COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021

September 1, 2021

Earlier this year, this Committee held a joint hearing with the Committee on Oversight and Reform to examine the SolarWinds supply chain attack. Our oversight revealed a number of gaps in Federal authorities, policies, and capabilities that Congress must address to secure its own networks and better serve its private sector partners. But what stood out to me was how lucky we were that FireEye disclosed that it had been compromised. Where we would be if they had chosen not to?

At the hearing, I asked whether we would benefit from implementing a mandatory cyber incident reporting framework. Microsoft President Brad Smith observed that today "information is siloed" and that we need "one entity is in a position to scan the entire horizon and connect the dots between all of the attacks or hacks that are taking place."

SolarWinds President Sudhakar Ramakrishna testified: "[h]aving a single entity to which all of us can report to will serve the fundamental purpose of building speed and agility," and argued that private enterprises "should be instructed with reporting requirements and be made part of this community vision where public and private sectors can work together on addressing this issue." At the same hearing, FireEye CEO Kevin Mandia testified about the importance of centralizing intelligence to "improve the speed at which that picture and vision will come together." That hearing convinced me that Congress must act to ensure the Cybersecurity and Infrastructure Security Agency (CISA) receives timely cyber incident information from critical infrastructure owners and operators.

Since then, I have worked with Chairman Thompson and Ranking Member Katko to draft legislation to establish a mandatory cyber incident reporting framework at CISA and I would like to thank them both for their support in this effort. The draft legislation we are discussing today is the product of months of dialogue with government officials and private sector stakeholders.

I want to express my gratitude to those who worked with the Committee to provide feedback on various drafts of the legislation. We have worked hard to draft the legislation in a manner that will result in the greatest security impact for both the Federal government and the private sector, and I am proud of the draft we have developed. Our bill would direct CISA, after a 270-day period with mandatory windows for stakeholder consultation and comment, to issue an interim final rule describing:

- which critical infrastructure owners and operators are subject to the reporting requirement.
- which cyber incidents need to be reported.
- the mechanism for submitting reports.
- and other details necessary for implementation.

Importantly, our bill seeks to establish this new mandatory reporting program in a way that sets it apart from CISA's voluntary cyber programs by establishing a new Cyber Incident Review Office and tasking this new office with the discrete mission of receiving, aggregating, analyzing, and securing cyber incident reports. The bill also aims to ensure that covered entities benefit from the new reporting requirement in three ways:

- First, our bill requires CISA to publish quarterly reports with anonymized findings to provide better situational awareness to its partners.
- Second, it directs CISA to identify any actionable threat intelligence that should be shared rapidly and confidentially with cyber 'first responders' to prevent or respond to other attacks.
- Third, it requires CISA to notify private sector entities that may have been impacted by data breaches or intrusions on Federal networks.

I am pleased with the progress we have made on this legislation but want to be clear that our work is ongoing. We remain open to additional questions and feedback because it is important to get this right. In recent days, I have been asked whether we would consider compliance challenges that certain small businesses may have. I want to be clear that we do not expect all critical infrastructure owners and operators to be subject to this reporting requirement – rather we expect it to apply only to a subset. That said, I would certainly be happy to explore whether we need to add language directing CISA to provide additional compliance assistance to small businesses that are determined to be covered entities.

# # #

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