United States Senate
WASHINGTON, DC 20510

October 11, 2018

President Donald J. Trump
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear President Trump:

We write to express our serious concern regarding recent reports of Chinese government efforts to physically manipulate computer servers used in the United States to allow illicit access. Given the seriousness of the alleged activities, it is the responsibility of the administration to ensure that hardware in use throughout the U.S. government does not contain devices capable of infiltrating networks containing sensitive information. If the problems raised in this report are true, this raises important questions about what steps the government should take to protect commercial servers used by American companies. When reviewed in light of the full range of Chinese government activities to compromise U.S. national security, these reports demand a strong response by the administration.

According to Bloomberg Businessweek, the People's Liberation Army (PLA) "designed and manufactured" microchips to be surreptitiously planted within the motherboards of servers assembled by Super Micro Computer Inc. (also known as Supermicro).[1] Elemental technologies, which has contracts to sell technology to U.S. national security agencies, installed these motherboards in servers eventually used by the Central Intelligence Agency and the Department of Defense. This Chinese government effort also is alleged to have affected at least 30 companies.

We are concerned that the PLA tampering could have effects more extensive than has been reported. According to the media report, a former U.S. intelligence official familiar with the Supermicro case said that "attacking Supermicro motherboards is like attacking Windows. It's

[1] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2&utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

like attacking the whole world."[2] If true, the U.S. government servers, networks, and the sensitive information they contain could be compromised by a country that poses a significant strategic challenge to the United States. Additionally, any malicious PLA effort could have severe implications for the privacy of data for American consumers purchasing products from American technology firms.

To better understand this ongoing issue, we respectfully request your response to the following questions by November 2, 2018.

1. Does the U.S. government own and operate any computers, servers, or other information technology hardware or systems that contain Supermicro motherboards?
    a. As the Bloomberg report named the Central Intelligence Agency and the Department of Defense as government agencies that conducted business with Supermicro and Elemental, do those organizations continue to operate equipment from these companies? If so, what steps have been taken or are being taken to identify risk posed by hardware implants, and ultimately mitigating risk, including by removing affected equipment?
    b. Are there other agencies that have purchased, or are planning to purchase, equipment that contain servers with Supermicro motherboards? If so, do they agencies continue to either use this equipment or proceed with the purchases?

2. If equipment from those companies are operating within U.S. agencies and private technology firms, what efforts has the U.S. government taken to ensure that they do not contain illicit microchips capable of compromising sensitive information about either the government, companies, or citizens?
    a. When did the government become aware of the illicit microchips, and what steps did the government take to alert U.S. agencies and private technology firms?
    b. Has the U.S. government conducted thorough investigations of motherboards and hardware from other companies that could also contain illicit microchips or other technologies designed to penetrate networks?
    c. If not, what steps is the government taking to ensure that such devices do not make it into U.S. agencies, offices, or other official locations?
    d. Recognizing the difficulty of detecting "hardware hacks," what is the U.S. government's long-term strategy to protect hardware from being penetrated by illicit microchips or similar technologies?

3. Do you know of other similar instances of the Chinese government infiltrating technology manufactured for end users in the United States?
    a. If so, and given the implications this might have on hundreds of millions of Americans, what steps is the U.S. government taking regarding the findings of

[2] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2&utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

previous investigations – or plans for investigations responding to this report – and what effect this would have on private citizens' data?

Thank you in advance for your attention to this matter.

Sincerely,

Edward J. Markey
United States Senator

Sherrod Brown
United States Senator

Catherine Cortez Masto
United States Senator