

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
WASHINGTON, DC

The Honorable Ron Wyden  
Chairman  
Committee on Finance  
United States Senate  
Washington, DC 20510

Chairman Wyden:

This letter responds to your letter, dated 04 November 2021, to the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), the Department of Defense, the Department of State (DoS), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Communications Commission (FCC). The FBI and ODNI are providing this coordinated response on behalf of all recipients.

We appreciate and share your concern about the potential for foreign government actors to exploit cell-site simulator technologies and the potential counterintelligence (CI) threats posed by such technologies. We are committed to addressing this issue with our interagency partners. As you are aware, on 19 October 2021, the ODNI and FBI provided a classified briefing on this topic to Senate Select Committee on Intelligence staff and sought to convey our assessment of the potential threat and provide more context with respect to the potential CI concerns.

The security of our nation's communications networks, including the mobile and landline phones dependent on those networks, is integral to the safety and security of all Americans. While there is no government department or agency that is solely responsible for ensuring that domestic phone networks cannot be easily surveilled or for protecting U.S. government facilities in the United States from cell-site simulators, we continue to take a unified interagency approach to address such threats.

Several departments and agencies work collaboratively to address these potential threats, including: the FBI, through the Attorney General, as both the lead domestic CI agency under Executive Order 12333, and the lead federal investigative agency for a number of substantive criminal offenses that might involve the use of cell-site simulators; CISA, the lead federal agency responsible for coordinating efforts by both government and industry, including the communications sector, to protect and improve the nation's cybersecurity and resilience; the FCC, which regulates interstate and international communications by radio, television, wire, satellite, and cable, and implements and enforces America's communications law and regulations; and the ODNI, which integrates intelligence to support IC efforts to identify and counter such threats. In addition, the Committee on Foreign Investment in the United States, which is chaired by the Department of the Treasury, is the interagency committee responsible for identifying and mitigating risks to U.S. national security arising from foreign acquisitions, mergers, and certain investments involving U.S. businesses. Similarly, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (formerly known as Team Telecom), chaired by the Department of Justice (DoJ), reviews the

UNCLASSIFIED

The Honorable Ron Wyden

applications of foreign telecommunications carriers seeking to operate in the United States for any potential national security risks.

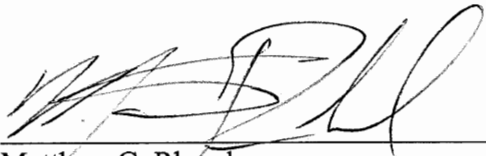
There currently is no single agency with sole responsibility for protecting U.S. Government devices outside the United States from cell-site simulators. When using host nation cellular networks, it is assumed that host intelligence services, and possibly those of other foreign intelligence services, are tracking and collecting voice and data information from the phones of U.S. citizens operating on that network. DoS Regional Security Officers brief all mission personnel on the vulnerabilities that exist when using host nation cellular networks.

In addition, we are not aware of any specific federal agency that has existing authority to implement your proposed solution of requiring intra-executive unclassified voice calls to be end-to-end encrypted. The solution you propose includes challenges that would need to be further examined, including potentially significant associated costs and implementation challenges. In addition, it could present operational challenges that could, in some cases, obstruct normal government operations. With regard to sensitive and classified federal government communications, it should be noted that the government does maintain multiple secure, classified, managed, encrypted communications systems, which it operates between agencies and departments in which the government maintains confidence.

We continue to be vigilant in coordinating our activities, sharing threat information, and maintaining collaborative working relationships with U.S. providers. Each department or agency coordinates with U.S. phone carriers at varying levels to address a broad scope of network vulnerability issues, consistent with our respective legal authorities and subject to executive directive. For example, the FBI and DoJ continue to work with government, private industry partners, and within the interagency, including CISA and the FCC, to address cyber threats and network vulnerabilities within networks as they arise. We also continue to engage with our industry partners on implementing best practices championed by the National Institute of Standards and Technology, CISA, and the FCC's Communications Security Reliability and Interoperability Council advisory committee, to strengthen the cyber security posture of our nation's communications networks. There is limited compulsory authority to order a carrier to take certain actions, particularly if it is majority-owned by U.S. persons.

We hope this information is helpful. Thank you for your support of our agencies and our people.

Sincerely,



Matthew C. Rhoades  
Assistant Director for Legislative Affairs  
Office of the Director of National  
Intelligence



Jill C. Tyson  
Assistant Director  
Office of Congressional Affairs  
Federal Bureau of Investigation

UNCLASSIFIED

The Honorable Ron Wyden

Cc:

The Honorable Antony Blinken

The Honorable Lloyd J. Austin III

The Honorable Jen Easterly

The Honorable Jessica Rosenworcel