

United States Senate

WASHINGTON, DC 20510

April 25, 2023

The Honorable Janet Yellen
Secretary of the Treasury
Department of the Treasury
1500 Pennsylvania Ave. NW
Washington, D.C. 20220

The Honorable Gina Raimondo
Secretary of Commerce
Department of Commerce
1401 Constitution Ave. NW,
Washington, D.C. 20230

The Honorable Antony Blinken
Secretary of State
Department of State
2201 C St. NW
Washington, D.C. 20520

Dear Secretaries Yellen, Raimondo, and Blinken:

We write to express our deep concern with the threat to American national security from Huawei Cloud and other People's Republic of China (PRC) cloud computing services. Open-source information shows that Huawei Cloud and PRC-based cloud computing services not only pose a threat to U.S. national security and economic security, but also are increasingly engaging with foreign entities—in some cases sanctioned foreign entities—that are directly challenging the national security and economic security interests of the United States and our allies and partners. We urge you to use all available tools to engage in decisive action against these firms, through sanctions, export restrictions, and investment bans, and to further investigate PRC cloud computing service companies.

Huawei Cloud

The U.S. Commerce Department has already recognized the national security threat posed by Huawei adding it to its “Entity List” of companies to which U.S. persons need a license to export. The subsidiary Huawei Cloud was also added to the Entity list in August 2020, because the Commerce Department found there was “reasonable cause to believe, based on specific and articulable facts” that Huawei Cloud had “been involved, [is] involved, or pose[d] a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States.”

Since this listing, further alarming information on Huawei Cloud has come to light. On December 14, 2021, a news report by the *Wall Street Journal* revealed that Huawei Cloud uses its technologies to help the PRC government identify individuals by voice, monitor political dissidents, manage ideological reeducation and labor schedules for prisoners, and help retailers use facial recognition to track shoppers.

Even more damning, Huawei Cloud announced on December 7, 2021, that it had launched its “Sky Computing Constellation” in co-sponsorship with Changsha Tianyi Space Science and Technology Research Institute (also known as “Spacety China”) and the Beijing University of Posts and Telecommunications (BUPT). As you are aware, on January 26, 2023, the Treasury Department imposed sanctions against Spacety China and its Luxembourg-based subsidiary for providing synthetic aperture radar (SAR) satellite imagery orders of locations in Ukraine to the Russian entity Terra Tech.

Moreover, BUPT is one of eight Chinese universities known to have received top-secret security credentials from the PRC government. BUPT's School of Cyberspace Security is home to one of the university's two defense laboratories—the Key Laboratory of Network and Information Attack and Defense Technology of Ministry of Education—that carries out research for the Chinese military related to cyber-attacks. BUPT was also added to the Entity List in December 2020 because it “directly participates in the research and development, and production, of advanced weapons and advanced weapons systems in support of People’s Liberation Army modernization.”

In light of this, we therefore urge you to impose sanctions on Huawei Cloud under existing authorities for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of recently-sanctioned Spacety.

Alibaba Cloud

Other PRC cloud service companies are rapidly expanding their presence in America and beyond, posing similar national security concerns.

We are gravely concerned by Alibaba Cloud (Aliyu)—the cloud services arm of Alibaba, a “national champion” company of the Chinese Communist Party (CCP)—having opened two cloud data centers in Santa Clara, California, in 2015—in the heart of Silicon Valley. These data center reportedly provide a variety of cloud computing services that initially focused on PRC companies based in the U.S. and have gradually expanded services and products to international clients.

Alibaba Cloud is widely known to provide services to the PRC military, security, and intelligence services. For example:

- In 2017, Alibaba Cloud signed a military-civilian fusion (MCF) cloud cooperation agreement with PRC state-owned defense company China North Industries Group Corporation Limited (Norinco Group) and a cooperative agreement with China’s National University of Defense Technology.
- In July 2018, Song Jie, the vice president of Alibaba Cloud Computing, spoke at the inaugural Military Big Data Forum hosted by the People’s Liberation Army’s Academy of Military Sciences (AMS), in which military, academic, and business leaders deliberated on ways to transition the benefits and technologies of e-commerce to national defense. The forum was co-organized by the Chinese Academy of Sciences, Tsinghua University, and the Chinese Academy of Command and Control.
- In January 2019, executives from Alibaba Cloud’s parent company, Alibaba, and Ant Group reportedly met with representatives from the Military-Civilian Fusion Division of the Xi’an Development and Reform Commission and the Xi’an Weapons Science and Technology Industrial Base to discuss the development of next-generation information technology (IT) and opportunities for military-civil fusion. The Xi’an Weapons Science and Technology Industrial Base is a collaboration between Shaanxi Province and Norinco Group and serves as the central node for several defense innovation incubators that were unveiled in November 2018.

The U.S. government should take at least two other actions against Alibaba Cloud. First, Alibaba Cloud should be added to the Entity List. Its close ties to the PRC military renders it a clear ongoing national security threat. Furthermore, the Entity List has proven porous, as the Commerce Department has liberally granted licenses to export to listed companies. We therefore urge Commerce not only to list Alibaba Cloud, but also to deny license applications to export to the company. U.S. companies should not be aiding Alibaba Cloud with exported U.S. technology.

Second, the Secretary of the Treasury, in consultation with the Secretary of State, maintains the Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List) of PRC companies involved in the PRC military-industrial complex. U.S. persons may not trade these companies' publicly-traded securities. Specifically, under Executive Order 13959, the Secretary is directed to apply this ban to any company the Secretary determines "operate[s] or ha[s] operated in the defense and related material sector...of the economy of the PRC." Given the above evidence about Alibaba Cloud, Alibaba's parent company should be added to the NS-CMIC List.

In conclusion, we are deeply concerned about this growing trend of PRC-based cloud computing services engaging with entities that directly impact the national security interests of the United States. In addition to taking the above actions, we ask that you further investigate and act against China's other cloud service providers—including those not mentioned in this letter, such as Baidu Cloud and Tencent Cloud—and their direct or indirect operations in the United States that negatively impact our national security and foreign policy interests.

Thank you very much for your consideration of this vitally important national security matter.

Sincerely,



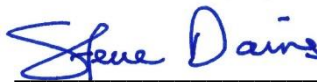
Bill Hagerty
United States Senator



Thom Tillis
United States Senator



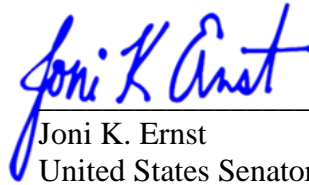
Marco Rubio
United States Senator



Steve Daines
United States Senator



Ted Cruz
United States Senator



Joni K. Ernst
United States Senator



Katie Boyd Britt
United States Senator



Kevin Cramer
United States Senator



Dan Sullivan
United States Senator