FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

GREG WALDEN, OREGON
RANKING MEMBER

ONE HUNDRED SIXTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

January 15, 2020

Chad F. Wolf
Acting Secretary
U.S. Department of Homeland Security
Washington, DC 20428

Dear Acting Secretary Wolf,

We write to inquire about your efforts to ensure the security of American telecommunications networks in the wake of the killing of Iranian General Qasem Soleimani. Specifically, we request a briefing—in a classified setting if necessary—regarding what steps the Administration has taken to warn telecommunications providers of potential cyberattacks to critical communications networks and how the providers should prepare for and defend against such attacks. We similarly request an update on what mitigating and defensive efforts providers have already taken.

A militia group with ties to Iran first attacked an American military base in Iraq with rockets on December 27, killing an American contractor.[1] Two days later, the United States responded with air strikes. Following those airstrikes, the U.S. embassy in Baghdad, Iraq was stormed on New Year's Eve.[2] Shortly thereafter, the Pentagon confirmed a U.S. drone strike killed Qasem Soleimani outside the Baghdad airport on January 2.[3] Since that time, Iranian officials have vowed revenge,[4] and Iran has used conventional forces to strike American military

---

[1] *Timeline: How The U.S. Came To Strike And Kill A Top Iranian General*, NPR.Org (Jan. 4, 2020). (www.npr.org/2020/01/04/793364307/timeline-how-the-u-s-came-to-strike-and-kill-a-top-iranian-general).

[2] *Id.*

[3] *Id.*

[4] *"52 targets": Trump Tweet sparks Iranian Furor*, Axios (Jan. 5, 2020) (www.axios.com/trump-iran-cultural-sites-war-crimes-0c8a6f13-7c3d-4556-ac87-61f540dfeb83.html).

bases and, apparently mistakenly, shot down a commercial airliner it misidentified as a cruise missile.[5]

Iran has conducted cyberattacks against American businesses in response to U.S. Government actions in the past, and according to security experts, has the capability and motivation to do so again.[6] Such attacks may be conducted through communications networks—critical infrastructure that connects and enables businesses, public safety organizations, and government agencies.[7] We are concerned that Iran or its allies, or other entities wishing to take advantage of this situation, might retaliate by attacking U.S. communications networks or use such networks to attack other targets.

To protect the American people, the government must proactively work with industry to identify potential threats and aid carriers in the defense of critical communications infrastructure. It is paramount that the U.S. Government work with all network providers, and particularly smaller carriers and those that might not otherwise have the means or ability to defend against any attack. This is especially imperative in situations, like this one, where the Administration's actions foreseeably increase the threat of attack to vital U.S. networks and those who rely upon them.

Unfortunately, the Trump Administration made the shortsighted decision to eliminate the White House cyber coordinator position, which was responsible for overseeing cyber policy

---

[5] *Iran Fires Missiles at Iraqi Bases Hosting U.S. Troops*, Axios (Jan. 7, 2020) (www.axios.com/iran-rocket-attack-al-asad-soleimani-78d00f09-1208-491d-b382-f0c6e1fb5da9.html?stream=top&utm_source=alert&utm_medium=email&utm_campaign=alerts_all); *Ukraine Plane Shot Down Because of Human Error, Iran Says*, New York Times (Jan. 11, 2020).

[6] *The Cybersecurity 202: Get Ready for Serious Cyberattacks from Iran, Experts Say*, Washington Post (Jan. 13, 2020) (www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/01/13/the-cybersecurity-202-get-ready-for-serious-cyberattacks-from-iran-experts-say/5e1b7ef288e0fa2262dcbc70/); *Iran Has Shown a Talent for Cyberattacks, and Businesses May Be a Prime Target for Retaliation*, CNBC, (Jan. 3, 2020) (www.cnbc.com/2020/01/03/iran-has-shown-a-significant-talent-for-cyberattacks.html); *see also* Department of Homeland Security, National Terrorism Advisory System, *Bulletin: Summary of Terrorism Threat to the U.S. Homeland* (Jan. 4, 2020).

[7] *Critical Infrastructure Sectors*, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security (www.cisa.gov/communications-sector).

across the Federal government.[8] As a result, we request a briefing from the Department by February 5, 2020, to address the following questions:

1. What actions, if any, has the Administration taken to ensure private network operators are prepared for a potential cyberattack from Iran, its allies, or others wishing to take advantage of the current escalation of tensions?

2. When did the Administration take such action(s), if at all?

3. Whether in response to a specific Administration warning, the current escalation of tensions, or more generally, what actions have network providers taken to protect their networks from cyberattack by nation states, including Iran?

4. When did network providers take such actions, if any, and to what events were they responding?

5. Have network providers been subject to an increase in cyberattacks since January 2?

Thank you for your attention to this important matter. If you have additional questions, please contact Jennifer Epperson of the Majority Committee Staff at (202) 225-3641.

Sincerely,

Frank Pallone, Jr.
Chairman

Mike Doyle
Chairman
Subcommittee on Communications
and Technology

[8] *White House Eliminates Cybersecurity Coordinator Role*, New York Times (May 15, 2018).