LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

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

January 14, 2016

Mr. Austin McChord
Chief Executive Officer
Datto, Inc.
101 Merritt 7, 7th Floor
Norwalk, CT 06851

Dear Mr. McChord,

The Committee on Science, Space, and Technology is conducting oversight of federal cyber security policies and guidelines. Because of Datto Inc.'s work in managing software that provides backup 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).[1] The Framework sets industry standards and best practices to help organizations manage cybersecurity risks,[2] 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.[3] 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 about national security will be transferred and stored on this network.[4] Mr. Wood told the

---

[1] 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).
[2] *Id.*
[3] 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).
[4] *Id.* (question and answer by Chairman Lamar Smith).

Committee if his company were faced with such a request, his company would choose not to accommodate the request outlined in the scenario.[5] Mr. Wood called such an arrangement "illegal" and noted that the proposed scenario is "exposing classified data in the open."[6] 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 Datto's role in providing backup data for former Secretary of State Hillary Clinton's private server is critical to improving government cybersecurity standards, specifically NIST's cybersecurity Framework. According to an October 7, 2015, news report, Datto was responsible for ensuring that Secretary Clinton's emails were properly backed up on an off-site cloud.[7] The sensitive nature of the information that could be found in Secretary Clinton's backup data created a unique challenge to ensure all cybersecurity risks were mitigated. Datto's practices in backing up the off-site cloud are 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.[8]

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."[9] According to the Government Accountability Office, in 2014, federal agencies reported 67,168 cyber security incidents that exposed personally identifiable information.[10] 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.[11] 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.

---

[5] *Id.*
[6] *Id.*
[7] Rachel Bade, *Data Firm Gives FBI All Backed-up Clinton Emails*, POLITICO, Oct. 7, 2015, *available at* http://www.politico.com/story/2015/10/hillary-clinton-email-server-fbi-platte-river-214521.
[8] The White House, *Executive Order – Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (last visited Jan. 14, 2016).
[9] 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).
[10] 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).
[11] 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 Datto 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 Datto providing any backup device or service for 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.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member