BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

April 23, 2020

The Hon. Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Director Krebs:

Ensuring the security of Federal telework infrastructure is a central factor in reducing cybersecurity risks related to the coronavirus. The Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) have warned of a wide range threats from malicious cyber actors that seek to exploit vulnerabilities associated with COVID-19.[1] I am writing to understand how CISA's current Trusted Internet Connections (TIC) guidelines[2] will ensure a safe and secure teleworking environment and utilize the full functionalities of Federal network protection programs.

In response to the coronavirus pandemic, Federal agencies have taken unprecedented measures to ensure the health and safety of workers and the general public. Compliance with social distancing measures issued by the Centers for Disease Control and Prevention (CDC) has required most agencies to implement mass telework policies on a scale not previously seen in the Federal government.[3] The drastic increase in telework presents significant security challenges. CISA's existing network security programs, tools, policies, and guidelines must all work together seamlessly to protect Federal information systems and data.

---

1 CISA, *Alert AA20-099A COVID-19 Exploited by Malicious Cyber Actors* (Apr. 8, 2020), https://www.us-cert.gov/ncas/alerts/aa20-099a [hereinafter *Alert*].

2 *Trusted Internet Connections*, CISA, https://www.cisa.gov/trusted-internet-connections (last visited Apr. 15, 2020).

3 Joseph Marks, "The Federal Government May Be About to Engage in the Biggest Telework Experiment Yet. But Hacking and Other Cyber Dangers Pose Serious Challenges," *The Washington Post* (Mar. 13, 2020) https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/03/13/the-cybersecurity-202-the-coronavirus-could-force-government-officials-to-work-remotely-that-raises-a-slew-of-cyber-dangers/5e6a953b602ff10d49aca406/.

The TIC program was originally instituted to reduce the number of access points to the public internet available from Federal networks.[4] Funneling network traffic through these points allows for the strategic placement of network security tools to guard against cybersecurity vulnerabilities. However, there is a lack of information detailing whether these tools operate adequately with heavy use of virtual private networks (VPNs), a capability that has significantly increased due the increase in telework.[5] CISA recently released interim teleworking guidance that seeks to address this very problem.[6] However, there are still questions as to whether this guidance goes far enough in addressing potential gaps in telework cybersecurity.

The April 8, 2020 alert issued by DHS and NCSC paints a grim picture of the COVID-19-related cybersecurity threats.[7] Exploits of teleworking infrastructure, various phishing campaigns, and other social engineering methods designed to compromise Federal networks and information create an extremely risky environment for Federal employees who are teleworking.[8] Those risks are only exacerbated if the capabilities of Federal network protection programs cannot be adequately employed in a remote environment.

This crisis has created an opportunity for malicious cyber actors to compromise Federal networks, and CISA's Federal network security programs are more important now than ever. Accordingly, pursuant to Rule X(3)(g) and Rule XI of the Rules of the House of Representatives, I respectfully request that you provide the following no later than May 8, 2020:

1. How does the drastic increase in telework impact the effectiveness of Federal network protection programs like CDM and EINSTEIN?
2. If devices are connecting to cloud service providers through home or public wifi, without being routed through VPNs, can CDM and EINSTEIN still be effective?
3. How is CISA ensuring that personal devices that connect to Federal networks are not being used as attack vectors by malicious cyber actors?
4. How much of the current network traffic is not being routed through tools that provide anti-phishing, DMARC, and other risk mitigation protections?
5. In response to the substantial increase in telework, CISA released interim guidance for TIC 3.0 that will expire at the end of the year. To what extent have agencies begun to submit TIC 3.0 use cases pursuant to the OMB Memorandum that was released in September 2019.
6. The interim guidance that CISA released is optional. How can CISA ensure that agencies are adopting best practices to ensure the security of the .gov from COVID-19 related threats?

Thank you for your attention to this important subject.

---

[4] Chris Jaikaran, *Federal Telework During the COVID-19 Pandemic: Cybersecurity Issues in Brief*, Congressional Research Service (Apr. 10, 2020) 8, https://www.crs.gov/reports/pdf/R46310.
[5] *Id*. at 8.
[6] Trusted Internet Connections 3.0 Interim Telework Guidance, CISA, https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf (last visited Apr. 14, 2020).
[7] *See, Alert*.
[8] *Id.*

Sincerely,

Bennie G. Thompson
Chairman
Committee on Homeland Security