PARROT SE RANGE SECURITY INFORMATION

JUNE 2020

HIGHLY SECURE TO KEEP YOUR DATA SAFE

- **Designed in EUROPE, France**
- **Cyber-secured** drone and connections
- **Authentication and AES encryption of the wireless link between Anafi and the remote controller using WPA2 :** Prevents an attacker from sending fake control orders to ANAFI Thermal SE or viewing the video feed.
- **Denial of Service (DoS) mitigation** : Enhancement against WiFi DoS. Resilient to WiFi and GPS denial of service.
- **Integrity of ANAFI Thermal SE**: **Digital signature** of ANAFI Thermal SE firmware and **restricted access** to the drone operating system. Prevents attackers to tamper the firmware with malicious software
- **Protect user data** : No data sent to Parrot servers by default.
- **Protect your location** : If the drone is caught by an adversary party, the adversaries are prevented to get information on the take-off position, flight data or remote pilot position.

CYBER SECURED

Authentication and encryption

- WPA2 is based on AES-CCMP cipher, which is an industry standard. In addition to cipher, AES-CCMP includes a CBC-MAC mechanism providing authentication and integrity.
- WPA2 provides AES128 encryption and the key length is up to 256 bits.
- Unique WPA2 key generated for each pair of ANAFI Thermal SE and remote controller (the user can easily set his own WPA2 key in FreeFlight6 settings).

Denial of Service (DoS) mitigation

- Any wireless protocol can be blurred by an attacker. When using a flight plan, losing the WiFi connection has no effect: ANAFI Thermal SE continues to fly accordingly to its flight plan. In manual flight, when ANAFI Thermal SE loses connection with the remote controller, it activates the Smart RTH (Return To Home): the drone gets closer to the take-off position or a configurable position till the remote controller reconnects to the drone.
- To identify attempt of an attacker to blur GPS signal, an indicator of the quality of the signal is displayed. A specific warning indicates to the operator if the signal is lost. Loss of GPS has no effect on manual flight.

Integrity of Anafi

- Each ANAFI Thermal SE firmware is digitally signed by Parrot, in FRANCE. Before installation of the new firmware, ANAFI Thermal SE verifies this digital signature. Thus, an attacker can't push a tampered firmware modified with malicious content.
- Access to the operating system of ANAFI Thermal is protected. ANAFI Thermal doesn't provide a mechanism to connect to the operating system locally or remotely.

Protect user data

- The user can choose to send anonymous data to help Parrot enhance ANAFI Thermal SE or synchronize its flight data with its My.Parrot account. These options are opt-out by default: no data is sent to Parrot servers unless the user chooses to.

Protect your location

- On ANAFI Thermal SE, in addition to protecting access to the operating system and its memory, flight plans and temporary Blackbox files are written in volatile memory only. No log file is written on the SD Card. If the drone is caught by an adversary party, they won't be able to get information on the take-off position, flight data or remote pilot position.