TED W. LIEU
33RD DISTRICT, CALIFORNIA

COMMITTEE ON THE JUDICIARY

COMMITTEE ON FOREIGN AFFAIRS

Congress of the United States
House of Representatives
Washington, DC 20515–0533

236 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3976

5055 WILSHIRE BOULEVARD, SUITE 310
LOS ANGELES, CA 90036
(310) 652-3095

1600 ROSECRANS AVENUE, 4TH FLOOR
MANHATTAN BEACH, CA 90266
(310) 321-7664

February 10, 2017

The Honorable Gregg Harper
Chairman
House Administration Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Robert A. Brady
Ranking Member
House Administration Committee
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Harper and Ranking Member Brady:

Thank you for your work on the important issue of information security and cybersecurity threats, particularly as they relate to Members and their staff. In an interview published in *USA Today*, Chairman Harper recently said, "Every office, every committee, every part of Capitol Hill" is vulnerable to attack, and I strongly agree.[1] With this in mind, I write to request that the House Administration Committee, which is responsible for modernizing the House's internal operations[2], consider undertaking a series of practical measures designed to improve employees' awareness of and resilience to information security threats.

As a computer science major and former active duty officer in the U.S. Air Force, I am keenly aware of the diversity of threats our country faces— whether from "hactivists" looking to expose Members' personal information, criminals using ransomware to extort American businesses, or sophisticated foreign actors seeking to damage our nation's critical infrastructure. Each threat targets different attack vectors, but all rely on one common vulnerability—lack of preparation. I believe there are three actions the Committee should take to address this:

1. Recognize the vulnerability that Members' personal devices and home networks pose to House of Representatives official business and data, and develop a plan to secure them;
2. Hold a briefing for Members in a potentially classified setting on information security threats and best practices;
3. Shorten the time-period during which new House employees are required to take information security training to within 7 days.

Due to ethics restrictions that bar Members from using government phones for political activity, most Members choose to operate primarily on their personal devices. While Members' mobile phones are equipped with commonsense security measures like encryption through the *AirWatch* app, this protection becomes compromised if the phone itself is hacked. We cannot afford to ignore this reality and leave Members' devices – and the official government business they conduct – unprotected.

[1] Deborah Barfield Berry. "Congress to step up its own cybersecurity protections," *USA Today*, January 6, 2017.
[2] "History and Jurisdiction," *Committee on House Administration*. 2017.

Additionally, we must raise awareness among Members. I believe that a Committee-led briefing for Members, in a classified setting if necessary, on the specific threats and safety measures Members can use to protect themselves would bring clarity to topics that are too often discussed in the abstract. My office is planning a public briefing for staff and Members featuring outside experts to foster discussion and understanding among our colleagues, and we stand ready to work with the Committee on that initiative.

It is not only Members who are vulnerable. As you may know, all incoming House employees are required to take a security awareness training test 30 days after their initial employment and must retake the test annually. In that 30-day timeframe, employees are vulnerable to a range of attacks that prey on users' lack of awareness, including spear phishing, whereby malicious actors target a specific individual inside an organization, and drive-by attacks, which rely on a random user unintentionally downloading malware simply by visiting a website. Closing the gap between initial employment and security training by reducing the amount of time employees have to complete their training to seven days would help diminish these vulnerabilities.

These measures build on the important work the Committee has done to secure our information and protect our privacy. Now more than ever, we must be proactive and adopt commonsense measures to increase consciousness surrounding these serious challenges. I look forward to working with you to continue improving cybersecurity in the House of Representatives, and stand ready to assist with your Committee's actions on this issue.

Sincerely,

Ted W. Lieu

Rep. Ted W. Lieu
Member of Congress

cc: The Honorable Rodney Davis
The Honorable Zoe Lofgren
The Honorable Barbara Comstock
The Honorable Jamie Raskin
The Honorable Mark Walker
The Honorable Adrian Smith
The Honorable Barry Loudermilk