Congress of the United States
Washington, DC 20515

October 8, 2021

The Honorable Merrick B. Garland
U.S. Attorney General
Department of Justice
Washington, DC 20530

The Honorable Janet Yellen
Secretary of the Treasury
Department of the Treasury
Washington, DC 20220

The Honorable Antony J. Blinken
Secretary of State
Department of State
Washington, DC 20520

The Honorable Alejandro N. Mayorkas
Secretary of Homeland Security
Department of Homeland Security
Washington, DC 20528

Dear Attorney General Garland, Secretary Yellen, Secretary Blinken, and Secretary Mayorkas:

We write to urge the Department of Justice (DOJ), the Department of the Treasury (Treasury), the Department of State (State Department), and the Department of Homeland Security (DHS) to pursue all options available to protect American communities and infrastructure from the growing threat of ransomware. In particular, we believe that stronger coordination between your departments is necessary, especially to address the role of cryptocurrency in facilitating ransomware attacks.

Ransomware attacks — which occur when a criminal entity uses malicious software to lock or encrypt a victim's computer system or files and demands a ransom payment to unlock the system or retrieve the files — are an increasingly difficult, dangerous, and expensive problem for government, private corporations, and small businesses across the country. In 2020 alone, the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) received reports of 2,474 ransomware attacks involving losses of over $29.1 million. This represents a 20% increase in reported ransomware incidents and a 225% increase in ransom amounts demanded by hackers since 2019.[1] Worse still, an estimated 70 to 75% of ransomware attacks continue to go unreported,[2] often out of fear that reporting an attack will bring bad publicity and, for publicly traded businesses, negatively impact share price.[3] The rapid rise in ransomware attacks not only financially impacts local governments and businesses, but also threatens U.S. national security because ransomware can disrupt critical infrastructure and capture sensitive data.[4]

---

[1] Federal Bureau of Investigation's Internet Crime Complaint Center, *Internet Crime Report* (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
[2] *Id.*
[3] Testimony of Bryan A. Vorndran, Assistant Director of the Cyber Division of the Federal Bureau Investigation, before the Senate Committee on the Judiciary (Jul. 27, 2021), https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf.
[4] United States Cybersecurity and Infrastructure Security Agency & the Multi-State Information Sharing and Analysis Center, *Ransomware Guide* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

The proliferation of cryptocurrency has facilitated this explosive growth in ransomware attacks, largely by offering easy, fast, and difficult to trace methods for laundering illicit gains.[5] We believe that increasing enforcement of existing money laundering and financial crimes statutes would play an important role in deterring ransomware attacks and facilitating the recovery of cryptocurrency paid to ransomware attackers.

We also recognize the practical and technological challenges involved in efforts to seize cryptocurrency ransoms. Many ransomware attacks originate in jurisdictions outside the reach of U.S. domestic law enforcement, requiring U.S. agencies to work with foreign partners and cryptocurrency exchanges in order to seize ransomware payments or other related assets.[6] More to the point, many threat actors reside in nations such as Russia, China, and North Korea, countries that have actively or tacitly supported ransomware attacks against the United States and interfered with U.S. efforts to expatriate cryptocurrency ransoms.[7] To address the growing threat of ransomware attacks, U.S. agencies must pursue a comprehensive enforcement approach involving both domestic and international partners.[8]

It is reassuring that, despite the technical and diplomatic challenges posed by ransomware attacks, your departments have recognized the urgency of protecting our communities and infrastructure from ransomware attacks. Recent efforts by DOJ to recover over $2.7 million in cryptocurrency following the Colonial Pipeline and NetWalker attacks are indeed encouraging. We also commend Treasury's Office of Foreign Assets Control for placing Suex, a virtual currency exchange, on its Sanctions List for Suex's role in facilitating ransomware payments.[9] We believe that expanding efforts to seize cryptocurrency ransoms and increasing the costs associated with facilitating ransom payments can certainly help deter ransomware attacks by decreasing their profitability and changing threat actors' incentives.

In order to now help us better understand how Congress can assist these and other efforts, we respectfully request that you respond to the following questions no later than October 29, 2021:

1) In what ways has the United States worked with partners within regional organizations and international organizations to attribute ransomware attacks and hold bad actors accountable?

---

[5] Greg Myre, *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks; Kristine Johnson and Michael Garcia, *Digital Currencies' Role in Facilitating Ransomware Attacks: A Brief Explainer*, ThirdWay.org (May 3, 2021), https://www.thirdway.org/memo/digital-currencies-role-in-facilitating-ransomware-attacks-a-brief-explainer.

[6] Statement of Bryan A. Vorndran, Assistant Director of the Cyber Division of the Federal Bureau Investigation, before the Senate Committee on the Judiciary (Jul. 27, 2021), https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf.

[7] *Id.*; *see also* Press Release, Department of Justice, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[8] We note that the President's recent announcement of an international summit on ransomware seems an excellent step in this direction. *See*, Statement by President Joe Biden on Cybersecurity Awareness Month (Oct. 1, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month.

[9] Department of the Treasury, *Publication of Updated Ransomware Advisory; Cyber-related Designation* (Sept. 21, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921.

2) How is the United States working with its close allies to develop norms and best practices around enforcement related to illicit financial transactions that utilize cryptocurrency?

3) How have your agencies coordinated with foreign counterparts to locate and repatriate cryptocurrency assets? For attacks implicating nations that have not signed a Mutual Legal Assistance Treaty with the United States, how have your agencies pursued recovering cryptocurrency ransoms?

4) In the past five years, how many attempts have been made to seize cryptocurrency assets from ransomware attackers? How many have been successful? Of these successful attempts, what obstacles have your agencies faced when attempting to recover the full amount of cryptocurrency ransoms?

5) Have any of your agencies considered sharing data with insurers to facilitate private subrogation actions against cryptocurrency exchanges or cyber criminals?

6) Would DOJ need specific statutory authority to direct asset forfeiture funds back into endpoint security and other cybersecurity defenses, or to provide assistance to victims?

7) How are cryptocurrency exchanges treated when they fail to adhere to Know Your Customer (KYC) or Anti-Money Laundering (AML) / Counter Terror Financing (CTC) practices?

8) What resources or authorities, if any, do your agencies need from Congress in order to better coordinate with partner nations on illicit activity facilitated through cryptocurrency exchanges or to seize ill-gotten virtual assets?

Thank you for your attention this important matter.

Sincerely,

Edward J. Markey
United States Senator

Sheldon Whitehouse
United States Senator

Ted W. Lieu
Member of Congress

James R. Langevin
Member of Congress