COMMITTEE ON HOMELAND SECURITY

**FOR IMMEDIATE RELEASE**

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

## Joint Hearing - *Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign*

**February 26, 2021**

Just over two months ago, we learned that a state actor - likely Russia - had engaged in a large-scale cyber campaign, infiltrating government and private sector networks and burrowing inside them. By the time FireEye voluntarily shared information about the breach of its network, the Russian actors had established a presence on victim networks, undetected, for nearly a year. That is hardly comforting.

While this campaign is notable for its patience, persistence, scope, and scale, the methods and tools used - though sophisticated - are not entirely new. NotPetya, a 2017 destructive supply chain attack with a global impact, involved Russian actors compromising Ukrainian tax preparation software to access victim networks. The same year, security researchers published their findings regarding an attack vector using forged SAM-L tokens. Nevertheless, the Federal government and the private sector were caught flat-footed.

I do not mean to diminish the complexity of the attack or to suggest we could have prevented it. But I want to make the point that our collective failure to make cybersecurity a central component of our national security – and invest in it accordingly – contributed to the success of the campaign and the difficulty we face in understanding its impact. In short, past warnings of what could come failed to trigger a meaningful shift in our approach to security.

My goal in our joint investigation is to move beyond admiring the complexities of this campaign and the challenges associated with stopping one like it and start charting a path forward. In the 15 years I have served on the Homeland Security Committee, one thing has become clear: We can't become so consumed by preventing the last attack that we're blind to the threats of the future. Instead, we must identify systemic opportunities to improve our ability to prevent, defend against, mitigate, and raise the costs of all malicious cyber activity.

Toward that end, I hope to identify a combination of near-term fixes and longer-term structural solutions that will improve our ability to better understand the adversary, defend our networks, and identify attacks more quickly. None of the witnesses here today can have a conversation with me, or with the Cybersecurity and Infrastructure Security Agency, about malicious activity occurring on an agency network because of restrictions agencies add in their contracts. That unnecessarily complicates our oversight work, limits CISA's situational awareness, and slows recovery. I believe that is a problem we can fix quickly.

In recent days, I have been encouraged to learn of growing interest in enacting a cyber incident reporting law. Former Chairman of the Cybersecurity Subcommittee Cedric Richmond authored an amendment included in the House-passed National Defense Authorization Act that would have established a cyber incident notification requirement. Unfortunately, we were unable to reach agreement with our Senate counterparts, but we look forward to trying again this year and hope we can enact cyber incident notification legislation in short order.

In the longer term, we must figure out how to make security a value proposition, not only for policy makers, but for investors and the private sector who are focused on earnings. We must address persistent challenges in threat information sharing and find more strategic ways to effectively leverage the unique capabilities of the government and private sector in our shared goal of better security.

In that vein, it may be time to reassess the obligations of large, highly resourced companies with outsized footprints in our economy and our government, and evaluate whether more should be expected of them. And we need to find ways to change behavior in the private sector – particularly those in the government supply chain – so executives value security as much as earnings statements and fast product roll outs. I look forward to candid conversations about these issues today.

Before I close, I want to thank our witnesses for being here today. Since December, I have been impressed by the degree of transparency in their conversations with us. It is important to have a complete record of what happened and how, so we can have a candid conversation about what needs to change.

# # #

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