

# Congress of the United States

## House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

[www.science.house.gov](http://www.science.house.gov)

January 14, 2016

Mr. Ken Xie  
Chief Executive Officer  
Fortinet, Inc.  
899 Kifer Road  
Sunnyvale, CA 94086

Dear Mr. Xie,

The Committee on Science, Space, and Technology is conducting oversight of federal cyber security policies and guidelines. Because of Fortinet's business of providing software that encrypts network data, the Committee requests your company's assistance in improving the National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (the Framework) and the Federal Information Security Act (FISMA).<sup>1</sup> The Framework sets industry standards and best practices to help organizations manage cybersecurity risks,<sup>2</sup> and FISMA provides a mechanism for oversight of federal government information security programs. Both FISMA and the Framework are becoming more important as high profile cybersecurity attacks are becoming more common. As part of this oversight initiative, I am writing to request documents and information relating to work your company performed for a former government official.

On January 8, 2016, the Committee held a hearing entitled "Cybersecurity: What the Federal Government Can Learn from the Private Sector," where private sector cybersecurity experts testified on industry approaches and best practices for safeguarding against cybersecurity threats.<sup>3</sup> During the hearing, John Wood of the Virginia Cyber Security Commission was presented with the following scenario: a senior government official at an executive branch department approached a company to set up a private email account at their residence for conducting both official and personal business. It is likely that sensitive or classified information

---

<sup>1</sup> Nat'l Institute of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> (last visited Jan. 14, 2016).

<sup>2</sup> *Id.*

<sup>3</sup> H. Comm. on Science, Space, & Tech., *Hearing on Cybersecurity: What the Federal Gov't Can Learn from the Private Sector*, 114th Cong. (Jan. 8, 2016).

about national security will be transferred and stored on this network.<sup>4</sup> Mr. Wood told the Committee if his company were faced with such a request, his company would choose not to accommodate the request outlined in the scenario.<sup>5</sup> Mr. Wood called such an arrangement “illegal” and noted that the proposed scenario is “exposing classified data in the open.”<sup>6</sup> As a technology expert, Mr. Wood’s testimony confirms the Committee’s concerns with deviating from government information security requirements. This exchange raises significant concerns because it flagged a potential violation of FISMA and it exposed an information security network vulnerability of a high profile government official.

Understanding Fortinet’s role in providing encryption software for former Secretary of State Hillary Clinton’s private server is critical to improving government cybersecurity standards, specifically NIST’s cybersecurity Framework. The Committee understands that Fortinet provided encryption software for Secretary Clinton’s private network.<sup>7</sup> The sensitive nature of the information stored on Secretary Clinton’s private server created a unique challenge for Fortinet to ensure all information stored on the server was properly safeguarded. Fortinet’s practices in maintaining the server is of value to the Committee’s ongoing oversight as well as NIST, as they seek to implement President Obama’s Executive Order to update the Cybersecurity Framework.

Cybersecurity is becoming a greater threat to our nation than ever before. Last year “more than 178 million records on American’s were exposed in cyberattacks.”<sup>8</sup> According to the Government Accountability Office, in 2014, federal agencies reported 67,168 cyber security incidents that exposed personally identifiable information.<sup>9</sup> More troubling, the State Department scored a 42 out of 100 on the federal government’s cyber security report card. This score is lower than the Office of Personnel Management’s score, which recently experienced an attack exposing 20 million Americans’ private information.<sup>10</sup> In light of this ever increasing threat, the Committee takes seriously its duty to ensure the NIST Cybersecurity Framework is properly equipped to safeguard our nation’s information.

---

<sup>4</sup> *Id.* (question and answer by Chairman Lamar Smith).

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> Michael Riley, *Clinton’s E-Mail Built for Privacy Though Not Security*, BLOOMBERG, Mar. 4, 2015, available at <http://www.bloomberg.com/news/articles/2015-03-04/clinton-s-e-mail-system-built-for-privacy-though-not-security> (last visited Jan. 14, 2016).

<sup>8</sup> Keith Wagstaff, *Hack to the Future: Experts Make 2016 Cybersecurity Predictions*, NBC NEWS, Jan. 2, 2016, available at <http://www.nbcnews.com/tech/internet/hack-future-experts-make-2016-cybersecurity-predictions-n486766> (last visited Jan. 14, 2016).

<sup>9</sup> Pierluigi Paganini, *Incidents at Federal Gov’t Agencies Increased More Than 1,000 Percent Since 2006*, CYBER DEFENSE MAG., Jul. 21, 2015, available at <http://www.cyberdefensemagazine.com/incidents-at-federal-government-agencies-increased-more-than-1000-percent-since-2006/> (last visited Jan. 14, 2016).

<sup>10</sup> Ken Dilanian, *Under Clinton, State’s Cybersecurity Suffered*, ASSOC. PRESS, Oct. 19, 2015, available at <http://www.apnewsarchive.com/2015/AP-Exclusive-Years-of-poor-network-security-at-State-predated-a-hack-linked-to-Russia/id-3dfcd8ad743945c9b19ff45870f5e2ec> (last visited Jan. 14, 2016).

To assist the Committee in understanding how Fortinet utilized the NIST Cybersecurity Framework in safeguarding Secretary Clinton's server, I request the following documents and information as soon as possible, but by no later than noon on January 28, 2016. Please provide the requested information for the time frame from January 1, 2009, to the present:

1. All documents and communications referring or relating to Secretary Clinton's private server or network, including but not limited to documents referring or relating to FISMA.
2. All documents and communications referring or relating to Fortinet's role in encrypting Secretary Clinton's private server.
3. All documents and communications referring or relating to any security breaches to Secretary Clinton's server or network which took place at any time, including but not limited to the time period January 1, 2009, to the present.
4. All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

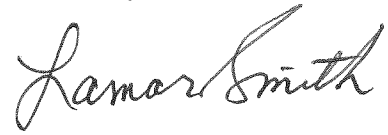
The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology which develops cybersecurity standards and guidelines as set forth in House Rule X.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Drew Colliatie or Caroline Ingram at 202-225-6371. Thank you for your attention to this matter.

January 14, 2016  
Page 4

Sincerely,

A handwritten signature in cursive script that reads "Lamar Smith". The signature is written in black ink and is positioned to the right of the word "Sincerely,".

Lamar Smith  
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member