

United States Senate

WASHINGTON, DC 20510

December 18, 2019

The Honorable Elaine L. Chao
Secretary
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

The Honorable Stephen Dickson
Administrator
Federal Aviation Administration
800 Independence Avenue, SW
Washington, D.C. 20591

Dear Secretary Chao and Administrator Dickson:

We write to express concern regarding the national security threats posed by Chinese drones and urge the Department of Transportation (DOT) and Federal Aviation Administration (FAA) to ensure that the use of such drones is excluded from its programs and partnerships.

Given the information presented in several government directives regarding the use of Chinese-manufactured drones, we were dismayed to learn that on December 3, 2019, one of the ten lead participants of DOT and FAA's Unmanned Aircraft System (UAS) Integration Pilot Program (IPP) announced its decision to partner with Da Jiang Innovations (DJI) Inc., a Chinese drone company, and use DJI drones for aircraft inspections, delivery of aircraft parts, airport perimeter security, and various airport safety inspections.

On August 2, 2017, the Department of the Army released a memorandum ordering a halt on the use of DJI applications and products, citing an "increased awareness of cyber vulnerabilities associated with DJI products."¹ Subsequently, on August 9, 2017, Immigration and Customs Enforcement (ICE) released an unclassified bulletin which specifically warned against DJI for targeting critical infrastructure and law enforcement and providing U.S. data to the Chinese government. The bulletin states with "high confidence" that "the company [DJI] is selectively targeting government and privately owned entities within these sectors to expand its ability to collect and exploit sensitive U.S. data." The bulletin also warns that DJI-created apps, when used in conjunction with their UAS hardware, collect GPS locations and photographs taken by the device, register facial recognition data even when the system is off, and automatically upload information to cloud storage to which the Chinese government most likely has access. The bulletin continues, "[a] foreign government with access to this information could easily coordinate physical or cyber attacks against critical sites."²

¹ Gary Mortimer, "US Army Calls for Units to Discontinue Use of DJI Equipment," sUAS News (The Business of Drones, August 5, 2017), <https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment>

² "Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government" (Immigration and Customs Enforcement, August 9, 2017), <https://info.publicintelligence.net/ICE-DJI-China.pdf>

On May 20, 2019, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) issued an industry alert of the potential risks to an organization's information posed by Chinese-made drones and DJI in particular. The alert states that the products "contain components that can compromise data and share information on a server accessed beyond the company itself."³

More recently, on October 30, 2019, the Department of Interior announced that it was grounding its fleet of more than 800 non-emergency drones purchased from China until a security review is completed.⁴ Further, Section 848 of the Fiscal Year 2020 National Defense Authorization Act specifically prohibits the Department of Defense from operating or procuring UAS manufactured in China.

We commend the goal of the UAS IPP to partner federal, state, local, and tribal governments with the FAA to evaluate and integrate new technologies into airspace operations. We, however, urge you to immediately restrict the use of this equipment and technology that has the potential to jeopardize the security of critical information and infrastructure gained through this and other FAA programs. American taxpayer dollars should not fund state-controlled or state-owned firms that seek to undermine American national security and economic competitiveness. We therefore request the following information:

1. Have the DOT and FAA reviewed the reports by ICE, CISA, the Army, and any other agencies to appropriately grasp the magnitude of the threat posed by the use of DJI hardware and software, and if so, what conclusions were drawn?
2. Have the DOT and FAA conveyed their concerns with regard to data protection to the relevant state, local, and tribal partners in the IPP and any other program that may involve the use of drones?
3. What, if any, security efforts have the DOT and FAA worked to implement with state, local, and tribal officials to ensure critical infrastructure data does not fall into the hands of the Chinese government?

Thank you for your attention to this matter. We look forward to your prompt response.

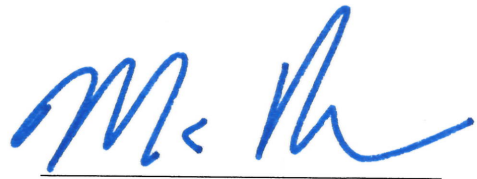
Sincerely,

³ David Shortell, "DHS Warns of 'Strong Concerns' That Chinese-Made Drones Are Stealing Data," CNN (Cable News Network, May 20, 2019), <https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html>

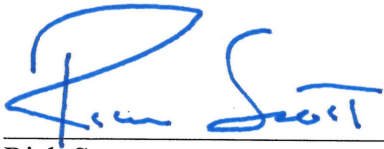
⁴ Timothy Puko and Katy Stech Ferek, "Interior Department Grounds Aerial Drone Fleet, Citing Risk From Chinese Manufacturers," The Wall Street Journal (Dow Jones & Company, October 30, 2019), <https://www.wsj.com/articles/interior-dept-grounds-aerial-drone-fleet-citing-risk-from-chinese-manufacturers-11572473703>



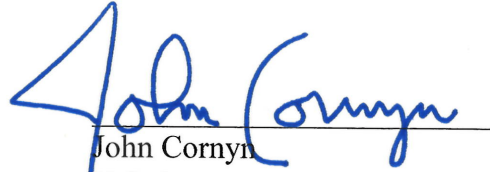
Marsha Blackburn
U.S. Senator



Marco Rubio
U.S. Senator



Rick Scott
U.S. Senator



John Cornyn
U.S. Senator



Tom Cotton
U.S. Senator