biden assembled a top-notch cybersecurity team that has brought together leading cybersecurity experts with decades experience in both the public and private sector. The Administration worked expeditiously, but methodically, to put together Executive Order 14028, which President Biden signed just over one year ago.

This Executive Order represents a landmark effort to transform Federal cybersecurity by modernizing Federal agency cyber practices, strengthening supply chain security, and improving incident response and information sharing, among many other necessary enhancements. Security experts have hailed this Executive Order as a historic action to protect our Federal government networks, while using the Federal government's purchasing power to lift the cybersecurity baseline for the private sector.

Now that the initial deadlines set by the Executive Order have largely passed and the relevant agencies have had a year to implement its mandates, I look forward to the discussion today on what has been achieved so far and what the strategy is for continued implementation going forward.

High-profile cyber incidents and the concerns about of Russian cyber activity associated with the ongoing conflict in Ukraine has made the importance of cybersecurity a front-page story. But this isn't the first time cybersecurity issues have captured headlines. And it isn't the first time Congress and the Executive Branch have committed to prioritizing cybersecurity and modernizing security policy.

Historically, however, government focused has shifted after the headlines fade, and we have suffered the consequences. For example, in the aftermath of the 2015 OPM breach, Congress passed the Federal

Cybersecurity Enhancement Act, which included mandates for agencies to implement multi-factor authentication and encryption. But not all agencies have not complied. We must ensure that we do not lose focus and momentum this time. Fortunately, I am confident that the Biden Administration shares my commitment to ensuring we continue to accelerate our efforts to protect Federal networks.

Today, I hope to hear more about how this subcommittee can partner with the Administration to provide the necessary resources and authorities to continue the Executive Order's work. I also look forward to hearing more about how CISA has utilized the $650 million in funding Democrats in Congress included in the American Rescue Plan to strengthen our Federal cybersecurity.

I know our witnesses agree that it is a down payment on much-needed sustained investment in Federal cybersecurity, and we must continue to build on it by ensuring CISA has the necessary resources to modernize its National Cybersecurity Protection System and continue to mature its Continuous Diagnostic and Mitigation Program. Cybersecurity must be a priority for every single agency, but the ones represented here today have the expertise that other agencies may lack.

Continuing to build out CISA's role as the operational lead for Federal network security is a priority for me, and today's hearing will be an important opportunity to hear from the witnesses on how their agencies can better support the cybersecurity needs of the entire Federal enterprise.

# # #

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