# IMPLEMENTING MITIGATION MEASURES RECOMMENDED BY THE DHS

DJI values the trust our customers place in us to improve their businesses with drone technology, to make their operations safer and more efficient, and to help empower them to safeguard the data generated using our products. Safety and security are at the core of everything we do, because greater confidence in our technology will help unlock the full promise of drones. As technology has advanced, we have worked collaboratively with industry and government agencies to ensure the safe and secure use of our technology.

We would like to address the recent concerns driven by the **U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency Industry Alert** that was issued this week. In this Alert, four specific mitigating measures are referenced. Below are some guidelines on how to implement these mitigating measures when using DJI drones.

**1. DHS Recommendation: Deactivate Internet Connection from Device Used to Operate the UAS**

- Background: DJI aircraft are not directly connected to the internet, but instead use your mobile device, or a hotspot enabled controller with a built-in screen, to connect to the internet for updating apps, firmware and handle other basic functions.

- Solution: DJI's Pilot app for commercial operators offers 'Local Data Mode', a software feature that disables all external activity by the flight control app. The app supports DJI's enterprise aircraft including Matrice 200 Series, Mavic 2 Enterprise series and others. If you are using consumer aircraft compatible with DJI Go 4 only, you can easily disconnect your DJI UAS from the internet by enabling airplane mode on the mobile device.

**2. DHS Recommendation: Take Precautionary Steps Prior to Installing Updated Software or Firmware**

- Background: DJI releases a variety of different software, from flight control and fleet management to photogrammetry, across mobile, PC and cloud platforms. As with all software, there are regular updates that improve core functionality and stability. All updates go through DJI's software QA process to ensure they are secure prior to publication.

- Solution: For users concerned about updates to their existing flight control software on their mobile device, users can choose to disconnect their flight control applications from connecting to the internet as referenced above. This will prevent any software updates to the aircraft and flight control software.

- Solution: DJI's FlightHub Enterprise and FlightHub Government fleet management software provide your organizations IT team full control over release of all software and firmware updates to your UAS fleet, meaning that no software or firmware updates are pushed out unless mandated by your IT administrator. For users concerned about updates to their existing fleet management and other cloud or desktop-based software, please contact your organization's IT team to review the software before implementing it.

- Note: DJI's cloud and PC-based software are not critical for operating DJI drones and there are 3rd party options available from DJI's US-based partners.

**3. DHS Recommendation: Remove Secure Digital Card from the Main Flight Controller/aircraft**

- Background: SD cards are removable storage used to store images and videos the UAS captures. In most cases they are removable; the data is always accessible only to the user. DJI aircraft are not directly connected to the internet, and no DJI drone or controller is built with a cellular modem installed. Users may choose to connect a 4G dongle to the controller or connect to internet on their mobile phone to enable workflow-specific capabilities.

- Solution: SD cards would fall under each organization's data management policy, which would typically be administered and monitored by the IT Team. DJI encourages all organizations to manage their data in accordance with the policies they set, including the removal and storage of SD cards.

**4. DHS Recommendation: If SD Card is Required to Fly the Aircraft, Remove All Data from the Card After Every Flight**

- Background: To store footage users choose to capture during flight, each DJI aircraft can hold a single removable SD card and the newer Mavic 2 series also has in-built memory for storing image data.

- Solution for removable SD cards: Remove your SD card after each flight, retrieve data required, and clear contents of SD card prior to next flight.

- Solution for in-built storage: Download all footage captured then delete data stored on internal storage after each flight.

We will continue to directly address concerns about our products, and have invested significant resources in bolstering our security infrastructure so enterprise and government customers can securely integrate DJI hardware and software into their workflows.

DJI is committed to our partners and providing the best, safest, and most secure aerial platform for their work. We will continue to be available to discuss these issues further.