CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

MEMORANDUM

November 10, 2021

To: Members of the Committee on Oversight and Reform

Fr: Committee Staff

Re: Hearing on "Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats"

On **Tuesday, November 16, 2021, at 10:00 a.m. ET,** the Committee on Oversight and Reform will hold a hybrid hearing in **room 2154 of the Rayburn House Office Building and on the Zoom video platform.**

I. BACKGROUND

Ransomware is a form of malicious software that enables cyber attackers to encrypt computer systems, deny access to data and systems, and extort victims for payment, usually in the form of cryptocurrency, in exchange for restoring access.[1] In recent years, ransomware has grown into a multi-billion dollar criminal industry as attackers have targeted private businesses, state and local governments, hospitals, school districts, critical infrastructure, and emergency services, such as police and fire departments.[2]

In 2021, there have been several high-profile ransomware attacks against private sector companies in critical industries, and many of these companies have made ransom payments.[3] In

[1] Cybersecurity and Infrastructure Security Agency, *Stop Ransomware: Resources* (online at www.cisa.gov/stopransomware/resources) (accessed on Oct. 27, 2021), *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021) (online at www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks).

[2] Department of Homeland Security, *Homeland Threat Assessment* (Oct. 2020) (online at www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf); National Cyber Investigative Joint Task Force, *Ransomware: What It Is and What to Do About It* (Jan. 2021) (online at www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf).

[3] *See, e.g.*, CNA Financial Corporation, *Formal Notice of Cybersecurity Incident* (July 9, 2021) (online at www.cna.com/web/wcm/connect/1077e9ef-e397-47f1-ad3c-27470e1b3fbc/July+9_Security+Incident+Update.pdf?MOD=AJPERES); *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, Bloomberg (May 20, 2021) (online at www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack).

May 2021, Colonial Pipeline suffered a ransomware attack connected to the cybercriminal group DarkSide, which is likely Russia-based, and paid $4.4 million in cryptocurrency to the cybercriminals.[4] As a result of the attack, Colonial Pipeline shut down 5,500 miles of pipeline on the East Coast for several days, which had far-ranging impacts, from gasoline shortages and delays, to skyrocketing gas prices, to major airlines canceling daily flights.[5] Also in May 2021, JBS Foods, one of the largest meat suppliers in the United States, paid $11 million in cryptocurrency to the criminal ransomware group REvil after a ransomware attack forced it to shut down all of its beef processing plants in the United States.[6] In July 2021, the Miami-based software company Kaseya was compromised by REvil, which led to ransomware attacks against Kaseya's customers, affecting between 800 and 1,500 businesses around the world, including schools, small businesses, and local governments.[7]

The Committee has been actively investigating this issue for more than five months. In June 2021, the Committee sent requests for documents and information to three companies that were hit with ransomware attacks and paid ransoms: Colonial Pipeline, JBS Foods, and CNA Financial.[8] In September 2021, Chairwoman Maloney and Ranking Member Comer sent a bipartisan letter to the Federal Bureau of Investigation asking about its strategy on ransomware and its response to a recent attack.[9] On November 8, 2021, the Department of Justice announced charges against two foreign hackers who are affiliated with the criminal ransomware group REvil, which is responsible for thousands of ransomware attacks, including on JBS Foods and

[4] *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall Street Journal (May 19, 2021) (online at www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636); Varonis, *Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign* (July 6, 2021) (online at www.varonis.com/blog/darkside-ransomware/).

[5] *Gas Pipeline Hack Leads to Panic Buying in the Southeast*, New York Times (May 11, 2021) (online at www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html).

[6] *JBS Paid $11 Million to Resolve Ransomware Attack*, Wall Street Journal (June 9, 2021) (online at www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781); *All of JBS's U.S. Beef Plants Were Forced Shut by Cyberattack*, Bloomberg (May 31, 2021) (online at www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs).

[7] *Updated Kaseya Ransomware Attack FAQ: What We Know Now*, ZDNet (July 23, 2021) (online at www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/); *FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers*, Washington Post (Sept. 21, 2021) (online at www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html).

[8] Committee on Oversight and Reform, *Press Release: Chairwoman Maloney Presses Private Companies to Provide Details on Ransomware Payments to Cybercriminals* (June 3, 2021) (online at https://oversight.house.gov/news/press-releases/chairwoman-maloney-presses-private-companies-to-provide-details-on-ransomware); Committee on Oversight and Reform, *Press Release: Chairwoman Maloney Expands Committee's Ransomware Investigation to JBS Foods* (June 11, 2021) (online at https://oversight.house.gov/news/press-releases/chairwoman-maloney-expands-committee-s-ransomware-investigation-to-jbs-foods).

[9] Committee on Oversight and Reform, *Press Release: Oversight Committee Seeks Answers on FBI's Handling of Widespread Ransomware Attack* (Sept. 29, 2021) (online at https://oversight.house.gov/news/press-releases/oversight-committee-seeks-answers-on-fbi-s-handling-of-widespread-ransomware).

Kaseya.[10] The Department also announced that it seized $6.1 million in ransom payments received by the attackers.[11]

II. HEARING PURPOSE

This hearing will examine threats that ransomware poses to the United States, including to our economy, public health, infrastructure, and national security, as well as the Biden Administration's whole-of-government efforts to disrupt criminal ransomware networks and help state and local governments and the private sector prepare for and respond to attacks.

III. WITNESSES

The Honorable Chris Inglis
National Cyber Director
Executive Office of the President

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Mr. Bryan Vorndran
Assistant Director, Cyber Division
Federal Bureau of Investigation

Staff contacts: Peter Kenny, Courtney Callejas, Arthur Ewenczyk, Trinity Goss, and Todd Corum at (202) 225-5051.

[10] Department of Justice, *Press Release: Ukrainian Arrested and Charged with Ransomware Attack on Kaseya* (Nov. 8, 2021) (online at www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya); *U.S. and Europe Crack Down on REvil Ransomware Group*, Wall Street Journal (Nov. 8, 2021) (online at www.wsj.com/articles/hackers-linked-to-ransomware-attacks-on-jbs-kaseya-arrested-in-romania-11636390527).

[11] *Id.*