MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

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

May 23, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Director Easterly:

The Committee on Homeland Security (Committee) is conducting oversight of the threats posed to the United States' information and communications technology (ICT) supply chain within our federal civilian and private sector systems, and the role of the Cybersecurity and Infrastructure Security Agency (CISA) as the Information Sharing Agency (ISA) for the Federal Acquisition Security Council (FASC) to address these risks.

We write to follow up on the letters sent to the Department by Members of the Committee regarding threats posed to the U.S. ICT supply chain, specifically by the Chinese Communist Party (CCP).[1] We remain concerned the CCP exerts undue influence on our ICT supply chain but remain confident in the authorities Congress granted the FASC to mitigate this risk.

Given the role of the Department of Homeland Security (DHS), and specifically CISA's role as the ISA on the FASC, we urge you to consider exploring the CCP's use of source code, including where it is located, how it is updated, and who has access to it, to infiltrate and maintain access to federal civilian and critical infrastructure ICT supply chains.[2]

The 2023 Annual Threat Assessment of the U.S. Intelligence Community (IC) states, "Globally, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years."[3] This assessment by the IC makes clear the threat. To combat it, we must ensure companies who wish to do business with the United States Government and critical infrastructure take action to ensure their products are not compromised as a result of business dealings in China that may require sharing or review of source code by the CCP.

---

[1] Letter from John Katko et al, Ranking Member, H. Comm. on Homeland Sec., to Alejandro Mayorkas, Secretary, U.S. Dep't of Homeland Sec. and Gina Raimondo, Secretary, U.S. Dep't of Commerce (Apr. 13, 2021) (on file with author); Letter from John Katko et al, Ranking Member, H. Comm. on Homeland Sec., to Alejandro Mayorkas, Secretary, U.S. Dep't of Homeland Sec. and Gina Raimondo, Secretary, U.S. Dep't of Commerce (Jan. 11, 2022) (on file with author).

[2] 41 C.F.R. § 201-1.200 (2021).

[3] U.S. DIR. OF NAT'L INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2023).

Article 7 of the People's Republic of China's National Intelligence Law, as amended in 2018, states, "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."[4] Under this law, Chinese companies and companies who do business in China, such as ByteDance, and therefore TikTok America, are required to hand all data in its possession to the Chinese government if asked, including source code. TikTok is just one example—the pervasiveness of this issue spreads far and wide within the ICT supply chain and has the potential to increase systemic risk across critical infrastructure sectors.

To assist the Committee with its oversight of the threats posed to the U.S. ICT supply chain, please provide a staff briefing as soon as possible, but no later than 5:00 p.m. on June 23, 2023 to address the following questions:

1. What is CISA's role as the ISA for the FASC?
    a. What is CISA's role specifically on the FASC supply chain and risk management Task Force (Task Force)?

2. What is your assessment of the risk posed by exposing source code to the CCP?

3. In its role as the ISA for the FASC, has CISA collected any data or done any analysis to better understand the extent to which source code for software currently deployed in United States Government and critical infrastructure networks has been shared with or reviewed by the CCP? If not, why not?

4. What other foreign dependency risk factors is the FASC taking into account for purposes of making exclusion and removal orders?

5. What is the process for referring potentially concerning data points about the practices of ICT vendors to the FASC, and what safeguards will be installed around these processes?

6. What progress has been made on the Task Force to date? What planned activities do you have for the future?

7. How does CISA's work on the FASC Task Force relate to its work on DHS's ICT Supply Chain Risk Management (SCRM) Task Force?
    a. Are these efforts complementary or duplicative?
    b. Who is ultimately responsible for implementing ICT SCRM across both federal civilian and private sector systems?

[4] Press Release, U.S. Dir. of Nat'l Intelligence, NCSC Director Warns of Nation-State Cyber Threats to Law Firms In June 4 Remarks at ILTA LegalSEC Summit 2019 (June 7, 2019) (on file with author), *available at* https://www.dni.gov/index.php/ncsc-newsroom/item/2002-ncsc-director-warns-of-nation-state-cyber-threats-to-law-firms-in-june-4-remarks-at-ilta-legalsec-summit-2019.

8. As the Sector Risk Management Agency (SRMA) for both the Information Technology (IT) Sector and the Communications Sector, how does CISA work with the private sector to relay the urgency of this systemic risk and remove potentially compromised or vulnerable ICT from our critical infrastructure supply chains?

9. What challenges does CISA face in its role on the FASC, and as the SRMA for the IT and Communications sectors?

Thank you for your prompt attention to this important matter.

Sincerely,

ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity
and Infrastructure Protection

AUGUST PFLUGER
Chairman
Subcommittee on Counterterrorism, Law
Enforcement, and Intelligence

cc: The Honorable Eric Swalwell, Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection

The Honorable Seth Magaziner, Ranking Member
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence