Congress of the United States
Washington, DC 20515

April 25, 2018

The Honorable Daniel Coats
Director of National Intelligence
Office of the Director of National Intelligence
ATTN: 6B-100, Liberty Cross-2
Washington, DC 20511

Vice Admiral Nancy A. Norton
White House Communications Agency/Defense Information Systems Agency, Joint Force Department of Defense Information Network
2743 Defense Blvd, SW
Anacostia Annex, DC 20373

The Honorable Randolph D. Alles
Director
U.S. Secret Service
950 H Street, NW
Washington, DC 20223

Dear Director Coats, Vice Admiral Norton, and Director Alles:

Thank you for your service. Each of your agencies plays a crucial role in defending U.S. national security, the integrity of classified information, and the personal safety of the President and his or her family. As Members of Congress and veterans who understand the importance of secure communications, we are deeply disturbed by reports of President Trump's continued and increasing use of his personal, unsecured Android phone.[1] We write to request information from each of your offices on the specific steps you have taken to mitigate the unique threats posed by the reckless behavior of the Commander-in-Chief. We appreciate that answers to some of these questions may be sensitive in nature and thus request that any information not transmissible publicly is relayed to us in the appropriate classified setting.

While cybersecurity is a universal concern, the President of the United States stands alone as the single-most valuable intelligence target on the planet. Given the apparent lack of progress the Administration has made since initial reports in 2016 of the President's poor operational security, it appears the only thing standing between the Office of the President and the next national security nightmare is a combination of President Trump's personal restraint and sheer luck.[2] Our national security should not depend on whether the President clicks on a malicious link on Twitter or his text application, or the fortuity of foreign agencies not knowing his personal cell number.

---

[1] Pamela Brown and Sarah Westwood, "Trump ramps up personal cell phone use," CNN April 24, 2018. https://www.cnn.com/2018/04/23/politics/donald-trump-cell-phone/index.html

[2] Cara McGoogan, "Donald Trump's personal phone could be a major security risk, experts warn," *Telegraph* November 28, 2018. https://www.telegraph.co.uk/technology/2016/11/28/donald-trumps-personal-phone-could-major-security-risk-experts/

Mobile security vulnerabilities are well-documented. In particular, the Signaling System 7 vulnerability (SS7) allows foreign governments and malicious actors to use the architecture of our cell phone networks to intercept calls and SMS messages if they simply know a person's cell phone number.[3] Foreign agencies can also intercept cell phone calls and text messages if they are monitoring the unsecure cell phones of people that the President calls. Additionally, malware such as Pegasus can provide access to a phone's microphone and camera even while the phone is not being used.

These vulnerabilities are just some of the reasons that Director of National Intelligence James Clapper recently called President Trump's use of a personal cell phone a "goldmine of intelligence."[4] Hostile foreign intelligence agencies routinely attempt to breach White House communications operations, and the President is effectively handing them the keys to the office.

The American people deserve to know whether steps are being taken to prevent the President's personal phone from jeopardizing his own safety, the integrity of the Office, and critical national security information. We request that you answer the following questions as indicated below:

White House Communications Agency (WHCA)

- Is the WHCA aware of reports indicating the President is using an unsecured Android phone, as referenced above?

- President Barack Obama's Blackberry was modified to disallow text messages, which the WHCA recognized could pose a national security threat if a malicious link was inadvertently clicked. Is President Trump tweeting from a secure device that has been properly vetted by the WHCA to account for basic threats like spearfishing?

- Is the Trump administration following proper protocols to ensure the President's personal phone does not connect to open and vulnerable wireless networks, either in Washington D.C. or at his other residences, or when he travels to other locations?

- How frequently does the WHCA update the President's phone's operating system?

- Does the President use encryption when he makes phone calls or texts from his personal cell phone?

- How has WHCA adapted to the growing threat of "Stingray" devices, or IMSI catchers, in Washington D.C., especially given the President's alleged proclivity for making outgoing voice calls on his personal cell phone?

- Before the President travels abroad, is his personal phone serviced by WHCA and/or relevant Intelligence Community organizations to ensure it has robust technical defenses against intrusion or foreign intelligence collection efforts?

---

[3] "Hacking Your Phone," *CBS* April 17, 2016. https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

[4] https://www.cnn.com/videos/politics/2018/04/24/trump-personal-cell-phone-clapper-ctn-sot.cnn

- After the President travels abroad, is his personal phone screened in accordance with proper procedures to ensure that it has not been compromised by foreign intelligence services or other parties?

U.S. Secret Service

- Is the U.S. Secret Service aware of reports indicating the President is using an unsecured Android phone, as referenced above?
- Given the unique threats posed by POTUS' alleged use of a personal cell phone, what steps is the U.S. Secret Service currently taking to ensure the President's personal physical security is not comprised, either by geolocation tracking or other means?

Office of the Director of National Intelligence (ODNI)

- Is ODNI leadership aware of reports indicating the President of the United States frequently uses an unsecured Android device?
- How has ODNI coordinated with relevant USG agencies and entities to prevent classified information from leaking via the President's unsecured Android phone?
- Has ODNI conducted a review of threats posed by the President's unsecured Android device?
- If so, have recommendations been made to relevant USG entities following such a review?
- Has the WHCA met with or discussed with ODNI staff possible solutions to the threat of foreign intelligence gathering via a compromised phone?
- When the President receives a classified briefing, does he follow security procedures and leave his personal cell phone outside the secured briefing room?

Thank you for your attention to these critical issues.

Sincerely,

Ted W. Lieu
Member of Congress

Ruben Gallego
Member of Congress