FCC NEWS from the Federal Communications Commission

CITING NATIONAL SECURITY RISKS, CARR CALLS FOR STARTING PROCESS OF ADDING DJI—A CHINESE DRONE COMPANY—TO FCC'S COVERED LIST

DJI Drones Are Collecting Vast Troves of Sensitive Data on Americans and U.S. Critical Infrastructure, Potentially Operating as a Huawei on Wings

WASHINGTON, DC, October 19, 2021—Today, at an event focused on strengthening America's national security, FCC Commissioner Brendan Carr called for commencing the process of adding DJI, a Shenzhen-based drone company that accounts for more than 50 percent of the U.S. drone market, to the FCC's Covered List.

Adding DJI to the Covered List would prohibit federal USF dollars from being used to purchase its equipment. The FCC also has a proceeding under way examining whether to continue approving equipment from entities on the Covered List for use in the U.S., regardless of whether federal dollars are involved. Huawei and four others are already on the Covered List based on a determination that they pose an unacceptable security risk.

"DJI drones and the surveillance technology on board these systems are collecting vast amounts of sensitive data—everything from high-resolution images of critical infrastructure to facial recognition technology and remote sensors that can measure an individual's body temperature and heart rate," Commissioner Carr stated. "Security researchers have also found that DJI's software applications collect large quantities of personal information from the operator's smartphone that could be exploited by Beijing. Indeed, one former Pentagon official stated that 'we know that a lot of the information is sent back to China from' DJI drones.

"DJI's collection of vast troves of sensitive data is especially troubling given that China's National Intelligence Law grants the Chinese government the power to compel DJI to assist it in espionage activities. In fact, the Commerce Department placed DJI on its Entity List last year, citing DJI's role in Communist China's surveillance and abuse of Uyghurs in Xinjiang. Add to this information the widespread use of DJI drones by various state and local public safety and law enforcement agencies as well as news reports that the U.S. Secret Service and FBI recently bought DJI drones, and the need for quick action on the potential national security threat is clear.

"After all, the evidence against DJI has been mounting for years, and various components of the U.S. government have taken a range of independent actions—including grounding fleets of DJI drones based on security concerns. Yet a consistent and comprehensive approach to addressing DJI's potential threats is not in place. That is why the FCC should take the necessary steps to consider adding DJI to our Covered List. We do not need an airborne version of Huawei. As part of the FCC's review—and in consultation with national security agencies—we should also consider whether there are additional entities that warrant closer scrutiny by the FCC."

In his remarks today calling for action, Commissioner Carr noted that since 2017 U.S. intelligence services have warned that DJI poses a security threat due to the level of sensitive information it collects and the risk of that data being accessed by Chinese state actors. Carr pointed to the following evidence:

- In 2017, an Intelligence Bulletin from a DHS field office stated that DJI is likely providing sensitive U.S. infrastructure and law enforcement data to the Chinse government.

- In 2019, the Department of Homeland Security issued an alert regarding Chinse-made drones like DJI, stating that "[t]he United States government has strong concerns about any technology product that takes American data into the territory of an authoritarian state that permits its intelligence services to have unfettered access to that data or otherwise abuses that access."

- In 2019, in passing the FY 2020 NDAA, Congress broadly prohibited the Department of Defense from purchasing Chinese-made drones, including DJI drones, based on national security concerns.

- In January 2020, the Secretary of the U.S. Department of the Interior issued an order that largely grounded the Department's fleet of drones, most notably DJI drones, based on concerns about cybersecurity and safeguarding access to sensitive data and information.

- In October 2020, DOJ's Office of Justice Programs barred the use of their funds for drones made by a "Covered foreign entity…determined or designated, within the Department of Justice, to be subject to or vulnerable to extrajudicial direction from a foreign government," including DJI.

- In December 2020, the Department of Commerce added DJI to its "Entity List," for having "enabled wide-scale human rights abuses within China through abusive genetic collection and analysis or high-technology surveillance, and/or facilitated the export of items by China that aid repressive regimes around the world, contrary to U.S. foreign policy interests."

- In January 2021, President Trump issued an Executive Order detailing the risks of Chinese-made drones, including DJI, and stated the U.S. policy "to prevent the use of taxpayer dollars to procure UAS that present unacceptable risks and are manufactured by, or contain software or critical electronic components from, foreign adversaries, and to encourage the use of domestically produced UAS."

- In July 2021, DOD stated that it remains convinced DJI systems "pose potential threats to national security," and DJI drones are still barred from use by DOD.

* * *

Carr has led FCC efforts to crack down on the threats posed by Communist China. In 2018, he urged the Commission to remove insecure network gear from our communications networks, a process that is now underway. In 2019, Carr called for the FCC to conduct a top-to-bottom review of every telecom carrier with ties to Communist China. The FCC has now launched proceedings to revoke the authorizations of several carriers. Earlier this year, Carr proposed that the FCC use its equipment authorization process to safeguard against security threats. The FCC initiated a proceeding to accomplish that in June. Today's call for action marks another step in his efforts to address the threats posed by Communist China.

###

Office of Commissioner Brendan Carr
www.fcc.gov/about/leadership/brendan-carr

Media Contact: Greg Watson
(202) 418-0658 or gregory.watson@fcc.gov