Republican Leader Cathy McMorris Rodgers
Oversight & Investigations Hearing:
"Stopping Digital Thieves: The Growing Threat of Ransomware"
July 20, 2021
As Prepared for Delivery

RISE IN ATTACKS

In recent months, we have seen a significant increase in ransomware attacks coming from Russia.

- In May, DarkSide – a ransomware group operating out of Russia – attacked the Colonial Pipeline – which accounts for about 45 percent of the East Coast's fuel.

- In June, REvil [are-evil] – another ransomware group operating in Russian – attacked JBS USA, which temporarily knocked out plants that process roughly one-fifth of our nation's meat supply.

- Earlier this month, REvil [are-evil] executed another ransomware attack. This time on American IT management software company Kaseya [KUH-SAY-AH] – which affected hundreds of businesses across the globe.

While President Putin may not be directly connected to these attacks, he refuses to crack down on them.

White House Press Secretary Jen Psaki (saw-key) recently said that quote "responsible states do not harbor ransomware criminals."

Well, Mr. President, Russia is NOT a responsible state.

And greenlighting a pipeline for Putin after Russian cyber criminals attack one of our most critical pipelines certainly will not deter Russia.

But this threat is not unique to Russia.

We know the Chinese government engages in malicious cyber behavior too.

Just yesterday, the Biden administration publicly blamed hackers affiliated with China's main intelligence service for a far-reaching cyberattack on Microsoft.

While this administration must do more, I applaud them for taking this step and publicly addressing the threat China poses.

ADMIN RECENT ANNOUNCEMENTS

The White House also recently announced a cross-government task force to combat the rise in ransomware attacks.

President Biden's nominee to lead the Cybersecurity and Infrastructure Security Agency – Jen Easterly – was also unanimously confirmed.

These are all welcomed steps, but only if done right.

I caution this administration and this Congress from consolidating cyber at one agency.

Doing so is a wrong and dangerous approach because it weakens an agency's ability to leverage their expertise in cyber preparedness for their specific and unique sectors.

I urge the Biden Administration to lean on that expertise.

Director Easterly, I urge you to rely on your colleagues at HHS, DOE, the FCC, the FTC, DOT, and others to address cyber threats in their sectors.

E&C Cyber Work

As the Committee which oversees our economy's most critical sectors, we know firsthand the work many of these federal agencies have done on cyber.

This Committee itself has a history of working on cybersecurity issues to strengthen American defenses against bad actors.

The Committee has conducted significant oversight over cyber incidents dating back to the Target hack in 2013.

In 2017, we brought in the Equifax CEO to answer for the hack of their systems that resulted in the loss of 143 million Americans' personal information.

In 2018, following dozens of briefings, hearings, letters, reports, and roundtables, the Republicans on this committee issued a Cybersecurity Strategy Report that provided specific priorities for more effective protection against vulnerabilities.

Earlier this year, we sent bipartisan letters to the Department of Energy, the Department of Commerce, the U.S. Department of Health and Human Services, the Environmental Protection Agency and the National Telecommunications and Information Administration following the SolarWinds attack.

Cyberthreats and ransomware attacks will only continue to grow and it is important for this Committee to continue lead on cyber issues.

The Colonial pipeline attack underscored the Committee's long work to ensure the secure, reliable delivery of energy.

The *Pipeline and LNG Facility Cybersecurity Preparedness Act*, reintroduced by Energy Subcommittee Republican Leader Upton and Chairman Rush will provide DOE with strong, clear coordinating authorities to respond to future threats.

And soon, our Consumer Protection and Commerce Subcommittee Republican Leader Gus Bilirakis will introduce a bill to ensure the FTC is focused on ransomware attacks from abroad and working with foreign law enforcement agencies to hold those cybercriminals accountable.

Yet, there is more to do.

Energy and Commerce should continue to explore ways to identify and patch cybersecurity vulnerabilities before they are exploited...

...and we should also encourage reporting by entities of cyberattacks to the federal agencies who oversee them and consider certain liability protections for our critical infrastructure.

This is an important and timely discussion and I look forward to hearing from our esteemed witnesses. Thank you. I yield back.