



INFORMATION AWARENESS BULLETIN



29 June 2021

(U//FOUO) Chinese Drones Present Risks to Sensitive Data

(U) Background

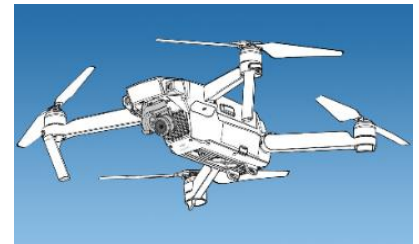
(U//FOUO) In June 2018, Chinese company DJI, also known as Da Jiang Innovations Science and Technology Co., Ltd., began a partnership with a US business to sell DJI's unmanned aerial systems (UAS) – or drones – to public safety and law enforcement (LE) agencies. The US government (USG) previously warned the People's Republic of China government may be able to access, collect, and manipulate data and information from users of Chinese made drones, including data related to US Critical Infrastructure and Key Resources (CIKR). As of April 2020, DJI offered disaster relief support to local law enforcement and safety partners by providing a drone donation or loaning drone equipment for three months in response to the COVID-19 pandemic.



(U) Information Gathering

(U//FOUO) The FBI is seeking information about DJI and its use by public safety and law enforcement agencies. Information of interest to the FBI includes, but is not limited to, the following:

- (U//FOUO) **DJI-provided information and materials:** presentations, trainings, terms-of-service policies, financial or legal obligations, equipment rights and responsibility agreements, bills of sale or equipment loan documents, and security policies;
- (U//FOUO) **Equipment-related details about donated or loaned drones:** model numbers, accessories, any required software and/or apps;
- (U//FOUO) **Donated or reduced price drone recipient agency location:** LE agency proximity to key US CIKR (e.g., military base, national laboratory, government facility, etc.);
- (U//FOUO) **Drone data policies (for user agencies and from DJI):** access, collection, analysis, storage, and protection/security;
- (U//FOUO) **Installation process and technical requirements:** associated software, apps, and network connection set up details;
- (U//FOUO) **Maintenance and repair:** process for maintenance or repair requests, software update requirements and process;
- (U//FOUO) **Reporting suspicious incidents:** cyber security events; unusual network behavior (e.g., delays or glitches); drone set-up anomalies; personnel solicitation for information; video/photography of employees, grounds, or agency activities;
- (U//FOUO) **Third-Party Platforms:** for DJI connectivity; operation; data collection, sharing, and management; and
- (U//FOUO) **Service providers:** Use of DJI or other Chinese-made drones by public safety agency service providers or contractors.



(U//FOUO) Responses to this request will provide the FBI with the necessary information to help inform guidance regarding the secure operations of these devices and services.

(U) RELEASABLE TO: Federal, State, Local, Fusion Centers, and TLOs.

Submit responsive information to this request via
<https://survey123.arcgis.com/share/2ca3022add9746fca949809f0bc3f3c9?portalUrl=https://aleagis.usgovcloudapp.virginia.cloudapp.usgovcloudapi.net/portal>