Thank you very much for your interest in DJI.

DJI products are safe and secure when flying even the most sensitive missions. Governments and businesses around the world trust and use our products because they keep their data safe. A wide range of independent security validations, from government agencies as well as private cybersecurity firms, have confirmed that DJI products are built with robust safeguards for data integrity. We are aware of critics and competitors who have claimed otherwise; simply put, their claims are false.

As we are sure you appreciate, we respect our customers and partners, and we never share any information about whether or how they use DJI products. Thus, we are unable to confirm or deny whether the Dutch government, or any other customer, uses our products, or what security measures they would use if they did. Speaking generally, however, DJI products are designed and built so customers do not have to share any of their data with anyone – including DJI. DJI does not have access to the flight logs, photos or videos generated during drone flights unless customers choose to actively share that data by syncing flight logs with DJI servers, uploading photos or videos to our platforms, or physically delivering the drone to DJI for service.

In addition, DJI government and enterprise customers who are concerned about data security can use Local Data Mode in the DJI Pilot, DJI GO4 or DJI Fly control apps to provide enhanced data privacy assurance when flying sensitive missions. It is an internet connection "kill switch" feature that, when enabled, prevents the app from sending or receiving any data over the internet. With this feature enabled, drone operators can easily and effectively cut off all network connections from DJI's mobile applications and prevent any data from being transferred to DJI or other parties.

Government agencies can also use DJI's Government Edition, which was developed to U.S. government requirements and has been repeatedly validated by U.S. government agencies – including the Department of Defense. It includes:

- No Data Transmission – A permanently enabled Local Data Mode within the custom DJI Pilot application prevents users from accidentally or even intentionally transferring data from the mobile application over the internet to third parties or to DJI.
- Firmware Reviews – Government agency aviation and IT departments can review firmware updates in electronic isolation before applying them to their fleets, and have full control over how to validate them and when to install them on DJI drones.
- Restricted Hardware Pairing – Drones and remote controllers running Government Edition solution firmware can only be linked with each other and are not compatible with other off-the-shelf DJI products, preventing the use of unsecure hardware and unauthorized third-party applications.

Our Government Edition products have previously been validated by the U.S. Department of Interiorand U.S. Department of Homeland Security. In addition, independent audits of our products have also validated the data protections we build into them:

- FTI Consulting conducted a comprehensive analysis of DJI hardware and softwareincluding a source code review of DJI applications as well as a hardware cybersecurity review of devices. All DJI products were procured independently for testing and DJI provided FTI with access to more than 20 million lines of application source code for an audit focused on understanding communication protocols and destinations. The FTI audit found that when Local Data Mode was enabled, no data generated by the drone or application was sent externally to infrastructure operated by any third party, including DJI, validating DJI's assertions about the utility and function of the feature.

- The cybersecurity team at global consulting firm Booz Allen Hamilton, on behalf of PrecisionHawk's Unmanned Aerial Intelligence Technology Center of Excellence (UAS COE), examined three specific DJI commercial drone products: The Government Edition Mavic Pro, Government Edition Matrice 600 Pro, and the Mavic 2 Enterprise. The audit found no evidence of data transmission connections between these drones and DJI, China, or any other unexpected party. From our perspective, this important finding from an independent, globally recognized leader in cybersecurity indicates that DJI customers have control over the data they collect when using our drones, contradicting reports that data from DJI devices is surreptitiously routed to other parties.

We are aware of various claims made over the years by cybersecurity researchers who have found vulnerabilities in our products, as happens with all software from all manufacturers. DJI has addressed this challenge forthrightly, and led its competitors by developing the first Bug Bounty Program in the drone industry. To date, DJI has paid more than $90,000 to more than 100 researchers who have responsibly identified vulnerabilities so we could fix them (a partial list of those researchers is available at this link.) As you noted in your list, while some of the claimed vulnerabilities were greatly exaggerated or misunderstood how our products are used, others were legitimate vulnerabilities which were patched promptly after disclosure.

The data security of DJI products has been reviewed repeatedly, and the fundamental strength of their security architecture remains unchallenged. The fact that drone users in government and critical industries continue relying on DJI illustrates that when our products are evaluated on a factual and technical basis, not headlines or innuendo, their utility and security remains unmatched.