COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

A Whole-of-Government Approach to Combatting Ransomware: Examining DHS's Role

November 17, 2021

The threat of ransomware attacks is one of those rare national security issues where the high-level policy debate here in DC very directly connects to the tangible impact it's having on families back home in our districts, every day. Ransomware attacks against the United States have exploded in number and cost over the last few years, especially during the COVID-19 pandemic.

During a year when we've been more reliant on digital technology than ever, ransomware has disrupted half the fuel supply for the East Coast, and the world's largest meat processor — in addition to countless attacks on our hospitals, schools, police departments, and businesses. These attacks are overwhelmingly carried out by foreign groups, but their victims are our constituents. Ordinary Americans, not soldiers in tanks and planes, are on the front lines of this threat.

After the attacks on the Colonial Pipeline and JBS Foods, I'd find myself in rural communities in my district, talking about agriculture or education — and everyone from farmers to school superintendents would come up and ask me about what we were doing to protect them from this onslaught of attacks. We're seeing the impact of ransomware all over Michigan. During the peak of the pandemic last fall, a nationwide attack affected hospitals in St. Johns and Auburn Hills. And our schools have been hit particularly hard. Our state's leading insurer of K-12 schools told me that they've worked with forty-three Michigan school districts that have been hit by ransomware attacks, just since the start of 2019, and paid out millions of dollars in claims.

Earlier this month, K-12 superintendents from across Michigan told me that the ransomware risks they face have become so severe that, according to insurers, their schools may be uninsurable by the end of this school year. These attacks can be incredibly disruptive for schools: last summer, a ransomware attack on a single department at Michigan State University, which I represent, cost the university over a million dollars to recover from. The attack knocked labs and networks offline for months and caused the loss of over a year's worth of research data — forcing some researchers to start over from scratch. And when MSU refused to pay a $6 million ransom, the attackers leaked personal information affecting over 9,000 students.

I know all my colleagues on this committee have heard similar stories from their communities.
The ransomware threat isn't going away anytime soon. Over the last five years, we've seen the illicit infrastructure that enables ransomware attacks metastasize, and evolve into a new business model — "ransomware as a service." Under this new model, which enabled the attack on Michigan State University, criminals no longer need the technical skills to build ransomware themselves — they just agree to pay the ransomware developer a licensing fee, or a cut of the ransom.

As a result, ransomware has become an incredibly profitable business for international cyber criminals: between 2017 and 2020, we saw ransom payments increase from around $37 million annually, to over $406 million per year. Taxpayers and business owners, including the Michiganders I represent, end up paying those bills. As Secretary Mayorkas, Director Wray, and countless others have made clear, ransomware is a direct threat to our national security.

I was pleased to see the President lay down a marker with Vladimir Putin, in June: that we hold Russia responsible for stopping ransomware attacks coming out of its territory — regardless of who's conducting them — against the sixteen U.S. critical infrastructure sectors. I'm also pleased that the federal government is taking aggressive steps to combat these attacks and bring cybercriminals to justice.The Administration has required stronger cybersecurity across Federal agencies and vendors; given ransomware investigations similar priority to terrorism investigations; and engaged more than thirty countries to combat international cyber crime. And earlier this year, President Biden appointed the first National Cyber Director, to quarterback the federal response.

These efforts to go after attackers are starting to pay off: just last week, the Department of Justice announced the indictment and arrest of a Ukrainian national charged with deploying ransomware to attack U.S. businesses and government entities — as well as the recovery of over $6 million worth of ransom money. I'm also pleased that taking on the ransomware threat and strengthening our cybersecurity is still a largely bipartisan cause. On Monday, I was proud to join President Biden as he signed the bipartisan infrastructure bill into law — including a billion dollars in cybersecurity preparedness grants for State, local, tribal, and territorial governments.

I want to recognize my Committee partner, Chairwoman Clarke, for leading that provision — and I thank her for working with me to include language that will help innovative local cybersecurity partnerships, like the ones we have in Michigan, benefit from this transformative investment. For its part, the Department of Homeland Security has been a key player in Federal cybersecurity efforts and is at the center of the country's counter-ransomware efforts. We are fortunate to have witnesses before us today who can speak to DHS's contribution to this whole-of-government fight against ransomware.

I'm particularly interested in hearing about how the threat landscape has evolved — as well as how DHS is using its technical expertise, law enforcement and intelligence capabilities, and its industry and international partnerships, to take on this threat. I also look forward to discussing how DHS can help ensure that our local communities can access the resources they need, as quickly and easily as possible. This year has made clear that cybersecurity isn't just a tech issue — it's at the heart of protecting our daily lives. I look forward to today's discussion on how DHS is leading that effort.

# # #

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