Secure Your Drone

PRIVACY AND DATA PROTECTION GUIDANCE

Drones are quickly becoming integrated into our everyday lives, similar to our smartphones and computers. As drones grow in popularity, they could become easy targets for those who want to exploit the vulnerabilities of connected devices to compromise our individual privacy.

This security guidance presents options for drone users to protect their data and minimize privacy risks.

What is a Connected Device?

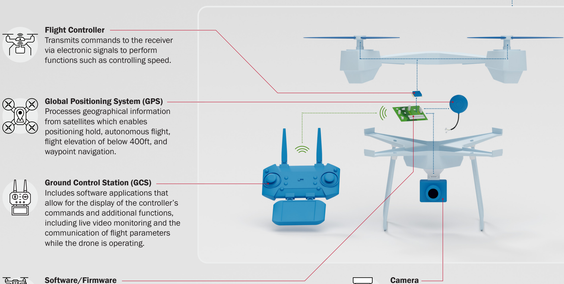
Connected devices are physical objects that connect and exchange data with other devices and systems via the internet.

Across the country, individuals and organizations use connected devices and systems daily. Connected devices include laptops, smartphones, tablets, smart home systems, cars, and drones.

As connected devices, drones are often connected to the internet and other devices via Bluetooth. As a result, they take on many of the vulnerabilities of these connections and are susceptible to cyberattacks and privacy violations.

Connected Components

Drone components that gather and communicate information via the internet or Bluetooth are vulnerable to exploitation.



Flight Controller
Transmits commands to the receiver via electronic signals to perform functions such as controlling speed.

Global Positioning System (GPS)
Processes geographical information from satellites which enables positioning hold, autonomous flight, flight elevation of below 400ft, and waypoint navigation.

Ground Control Station (GCS)
Includes software applications that allow for the display of the controller's commands and additional functions, including live video monitoring and the communication of flight parameters while the drone is operating.

Software/Firmware
Synchronizes all components of drone operation by sending commands received from the controller to various physical components of the drone. In most cases, the operator must update software and firmware via Wi-Fi to operate the drone reliably.

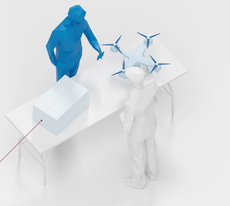
Camera
Enables first-person view for real-time and advanced image processing via analog wireless transmission.

Drone Security at Every Stage

To make a data or privacy breach less likely, commercial and recreational drone users should ensure that their devices are protected throughout all stages of drone activity.

PRE-FLIGHT

Ensuring your drone's security begins before your purchase is even complete. Consider the following recommendations before purchasing a drone and during set-up to protect your data privacy.



Buying your drone

Beware: Using a drone and critical components manufactured and developed by foreign countries carries an increased risk of a foreign adversary gaining unauthorized access to your personal information.

Consider:

- Understanding where your drone is manufactured.
- Taking time to understand the manufacturer's privacy policy before purchasing, including how and where your data will be stored and shared.

Setting up your drone account

Beware: When signing up on applications, your personal information, including credit card information, may be stored and shared with the manufacturer.

Consider:

- Looking into the manufacturer's registration requirements and determining what information you can opt out of sharing.
- Using strong passwords for accounts and/or changing any default passwords.
- Setting up two-factor authentication, if possible.
  - A code is sent to your mobile phone or computer when your drone is used. Without entering the correct code, your drone cannot be used.

Connecting to the internet or other connected devices

Beware: Your drone is a remotely controlled connected device vulnerable to hacking and hijacking by those with criminal intent.

Consider:

- Only connecting to secure Wi-Fi.
- Enabling airplane mode whenever possible and taking precautions to protect yourself when using the internet.
- If you own a foreign-manufactured drone, turning on Local Data Mode (LDM) to block your data from being transmitted or shared.

Downloading and maintaining software and firmware required to fly your drone

Beware: Your drone's system includes software and firmware that synchronizes all components of drone operation. The drone cannot operate without the software applications. Hackers may attempt to manipulate the software to disrupt the functionality of your drone and to access data.

Consider:

- Updating your software and firmware on a regular basis to address specific vulnerabilities.
- Downloading software from authenticated and secure vendor websites.
- Reviewing any licensing agreements prior to software approval.
- Understanding software updates before installing.

DURING FLIGHT

Now that your drone is set up, ensure that all of its components are secure while conducting flight activities.

Utilizing GPS while in flight

Beware: Your drone relies on GPS for navigation and positioning, and criminals can misdirect or even control the receivers.

Consider:

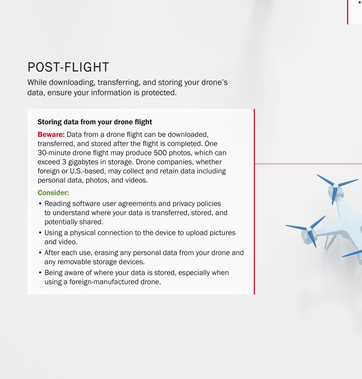
- Setting a determined Return to Home (RTH) location to ensure drone recovery.
- Taking the time to do a GPS calibration before flight.
- Avoiding sources of signal interference.

Using your camera to take pictures or recordings during flight

Beware: Cameras are susceptible to hacking, allowing criminals to gain access to personal footage and photos taken during flight.

Consider:

- Obtaining camera lens covers. Remove lens cover prior to launch and then reinstall immediately after motor(s) stop.
- Engaging the kill function on the GCS to ensure that the camera does not provide unintended visibility to areas surrounding your drone.
- Using a virtual private network (VPN) when sharing videos.



Commanding and controlling your drone via a GCS (e.g., hand controller, laptop, tablet, or smartphone)

Beware: Your drone and the GCS send signals back and forth to communicate and share location data, videos, and photos acquired during flight. Those with criminal intent may seek to hack into the GCS to disrupt operations, gain control of your drone, or access the data being transmitted.

Consider:

- Ensuring GCS firmware is up to date to bridge any patches.
- Using a VPN if you are operating your drone using a wireless network.

POST-FLIGHT

While downloading, transferring, and storing your drone's data, ensure your information is protected.

Storing data from your drone flight

Beware: Data from a drone flight can be downloaded, transferred, and stored after the flight is completed. One 30-minute drone flight may produce 500 photos, which can exceed 3 gigabytes in storage. Drone companies, whether foreign or U.S.-based, may collect and retain data including personal data, photos, and videos.

Consider:

- Reading software user agreements and privacy policies to understand where your data is transferred, stored, and potentially shared.
- Using a physical connection to the device to upload pictures and video.
- After each use, erasing any personal data from your drone and any removable storage devices.
- Being aware of where your data is stored, especially when using a foreign-manufactured drone.

Additional Resources

- **CISA UAS Website:** cisa.gov/unmanned-aircraft-systems
- **CISA Cybersecurity Best Practices for Operating Commercial sUAS:** cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems
- **CISA Cybersecurity Performance Goals:** cisa.gov/cpg
- **CISA Cyber Essentials:** cisa.gov/publication/cisa-cyber-essentials
- **CISA Multi-Factor Authentication:** cisa.gov/mfa
- **CISA Report Phishing:** cisa.gov/uscert/report-phishing
- **CISA Shields Up:** cisa.gov/shields-up
- **CISA Stop Ransomware:** cisa.gov/stopransomware
- **Blue UAS Cleared List:** diu.mil/blue-uas-cleared-list
- **FAA guidance on safe and secure drone operation:** faa.gov/uas
- **The Recreational UAS Flyers Safety Test:** faa.gov/uas/recreational_flyers/knowledge_test_updates

What to do if you are the victim of a cyber crime

- ☐ If your drone is compromised, CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities at us-cert.cisa.gov/forms/report.
- ☐ If you are the victim of a network intrusion, data breach, or ransomware attack, contact your nearest Federal Bureau of Investigation (FBI) field office or report it at tips.fbi.gov.
  - You may also wish to call your local law enforcement or 9-1-1.
- ☐ If you are the victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3) at ic3.gov.