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

June 26, 2017

The Honorable John F. Kelly
Secretary of Homeland Security
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Kelly:

As of this writing, President Trump has traveled to his Mar-a-Lago estate seven times since taking office. While the U.S. Secret Service is no doubt well acquainted with traditional security protocols involving visits to the site at this point in the President's tenure, I am disturbed by a recent report that indicates security researchers affiliated with the website *Gizmodo* discovered weakly encrypted Wi-Fi networks at Mar-a-Lago, and completely open Wi-Fi networks at the Trump National Golf Club in Bedminster, New Jersey. As a computer science major, I can affirm that such lapses carry a host of implications for the President's personal security and the country's national security.

The report, which was published on May 17, 2017, details additional vulnerabilities at the Trump International Hotel in Washington, D.C. and a Trump-owned golf club in Sterling, Virginia. At both properties, researchers found liabilities including:

> *"weak and open Wi-Fi networks, wireless printers without passwords, servers with outdated and vulnerable software, and unencrypted login pages to back-end databases containing sensitive information... Sophisticated attackers could take advantage of vulnerabilities in the Wi-Fi networks to take over devices like computers or smart phones and use them to record conversations involving anyone on the premises."*

The Defense Information Systems Agency, responsible for securing White House and military networks according to the Sharing Peripherals Across the Network (SPAN) Security Technical Implementation Guide (STIG), bans the installation of internet-connected printers precisely because they can be used to intercept sensitive documents.

One cybersecurity expert, when asked about the report, stated, "What you're describing is typical hotel security." Most commercial properties, however, do not frequently house the President of the United States and his myriad staff cleared at the TS/SCI level. Moreover, since the election, President Trump has invited foreign leaders including President Xi Jinping, Prime Minister Shinzo Abe, and Nigel Farage to his various properties during which sensitive diplomatic conversations took place. Finally, Trump-owned commercial properties have been subject to cyberattacks in the past, and one can only assume such attacks have increased since Mr. Trump took office. When asked about these breaches, the White House reportedly declined to comment.

Given these reports, we would like to know the following:

1. Is the Department of Homeland Security aware of the May 17th report in question?

2. Are Secret Service staff who are responsible for cybersecurity familiar with the April 2017 DHS report entitled, "Study on Mobile Security," which details threats, vulnerabilities, and solutions to address identified weaknesses – and are they implementing DHS' recommendations on best practices?

3. Is any entity, public or private, responsible for securing Wi-Fi networks at properties belonging to the President – both while he is physically there, and when he is away – and if so, what entity is responsible?

4. Although Secret Service routinely establishes portable and secure communications equipment, the President has reportedly held meetings in public spaces at his properties. Has Secret Service taken measures to ensure President Trump does not connect his personal mobile device to insecure networks while visiting his family's properties?

5. What measures has DHS and/or U.S. Secret Service taken to address the increased presence of unsecured digital devices – for example, Internet of Things-connected devices – in close proximity to the President?

Thank you for your attention to this critical matter. We look forward to your response.

Sincerely,

Ted W. Lieu
Member of Congress

CC: Mr. Randolph Alles, Director of the U.S. Secret Service