

Congress of the United States
Washington, DC 20515

February 15, 2017

The Honorable Jason Chaffetz
Chairman
House Oversight and Government Reform
Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable Elijah Cummings
Ranking Member
House Oversight and Government Reform
Committee
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

Referring to the complex problem of cybersecurity, President Trump recently said in an interview, “I’m not sure you have the kind of security that you need.” We fully agree—which is why we are writing to request that the House Oversight and Government Reform Committee hold a public hearing into troubling reports that the President is jeopardizing national security by egregiously failing to implement commonsense security measures across the board, from using an insecure, consumer-grade Android smartphone to discussing nuclear strategy openly in a dining room at his Mar-a-Lago Club in Florida. In addition, we request that the hearing cover reports of senior White House staff using insecure, political email accounts from within the White House.

Cybersecurity experts universally agree that an ordinary Android smartphone, which the President is reportedly using despite repeated warnings from the Secret Service, can be easily hacked. The device President Trump insists on using—most likely the Samsung Galaxy S3—has particularly well-documented vulnerabilities. The use of an unsecured phone risks the President of the United States being monitored by foreign or domestic adversaries, many of whom would be happy to hijack the President’s prized Twitter account causing disastrous consequences for global stability. More frighteningly, hackers could present the President with alternative information, which, as the President has repeatedly demonstrated, can have a huge impact on his beliefs and actions.

While it is relatively easy to hack an Android phone, it is even easier to overhear a sensitive conversation or swipe a set of keys to a briefcase holding sensitive documents. This week, disturbing reports surfaced that President Trump—while meeting with Japanese Prime Minister Shinzo Abe—openly discussed nuclear security strategy with regard to the threat from North Korea at his club in Florida. It is unacceptable that restaurant staff and patrons may have been privy to conversations that should only be held in the most secure environments. Moreover, an *Associated Press* photo recently revealed President Trump had left the keys to a briefcase containing classified documents *in his briefcase*. This behavior is more than bad operational security—it is an egregious affront to national security.

Finally, reports that senior White House staff may have been using insecure, political email accounts from within the White House in connection with official business are deeply concerning and merit closer investigation. Reports indicate that a political email system used by senior White House staff was hacked in December by a Russian intelligence agency, yet again raising the prospect of the White House being monitored or influenced by unfriendly powers. We would remind the Chairmen of Congressional Republicans' concerns over the use of private email by Secretary Clinton, and of Congressional Democrats over the Bush White House's use of private email accounts. A public hearing is required to ensure the security of such communications as well as the adequacy of recordkeeping procedures as required under federal law.

For these reasons, we urge you to consider the following questions for a public hearing:

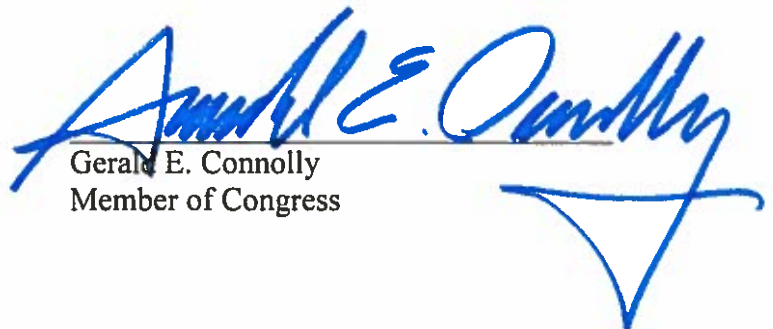
- Is the President of the United States actively using his unsecured Android device, and if so, how?
- Are the President and staff in the Office of the President thoroughly versed on the dangers of foreign entities monitoring White House communications through unsecured networks?
- What immediate actions do the President and the Office of the President intend to take to ensure the swift and safe transition of communications technologies?
- Are cybersecurity and national security practices active and in place for the President and the Office of the President?
- In addition to cybersecurity standards, have the President and his team received certifiable training in kinetic operational security—that is, non-electronic activity?
- Is it their assurance to the American people that the President and the Office of the President are meticulously following protocol and obeying the law for security, transparency, and appropriate disclosures with regard to cybersecurity and technological communications?
- Can the President and the Office of the President ensure that there are no missing emails, communications, and technological exchanges—in other words, can they confirm they are not actively being monitored?
- Have White House senior officials using RNC email addresses obeyed the law in accordance with the "Disclosure Requirement for Official Business Conducted Using Electronic Messaging Accounts," (44 U.S.C. 2209) by copying or forwarding communications into the government system within 20 days?

It is our hope that you can put our national security and the American people first and seriously investigate these concerns in a public hearing. Our country depends on it.

Sincerely,





Ted W. Lieu
Member of Congress




Gerald E. Connolly
Member of Congress


Grace Meng
Member of Congress



Jared Polis
Member of Congress

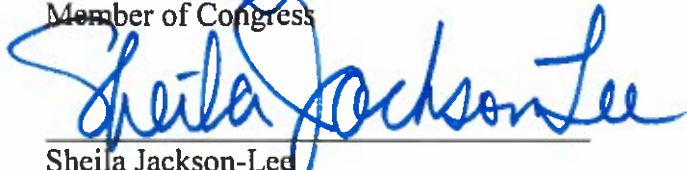

Louise M. Slaughter
Member of Congress



Kathy Castor
Member of Congress



Carl Shea-Porter
Member of Congress

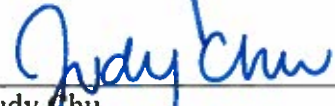

Luis Gutiérrez
Member of Congress



Daren Soto
Member of Congress


Sheila Jackson-Lee
Member of Congress


Colleen Hanabusa
Member of Congress


Betty McCollum
Member of Congress


Judy Chu
Member of Congress


Pete Aguilar
Member of Congress


Tony Cárdenas
Member of Congress