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 "Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats"
November 16, 2021

This has been an unprecedented year for cyberattacks. The country is still reeling from last year's cyberattack against the company SolarWinds that was linked to Russia and infected numerous federal agencies. These attacks have been described as a wake-up call for America.

Just this weekend, it was reported that the FBI—our premier law enforcement agency for investigating cybercrimes—was itself the victim of a hack that allowed emails to be sent from FBI email servers disguised as genuine FBI emails.

In short, we are at a tipping point as cyberattacks have become more common and potentially more damaging.

Several recent attacks have used a type of malicious software known as ransomware, which encrypts a victim's system and demands a payment in exchange for restoring access or refraining from publishing stolen data.

This is especially dangerous because it can shut down an entire system and can cause chaos in a community, an industry, or even the entire country. And cyber criminals are now demanding—and receiving—more money than ever.

In March, CNA Financial, an insurance company, reportedly paid the largest known ransomware payment ever, a staggering $40 million dollars.

In May, ransomware criminals from eastern Europe attacked the company Colonial Pipeline, resulting in the shutdown of more than 5,500 miles of gasoline pipeline spanning from Texas to New Jersey, and causing temporary gas shortages up and down the East Coast. The cost to unlock the system was $4.4 million dollars.

Also in May, JBS Foods, one of the largest meat suppliers in the United States, shut down its plants when it suffered a ransomware attack. The cost to unlock their system was $11 million.

In June, this Committee launched an investigation out of concern that these multi-million-dollar ransom payments would equip cyber criminals with even more financial resources and encourage future attacks.

Today, the Committee issued a staff memo with some of the Committee's preliminary findings.

We found that these attacks often stemmed from minor security lapses, even at companies with seemingly robust cybersecurity. Our report also highlights the importance of clearly established federal points of contact for companies to avoid wasting precious time when an attack is underway. Finally, we found that companies faced substantial pressure to pay these ransoms quickly, making it harder to stop these attacks.

And it is not just large companies that are targeted. Ransomware also harms small businesses, hospitals, schools, and local governments.

Since taking office, the Biden Administration has made countering ransomware a top priority. This included bringing together 30 nations for a White House summit last month, to discuss strategies to combat this threat. It also means taking a tougher line on countries, including Russia, that harbor cyber criminals.

The Biden Administration has also dedicated significant law enforcement resources to take ransomware networks offline and bring criminals to justice. Just last week, the Department of Justice announced criminal charges against two foreign nationals connected to the prolific ransomware criminal group, R-Evil. DOJ also recovered more than $6 million dollars in ransom money paid.

This is a good start, but we cannot afford to let up on our efforts. Congress must ensure coordination of anti-ransomware efforts across the entire federal government and between the public and private sectors.

Last Congress, this Committee held a hearing on the need to establish a position at the White House to lead the federal government's response to cyber threats. I was proud that President Biden nominated Chris Inglis to serve as the first National Cyber Director this year, and that he is testifying before us today.

I also am pleased that the Infrastructure Investment and Jobs Act, which President Biden signed just yesterday, included $21 million in funding for the Office of the National Cyber Director.

This law, which House Democrats passed over the objections of most House Republicans, will also provide $1 billion dollars to help state and local governments shore up their cybersecurity so we can prevent ransomware attacks, and $100 million dollars to help critical infrastructure respond to significant cyber incidents.

And the Build Back Better Act will provide new resources to CISA to help enhance cybersecurity in both the public and private sectors.

Ransomware attacks are a grave national security challenge. Today we will hear from our witnesses about the "whole-of-government" effort needed to disrupt ransomware networks and how we can help businesses, state and local governments, and others to prevent, prepare for, and respond to attacks.

###

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