

United States Senate

WASHINGTON, DC 20510

October 9, 2018

Mr. Charles Liang
Super Micro Computer, Inc.
980 Rock Avenue
San Jose, CA 95131

Dear Mr. Liang,

On October 4, 2018, *Bloomberg Businessweek* published stunning allegations of sophisticated cyber espionage operations by the Chinese government purported to involve the tampering of computer hardware manufactured and distributed by Supermicro. If this news report is accurate, the potential infiltration of Chinese backdoors could provide a foothold for adversaries and competitors to engage in commercial espionage and launch destructive cyber attacks. As Members of Congress, we are alarmed by any potential threats to national security and have a responsibility to ensure our nation's sensitive networks are kept safe. We write to request information from Supermicro on these reported attempts to subvert its computer products to spy on the United States.

Bloomberg reported that the Chinese People's Liberation Army engaged in a sophisticated operation to insert malicious surveillance and data manipulation components onto server motherboards. Chinese intelligence agents reportedly deceived, bribed, and coerced Supermicro's third-party manufacturers and subcontractors to alter motherboard designs. These added components—while appearing to be innocuous, common chips to an observer—would have been complex backdoors, and could quietly provide the Chinese government the ability to exfiltrate confidential data and bypass security controls on the nation's most sensitive systems.

According to *Bloomberg's* report, the infected servers were found in almost 30 companies, including important financial institutions, government contractors, and technology companies. Moreover, the operation was reportedly not found until Apple and Amazon detected abnormal network traffic and undocumented hardware components in audits of their networks and systems. When *The Information* reported in February 2017 on Apple's decision to end its contract with your company, Supermicro's senior vice-president of technology, Tau Leng, told the publication that malicious firmware from an outside manufacturer was found and committed to an independent investigation.

We note that Supermicro, Apple, and Amazon have issued strong denials regarding the *Bloomberg* report. However, the nature of the claims raised alarms that must be comprehensively addressed. In *The Information's* February 2017 article, Mr. Leng disclosed that “thousands of customers” were using the same hardware. These customers deserve answers immediately. While large tech firms may have the financial resources and expertise to mitigate sophisticated cyber security threats or completely remove affected hardware, most companies do not. Nor do they have the information to act.

We are alarmed about the dangers posed by backdoors, and take any claimed threat to the nation's networks and supply chain seriously. These new allegations require thorough answers and urgent investigation for customers, law enforcement, and Congress. We ask that you provide responses to following questions by October 17, 2018:

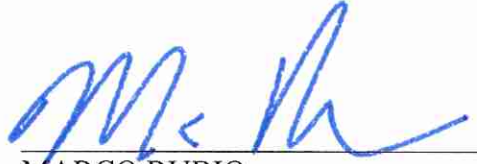
- 1.) When did Supermicro first become aware of reports regarding malicious hardware components and firmware in its computers and hardware? Has Supermicro ever found tampering of components or firmware that targeted its products?
- 2.) Has Supermicro conducted an investigation of its chain of suppliers to identify any possible modifications or security issues with its products? If it has found tampering, has it severed ties with those suppliers?
- 3.) If Supermicro has found or otherwise become aware of unaccounted-for modification on hardware or firmware, has it taken steps to remove the tampered product from the supply chain?
- 4.) When *The Information* reported in February 2017 that Apple had found compromised firmware, did Supermicro conduct any investigation into the potential infiltration of its supply chain as Mr. Leng had committed to do so? If so, what were the results of this investigation?
- 5.) Has Supermicro cooperated with law enforcement in the United States to address such reports? If tampering is found, will you provide a list of potentially affected customers to U.S. authorities and provide information to customers?
- 6.) Has Supermicro enacted screening measures or audits to assess its supply chain and detect and mitigate any such attempts to tamper with products?
- 7.) If tampering is found, does Supermicro assess that such tampering could be mitigated based on firmware updates, software patches, configuration changes, or operating system defenses?
- 8.) Has the Chinese government ever requested access to Supermicro's confidential security information or sought to restrict information regarding the security of Supermicro's products?

Thank you for your attention to these important issues. We look forward to your response.

Sincerely,



RICHARD BLUMENTHAL
United States Senator



MARCO RUBIO
United States Senator