



## CYBERSECURITY BEST PRACTICES FOR OPERATING COMMERCIAL UNMANNED AIRCRAFT SYSTEMS (UASs)



UASs provide innovative solutions for tasks that are dangerous, time consuming, and costly. Critical infrastructure operators, law enforcement, and all levels of government are increasingly incorporating commercial UASs into their operational functions and will likely continue to do so. Although UASs offer benefits to their operators, they can also pose cybersecurity risks, and operators should exercise caution when using them.<sup>1</sup>

To help UAS users protect their networks, information, and personnel, the Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) identified cybersecurity best practices for operating commercial UASs. This document can assist in standing up a new UAS program or securing an existing UAS program, and is intended for information technology managers and personnel involved in UAS operations. Similar to other cybersecurity guidelines and best practices, the identified best practices can aid critical infrastructure operators to lower the cybersecurity risks associated with the use of UAS, but do not eliminate all risk.

### Installation and Use of UAS Software and Firmware

- Ensure that the devices used for the download and installation of UAS software and firmware do not access the enterprise network.
- Properly verify and securely conduct all interactions with UAS vendor and third party websites. Ensure file integrity monitoring processes are in place before downloading or installing files.
- Run all downloaded files through an up-to-date antivirus platform before installation and ensure the platform remains enabled throughout installation. Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic.
- Thoroughly review any license agreements prior to approval. During installation, do not follow “default” install options. Disable automatic software updates. Necessary updates should follow the same process outlined for download and installation.

- Use complicated Service Set Identifiers (SSIDs) that do not identify UAS operations on the network. Set the UAS to not broadcast the SSID or network name of the connection.
- Use standalone UAS-associated mobile devices with no external connections, or disable all connections between the Internet and the UAS and UAS-associated mobile devices during operations.
- Run mobile device applications in a secure virtual sand-box configuration that allows operation while securely protecting the device and the operating system.

### Data Storage and Transfer

- Use a standalone computer to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network.
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused from the connection of the UAS or removable storage device. Verify and ensure that the computer has up-to-date antivirus installed.
- Follow data management policies for data at rest, data in transit, and any sensitive data.
- Erase all data from the UAS and any removable storage devices after each use.

### Securing UAS 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.

(Continued on Back)

<sup>1</sup>For more information on UAS cybersecurity risks, see: DHS Office of Cyber and Infrastructure Analysis. (2018). “Cybersecurity Risks Posed by Unmanned Aircraft Systems.” PDM17252. Additional information can be found in: DHS Cybersecurity and Infrastructure Security Agency. (2019). “Unmanned Aircraft Systems Industry Alert.”

## Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs)



### Information Sharing and Vulnerability Reporting

By participating in information-sharing programs and reporting non-public, newly-identified vulnerabilities, users will have access to timely information to mitigate cybersecurity threats.

- The Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely information exchange through trusted, public-private partnerships across all critical infrastructure (CI) sectors. For more information on the CISCP program, visit [cisa.gov/CISCP](https://cisa.gov/CISCP) or email [CISCP\\_Coordination@hq.dhs.gov](mailto:CISCP_Coordination@hq.dhs.gov).
  - The Automated Indicator Sharing (AIS) Program enables the quick exchange of cyber threat indicators between the Federal Government and the private sector through CISA. For more information on NCCIC 24/7 services, call 1-888-282-0870 or email [NCCICCustomerService@hq.dhs.gov](mailto:NCCICCustomerService@hq.dhs.gov). For more information on AIS and how to join, go to <https://www.us-cert.gov/ais/>.
  - The Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry. For more information about ISACs, go to <https://www.nationalisacs.org/>.
- If a UAS software or hardware vulnerability is discovered, or a suspicious or confirmed UAS cybersecurity incident occurs, CISA recommends reporting the vulnerability or incident through the following channels:
- Email CISA at [NCCICCustomerService@hq.dhs.gov](mailto:NCCICCustomerService@hq.dhs.gov) or call 1-888-282-0870. When sending sensitive information to DHS CISA via email, we recommend encryption of messages. For more information, visit <https://ics-cert.us-cert.gov/Report-Incident>.
  - To report a vulnerability to the CERT Coordination Center, go to <https://www.kb.cert.org/vuls/report/>.



### CONTACTS

National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
U.S. Department of Homeland Security

For More Information, contact [NRMCM@hq.dhs.gov](mailto:NRMCM@hq.dhs.gov)  
or visit our website:  
[www.cisa.gov/national-risk-management](https://www.cisa.gov/national-risk-management)

# UNMANNED AIRCRAFT IN THE HOMELAND SECURITY ENVIRONMENT

## DHS OFFICE OF INTELLIGENCE & ANALYSIS UAS THREAT INTEGRATION CELL

0001-19



Overall classification of this briefing is

**UNCLASSIFIED**

*Protecting the Homeland Through Predictive Intelligence and Analysis*

UNCLASSIFIED



# (U) Contents

(U) *Special Topic*: 14 September 2019 Attacks in Saudi Arabia

(U) Unmanned Aircraft Systems (UAS) – definition and scope

(U) Threat Environment

(U) Evolution of UAS as a Weapon

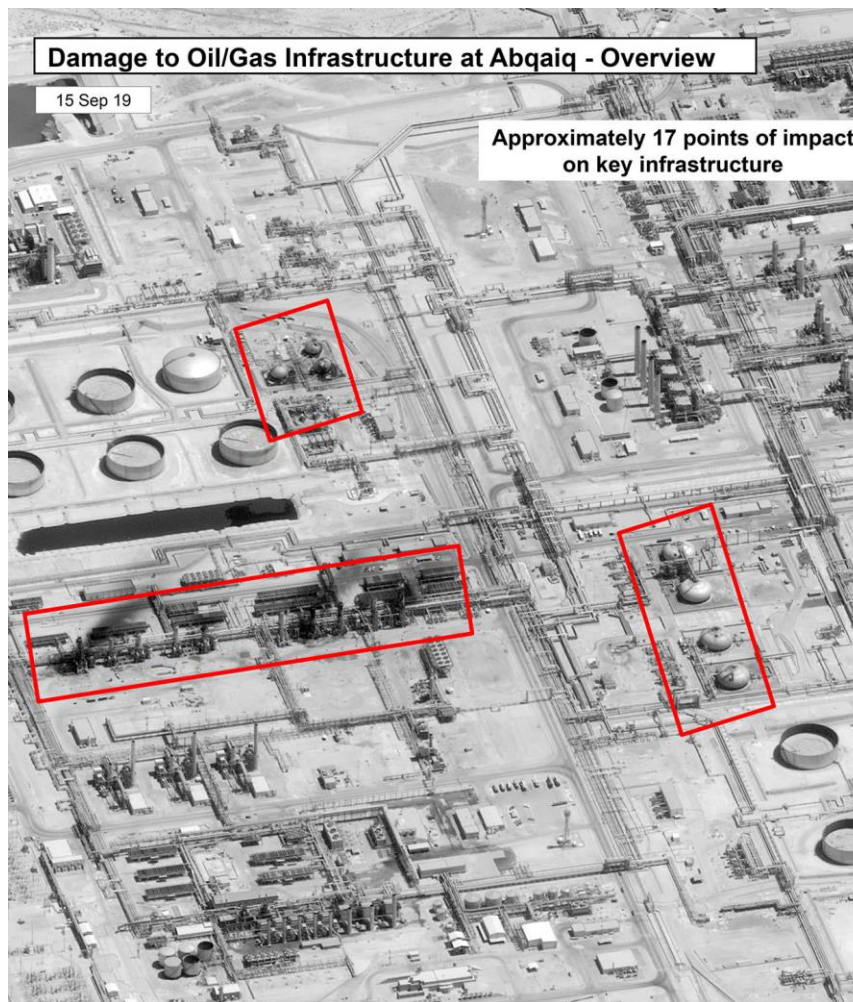
(U) Recent Incidents

(U) Mitigation





# (U) Special Topic: 14 September 2019 Attacks



*Protecting the Homeland Through Predictive Intelligence and Analysis*

UNCLASSIFIED

## (U) Moment of Zen



*Protecting the Homeland Through Predictive Intelligence and Analysis*

UNCLASSIFIED

# (U) UAS-Definitions and Scope

- (U) UAS, UAV, RPAS, Drone, etc
- (U) UAS is defined by statute, PL 112-095, Section 331:
  - (U) *“an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system”*
- (U) Functionally, UAS are:
  - a type of aircraft capable, without an on-board operator/pilot, which are generally internet-enabled, aerial collection platforms used by enthusiasts, commercial, and public entities*
- (U) This discussion focuses on small UAS (less than 55 lbs) which are available to the public for purchase (e.g. commercial off the shelf).





# (U) Evolution of Use as a Weapon, 2011-2018



Timeframe	2011-2012	2014-2016	2017-2018
Weight/Cost	40 lbs/\$3900	2-10 lbs/up to \$2000	20 lbs/N-A
Payload	~5 lbs*	2-4 lbs	15-20 lbs



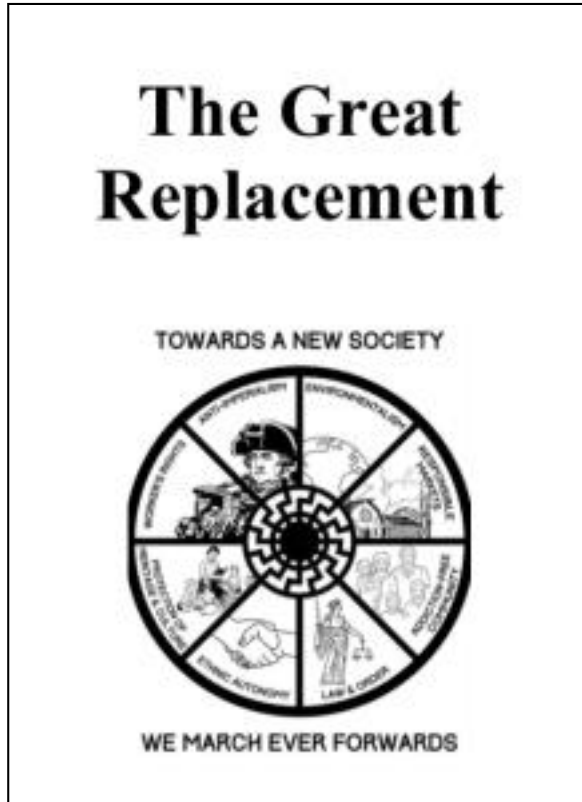
*Protecting the Homeland Through Predictive Intelligence and Analysis*

UNCLASSIFIED



# (U) Recent Incidents-New Zealand

(U) Manifesto released by gunman on 15 March 2019 promoted use of UAS with explosive to target political figures (pg 39)



*Protecting the Homeland Through Predictive Intelligence and Analysis*

UNCLASSIFIED//FOR OFFICIAL USE ONLY

## (U) UAS Near Manned Aircraft



(U) August 2018, UAS near helicopter in Hollywood, FL



(U) Early 2018, Video posted of UAS near commercial aircraft on approach into Las Vegas

(U) 21 September 2017, collision with Army helicopter supporting UNGA



*Protecting the Homeland Through Predictive Intelligence and Analysis*

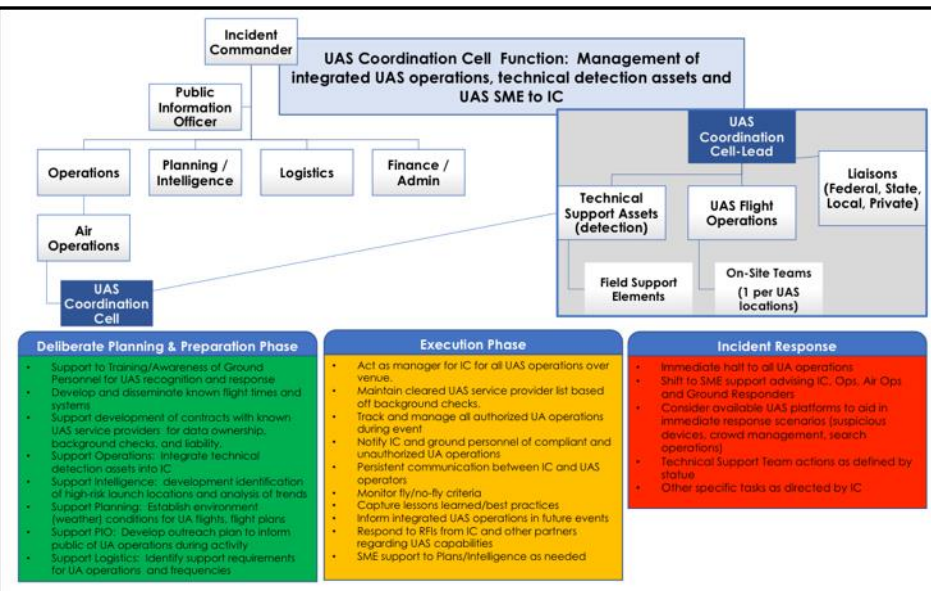
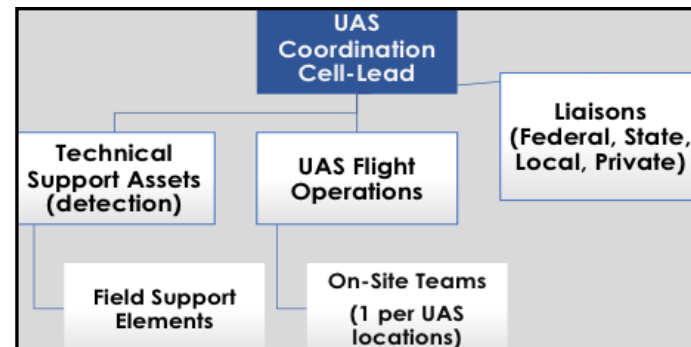
UNCLASSIFIED



# (U) Counter-UAS Operations

Prepare—Detect—Track—Characterize—Mitigate—Investigate—Analyze—Disseminate

(U//FOUO) Notional UAS Coordination Cell function: Management of Integrated UAS operations, technical detection assets and UAS SME to Incident Commander.



## Deliberate Planning & Preparation Phase

- Support to Training/Awareness of Ground Personnel for UAS recognition and response
- Develop and disseminate known flight times and systems
- Support development of contracts with known UAS service providers for data ownership, background checks, and liability.
- Support Operations: Integrate technical detection assets into IC
- Support Intelligence: development identification of high-risk launch locations and analysis of trends
- Support Planning: Establish environment (weather) conditions for UA flights, flight plans
- Support PIO: Develop outreach plan to inform public of UA operations during activity
- Support Logistics: Identify support requirements for UA operations and frequencies



Protecting the Homeland Through Predictive Intelligence and Analysis

UNCLASSIFIED



# UNMANNED AIRCRAFT IN THE HOMELAND SECURITY ENVIRONMENT

DHS OFFICE OF INTELLIGENCE & ANALYSIS  
UAS THREAT INTEGRATION CELL



## DISCUSSION



*Protecting the Homeland Through Predictive Intelligence and Analysis*

UNCLASSIFIED

# SECURING SOFT TARGETS AND CROWDED PLACES

## COUNTERING-UNMANNED AIRCRAFT SYSTEMS

DANIEL RIVERA  
SECURITY PROGRAMS



**CISA**  
CYBER+INFRASTRUCTURE

Unclassified / For Official Use Only

# DHS Threat Definition

**The reasonable likelihood that UAS 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.



**CISA**  
CYBER+INFRASTRUCTURE

Unclassified / For Official Use Only



# DHS C-UAS AUTHORITY

# C-UAS Legal Authorities

## Preventing Emerging Threats Act

Grants DHS and DOJ the authority to take certain actions to counter threats posed by UAS to “covered facilities or assets.” This authority sunsets in 2022.

Authorized Department of Homeland Security Components may protect Covered Facilities and Assets from unlawful UAS activity with the following actions:



Detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft.



Warn the operator of the unmanned aircraft system or unmanned aircraft.



Disrupt control of the unmanned aircraft system or unmanned aircraft.



Seize or exercise control of the unmanned aircraft system or unmanned aircraft.



Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.



Use reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

## Covered Facility or Asset

Directly relate to the following missions:

**An authorized Department of Homeland Security mission, including certain protection and security missions of:**

- U.S. Coast Guard
- U.S. Customs and Border Protection
- U.S. Secret Service
- Federal Protective Service

**An authorized joint Department of Homeland Security or the Department of Justice mission**

- National Special Security Events
- Special Event Assessment Rating events
- Supporting state, local, tribal, or territorial law enforcement at certain mass gatherings upon the request of a State's governor or equivalent
- Active Federal law enforcement investigations, emergency responses, or security operations in specified locations and for limited duration (e.g., airport disruption, disaster response, etc.)

“Covered facilities or assets” must be designated by the Secretary and:

- Located in the United States, including territories and possession, territorial seas and navigable waters
- Identified by DHS, in coordination with DOT, as high-risk and potential target for unlawful UA activity
- Does not include persistent protection of airports or critical infrastructure



**CISA**  
CYBER+INFRASTRUCTURE

# U.S. DEPARTMENT OF HOMELAND SECURITY ACTIONS




**CISA**  
CYBER+INFRASTRUCTURE

Unclassified / For Official Use Only



# Resources: Website & Fact Sheet

Provides access to resources that the Department of Homeland Security makes readily available to inform stakeholders and the general public about the threats posed by UAS and actions that can be taken to mitigate risk.



## Unmanned Aircraft Systems

Addressing Critical Infrastructure Security Challenges

### What Is the Threat?


In addition to recreational use, unmanned aircraft systems (UAS)—also known as unmanned aerial vehicles (UAV) or drones—are used across our Nation to support firefighting and search and rescue operations, to monitor and assess critical infrastructure, to provide disaster relief by transporting emergency medical supplies to remote locations, and to aid efforts to secure our borders. However, UAS can also be used for malicious schemes by terrorists, criminal organizations (including transnational organizations), and lone actors with specific objectives.

UAS-related threats may include:

- **Weaponized or Smuggling Payloads** – Depending on power and payload size, UAS may be capable of transporting contraband, chemical, or other explosive/weaponized payloads.
- **Prohibited Surveillance and Reconnaissance** – UAS are capable of silently monitoring a large area from the sky for nefarious purposes.
- **Intellectual Property Theft** – UAS can be used to perform cyber crimes involving theft of trade secrets, technologies, or sensitive information.
- **Intentional Disruption or Harassment** – UAS may be used to disrupt or invade the privacy of other individuals.

### Why Is This Threat Important to Critical Infrastructure?

Since UAS use in the United States has increased as a cost-effective, versatile business and national security tool, as well as a popular recreational hobby, the Federal Aviation Administration (FAA) estimates combined hobbyist and commercial UAS sales will rise from 2.5 million in 2016 to 7 million by 2020. As a result, potential threats associated with UAS will continue to expand in nature and



UAS flying over a bridge in New York City (Source: DHS)


increase in volume in the coming years. Because of their physical and operational characteristics, UAS can often evade detection and create challenges for the critical infrastructure community.

### What Actions Can You Take?

Recognizing and implementing security practices that meet Federal, State, and local regulatory requirements are key to successfully managing potential security incidents associated with UAS. Although no single solution will fully mitigate this risk, there are several measures that can be taken to address UAS-related security challenges:


- Research and implement legally approved counter-UAS technology.
- Know the air domain around the facility and who has authority to take action to enhance security.
- Contact the FAA to consider UAS restrictions in close proximity to fixed site facilities. More information can be found at [www.faa.gov/uas/](http://www.faa.gov/uas/).
- Update Emergency/Incident Action Plans to include UAS security and response strategies.
- Build Federal, State, and local partnerships for adaptation of best practices and information sharing. More information can be found at [www.dhs.gov/homelandsecurity](http://www.dhs.gov/homelandsecurity).
- Report potential UAS threats to your local law enforcement agency.

February 2017



## Unmanned Aircraft Systems (UAS) – Critical Infrastructure

In addition to recreational use, unmanned aircraft systems (UAS)—also known as unmanned aerial vehicles (UAV) or drones—are used across our Nation to support firefighting and search and rescue operations, to monitor and assess [critical infrastructure](#), to provide disaster relief by transporting emergency medical supplies to remote locations, and to aid efforts to secure our borders. However, UAS can also be used for malicious schemes by terrorists, criminal organizations (including transnational organizations), and lone actors with specific objectives.



[Download a printer-friendly fact sheet on UAS Challenges to Critical Infrastructure.](#)

[Expand All Sections](#)

- What Is the Threat? +
- Why Is the Threat Important to Critical Infrastructure? +
- What Actions Can You Take? +
- UAS and Critical Infrastructure – Understanding the Risk (Video) +
- DHS UAS Resources +






**CISA**  
CYBER+INFRASTRUCTURE

Unclassified / For Official Use Only



<https://www.dhs.gov/uas-ci>

# Resources: Pocket Card

Provides information on actions that security and operations officers can take if a UAS is seen operating near an infrastructure. It also contains information regarding the different types of UAS and their respective flight ranges and payload capabilities, along with quick tips on how to properly report UAS-related incidents.

Category	Range	Payload	<b>INCIDENT REPORTING QUICK TIPS*</b> <ul style="list-style-type: none"><li>● Identify Operator and Witnesses (Name &amp; Contact Info)</li><li>● Type of Incident (Commercial, Hobby, Public/Governmental)</li><li>● Type of Device (s) and UAS Registration Number</li><li>● Event Location and Incident Details (Date, Time, and Place)</li><li>● Evidence Collection (Photos, Video, Device (s))</li></ul>
Retail Quadcopter 	Up to 3 Miles	0-2 lbs.	
Retail or Custom Multi-rotor 	3-10 Miles	3-15 lbs.	
Commercial Applications 	Varies	15-30 lbs.	

**CRITICAL REFERENCE TIPS**

**Critical Infrastructure Security & Operations Officers  
Tips in Responding to a UAS Incident**

**D**irect attention outward and upward to attempt to locate individuals who are holding a controller or device (laptop, notebook, cell phone) and appears to be operating a UAS. Look at windows, balconies, rooftops, and open spaces. For special events, predetermine likely locations that would enable a person to control a UAS.

**R**eport incident to state or local law enforcement immediately and request a response if necessary. Execute organization's emergency response action plan if appropriate.

**O**bserve the UAS and maintain visibility of the device. Look for the direction of travel, damage to facilities, and individuals. NOTE: Battery life is typically 20-30 minutes.

**N**otice features and identify the type of device (i.e., Fixed-wing/Multi-rotor/Retail or Custom), size, shape, color, payload, video camera equipment, and activity.

**E**xecute appropriate security/emergency response action by maintaining a safe environment for the public and first responders in accordance with Federal, State, and local laws and regulations. Document event details including photos if possible.

# Resources: Instructional Video

Provides information on the threats posed by the nefarious use of UAS, potential implications to critical infrastructure operations, and options for risk mitigation. Subject matter experts and senior security officials are leveraged to further the message on the importance of mitigating the risks associated with this evolving threat.



**CISA**  
CYBER+INFRASTRUCTURE

Unclassified / For Official Use Only



# DHS UAS Mitigation Resources

## Public Website

## UAS – Critical Infrastructure Website



## Informational Video

## UAS and Critical Infrastructure – Understanding the Risk



## HSIN Website

## UAS and Emerging Threats Portal



## Fact Sheet

## C-UAS Legal Authorities



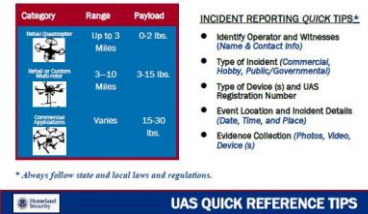
## Best Practices

# Cybersecurity Best Practices for Operating Commercial UASs



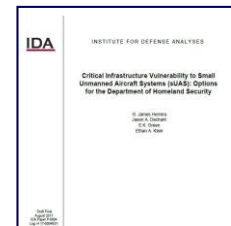
## Awareness Cards

## UAS CI Drone Pocket Card



## IDA Report

## Critical Infrastructure Vulnerability sUAS: Options for DHS



## Industry Alert

## Chinese Manufactured Aircraft Systems



Unclassified / For Official Use Only



CISA  
CYBER+INFRASTRUCTURE



**CISA**  
CYBER+INFRASTRUCTURE

Unclassified / For Official Use Only

# CYBERSECURITY BEST PRACTICES FOR OPERATING COMMERCIAL UAS



**CISA**  
CYBER+INFRASTRUCTURE

Christian Lowry  
National Risk Management Center  
November 18, 2019

# Why a best practices document?

- Critical infrastructure operators, law enforcement, and all levels of government are incorporating UASs into their operations
- UASs offer benefits to their operators, but can also pose cybersecurity risks
- These best practices are intended for information technology managers and personnel involved in UAS operations



**CISA**  
CYBER+INFRASTRUCTURE

Christian Lowry  
National Risk Management Center  
November 18, 2019



# Installation and use of UAS software and firmware

- Ensure that the devices used for the download and installation of UAS software and firmware do not access the enterprise network.
- Properly verify and securely conduct all interactions with UAS vendor and third party websites.
- Run all downloaded files through an up-to-date antivirus platform before installation and ensure the platform remains enabled throughout installation.
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic.
- Thoroughly review any license agreements prior to approval.



# Securing UAS Operations

- If using Wi-Fi, ensure the data link supports a secure encryption algorithm for securing Wi-Fi communications.
- Use complicated Service Set Identifiers (SSIDs) that do not identify UAS operations on the network.
- Use standalone UAS-associated mobile devices with no external connections, or disable all connections between the Internet and the UAS and UAS-associated mobile devices during operations.
- Run mobile device applications in a secure virtual sand-box configuration that allows operation while securely protecting the device and the operating system.



**CISA**  
CYBER+INFRASTRUCTURE

Christian Lowry  
National Risk Management Center  
November 18, 2019

# Data Storage and Transfer

- Use a standalone computer to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network.
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic. Verify and ensure that the computer has up-to-date antivirus installed.
- Follow data management policies for data at rest, data in transit, and any sensitive data.
- Erase all data from the UAS and any removable storage devices after each use.

# Information sharing and vulnerability reporting

- Cyber Information Sharing and Collaboration Program (CISCP)
  - Visit [cisa.gov/CISCP](https://cisa.gov/CISCP) or email [CISCP\\_Coordination@hq.dhs.gov](mailto:CISCP_Coordination@hq.dhs.gov).
- Automated Indicator Sharing (AIS) Program:
  - Call 1-888-282-0870 or email [NCCICCustomerService@hq.dhs.gov](mailto:NCCICCustomerService@hq.dhs.gov).
  - For more information on AIS and how to join, go to <https://www.us-cert.gov/ais/>.
- Information Sharing and Analysis Centers (ISACs)
  - For more information about ISACs, go to <https://www.nationalisacs.org/>.

**If a UAS software or hardware vulnerability is discovered, or a suspicious or confirmed UAS cybersecurity incident occurs:**

- Email CISA at [NCCICCustomerService@hq.dhs.gov](mailto:NCCICCustomerService@hq.dhs.gov) or call 1-888-282-0870.
- To report a vulnerability to the CERT Coordination Center, go to <https://www.kb.cert.org/vuls/report/>.







**CISA**  
CYBER+INFRASTRUCTURE

For more information:  
**[cisa.gov](https://cisa.gov)**

Questions?  
**[christian.lowry@cisa.dhs.gov](mailto:christian.lowry@cisa.dhs.gov)**



**CISA**  
CYBER+INFRASTRUCTURE