SECURING CRITICAL INFRASTRUCTURE AND PUBLIC GATHERINGS FROM SMALL UNMANNED AIRCRAFT SYSTEM (SUAS) THREATS

Agenda

Introduction

SUAS Threats

Cyber Security Options

CISA Resources

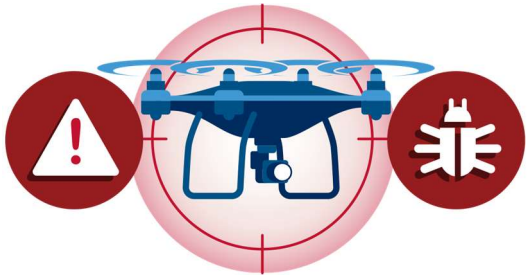
Conclusion

Introduction

Introduction

One of CISA's most important missions is to understand and advise on the physical and cyber risks to our Nation's critical infrastructure.

The use of **small unmanned aircraft systems** (sUAS), more commonly known as *drones*, has emerged as a particularly concerning cyber-physical risk.



Threats

DHS Threat Definition

The reasonable likelihood that sUAS or unmanned aircraft activity—if unabated—would:

Inflict or otherwise cause physical harm to a person; inflict or otherwise cause damage or harm to assets, facilities, or systems

Interfere with the operational mission, including movement, security, or protection of a covered facility or asset

Facilitate unlawful activity

Conduct unauthorized surveillance or reconnaissance

Result in unauthorized access to, or disclosure of classified, sensitive, or otherwise lawfully protected information

Threat Actors

Careless & Clueless

- Overwhelming majority in U.S.
- Common Commercial Off The Shelf (COTS) multi-rotor platforms
- Witting and unwitting violations of the NAS
- Effective detection and tracking by most C-UAS radio frequency sensors when present

Intentional & Criminal

- Primarily across international borders and prisons
- COTS sUAS modified to carry/drop payloads
- Drugs, money, cell phones, weapons
- Detection and tracking are possible, but mitigation is unlikely

Terrorists & Paramilitary

- Threats to populated areas/critical infrastructure
- Customized fixed wing sUAS (larger, faster, farther)
- Can avoid C-UAS detection through use of autopilot
- Similar attacks already occurring OCONUS
- Detection and tracking is difficult, mitigation very difficult

Cyber/IP Theft

The U.S. government has strong concerns about any technology product that takes American data into the territory of an authoritarian state that permits its intelligence services to have unfettered access to that data or otherwise abuses that access.

Those concerns apply with equal force to certain foreign- manufactured sUAS-connected devices capable of collecting and transferring potentially revealing data about their operations and the individuals and entities operating them.

Cyber Security Options

Cyber Security Best Practices

Installation and Use of sUAS Software and Firmware

- Ensure that the devices used for the download and installation of sUAS software and firmware do not access the enterprise network.
- Run all downloaded files through an up-to-date antivirus platform before installation and throughout installation. Verify a firewall is enabled on the computer or mobile device.
- Thoroughly review any license agreements prior to approval. During installation, do not follow "default" install options.

Securing sUAS Operations

- If using Wi-Fi, ensure the data link supports an encryption algorithm for securing Wi-Fi communications.
- Use the most secure encryption standards available and complicated encryption keys that are changed regularly.

Data Storage and Transfer

- Use a standalone computer to connect to the sUAS or removable storage device to ensure no access to the Internet or enterprise network.
- Follow data management policies for data at rest, data in transit, and any sensitive data.
- Erase all data from the sUAS and any removable storage devices after each use.

Sharing and Vulnerability Reporting

- The Cyber Information Sharing and Collaboration Program (CISCP) cisa.gov/CISCP or CISCP_Coordination@hq.dhs.gov.
- The Automated Indicator Sharing (AIS) Program us-cert.gov/ais/.
- The Information Sharing and Analysis Centers (ISAC) https://www.nationalisacs.org/.
- CERT Coordination Center: kb.cert.org/vuls/report/.

Incident Reporting

- Email CISA at Central@cisa.gov
- Call 1-888-282-0870.
- Visit us-cert.cisa.gov/report.

CISA Resources

CISA Resources

Exercises and Vulnerability Assessments

Tools and Best Practices

Legal Authorities Explainers
and guidance documents for non-federal public and private entities.

Analytical Information
Videos, Fact Sheets, Guides, FAQs.

For more information:
www.cisa.gov

Questions?
sUAS Security
Email: suassecurity@cisa.dhs.gov