

United States Senate

WASHINGTON, DC 20510

June 7, 2018

Director William Evanina
National Counterintelligence and Security Center
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Director Evanina:

Earlier this year, Director of National Intelligence Coats testified that “[p]enetrating the US national decision making apparatus” of the U.S. government is a primary objective for numerous foreign intelligence agencies. That is why we are especially concerned about recent reporting that President Trump has eschewed the advice of counterintelligence experts and opted to use unsecured commercial devices for telephone calls and internet use. We believe this conduct is reckless and could endanger sensitive U.S. national security interests.

Last month, Politico reported that President Trump has broken with the practices of his predecessors and routinely uses unsecured devices to communicate with friends and Twitter followers. According to the report, Trump has brushed aside the concerns of White House and Intelligence Community security experts and dismissed their pleas as “too inconvenient.” Furthermore, the report suggests that not only does the President use an unsecured cell phone to make calls, but that cell phone is also equipped with a camera and microphone that could be used to spy on the President and listen in on classified national security discussions.

Government officials with access to classified information must abide by strict security protocols that limit when, how, and in what manner they communicate with others. We agree with Secretary of State Mike Pompeo’s recent testimony that “every government official” must adhere to security protocols, even the President. Most officials with access to classified information must take draconian precautions, such as leaving their devices outside of their places of work and utilizing two separate sets of computers and phones for classified and unclassified work. It is our understanding that even White House aides are required to deposit their cell phones in lockboxes before entering the West Wing.

If the President has indeed been using unsecured devices to communicate with associates, it represents a grave danger to U.S. national security. Just last month, the Department of Homeland Security (DHS) revealed that it had detected cell-site simulator technology, which allows for the surreptitious surveillance of cell phone calls, deployed in locations in proximity to the White House and other sensitive facilities in the D.C. area. Although DHS has not attributed the cell-site simulator deployment to any specific entity, it is possible that foreign intelligence services or nefarious actors could attempt to intercept the President’s unsecured conversations.

We request that you provide the Senate Select Committee on Intelligence with a threat assessment to determine whether sensitive government information has been exposed and whether plans, strategies, operations, or classified information have been or could be

compromised by foreign adversaries due to the President's cell phone usage. In addition, we request an assessment of attribution of the deployment of hostile cell-site simulator technology detected by the Intelligence Community or other government agencies in the National Capital Region during the past two years.

Finally, since in recent correspondence both DHS and the Federal Communications Commission claim not to have the lead role in assessing the potential threat from the use of cell-site simulators, please help us understand NCSC's role in this regard and how your agency works with other IC entities to address this potential threat.

Thank you for your prompt attention to this request.

Sincerely,



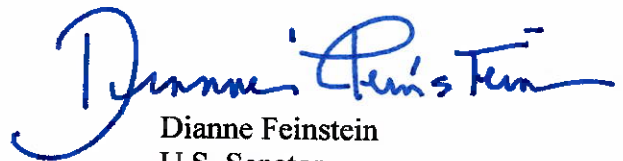
Martin Heinrich
U.S. Senator



Ron Wyden
U.S. Senator



Richard J. Durbin
U.S. Senator



Dianne Feinstein
U.S. Senator