COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Field Statement of Intelligence & Counterterrorism Subcommittee Chairwoman Elissa Slotkin (D-MI)

Combating Ransomware: From Our Small Towns in Michigan to DC

June 28, 2022

I am happy to be here in my congressional district in East Lansing, Michigan—bringing Congress and the Subcommittee I chair to the people I serve. The purpose of today's hearing is to bring some of D.C.'s best minds on cybersecurity to my district to detail the critical work they are doing to keep ordinary Americans, like Michiganders, safe from an increasingly disruptive threat: Ransomware**.** Ransomware is a national security threat that has a direct impact on the lives of Michiganders.

First, some definitions: a ransomware attack is defined as a digital form of traditional ransom, whereby computer systems, data, and electronic devices are held hostage by a criminal or group seeking a ransom payment in order for an organization to regain access to its systems. They are often carried out by a criminal or criminal group operating with the support or tacit approval of a State government, known as a State actor. We have seen these State Actors in adversaries like Russia, China, North Korea, and Iran. Other times they are carried out by criminals operating purely on their own behalf, known as Non-State actors.

According to a 2022 Cyber Threat Report by SonicWall, an internet cybersecurity company, ransomware attacks in the U.S. rose by 98% last year to record high levels. And a separate report by the CyberEdge group found that nearly two thirds of ransomware victims paid the ransom to regain access to their systems and data. In Michigan alone, we have heard from the State's Chief Information Officer that hackers try more than 90 million times a day to get into the state's servers. Let me say that again: 90 million times a day.

Ransomware has become a kitchen-table issue for Michiganders. It affects the people and organizations we rely on everyday – as our schools, small businesses, hospitals, and other organizations have been threatened by – and have even fallen victim to – ransomware attacks. When I first started as a Member of Congress, town supervisors, mayors, and local officials all surprised me by raising protecting data as something they were deeply concerned about. They were right to be concerned. From my first day as your Congresswoman, we have seen significant ransomware attacks against our critical infrastructure, local governments, entire hospital systems and school districts, all the way down to local mom-and-pop small businesses.

As a nation, two high-profile ransomware attacks last year, one on the Colonial Pipeline and one on the JBS Meat Company, showed Americans how vulnerable our critical infrastructure can be to these attacks, and how damaging the consequences can be. But many ransomware attacks have been much more hyperlocal to Michigan's 8th district, and that is why I am hosting this hearing here in East Lansing as opposed to in Washington. We have seen entire cities and townships targeted in these attacks. Local governments have had to create entire new websites, new email addresses, and new software to resolve the attack. All things which cost time and resources.

In a February Detroit Free Press article, Sgt. Matt McLalin, who investigates cyberattacks in the State Police's cyber command center, said local and county governments make up a lot of the center's victims. "Every single week we are getting multiple reports of local governments who have been affected," McLalin said. When an entire local government can be taken offline by a cyber criminal operating across the world, we have a significant issue that needs to be addressed. It's not just governmental entities that have been affected, either.

Last fall, I met with school superintendents from across my congressional district in my office in D.C. I asked them to raise their hands if they or their students had been hit by a ransomware attack—and every single hand in the room went up. We have seen schools come under attack in Walled Lake, Monroe, Richmond, and across the state. Just last month, classes at Kellogg Community College were canceled for two days as school officials noticed some issues with the computer systems related to a ransomware attack.

Two years ago, Michigan State University was targeted by this increasingly prevalent type of cyber attack, which cost the university more than 1 million dollars to recover from. Cyber criminals operating in permissive environments like Russia and China—have launched attacks aimed at holding our kids' educations, their school records, and their futures hostage because they presume that schools and parents will pay virtually any cost to shield children from educational disruptions.

As I alluded to earlier, it is not just our schools and our kids who are threatened. Ransomware attacks have disrupted hospital systems, gas pipelines, and – as the workers at JBS's processing plant in Plainwell know, it has threatened our Nation's food supply and our farmers' livelihoods. Further endangering our nation's food supply, we have seen ransomware attacks targeting the manufacturers of agricultural equipment and the data they collect. Ransomware attacks are a threat to people from the smallest family farm to the biggest Fortune 500 company, but it is the ordinary American, the farmer, schoolteacher, and small business owner, who bears the brunt of these attacks.

Just this past weekend, I heard from constituents in Brighton that they were fundraising for the owners of a local bookstore in Detroit, which was hit by a cyberattack and was forced to personally cover over thirty-five-thousand dollars in losses. That business, still fragile from the impacts of the pandemic, is now facing the prospect of imminent closure as a result of the attack. Computer systems are complex. Small businesses and local governments are already stretched thin, and not everyone can afford to have cyber insurance or an IT and / or cyber specialist on the payroll to respond.

That is why today's hearing is so important. We designed this hearing to help connect the average person with experts who can help them protect themselves. People want to know where to go when they are the victim of a ransomware attack. Do they call 9-1-1? Do they call the FBI? Do they call the State Police? Where should people turn when they realize someone is trying to steal data that they are responsible for protecting? People want to know what to do when they turn on their computer or cash register only to find out they are locked out by hackers demanding large sums of money, often in the form of cryptocurrencies, that they can't afford.

I have heard from constituents across many different industries about how concerned they are about the threat of ransomware. They feel like it's their business, their data, that is on the frontlines facing this threat. They are especially concerned because they don't know what their government is doing to protect them. I don't just want to draw attention to the problem: I want to use this hearing to discuss the ways that we are keeping Americans on the frontlines of the ransomware threat and their data safe.

I am pleased to welcome witnesses who I know are working hard to combat ransomware and other cyber attacks every day, and who are eager to help us answer these questions. Visiting us from Washington are two representatives from the Department of Homeland Security (DHS) —Mr. Iranga Kahangama and Mr. Matt Hartman. Mr. Kahangama – who was integral to the Federal government's response to the ransomware attacks on Colonial Pipeline and JBS Foods – is responsible for cyber and infrastructure protection strategic planning and analysis at DHS. And at DHS's Cybersecurity and Infrastructure Security Agency or CISA, Mr. Hartman, works on the frontlines with partners at the State and local levels, as well as in the private sector, to defend against today's cyber threats and build security and resiliency.

On our second panel we will be hearing from one of our State's best cybersecurity experts — Mr. James C. Ellis, Commander of Michigan State Police's Cyber Command Center. I look forward to hearing from our witnesses on the critical work they are doing to defend our local communities, our state, and our country, from the rising threat of ransomware and how they are partnering with the private sector to build resilience to ransomware attacks before they occur, because we know that the best way to defend against a ransomware attack is to take steps to protect yourself before an attack occurs.

# # #

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