



IT Security



Supply Chain



OT Security



Insider Threat



Physical Security



Interoperable Communications

ChemLock: Drone Activity



Overview

Owners and operators across all industries are encountering increased drone activity over and around their facilities and assets. Careless or malicious drone operations present a unique threat to chemical facilities that manufacture, store, use, or transport dangerous chemicals. This guidance presents options that owners and operators should consider in preparing for and responding to suspicious drone activity.

Threat

Although most instances of suspicious drone activity will involve “careless” or “clueless” operators, malicious actors may use drones:

- As weapons or to transport smuggled payloads
- To silently watch a large area from the sky
- To steal intellectual property or commit cyber crimes
- To intentionally disrupt or harass



Drones can easily fly over a fence or other physical barriers.

Prepare

Clear and consistent communication with your community—including, but not limited to, residents, businesses, and local law enforcement—is vital to preparing for suspicious drone activity over and around your facilities and assets. Actions that facilities with dangerous chemicals can consider to protect against and respond to drone activity include:

Engaging with law enforcement. Connect with federal, state, and local law enforcement before an incident occurs, including the Federal Aviation Administration (FAA) Law Enforcement Assistance Program (LEAP). Ask about available tools and resources (i.e., messaging, technological systems, etc.), and work together to develop a protection and response plan.

Connecting with local Cybersecurity and Infrastructure Security Agency (CISA) Chemical Security personnel who can provide chemical security expertise.

If you do not know your local CISA Chemical Security personnel, please submit a request for assistance on the CISA ChemLock program’s webpage: cisa.gov/chemlock.

Posting signage. Identify potential drone launch points around the facility and post signage that designates these areas and the facility as “no drone zones.” The FAA’s free digital toolkit includes No Drone Zone signage at faa.gov/uas/resources/community_engagement/no_drone_zone.

Conducting a site survey of the facility and surrounding area, taking note of critical assets, nearby property types, potential drone launch points (i.e., open or elevated areas, such as parking lots or balconies), options for positioning detection equipment, and additional security measures to enhance security against aerial threats.

Developing, updating, implementing, disseminating, and exercising security plans with facility security personnel and law enforcement. Incorporate drone response actions into security and emergency response plans, and ensure that all facility personnel are familiar with the drone response plans. Please visit cisa.gov/chemlock-exercises or email ChemLock@cisa.dhs.gov for more information on the drone CISA Tabletop Exercise Package (CTEP).

Reviewing laws and regulations.

- Review the advisory guidance document (cisa.gov/publication/advisory-application-federal-laws-acquisition-and-use-technology-detect-and-mitigate) issued by the Department of Homeland Security (DHS), FAA, and other federal agencies to assist state and local public and private entities interested in using technical tools, systems, and capabilities to detect and mitigate drones.
- Review the Unmanned Aircraft Systems: Counter Unmanned Aircraft Systems Legal Authorities (cisa.gov/publication/dhs-counter-unmanned-aircraft-systems-legal-authorities), which provides an overview of the authorized actions DHS components may take under the Preventing Emerging Threats Act to protect covered facilities and assets from unlawful drone activity.
- Determine whether your facility is covered under any existing temporary or permanent flight restrictions at tfr.faa.gov/tfr_map_ims. Violations of flight-restricted airspace provide law enforcement with the ability to enforce federally mandated flight restriction and may result in civil penalties or criminal charges.
- Review state laws, local ordinances/limitations, and private property policies. Laws regarding reckless endangerment, disturbing the peace, and voyeurism may apply to suspicious drone activity. Incorporate this information into a security or preparedness plan.

Training personnel on identifying and reporting suspicious indicators. Consider how the drone is flying in the context of FAA regulations. Suspicious drone activity may include:

- Violation of FAA regulations, such as flying:
 - More than 400 feet above ground level
 - Over people or moving vehicles
 - Beyond the drone operator's visual line of sight
 - At speeds over 100 miles per hour (mph)
- Suspicious payloads or modifications to the drone, such as:
 - Oddly shaped items, weapons, or contraband
 - Excessive tape used to conceal or attach additional items
 - Additional visible batteries attached
 - Lights taped over or removed
 - Visible loose wires
 - Obstructed or unidentifiable registration

Identifying drone detection resources. Connect with law enforcement to learn about mobile drone detection support. For those considering investing in a drone detection system, consulting legal counsel and conducting a thorough legal analysis with attention to both federal and state criminal, surveillance, and communications laws is vital.

Posting or sharing resources to aid personnel in identifying suspicious drone activity:

- Drone pocket card: cisa.gov/publication/uas-ci-drone-pocket-card
- Recognize Suspicious Unmanned Aircraft System (UAS) Information Poster and Postcard: cisa.gov/publication/recognize-suspicious-unmanned-aircraft-systems-uas-poster-and-postcard
- Unmanned Aircraft Systems: cisa.gov/uas-critical-infrastructure

Respond

When a drone is identified, **activate the facility's drone response plans** and communicate with security personnel and law enforcement. Tailor the response to the drone's location and flight activity.

If the drone crashes, secure and clear the area. Do not handle the drone until a bomb squad or appropriate authority clears the scene; it is evidence and a potential explosives threat.

Report all recorded details of the incident to law enforcement, including reports from eyewitnesses and detection systems. Once an incident has concluded and any emergency situations have been addressed, report incidents to CISA Central at central@cisa.gov.

If the drone is flying, clear the area. Dispatch security personnel to attempt to locate the drone operator and notify law enforcement. Document critical information including:

- **Drone Characteristics:** Type, size, color, payload, number of rotors, and other physical features
- **Date, Time, and Location:** When and where you noticed the drone
- **Activity:** Direction, distance above the ground, and flight path