COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Combating Ransomware: From Our Small Towns in Michigan to DC

June 28, 2022

I am pleased that Intelligence and Counterterrorism Subcommittee Chairwoman Slotkin is holding this hearing on such a pressing issue, in her district with her constituents. It is so important for communities to be heard, and hearings like these are a part of the Committee on Homeland Security's process to safeguard the American people and the Homeland from all threats, including cyber threats.

Cybersecurity is a topic that Chairwoman Slotkin has championed since she came to Congress, and she has worked tirelessly to keep the people of Michigan safe from cybercrime. Given her extensive background in national security, she knows the threats we face whether at home, abroad, or in cyberspace. Her leadership led to new legislation that would provide cyber forensics training for State and local law enforcement and create a program to help ensure the government is prepared for a major cyber attack.

Her work leading this Subcommittee and as a member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation has focused on emerging digital security issues that affect all of us—from the way we use our banks to the safety of our children's schools to how we can protect ourselves from criminals' latest techniques. The Internet is wired into nearly every part of our life—our homes, our cars, our schools, our businesses. It has become as important a utility as water, gas, and electricity. But it has also become perhaps the greatest tool for criminal mischief and theft in history.

In what we call ransomware attacks, cybercriminals seize computer systems, data, and electronic devices with the expectation that victims will be willing to pay a ransom to regain access to their electronic systems. Ransomware attacks have surged both in frequency and in the amount demanded by hackers. In 2020, an estimated 2,400 governments, hospitals, and school districts in the U.S. were victims of ransomware attacks, and the average payment was $312,493. According to data from the Cybersecurity and Infrastructure Security Agency (CISA), reported losses continued to increase last year.

As ransomware tactics and techniques continue to evolve, we can expect more incidents and more losses unless we do something to address the root causes of the issue—both in government and the private sector. Thanks to the Biden Administration, we have a National Cyber Director working to coordinate all of the Executive Branch's work in cyber space.

The Administration has also ensured that CISA is working across government agencies to improve our collective defense and with the private sector to ensure it has the tools to detect, disrupt, and investigate cyber criminals. In Congress, the Committee on Homeland Security has championed several critical pieces of legislation to combat the ransomware threat, including bills that:

- provide $1 billion in grants to State, local, Tribal, and territorial governments over the next four years to enhance their cybersecurity preparedness.
- make cyber incident reporting mandatory including the disclosure to CISA of ransom payments within 24 hours.
- direct CISA to conduct a study on K-12 cybersecurity and provide cybersecurity recommendations to K-12 educational institutions, which have faced numerous ransomware attacks in recent years.
- authorize the Secret Service to continue training local, state, tribal, and territorial law enforcement on cybersecurity investigations and responding to cyber incidents, including ransomware.

I am grateful for Chairwoman Slotkin's leadership and that of her Committee colleagues on these important measures. Although the Federal government has made great strides in bolstering our defenses, as the threat of ransomware continues to disrupt many aspects of our daily lives, we must make sure that Americans know what resources are available to them – at both the Federal and State level.

It is imperative that the public knows how to keep themselves safe from ransomware attacks, and if they do fall victim to an attack, who they can reach out to for help. If your car is stolen or your home is broken into, people know to call the police or 911—but when it comes to cyber theft, that common knowledge of who to call for help is not broadly known. Today's witnesses — representatives from DHS and its cyber-focused component CISA, and the State of Michigan — are in a position to help us understand ransomware prevention best practices, and what to do and who to call when catastrophe strikes.

# # #

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