CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

Opening Statement of Chairwoman Carolyn B. Maloney
Hearing on "Cybersecurity for the New Frontier: Reforming the Federal Information Security Management Act"
January 11, 2022

Today, we are discussing the urgent need to improve the federal government's defenses against cyberattacks.

Over the past year, we have seen devastating cyberattacks against federal agencies, state and local governments, and businesses. These attacks have caused real world damage—like stolen intellectual property, hundreds of millions of dollars paid in ransoms, and even shutdowns of critical infrastructure like oil pipelines.

Many of these attacks were carried out by America's geopolitical adversaries. Last January, a group of Chinese hackers unleashed a massive cyberattack that ripped through computer networks around the globe through Microsoft software. The attack spread to as many as 60,000 U.S. organizations, including businesses, hospitals, schools, and city governments, and posed a grave risk to federal agencies.

According to FBI Director Christopher Wray, economic espionage from China is, "the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality."

Director Wray has explained that this information theft amounts to, "one of the largest transfers of wealth in human history."

Federal agencies are also still reeling from the SolarWinds breach, in which Russian actors infiltrated and roamed the networks of at least nine agencies and a hundred private companies for months.

And today, we're dealing with the fallout from the Log-4-J software vulnerability, which the Director of CISA, Jen Easterly, described as the most serious vulnerability she's seen in her decades-long career.

The mounting attacks by China, Russia, and other bad actors are constantly changing. They are as dynamic as they are diabolical.

Today, we will be discussing how the federal government can protect itself against these threats.

The Federal Information Security Management Act, commonly known as FISMA, establishes a cybersecurity framework for the federal government. It's the best defense our federal information networks and supply chains have against cyberattacks. But the reality is that it's simply not enough to protect us in its current form.

Threats have transformed dramatically since FISMA was last updated in 2014, and in ways that were unimaginable when the law was first written twenty years ago.

Now, it's no longer enough to guard our networks at their perimeters, as was the focus in the past. Today, we must also guard within the perimeter, continuously monitoring for the smallest trace of abnormal activity that might signal an intruder. **Modernization cannot wait, because our adversaries certainly won't. And we're already woefully behind.**

Congress must reform FISMA and create a cutting-edge, whole-of-government approach to meet the challenges of the constantly evolving cyber frontier. That's why today, Ranking Member Comer and I are releasing a discussion draft to modernize FISMA, called the Federal Information Security Modernization Act of 2022.

The bill would improve the cybersecurity of federal networks through a risk-based approach that uses the most advanced tools, techniques, and best practices. It would also clarify and streamline the responsibilities of federal entities so they can respond quickly and decisively to breaches and major cyber incidents. By modernizing the law and focusing it on the most important security outcomes, we can ensure that federal agencies are better equipped to combat the evolving threats they face.

Our bill contains key similarities to its companion legislation in the Senate, which was introduced by our counterparts, Chairman Gary Peters and Ranking Member Rob Portman. I applaud their bipartisan leadership on this critical issue.

Our Committee has a strong, bipartisan track record of shining a light on the country's cybersecurity challenges and fighting to improve federal information technology.

Last year alone, we held hearings on ransomware attacks, the SolarWinds breach, and the hundreds of open recommendations by the Government Accountability Office to improve cybersecurity in the federal government.

Our Committee was also instrumental in creating the role of the National Cyber Director, who serves as the President's top advisor on cybersecurity and has a crucial role to play in the FISMA framework.

I also want to recognize our Government Operations Subcommittee Chairman, Mr. Connolly, for his crucial work on federal IT. He has led the charge on H.R. 21, the FedRAMP Authorization Act, which will enhance security and modernize cloud computing government-wide. That bill passed the House on suspension last year, and Chairman Connolly has my full support in encouraging the Senate to pass it, so it can reach the President's desk as soon as possible.

I want to extend my thanks to the witnesses for being here today, and to Ranking Member Comer for his partnership and diligence in working on the discussion draft with me. **We are committed to perfecting the bill together, and I'm confident that today's hearing will help our bipartisan, bicameral coalition get this priority across the finish line this year.**

###

Contact: Nelly Decker, Communications Director, (202) 226-5181