United States Senate
COMMITTEE ON FOREIGN RELATIONS
WASHINGTON, DC 20510–6225

January 24, 2020

The Honorable Mike Pompeo
Secretary of State
U.S. Department of State
2201 C Street, N.W.
Washington, D.C. 20520

Dear Secretary Pompeo,

I am deeply concerned by continuing efforts of foreign governments to abuse technology to target American citizens. I welcomed the Department's December 12 response to my letter expressing concern about Twitter employees allegedly spying on dissidents on behalf of Saudi Arabia, in which you described such behavior as "unacceptable." As I am sure you are aware, this week's report from Agnes Callamard, UN Special Rapporteur on summary executions and extrajudicial killings, and David Kaye, UN Special Rapporteur on freedom of expression, presents compelling evidence that the Saudi Arabian government, including Crown Prince Mohamad bin Salman himself, targeted, hacked, and attempted to blackmail Amazon CEO and *Washington Post* owner Jeff Bezos as part of a coordinated campaign to suppress dissent and stifle reporting on the murder of *Washington Post* columnist and American resident Jamal Khashoggi.

As we have seen from the brutal murder of Jamal Khashoggi, the detention and torture of activists, and the alleged use of former Twitter employees to spy on dissidents, the Saudi government has a troubling record of using technology to repress dissent. The apparent use of spyware to gain unauthorized access to the data of a U.S. citizen by the Crown Prince of Saudi Arabia raises fresh concerns about the ability and willingness of the Saudi government use technology to subvert U.S. national security interests. The abuse of technology to negatively impact American citizens or to flout American values, of course, is a concern that spans across the globe.

I have warned in previous letters that bad actors can, have, and will continue to use technological innovations for malign purposes and that governments have used these tools to repress and surveil dissidents. We must ensure that U.S. officials in particular, but all American citizens, are equipped to defend against these kinds of attacks. We must consider that foreign governments have and will continue to target government officials and other political figures in the U.S. in an effort to gain leverage or information on the U.S., thus putting U.S. security interests at risk.

In the December 12 letter you also noted that U.S. Embassy Riyadh continues to engage with the Saudi government on these issues, and I commend those efforts and hope they will continue. But it appears that there is more work to be done.

In light of these concerns, I request that you respond in writing to the following questions by February 5, 2020:

1. Is the State Department aware of any attempts by or on behalf of the Saudi government, Saudi officials, or members of the Saudi Royal family to hack, install malware or spyware, or gain unauthorized access to data or electronic communications of any U.S. government officials?
2. What mechanisms and practices has the State Department put in place to ensure that U.S. government devices are protected from attempts to gain unauthorized access to data or information? How have these practices changed over the last two years, as these attempts have increased in frequency?
3. How is the State Department working with allies and partners to mitigate the increased monitoring and hacking attempts from Saudi Arabia, including stopping the sale of spyware to the Saudi government, and conducting due diligence on the end use of technology that can be exploited for monitoring or hacking?
4. What specific steps have the State Department and the Administration taken to engage with Saudi Arabia in an effort to curb Saudi Arabia's malign activities?

I look forward to your responses to my questions. I also request a briefing by relevant officials on the steps the Department is taking to address these concerns.

Sincerely,

Robert Menendez
Ranking Member