EMANUEL CLEAVER, II

FINANCIAL SERVICES COMMITTEE
NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT, AND MONETARY POLICY SUBCOMMITTEE
CHAIRMAN

HOUSING, COMMUNITY DEVELOPMENT, AND INSURANCE SUBCOMMITTEE

Congress of the United States
House of Representatives

FIFTH DISTRICT, MISSOURI

HOMELAND SECURITY COMMITTEE

SELECT COMMITTEE ON THE MODERNIZATION OF CONGRESS

HTTPS://CLEAVER.HOUSE.GOV

January 7, 2020

Steven Mnuchin
Secretary
United States Department of Treasury
1500 Pennsylvania Ave NW,
Washington, DC, 20220

Dear Secretary Mnuchin,

We write to request that financial regulators take all possible precautions to protect their existing financial infrastructure against possible cyber-attacks in the wake of recent threats against the United States and its interests by Iran and its allies.

On January 2, the Department of Defense confirmed that—at the direction of President Trump—the U.S. military took actions to kill Qasem Soleimani who commanded the Islamic Revolutionary Guard Corps-Quds Force. [1] Following this confirmation, Iranian Supreme Leader Ayatollah Ali Khamenei vowed "harsh revenge" for the killing of Soleimani.[2] This call for retribution against the United States was echoed by other members of Iranian Leadership and affiliated organizations worldwide. The Department of Homeland Security issued a bulletin on January 4 noting an elevated and imminent alert warning of a credible, specific, and impeding terrorism threat against the United States in response to Soleimani's death.[3] The Bulletin highlighted that "Iran maintains a robust cyber program and can execute cyber-attacks against the United States [and that Iran] is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure in the United States." [4] As evidenced from other cyber-attacks against our financial infrastructure and firms in recent years, the threat of a possible attack is wide-ranging and may come by way of formal and informal networks as well as lone actors.

As you are aware, the financial services sector globally has been a primary target for attacks by cybercriminals and state actors because of the significant value of the information available. Reports indicate that financial services firms are hit by security incidents 300 times more often

---

[1] "Statement by the Department of Defense." U.S. DEPARTMENT OF DEFENSE, 2 January 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/.

[2] III, Fernando Alfonso, et al. "Iran's Supreme Leader Vows Revenge for Death of Soleimani." CNN, Cable News Network, 4 Jan. 2020, https://edition.cnn.com/middleeast/live-news/baghdad-airport-strike-live-intl-hnk/h_996c3bed1255e7e3e30357771c7be380.

[3] "National Terrorism Advisory System Bulletin - January 4, 2020." Department of Homeland Security, 7 Jan. 2020, https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-4-2020.

[4] Ibid

PLEASE REPLY TO:

2335 RAYBURN HOB
WASHINGTON, DC 20515
(202) 225-4535 (PHONE)
(202) 225-4403 (FAX)

101 WEST 31ST STREET
KANSAS CITY, MO 64108
(816) 842-4545 (PHONE)
(816) 471-5215 (FAX)

411 WEST MAPLE AVENUE, SUITE F
INDEPENDENCE, MO 64050
(816) 833-4545 (PHONE)
(816) 833-2991 (FAX)

1923 MAIN STREET
HIGGINSVILLE, MO 64037
(660) 584-7373 (PHONE)
(660) 584-7227 (FAX)

PRINTED ON RECYCLED PAPER

than businesses in other industries.[5] Cybersecurity experts in recent days have warned specifically of Iranian hackers' capacity to "destroy important financial records."[6] Iran has previously targeted, attacked, and infiltrated U.S. financial institutions. Experts note that in 2012, following the Obama Administration's sanctions against the regime, Iran initiated a rash of denial of services attacks against Bank of America, JPMorgan Chase, and Wells Fargo among other financial institutions.[7] In 2014, Iran also destroyed company data at Sands Casino. Iran's previous attacks against other sectors has destroyed computers and temporarily endangered the international flow of goods.

In response to these heightened and credible treats as articulated by U.S. national security elements, we urge financial regulators to strengthen their existing financial infrastructure against possible cyber-attacks. We urge you, our nation's financial regulators, to work in coordination with appropriate law enforcement and regulated entities to increase sharing of appropriate cyber threat information. We request that your institutions communicate a strategy to further mitigate existing cyber vulnerabilities within our financial infrastructure by March 2020.

Thank you for your careful attention to this important issue and we look forward to your response.

Sincerely,

Emanuel Cleaver, II
Member of Congress

Gregory Meeks
Member of Congress

---

[5] Ungarino, Rebecca. "Cyberattacks Are 300 Times as Likely to Hit Financial Firms than Other Companies. A Sweeping New Report Finds They're Not Prepared. | Markets Insider." Business Insider, Business Insider, 20 June 2019, https://markets.businessinsider.com/news/stocks/cyberattacks-impact-major-threats-to-financial-firms-not-prepared-2019-6-1028296130.

[6] Marks, Joseph. "The Cybersecurity 202: U.S. Should Brace for Iran to Cross Red Lines in Cyberspace, Experts Warn." The Washington Post, WP Company, 6 Jan. 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/01/06/the-cybersecurity-202-u-s-should-brace-for-iran-to-cross-red-lines-in-cyberspace-experts-warn/5e123521602ff125ce5bbf7b/.

[7] Marks, Joseph. "The Cybersecurity 202: Here's How Iran Disrupted U.S. Businesses the Last Time It Launched Major Cyberattacks." The Washington Post, WP Company, 25 June 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/06/25/the-cybersecurity-202-here-s-how-iran-disrupted-u-s-businesses-the-last-time-it-launched-major-cyberattacks/5d1107dea7a0a47d87c56e27/.