"Countering CCP Drones Act" – Frequently Asked Questions

What is the "Countering CCP Drones Act," and what does it do?

The "Countering CCP Drones Act" is a bill which would require the Federal Communications Commission (FCC) to add DJI to its "Covered List." If DJI is added to this list, the FCC could no longer approve new equipment authorizations for DJI products in the United States. The Agency could also create a process to revoke existing authorizations. This means that no new DJI products could be approved in the U.S. going forward, and the DJI drones currently approved for U.S. use may be grounded in the future.

What does the "Countering CCP Drones Act" mean for the drones I already have?

The "Countering CCP Drones Act" would not have an immediate impact on your current drone fleet. However, the FCC has the power to create a process to revoke the equipment authorizations for your existing drone models in the future, which would mean the federal government could decide at any point that you are no longer allowed to fly the DJI drones you have already purchased.

What will the "Countering CCP Drones Act" mean for future models of DJI drones?

The "Countering CCP Drones Act" would prohibit the FCC from authorizing or even reviewing equipment authorizations for new DJI products. This means that new DJI models would not be able to be sold or used in the United States going forward, cutting you off from the latest cutting-edge technology from DJI.

What data security safeguards does DJI have in place?

First, DJI drones do not need to connect to the internet to operate. Following initial activation, **DJI drones can be used entirely offline** via "airplane mode" on the phone or tablet attached to the remote controller if Internet access is not required. DJI also offers a "Local Data Mode" that allows a user to access the Internet for other reasons, such as accessing map services, but prevents any data from being transmitted to or from DJI's flight apps and the Internet. This essentially acts as an "airplane mode" that applies only to the drone's software, eliminating the possibility of accidental sharing of videos, photos or flight information during drone operations.

In addition, **DJI gives its drone operators control over the data they collect and generate**. DJI does not require operators to store any data with the company. If a user does not want to share their photos, videos and flight logs with DJI, the company cannot access it or provide it to anyone else. The only way that data gets shared is if the operator opts in to share it. Operators can also choose to grant or revoke data permissions at any time, and many models (such as the M300, M30, Inspire and Mavic 3 Enterprise) allow users to erase logs and cache through the DJI Pilot App. Certain DJI products also support password protection for onboard storage to guarantee the security of sensitive images and resources.

If users in the United States do choose to share photos, videos and flight logs with DJI, that data is kept in U.S.-based data centers and not transmitted to any other data centers or shared with third parties. Any sensitive information shared, such as location information, is given AES-256 encryption.

Finally, **DJI drones can also be used without DJI software** – if users prefer the features and security configurations of drone software developed by other companies around the world, they can choose from dozens of third-party options.

Has DJI's data security been confirmed by outside organizations?

Yes. Several government agencies and independent private sector firms have analyzed DJI products and issued reports attesting to their security. For example:

- San Francisco cybersecurity firm Kivu Consulting conducted a first-of-its-kind detailed examination of DJI drones, mobile apps, and servers, as well as the data streams they transmit and receive. Kivu purchased DJI drones off the shelf, downloaded DJI software from the Internet, then scrutinized every bit of data they exchanged over the Internet to determine whether customer data was in fact protected. The ensuing report concluded that DJI did not access photos, videos, or flight logs generated by the drones unless drone operators voluntarily chose to share them.
- A risk assessment conducted by Booz Allen Hamilton tested the data security of certain DJI drones and found no evidence that the data, or information collected by these drones was transmitted to DJI, China or any other unauthorized party.
- FTI Consulting found when Local Data Mode is enabled, "no data that was generated by the application was sent externally to infrastructure operated by any third party, including DJI." In its cybersecurity assessment, it also noted "a number of instances where DJI employed security best practices." The report also noted that when users opted to share their data with DJI, there was no data transmission to Chinese servers. All data went to servers in the U.S., or western Europe.
- The U.S. Department of the Interior (DOI), which has used drones for monitoring wildfires, conducting geological surveys, and inspecting volcanic activity, conducted a flight test and technical evaluation of its DJI drones. After a careful evaluation, DOI concluded that DJI drones were the best suited for accomplishing their missions while at the same time protecting the data they generate.
- The Idaho National Laboratory, which conducted a cybersecurity test and evaluation of two DJI drones on behalf of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, found that "there are no major areas of concern related to data leakage."
- The U.S. Department of Commerce validated DJI's Core Crypto Engine, confirming it meets NIST standard FIPS 140-2, for cybersecurity relating to government procurement.

How do you know DJI doesn't collect data?

Here's just one example. In 2017, DJI received a subpoena from the National Transportation Safety Board for information after a U.S. Army Black Hawk helicopter collided with a DJI drone over New York harbor. This data provided an obvious safety benefit, and DJI wanted to provide it – it was legally required, and it was the right thing to do. But because the drone pilot had never shared that data with DJI, the company simply didn't have any data to provide. Ultimately, the NTSB was able to access flight logs and other detailed information directly from the pilot, but it showed how DJI's commitment to data privacy works in practice.