COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Ranking Member Bennie G. Thompson (D-MS)

Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans

April 21, 2026

Today's hearing covers an important topic—the ongoing plague of cyber-enabled crimes that victimize Americans every day. Transnational criminal organizations have developed numerous ways to leverage technological advances to steal from Americans and enrich themselves, causing devastating harms to their victims and - at times - threatening our critical infrastructure.

Operating out of foreign countries where U.S. law enforcement has limited reach and funded through digital currencies that obscure their identities, these criminal gangs have proven resilient to many efforts to rein them in. Unfortunately, my home state of Mississippi recently experienced a ransomware attack that demonstrated just how devastating these transnational crimes can be.

Two months ago, the University of Mississippi Medical Center, the state's only Level 1 trauma center, fell victim to a ransomware attack, forcing doctors and nurses to revert to paper medical records, shutting clinics throughout the state, and canceling surgeries. The ransomware attack threatened patient safety and privacy and cost the hospital millions in lost revenue. Attacks like this one are not just criminal activity—they are national security threats, and preventing them requires coordination across government and industry.

We must continue to build on law enforcement efforts to investigate, prosecute, and sanction the criminals responsible for these incidents, which will require sustained investment in law enforcement agencies and in diplomatic efforts to improve cooperation with other countries on this global challenge. Doing so requires Federal law enforcement to prioritize these real threats to our security, not carrying out the President's personal political agenda. Additionally, we must invest in improving our defenses and educating the public on how to protect themselves from becoming victims of these crimes.

It is bizarre that at the same time as ransomware gangs are increasing their attacks on hospitals and other critical infrastructure, the Trump administration chose to force out roughly 1,000 employees at CISA and propose hundreds of millions of dollars in cuts to CISA's budget. Who hears about what just happened at the University of Mississippi Medical Center and thinks "Let's cut Federal resources for cybersecurity?" But, that's exactly what the Trump administration has been doing. And now, the President's recent executive order on preventing cybercrimes and scams directs CISA to expand efforts to defend state, local, tribal and territorial governments from cybercrimes.

The President can put out an EO saying whatever he wants to make it look like he is taking action on this problem, but actions speak louder than words. If the President were actually serious about expanding Federal support, he wouldn't have gotten rid of the people responsible for defending us.

Fortunately, unlike the President, this Committee has taken tangible action to counteract ransomware threats by establishing the State and Local Cybersecurity Grant Program and passing reauthorization legislation through the House last year. The Senate must step up and do the same.

Finally, if we are to truly get the threat of cyber-enabled crime under control, we must systemically secure the technology that enables them. We will never be able to prosecute our way out of this problem so long as criminals can operate out of parts of the world where law enforcement cannot reach them.

And we will never be able to defend against every cyber-enabled crime if we rely on under-resourced local governments, utilities, and small businesses becoming cybersecurity experts or if we expect every American to be able to distinguish between AI deepfakes and reality. These crimes are enabled by technology, and prioritizing security as technologies are developed and deployed can reduce risks to consumers. I thank this excellent group of witnesses for being here today and look forward to their testimony.

# # #

Media contact