COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience

February 10, 2021

We are here today to begin what I hope will be a bipartisan endeavor in the 117th Congress – making cyberspace more secure and networks more resilient. During the Trump Administration, Federal efforts to raise the national cybersecurity posture were stunted by a lack of steady, consistent leadership from the White House. In contrast, from Day One, President Biden has treated cybersecurity as an urgent national and economic security issue.

The President has started by surrounding himself with experts to spearhead sound cybersecurity policy. He has already confronted Vladimir Putin about Russian election meddling and the SolarWinds compromise and has publicly committed to an aggressive stance on China. Further, to bolster the cybersecurity of Federal networks, the President included much-needed funding for cybersecurity and technology modernization in the American Rescue Plan proposal. Thankfully, Congress now has a willing and able cybersecurity partner in the White House, and I am optimistic about the progress we can make.We must work quickly to make up for lost time.

Our witnesses today are a seasoned group of cybersecurity experts, many of whom recently served in government and made important contributions to our national cybersecurity posture. They are here to tell us about the challenges we face and how to chart a course toward cyber defense, deterrence, and resiliency. In the not-too-distant past, when our witnesses were serving in government – most of us had never heard of SolarWinds, but now it dominates cybersecurity conversations.

Late last year, we learned that Russian actors breached targeted Federal networks and critical infrastructure, in part through sophisticated supply chain compromise of the SolarWinds Orion platform. For almost a year, Russian actors burrowed into networks, hiding their tracks and patiently stealing data. Although we are engaged in an in-depth investigation with other key House Committees to learn more about this malicious Russian campaign, we know enough to begin asking difficult questions and start correcting course.

For instance, we know that it will take months to fully understand the scope and impact of the compromise and eradicate bad actors from our networks. We also know that despite prior significant investments in Federal network security and active defense, the Russian campaign evaded detection. The task before us is to zero in on how can we mature our defenses to match the capabilities of our adversaries.The Russian SolarWinds campaign threatens our nation and cannot be tolerated.

It is evident that prior responses to cyberattacks such as “naming and shaming,” sanctions, and indictments have not deterred bad actors from engaging in malicious cyber behavior that threatens our national security. I am interested in hearing from the witnesses how can we deter this behavior or raise the cost of it. We must also be mindful that not every cyberattack is a sophisticated one carried out by a well-resourced nation-state actor.

Cyber criminals – ranging in sophistication — continue to wreak havoc on State and local governments and private sector critical infrastructure with less mature cybersecurity capabilities. Just this week, for example, a hacker breached a water treatment facility in Florida and attempted to poison the water supply. This follows a year when cyber criminals hacked schools, hospitals, and workplaces transitioning to remote work. According to McAfee, cybercrime cost the global economy $1 trillion in 2020.

The Federal government must work to raise the baseline cybersecurity posture across government entities and the private sector to reduce avoidable, opportunistic attacks. This will free up talent and resources to focus on more sophisticated problems. We must also do as President Biden has done and treat cybersecurity as a central national security priority and not a “boutique add-on.”

To be sure, today is just the first of several hearings this Committee will hold on the cybersecurity threats facing the nation and how the government and private sector should work together to address them.

# # #

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