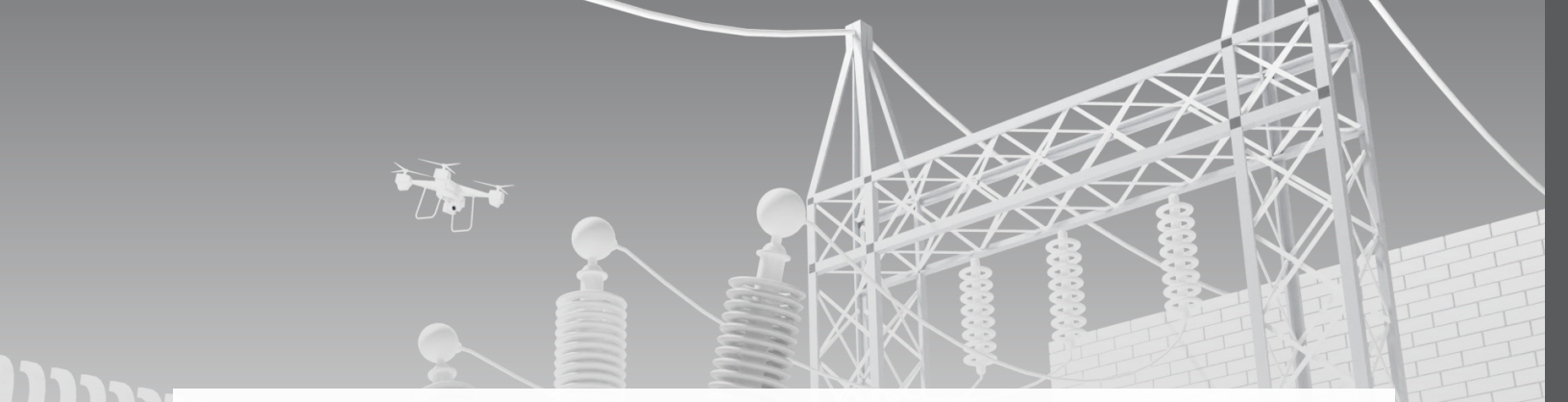
SUSPICIOUS UNMANNED AIRCRAFT SYSTEM ACTIVITY GUIDANCE

FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS

JULY 2025

Cybersecurity and Infrastructure Security Agency



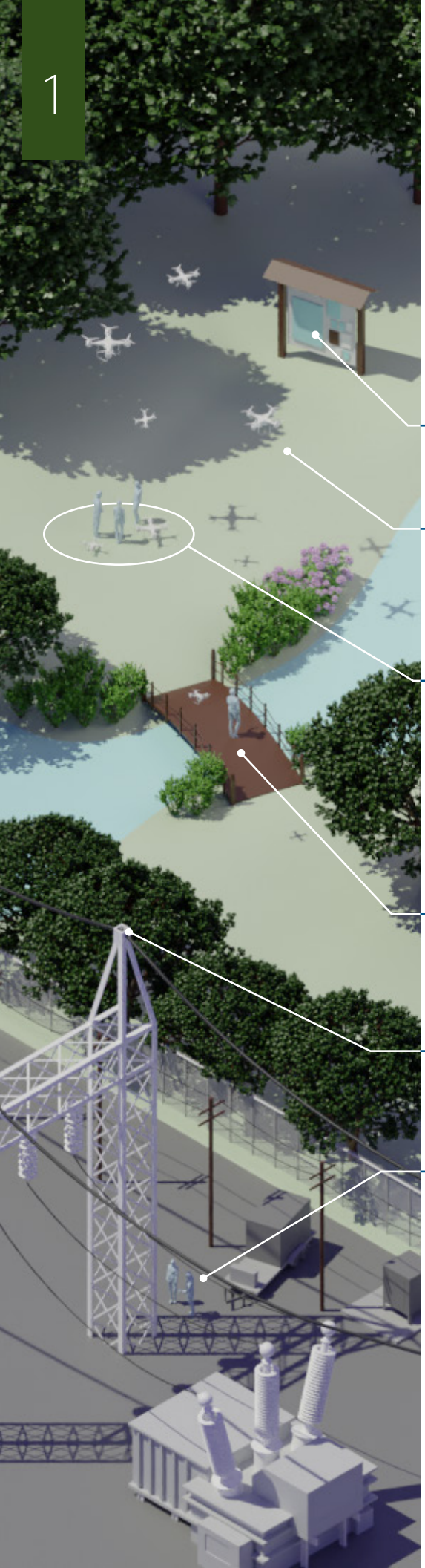
Introduction

The frequency of unmanned aircraft systems (UAS)[1] operating near critical infrastructure is expected to increase as the commercial and recreational use of UAS expands. Most UAS activity is likely non-threatening to critical infrastructure operations and compliant with Federal Aviation Administration (FAA) regulations. However, some UAS flights, based on their flight pattern and other indicators, may raise concerns of suspicious activity that requires further examination.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to establish procedures that help security personnel distinguish between routine and suspicious UAS activity. This will assist in preserving incident response resources while also helping to ensure an accessible airspace for compliant UAS operators. Organizations should consider the following key actions when responding to UAS activity:

1. **Determine routine UAS activity in the surrounding area.**
2. **Understand UAS risks to critical assets and operations.**
3. **Recognize indicators of potential criminal activity.**
4. **Respond appropriately to UAS activity.**

1 The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system. 49 USC 44801: Definitions. Retrieved from https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title49-section44801&num=0&edition=prelim



1

Determine Routine UAS Activity in the Surrounding Area

Identifying planned, or routine, UAS flights in the area surrounding critical infrastructure can help determine when and where UAS activity may be expected. Facility owners should communicate expected UAS activity to security staff and regularly update them to account for new flight patterns in the area.

Consider the following when mapping routine UAS activity:

Determine if the surrounding airspace is designated by the FAA as controlled or restricted.

Contact the FAA Flight Standards District Office (FSDO) to determine if UAS testing ranges or commercial delivery routes exist nearby that could explain multiple UAS flights.

Engage with local UAS hobbyist groups or radio-controlled (RC) aircraft clubs to identify areas where recreational flights are likely to occur, including popular takeoff and landing locations.

Connect with local government and community stakeholders, such as the chamber of commerce, to know when special events may include the use of UAS.

Survey surrounding areas to identify locations that may be of high interest to aerial photography enthusiasts, such as local attractions, iconic locations, natural features, or botanical gardens.

Identify critical infrastructure that may require beyond visual line of sight (BVLOS)[2] operations to conduct inspections such as rail tracks, pipelines, or energy lines.

Collaborate with nearby facilities and public safety officials to share information on planned UAS flights.

Visit FAA's B4UFLY to learn more about flight restrictions.

2 BVLOS refers to the operation of UAS beyond the visual line of sight of the operator and visual observer. For more information, see: Federal Aviation Administration's Unmanned Aircraft Systems Beyond Visual Line of Sight Aviation Rulemaking Committee. (2022). Final Report. Retrieved from https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS_BVLOS_ARC_FINAL_REPORT_03102022.pdf

2 Understanding UAS Risks to Critical Assets and Operations

When determining potentially suspicious UAS activity, a risk assessment considering UAS capabilities and asset vulnerabilities may provide valuable insight.

CAPABILITIES

Understanding the wide range of UAS capabilities may help determine how UAS could be used to compromise safety, security, or sensitive information. Common UAS capabilities that may present a hazard to critical infrastructure or facilitate criminal activity include:

High-definition cameras capturing high-resolution images and videos that may support surveillance or other actions to compromise security or sensitive information.

Light detection and ranging (LiDAR) systems providing highly detailed mapping of terrain and objects, which can expose structural vulnerabilities or exploitable site characteristics.

Thermal imaging sensors detecting heat emitted by objects, providing increased awareness of sensitive areas or possible vulnerabilities.

Infrared sensors detecting infrared radiation emitted by objects, providing increased awareness of sensitive areas or possible vulnerabilites.

Portable jammer emitting radio signals that may be used to disrupt radio frequency signals and other communication capabilities.

Cyber-based platforms, providing advanced capabilities to cybercriminals that can exploit networks and wireless communications. Examples include Raspberry Pi, Wi-Fi Pineapple, and Flipper Zero.

Drop mechanisms enabling UAS to remotely release items over crowds.

Sprayers dispersing liquid or aerosol chemicals that can cause harm or panic.

Cargo deliveries carrying hazardous payloads within established perimeters.

VULNERABILTIES

Identifying critical assets and operations vulnerable to potential UAS threats will assist in determining when suspicious UAS activity may pose a threat. Consider the following when conducting an evaluation:

Locations that host densely populated crowds, vulnerable to a physical attack.

Hazardous material storage and processing locations, vulnerable to possible sabotage or an attack.

Wirelessly controlled Industrial Control Systems (ICS) or Information Technology/Operations Technology (IT/OT) systems, vulnerable to a cyberattack.

Communication assets, vulnerable to a cyber or physical attack.

Sensitive operations, research, developments, and intellectual property, vulnerable to surveillance.

Security and access control assets, vulnerable to observation or cyberattack.

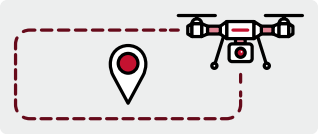
Power generation or distribution assets, vulnerable to a UAS collision or attack.

3

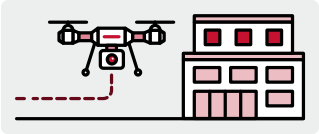
Recognize Indicators of Suspicious UAS Activity

Detecting suspicious UAS activity is dependent on several indicators, including both UAS and operator behaviors. Indicators may be observed by eyewitness accounts, UAS detection technology, or a combination of both.

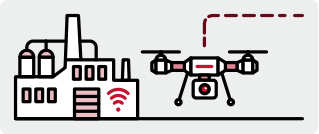
Consider the following when observing and documenting possible suspicious UAS activity:



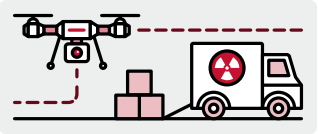
Is the UAS flying in observable patterns that may indicate mapping of restricted or sensitive locations? Examples may include flying along perimeter lines or intentionally moving between known sensitive assets.



Is the UAS hovering near locations vulnerable to video or audio surveillance? Examples may include windows, corporate headquarters locations, or research and development sites.

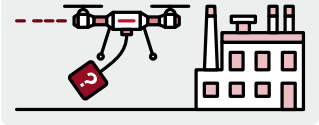


Is the UAS hovering near ICS or IT/OT locations, or moving in a pattern to suggest it is searching out open Wi-Fi access points?

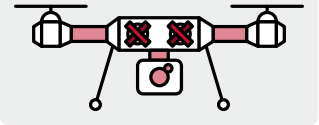


Is the UAS flying in a pattern that suggests a pre-operational plan to sabotage or attack sensitive locations? Examples include UAS consistently appearing during the delivery or transfer of sensitive or hazardous materials and during significant operational changes, such as security changes.

Is the UAS activity outside of normal facility operating hours? Examples may include flights during hours of darkness or low light.



Does the UAS have observable payloads that raise suspicion? Examples may include sprayers in a non-agriculture community or dangling wires.



Does the UAS have modifications that may suggests nefarious intent? Examples include disabled or masked lights.

Is the UAS detectable, either from Remote ID[3] or other UAS detection technology? If not, the UAS may be modified to prevent Remote ID broadcasts and/or evade detection technology.

3 Remote ID is the ability of a drone in flight to provide identification and location information that can be received by other parties through a broadcast signal. Federal Aviation Administration. (2024). Remote Identification of Drones. Retrieved from https://www.faa.gov/uas/getting_started/remote_id

Critical infrastructure security personnel may consider locating the UAS operator when appropriate and if security protocols allow. This can be achieved by direct visual observation or with the use of UAS detection technology, as permitted by law.[4] Direct visual observation involves physically scanning the surrounding area to locate the operator. UAS detection technology uses various modalities to geolocate the UAS's ground control station.

Upon locating the UAS operator, and in consultation with law enforcement, security personnel should carefully consider whether to approach operators about the UAS activity. Additionally, consider CISA's de-escalation series[5] for non-confrontational techniques to avoid unnecessarily escalating the situation.

Consult legal counsel prior to the use of UAS detection technology and before engaging with UAS operators. !

ENGAGEMENT

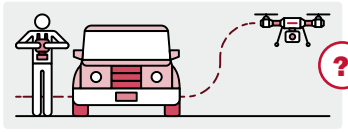
Consider asking the following questions if the operator is willing to engage:

What is the purpose of the flight? Examples may include recreational, commercial, media, or public service.

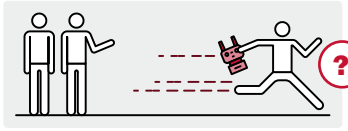
Can the UAS flight be adjusted to avoid operating over the facility?

OBSERVATION

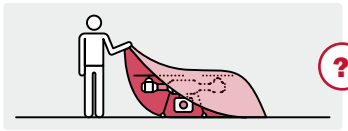
Consider the following when deciding whether to approach or engage a UAS operator:



Does the operator appear to be operating from a concealed location? Examples may include a vehicle, wooded area, or otherwise camouflaged.



Does the operator flee when approached?



Does the operator attempt to destroy or conceal the UAS or associated equipment?

Does the operator attempt to fly or land the UAS far away to prevent confiscation?

Does the operator behave aggressively or in a confrontational manner?

4 If considering using detection technology, entities are strongly encouraged to seek legal counsel informed by the interagency Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems, dated August 17, 2020, available at: https://www.dhs.gov/publication/interagency-legal-advisory-uas-detection-and-mitigation-technologies

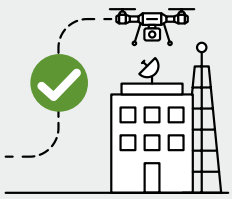
5 Cybersecurity and Infrastructure Security Agency. (December 2024). De-escalation Action Guide. Retrieved from: https://www.cisa.gov/resources-tools/resources/de-escalation-action-guide

4

Respond Appropriately to UAS Activity

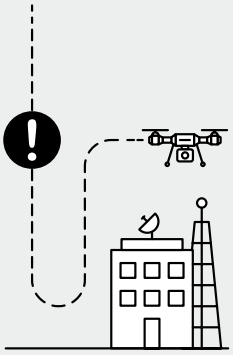
Use information collected through UAS observation and any operator engagement to make informed decisions on next steps. Physical security, cybersecurity, business continuity, safety, and operational representatives should be consulted when deciding on a course of action. **Possible scenarios include:**

UAS activity is non-threatening or determined to be authorized operations.



UAS activity near restricted or sensitive locations may be the result of a careless operator. These operators will **often present no threat and comply with security or law enforcement requests** to avoid critical infrastructure. Additionally, remote pilots operating under FAA regulations may be conducting authorized or pre-coordinated flights supporting public or commercial interests. **Incidents in this category can be logged as non-suspicious and included as part of future routine UAS activity, if appropriate.**

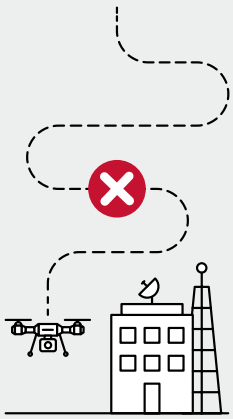
UAS activity remains suspicious but lacks sufficient indicators to suggest potential criminal activity.



UAS activity that lacks sufficient detail to determine intent may be considered suspicious. However, unless the totality of information suggests concerning activity, that may impact operations, **consider documenting the incident internally** for future tracking and use the information to adjust expectations of routine UAS activity. **Incident details can also be shared across the organization** for awareness. Encourage security staff to continue monitoring for similar activity that may be related or suggest a pattern.

Once put in context with other reports or information, certain UAS activity may indicate potential criminal activity—making the collection and maintenance of internal reporting information very important, as it can support law enforcement efforts.

UAS activity poses a security or safety risk and possible criminal activity is suspected.



UAS activity suspected of conducting or planning criminal acts should be reported to local law enforcement. Quickly activating elevated security responses may enhance protection of exploitable vulnerabilities. **A detailed summary of the possible criminal activity should be prepared and presented to law enforcement.** Information may also be shared with the FAA by contacting the local Flight Standards District Office (FSDO) or Law Enforcement Assistant Program (LEAP) agent.

Potential criminal activity may include:

- Pre-operational planning to sabotage critical assets, including surveillance.
- Conducting espionage or intellectual property theft.
- Transporting cyber-enabled tools to compromise networks.

Additional Resources

Be Air Aware™: cisa.gov/topics/physical-security/be-air-aware

De-escalation Action Guide and Power of Hello: cisa.gov/resources-tools/resources/de-escalation-action-guide and cisa.gov/topics/physical-security/conflict-prevention/power-hello

Suspicious UAS Identification Poster and Postcard: cisa.gov/resources-tools/resources/suspicious-uas-identification-poster-and-postcard

Suspicious Activity and Items: cisa.gov/suspicious-activity-and-items

TRIP*wire*: cisa.gov/resources-tools/resources/technical-resource-incident-prevention-tripwire-portal

CISA Tabletop Exercise Packages: cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

ChemLock: cisa.gov/chemlock

CISA Regional Security Advisors: cisa.gov/about/regions/security-advisors

CISA Regions: cisa.gov/about/regions

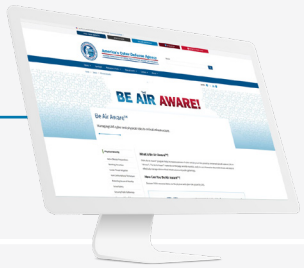
CISA Central: cisa.gov/cisa-central

FAA UAS Resources: faa.gov/uas

Flight Standards District Office (FSDO) | Federal Aviation Administration: faa.gov/about/office_org/field_offices/fsdo

Law Enforcement Assistance Program (LEAP) | Federal Aviation Administration: faa.gov/about/office_org/headquarters_offices/ash/ash_programs/investigations/leap

FAA B4UFLY: faa.gov/uas/getting_started/b4ufly



CISA's **Be Air Aware™** resources help increase awareness of cyber and physical risks posed by unmanned aircraft systems (UAS). **Be Air Aware™** materials provide essential, ready-to-use information about UAS threats and steps to effectively manage risk to critical infrastructure and public gatherings.

CISA developed this guidance in partnership with government, unmanned aircraft system subject matter experts, and industry representatives from across critical infrastructure sectors. To learn more about the 16 critical infrastructure sectors, visit Critical Infrastructure Sectors | CISA.