RO KHANNA
17TH DISTRICT, CALIFORNIA

COMMITTEE ON
ARMED SERVICES
Subcommittee on Intelligence,
Emerging Threats, and Capabilities
Subcommittee on Strategic Forces
COMMITTEE ON
THE BUDGET
COMMITTEE ON
OVERSIGHT AND REFORM
Subcommittee on Economic
and Consumer Policy
Subcommittee on Government Operations

Congress of the United States
House of Representatives
Washington, DC 20515-0517

221 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2631
(202) 225-2699 (F)

DISTRICT OFFICE:
3150 DE LA CRUZ BLVD, SUITE 240
SANTA CLARA, CA 95054
(408) 436-2720
(408) 436-2721 (F)

khanna.house.gov

December 9th, 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
290 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Graham,

I write today regarding the upcoming Judiciary Committee hearing that will take place on December 10th, 2019 titled "Encryption and Lawful Benefits and Risks to Public Safety and Privacy." Thank you for taking interest in this issue during such a critical time.

I passed an amendment to the National Defense Authorization Act for FY19 requiring the Department of Defense (DoD) to brief the House Armed Services Committee on the "information security technologies that the Department employs to protect the official unclassified email and official unclassified mobile communications of its employees."

The briefing recommends several technical security controls for protecting servicemembers' mobile devices and their stored data. For example, recommendations to "enable full device encryption" and to "enforce device password/passcode requirements." In addition, the DoD wrote in the briefing it recommends the use of secure VPNs to protect data in transit.

In September of this year, I wrote to the DoD's Chief Information Officer (CIO), Dana Deasy, to request further clarification of its policy and position on encryption and secure VPNs. I sent my letter in response to recent concerning public statements made by Attorney General William Barr. In a speech he delivered on July 23, 2019, AG Barr indicated interest in creating a back-door to encryption. Weakening encryption reduces the cybersecurity for all Americans, particularly our men and women in uniform.

In response to my letter dated October 15th 2019, Mr. Deasy explained, "All DoD issued unclassified mobile devices are required to be password protected using strong passwords. The Department also requires that data-in-transit, on DoD issued mobile devices, be encrypted (e.g., VPN) to protect DoD information is imperative." DoD CIO Deasy ended the letter by saying, "The Department believes maintaining a domestic climate for state of the art security an encryption is critical to the protection of our national security."

I could not agree more with the DoD stance on encryption and hope that you will take its policy into consideration for the hearing you will convene on this issue on December 10.

Both letters from myself and CIO Deasy are attached to this letter. Thank you for your time and attention to this matter.

Sincerely,

Ro Khanna
Member of Congress

RO KHANNA
17TH DISTRICT, CALIFORNIA

COMMITTEE ON
ARMED SERVICES
Subcommittee on Intelligence,
Emerging Threats, and Capabilities
Subcommittee on Strategic Forces

COMMITTEE ON
THE BUDGET

COMMITTEE ON
OVERSIGHT AND REFORM
Subcommittee on Economic
and Consumer Policy
Subcommittee on Government Operations

Congress of the United States
House of Representatives
Washington, DC 20515-0517

221 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2631
(202) 225-2699 (F)

DISTRICT OFFICE
3150 DE LA CRUZ BLVD, SUITE 240
SANTA CLARA, CA 95054
(408) 436-2720
(408) 436-2721 (F)

khanna.house.gov

Dana Deasy
Chief Information Officer
U.S. Department of Defense
1300 Defense Pentagon
Washington, D.C. 20301-1300

September 11, 2019

Dear Mr. Deasy,

Thank you for providing the briefing to the House Armed Services Committee (HASC) last year describing information security technologies the U.S. Department of Defense (DoD) uses to protect unclassified mobile communications. I was glad to see the DoD recommends employing cybersecurity best practices such as full device encryption and Virtual Private Networks (VPNs).

As part of the National Defense Authorization Act for FY19, DoD was required to brief HASC on the "information security technologies that the Department employs to protect the official unclassified email and official unclassified mobile communications of its employees." Given DoD employees are potential targets for hackers and foreign adversaries, we must ensure they are protected while serving our nation.

I was encouraged to see you recommend several technical security controls for protecting servicemembers' mobile devices and their stored data. Most notably were the recommendations to "enable full device encryption" and to "enforce device password/passcode requirements." In addition, you recommend the use of secure VPNs to protect data in transit. These are critically important and are congruent with the security recommendations of our nation's cybersecurity experts.

At a time when some in government would like to weaken encryption and create a "back-door", I was pleased to see you believe the use of strong encryption is critical to ensure the security of sensitive personal information stored on mobile devices. Thank you for recommending its use to protect the men and women who serve in our Armed Forces. I believe you can offer valuable insights to other agencies and employees across our government.

Thus, I would like your answers to the following questions at your earliest convenience:

1. Do you recommend federal employees secure their personal mobile devices with strong passwords and enable full device encryption?
2. Do you recommend federal employees use secure VPNs to communicate sensitive information to their constituents and colleagues?
3. Do you believe DoD personnel should have personal mobile devices that only they can unlock?
4. Are you concerned foreign actors may try to obtain access to personal devices from DoD personnel to gain access to sensitive information on DoD networks?
5. Do you believe maintaining a vibrant domestic climate for security and encryption innovation is critical to the future of national security?

Thank you for your time and leadership on this matter. I look forward to receiving these answers from you and discussing the issue further with you.

Sincerely,

Ro Khanna
Member of Congress

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT 15 2019

The Honorable Ro Khanna
House of Representatives
Washington, DC 20515

Dear Representative Khanna:

I am responding to your letter from September 11, 2019 regarding the security of the Departments' personal mobile devices. Department policies only mandate protection standards for government-issued devices, and do not address personally owned devices.

I am also concerned about the issues addressed in your letter. The Department has taken a number of steps to address these concerns. All DoD issued unclassified mobile devices are required to be password protected using strong passwords. The Department also requires that data-in-transit, on DoD issued mobile devices, be encrypted (e.g., VPN) to protect DoD information and resources. The importance of strong encryption and VPNs for our mobile workforce is imperative. Last October, the Department outlined its layered cybersecurity approach to protect DoD information and resources, including service men and women, when using mobile communication capabilities.

DoD personnel are trained to operate the same as we fight to prevent cybersecurity attacks on all systems and information. All DoD personnel are required to complete annual cybersecurity awareness training which provides information and resources to protect both DoD information and personnel, in the workplace and at home, from foreign actors and cybersecurity related attacks.

As the use of mobile devices continues to expand, it is imperative that innovative security techniques, such as advanced encryption algorithms, are constantly maintained and improved to protect DoD information and resources. The Department believes maintaining a domestic climate for state of the art security and encryption is critical to the protection of our national security.

Please let me know if you have any further questions.

Sincerely,

Dana Deasy