DEPARTMENT OF THE NAVY
PROGRAM EXECUTIVE OFFICER
UNMANNED AVIATION AND STRIKE WEAPONS
RADM WILLIAM A MOFFETT BUILDING
47123 BUSE ROAD BLDG 2272
PATUXENT RIVER, MD 20670-1547

5230
Ser PMA-263/17-183
MAY 24 2017

From: Program Manager, Navy & Marine Corps Small Tactical Unmanned Aircraft Systems (PMA-263)
To: Small Unmanned Aircraft System Program Managers (SUAS-PM)

Subj: OPERATION RISKS WITH REGARDS TO DJI FAMILY OF PRODUCTS

1. Background. New counter Unmanned Aircraft Systems (UAS) technologies have been fielded to counter the increasing use of commercially available small UAS by our adversaries. To support training and Tactics, Techniques and Procedures development associated with these counter UAS systems, operational forces require threat representative Small Unmanned Aircraft Systems (SUAS). The most prevalent of these SUAS are the DJI family of quadcopters. While these systems are commonly available and low cost, the DoD has minimal technical information to thoroughly understand the impact of their use. The following operational risks have been identified and should be acknowledged prior to employment of these commercially procured SUAS assets for CONUS-based training.

2. Operational Risks.

a. Cyber vulnerabilities. A thorough study of the cyber vulnerabilities of these systems is not available at this time. Additionally, due to the rapidly changing configurations and open nature of the available software, cyber threats will continue to evolve. Of particular concern is the data link between the aircraft and the ground station. While encrypted, open source research indicates numerous techniques available to passively view the video and metadata from the air vehicle as well as assume control over the air vehicle by adversaries. Also, the typical Ground Control Station (GCS) configuration includes a COTS transmitter, controller, phone or tablet utilizing WiFi or DJI proprietary Lightbridge. Open source research indicates when the transmitter, controller, tablet or phone is connected to the web, images, video and flight records could be uploaded to unsecure servers in other countries via live streaming, or transmitted once the air vehicle is connected to a computer using the DJI assistant application. Overall, the system should be considered highly vulnerable in the cyber security realm and employed accordingly.

Recommended mitigations:

- Conduct training operations in areas that limit the potential of adversaries to be in reception range of the GCS and Air Vehicle signals.
- Conduct training in areas that are not operationally sensitive.
- Do not connect the GCS to military networks using wired or wireless connections.

- Avoid connecting the GCS to the world wide web using wired or wireless connections, but if necessary, ensure all images, video and flight records are deleted from the GCS cache and micro-SD cards prior to connection to the web.
- The Air Vehicle has the capability to store images/video on a micro- SD card when installed in the GCS, the air vehicle, or a combination of both. Due to the potential for loss of the air vehicle, operation with the SD card installed is NOT RECOMMENDED. The DJI platforms can perform all necessary flight functions without the use of recording media. This means both GCS internal memory (cache), and external memory.
- Cover the camera when not in use using the plastic gimbal support included in the kit.
- Do not use Personal Phones (i.e. 3G/4G/LTE Network) or Hot spots to access Map Data.

b. Electromagnetic compatibility. To date, a thorough investigation of electromagnetic susceptibility has not been conducted on these systems; therefore the potential to experience interference is high. Interference can disrupt or preclude operation of the system and potentially loss of control of the air vehicle.

Recommended mitigations:

- Operation should be conducted with maximum practical standoff distance between the GCS/Air Vehicle and other RF transmitters to reduce the potential for unintended interference.
- Closely monitor link quality indications (GPS signal strength) to minimize possibility of loss of link.

c. Low reliability. While these systems are commonly available, anecdotal evidence demonstrates that they are not highly reliable when employed in typical military environments. Loss of the air vehicle through damage, or malfunction should be considered highly probable over time; DJI systems are expendable.

3. Training and Technical Support. The Group 1 Unmanned Aircraft System Training and Readiness Manual require completion of the course of instruction specific to the system assigned to operate. It also requires that the SUAS Operators be designated by the unit commanding officer before being authorized to operate a SUAS on the unit's table of equipment or other fielded equipment. Formal training and limited technical assistance is available for DJI systems procured by PMA-263 are available at the Training and Logistics Support Activities (TALSA) located on Camp Lejeune and Camp Pendleton. No supply support will be provided beyond the spare parts delivered with fielded systems.

Recommended mitigations:

- Ensure SUAS operators are certified and designated prior to operating the systems.
- Commanders should allow operators to build experience with the systems under controlled conditions prior to employment in more complex training scenarios.
- Care should be exercised in operation to minimize damage to the systems in order to prolong the life of these assets to the maximum extent practical.

4. PMA-263 requests that these risks be reviewed and unit operators complete applicable formal training. Any questions concerning this letter should be addressed to the PMA-263 Group I Class Desk: (b) (6), at (b) (6) or (b) (6), at (b) (6).

(b) (6)

COL USMC