Prepared Statement by U.S. Senator Chuck Grassley (R-Iowa)
Ranking Member, Senate Judiciary Committee
Hearing titled: America Under Cyber Siege: Preventing and Responding to Ransomware Attacks
Tuesday, July 27, 2021

I'd like to thank the Chairman for agreeing to hold this important bipartisan hearing on the problem of ransomware. I've appreciated working with you on this, and look forward to continuing to work together to combat cyber threats.

The threat we face from ransomware is increasing. Criminal actors are using techniques like phishing emails to gain access to the data of a business, a nonprofit, or a government. The criminal actors then lock the data down and demand that a large ransom be paid, usually in difficult-to-trace virtual currencies like Bitcoin.

Yet paying a ransom is no guarantee that the victim will have their data returned, or that they will not be re-victimized and asked to pay another ransom.

Earlier this year, FBI Director Chris Wray compared the challenges of fighting ransomware to those we faced after 9/11. Estimates on the amount of ransoms paid in 2020 run into the hundreds of millions of dollars. Ransomware has targeted schools, local governments, and, during this pandemic, even hospitals and healthcare providers.

In May, two massive ransomware attacks hit a critical supplier of gas, Colonial Pipeline, and a major supplier of meat, JBS. These events created very disturbing questions about the security of our supply of essential goods like fuel and food.

Since that time, I've received questions from many Iowans about what we can be doing as a nation, and as individuals, to fight the threat of ransomware. This hearing will help us to answer those questions.

Ransomware does not just affect the deeper pockets of large companies like Colonial Pipeline and JBS. An estimated three out of every four victims of ransomware is a small business. Small businesses already operate on thin margins, and many have been pushed to the brink by the pandemic. I'm glad we'll be hearing today what government agencies like the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security can do to help small business owners to practice good cyber hygiene to avoid ransomware attacks. We will also be hearing what investigators like the FBI and the Secret Service can do for those who have been victimized.

Ransomware often originates from countries with a permissive law enforcement environment that allows these cyber criminals to flourish. So-called "Ransomware as a service" is a business model, employed by criminal networks such as Darkside and REvil. Darkside and REvil are behind many of these recent ransomware attacks.

These criminal organizations work like illicit software providers, creating ransomware and leasing it to other criminal actors, known as “affiliates” for a share of the profits. We will be hearing from the Department of Justice how these criminal actors can be targeted and punished.

The situation would be dire enough if ransomware was used only by sophisticated criminal actors, in countries unwilling to help bring them to justice. However, just last week, the Biden Administration, and many countries which are allies of the United States, formally blamed China for a massive hack of the Microsoft Exchange email server. Hackers operating under the umbrella of China’s own Ministry of State Security appear to have used the hack to engage in ransomware schemes for their own profit. They may have extorted millions in ransom payments from U.S. victims.

I have spoken many times on the dangers of cyber attacks, theft of intellectual property, and other aggressive behavior by China. I fear ransomware will be a new method used by the Chinese Communist Party against Americans, and I will be pursuing opportunities to combat that danger.

I look forward to hearing more about what the Executive Branch agencies are doing to fight ransomware, and what we as a country can do, and I thank the witnesses for being here today.