Security Guidelines for Drone Operating Systems

August 3, 2020

Aviation security regulator BCAS has issued guidelines for drone operating systems, which **act like cockpits on the ground to remotely pilot the unmanned aerial vehicle.**

Security Guidelines

The BCAS has listed out rules that should be followed for cyber security, storage facility, training and background check of staff for drone operating systems or remotely piloted aircraft systems. **A remotely piloted aircraft (RPA), its associated remote pilot station, its required command and control links and any other components constitute a remotely piloted aircraft system (RPAS).**

- It should be ensured that **CCTV cameras are installed inside RPAS and the storage facility. The capacity to retain recording of minimum 30 days shall be in place** for all categories of RPAs except for mini and micro. An RPA or drone is in nano or mini category if it has weight less than 250 grams. If its weight is between 250 grams and 2 kg, it is in the micro category.
- **Access control of the RPAS and RPA storage area must be ensured.** As RPAS is similar in purpose and design to a cockpit, it is understood that it must likewise be **secured from sabotaged or unlawful malicious interference.** According to BCAS, the remote pilot station in the RPAS is of "fixed and exposed" nature as opposed to the "restricted nature" of a commercial plane where the intrusion and use of heavier weapons is less likely.
- Therefore, further consideration must be given to the potential vulnerability of the premises of the remote

pilot stations against unlawful interference. The aircraft (drones) itself shall be stored and prepared for flight in a manner that will **prevent and detect tampering and ensure the integrity of vital components.**

- Safety and security of data and communication links and services are equally important as those for the drones and their remote pilot stations, as per the guidelines issued. Accordingly, it shall be ensured that **they (links and services) are free from hacking, spoofing and other forms/interference or malicious hijack.**
- Moreover, the drone operator must ensure that all of its **staff are provided one-day aviation security awareness training online** as recommended by BCAS. Background check of remote pilots and support personnel (visual observer, launch crew and recovery crew) shall be carried out following due procedure.
- If there is any security incident or accident, it must be reported to the local police, the BCAS control room and the regional director of BCAS without any unnecessary delay. Each RPA and RPAS operator must **establish, implement and maintain a security programme, based on the aforementioned guidelines, and it must be submitted to BCAS before its operation.**
- The operator of RPAS must obtain relevant permissions from the local administration and the Directorate General of Civil Aviation (DGCA) before operating the RPAS.

From June 8, the Civil Aviation Ministry has started the registration process for non-compliant drones which were not registered with the DGCA and have not been granted the drone acknowledgement numbers (DANs). On June 5, the ministry had issued draft rules for manufacturing and use of drones in the country wherein it has proposed that an authorised drone manufacturer or importer can sell its devices only to an individual or entity approved by the DGCA.