United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 16, 2018

The Honorable Kirstjen Nielsen
Secretary
U.S. Department of Homeland Security
3801 Nebraska Avenue, NW
Washington, DC 20528

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Secretary Nielsen and Director Wray:

During the Committee's hearing on October 10, 2018, there was a discussion of recent news reports that foreign adversaries may have inserted microchips on servers that are used by a number of major U.S. companies and U.S. government agencies.[1] According to the reports, there is an ongoing, three-year-old federal investigation into the alleged cybersecurity vulnerability.[2]

Companies named in the reports have categorically denied the accuracy of the stories.[3] Secretary Nielsen supported the companies' denials, testifying: "With respect to the article, we at DHS do not have any evidence that supports the article. We have no reason to doubt what the companies have said. We continue to look into it."[4] Director Wray likewise testified, "As to the newspaper article or the magazine article, I would just say be careful what you read in this context."[5]

---

[1] *Threats to the Homeland, S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. (2018); *see also* Jordan Robertson and Michael Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, Bloomberg (Oct. 4, 2018), *available at* https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies; Jordan Robertson and Michael Riley, *New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom*, Bloomberg (Oct. 4, 2018), *available at* https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom.

[2] *Id.*

[3] Jordan Robertson and Michael Riley, *The Big Hack: Statements from Amazon, Apple, Supermicro, and the Chinese Government*, Bloomberg (Oct. 4, 2018), *available at* https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond.

[4] *Threats to the Homeland, S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. (2018).

[5] *Id.*

This Committee is tasked with legislative and oversight responsibility over federal information technology and supply chain risk management. To fully understand the accuracy of public reports about the potential cybersecurity and supply chain threat, we respectfully request that DHS and FBI provide a classified briefing with the appropriate subject-matter experts as soon as possible but no later than October 25, 2018.

The Senate Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[6] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of Government with particular references to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[7]

If you have any questions, please ask your staff to contact Michael Lueptow of Chairman Johnson's staff at (202) 224-4751 or Julie Klein of Ranking Member McCaskill's staff at (202) 224-2627. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

Claire McCaskill
Ranking Member

[6] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[7] S. Res. 62 § 12, 115th Cong. (2017).