INTERAGENCY SECURITY COMMITTEE

PROTECTING AGAINST THE THREAT OF UNMANNED AIRCRAFT SYSTEMS (UAS)

An Interagency Security Committee Best Practice

November 2020 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Message from the Chief

One of the priorities of the Department of Homeland Security (DHS) is the protection of federal employees and private citizens who work within and visit federally-owned or -leased facilities. The Interagency Security Committee (ISC), chaired by the DHS, consists of 64 departments and agencies and has a mission to develop security policies, standards, and recommendations for nonmilitary federal facilities in the United States.

As Chief of the ISC, I am pleased to introduce this document, *Protecting Against the Threat of Unmanned Aircraft Systems (UAS): An Interagency Security Committee Best Practice*. This document outlines awareness and mitigation measures for use by federal departments and agencies to protect against malicious unmanned aircraft systems (UAS) operations. Topics covered in this document include the following:

- An overview of UAS;
- Threats posed by UAS;
- Vulnerability assessments;
- Protective measures and activities;
- How to develop a facility response plan for UAS incidents;
- How to increase workforce awareness; and
- How to engage with community partners.

Although most agencies do not have the authority to disable, disrupt, or seize control of an unmanned aircraft, there are other effective risk reduction measures they may implement. This document provides best practices that any organization or facility can use to mitigate UAS threats.

This document represents exemplary collaboration within the ISC Unmanned Aircraft Systems Working Group and across the entire ISC.

Daryle Hernandez
Chief, Interagency Security Committee
Cybersecurity and Infrastructure Security Agency

Table of Contents

1.0 Purpose

This document provides guidance for federal Executive Branch departments and agencies regarding best practices, lessons learned, and recommendations to protect against the threat of malicious unmanned aircraft systems (UAS) operations.

2.0 Background

The development of UAS is a significant technological advance. In addition to recreational and commercial use, unmanned aircraft are used across the United States 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 border-security efforts. However, UAS can also be used for malicious schemes by terrorists, criminal organizations (including transnational organizations), and lone actors.

The potential safety hazards and security threats presented by malicious UAS activity in the national airspace system requires security professionals to address the associated risks. Organizations should be aware of the potential exposure of private data through operating UAS. Sensitive data may be at greater risk of exposure when operating UAS designed, manufactured, or supplied abroad where the data is stored, transferred to, or accessible by servers in a foreign country.[1] UAS incorporate technologies that generate or collect sensitive data or otherwise access critical systems.

The ISC details the threat of adversarial use of UAS as an increasing concern in *The Design-Basis Threat (DBT) Report*.[2] Adversarial uses of UAS include hostile surveillance, smuggling, disruption, and weaponization. From a cybersecurity perspective, an adversary may use UAS as a mobile platform to interrupt or modify digital services or gain unauthorized access to data systems.

The capabilities of UAS continue to grow with longer flight times, greater ranges, and increased payload capacities. These greater capacities, when coupled with malicious intent, increase the threat to federal facilities.

3.0 Applicability

Consistent with Executive Order (EO) 12977, *Protecting Against the Threat of Unmanned Aircraft Systems (UAS): An ISC Best Practice* is intended to assist security professionals responsible for facilities in the United States occupied by federal employees for non-military activities. These facilities include: existing owned, to-be-purchased, or leased facilities; standalone facilities; federal campuses; and, where appropriate, individual facilities on federal campuses and special-use facilities.

[1] Federal Bureau of Investigation (FBI), Cyber Division Private Industry Notification. November 20, 2019.

[2] *The Risk Management Process for Federal Facilities: An ISC Standard, Appendix A: Design-Basis Threat (DBT) Report*. This appendix is For Official Use Only (FOUO). To request access, contact the ISC at: ISCAccess@hq.dhs.gov.

4.0 Overview of Unmanned Aircraft Systems

An unmanned aerial vehicle (UAV), or drone, is an aircraft operated without direct human intervention in or on the aircraft. The term unmanned aircraft system (UAS) applies to the UAV and its associated elements, including communication links and unmanned- aircraft control components, which are required for the operator to maneuver safely and efficiently in the national airspace system.[3]

UAS include three key components:

1. A UAV that can operate without a pilot on board.
2. A ground control system (GCS) that allows the pilot to remotely control or monitor the operation of the UAV.
3. A bidirectional link between the UAV and the GCS that provides control, status, and imagery information.

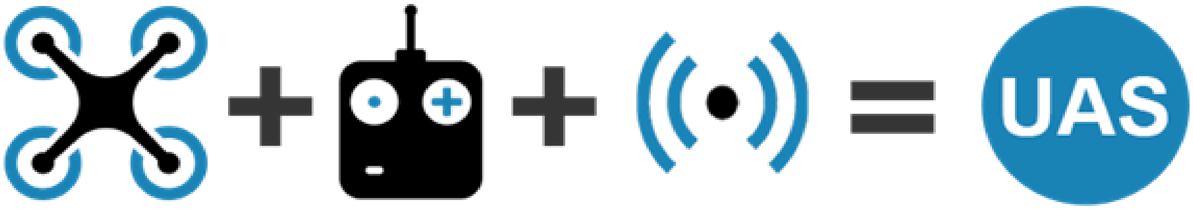


Figure 1: Components of an Unmanned Aircraft System[4]

Unmanned aerial vehicles come in fixed-wing and rotary-wing configurations with one or more propellers or jet motors to provide propulsion. Power sources are either electric (on-board battery) or internal combustion (engine). Capabilities vary widely from recreational models to commercial versions. The weight of a UAV can range from a few ounces to over 50 pounds and their size can range from a few inches to several feet across. The operational ceiling for UAVs can extend to several thousand feet. The flight time ranges from a few minutes to over 30 minutes for electrically-powered models and several hours for models powered by internal combustion. Many UAVs are available with an integrated camera and the ability to stream live video and audio.[5]

The following chart shows the most common drone types and their identifying features. For more information about drone types, refer to the Department of Homeland Security Science and Technology Directorate (DHS-S&T)'s *Counter-Unmanned Aircraft Systems Technology Guide* (2019).[6]

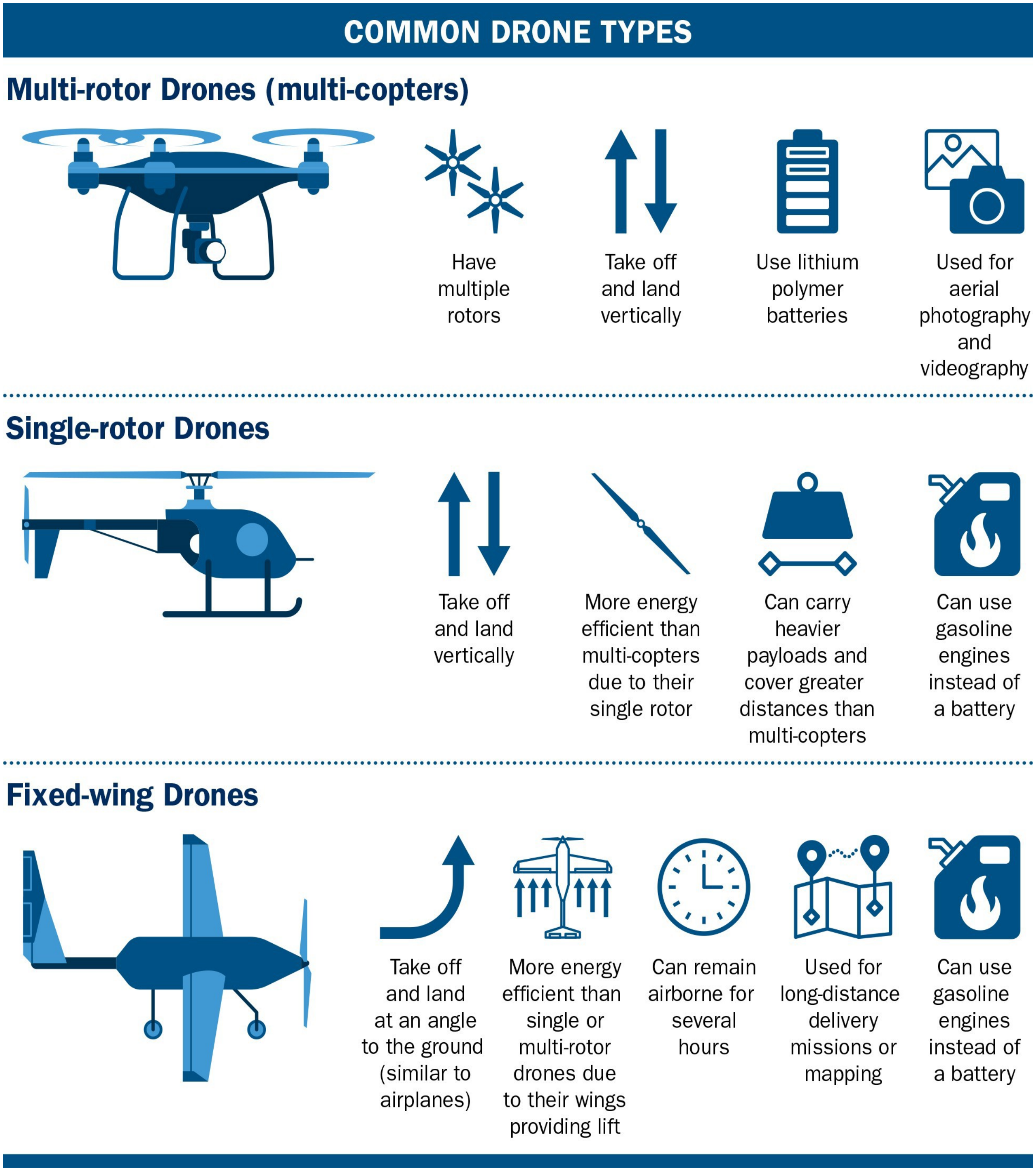
[3] United States Code (USC) Title 49 § 44801.

[4] Centre for the Protection of National Infrastructure (CPNI). Image used with permission.

[5] DHS. "Unmanned Aircraft Systems: Considerations for Law Enforcement Action," fact sheet. Published 2017.

[6] DHS Science and Technology Directorate. "Counter-Unmanned Aircraft Systems Technology Guide." Published 2019. Available online: https://www.dhs.gov/publication/st-c-uas-technology-guide#

Figure 2: Overview of Common Drone Types



COMMON DRONE TYPES

Multi-rotor Drones (multi-copters)

- Have multiple rotors
- Take off and land vertically
- Use lithium polymer batteries
- Used for aerial photography and videography

Single-rotor Drones

- Take off and land vertically
- More energy efficient than multi-copters due to their single rotor
- Can carry heavier payloads and cover greater distances than multi-copters
- Can use gasoline engines instead of a battery

Fixed-wing Drones

- Take off and land at an angle to the ground (similar to airplanes)
- More energy efficient than single or multi-rotor drones due to their wings providing lift
- Can remain airborne for several hours
- Used for long-distance delivery missions or mapping
- Can use gasoline engines instead of a battery

5.0 Threats Posed by UAS

The Department of Justice defines credible threat as the reasonable belief based on the totality of circumstances that the activity of a UAV or UAS may, if unabated:

- Cause physical harm to a person;
- Damage property, assets, facilities, or systems;
- Interfere with the mission of a covered facility or asset, including its movement, security, or protection;
- Facilitate or constitute unlawful activity;
- Interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons;
- Result in unauthorized surveillance or reconnaissance; or
- Result in unauthorized access to or disclosure of classified, sensitive, or otherwise lawfully protected information.[7]

Many UAS events are caused by careless or reckless operators. An adversary can also use UAS in a variety of malicious ways, which include the following:

- **Hostile Surveillance.** An adversary uses UAS to collect information about federal government operations, security measures, or law enforcement operations.

- **Smuggling or Contraband Delivery.** An adversary uses UAS to bypass security measures to deliver illegal or prohibited items onto federal property.

- **Disruption of Government Business.** An adversary uses UAS to interfere with federal government operations through the presence of the UAS, use of on-board cyber-capabilities, or by using the UAS to distribute propaganda onto federal property.

- **Weaponization.** An adversary mounts a firearm, explosive, chemical, or biological agent on a UAV or deliberately crashes the UAV in an attack.

An organization or facility should consider the totality of threats posed by UAS, whether these threats are caused by negligent or reckless use of UAS, criminality, terrorism, or espionage. The risks associated with UAS should not be considered in isolation of other prevailing threat conditions. Considering the full range of threats will facilitate the development of a risk-based mitigation strategy that minimizes those risks most pertinent to the site or organization.

When considering the likelihood of an adversary using UAS, it is important to consider both the intent and the capability of the adversary, including their desired effect. The following table details several basic UAV characteristics structured by the threat actor's capability level and intended effect.[8]

[7] Department of Justice: https://www.justice.gov/ag/page/file/1268401/download

[8] CPNI. *Conducting Site Vulnerability Assessments for Unmanned Aerial System Threats*. Published 2018 and used with permission.

Table 1: Examples of UAS as a Threat

Threat Actor - Capability Level	Likely UAS type	Possible scenario use	Flight Method	Range
Low	Multi-copter	Disruption, surveillance	Line of Sight (LoS) with First Person View (FPV) assistance	400m
	Multi-copter + additional payload	Delivery of restricted item/ explosives	LoS with FPV assistance	400m
Medium	Multi-copter	Disruption, surveillance	FPV	1km
	Multi-copter + additional payload	Delivery or restricted item/ explosives	FPV	500m
	Fixed-wing	Disruption, surveillance	GPS with FPV assistance	5km – 30km
	Fixed-wing + additional payload	Delivery or restricted item/ explosives	GPS with FPV assistance	5km – 30km

6.0 Vulnerability Assessment

A UAS-specific vulnerability assessment will assist organizations and facilities in understanding how a site may be vulnerable to the risks posed by UAS and will aid in identifying mitigation options to build resiliency and response procedures. Completing such an assessment increases understanding by focusing on site- specific threats, launch points, flight profiles, and platforms. The following figure provides an example of a UAS-specific vulnerability assessment and mitigation options.

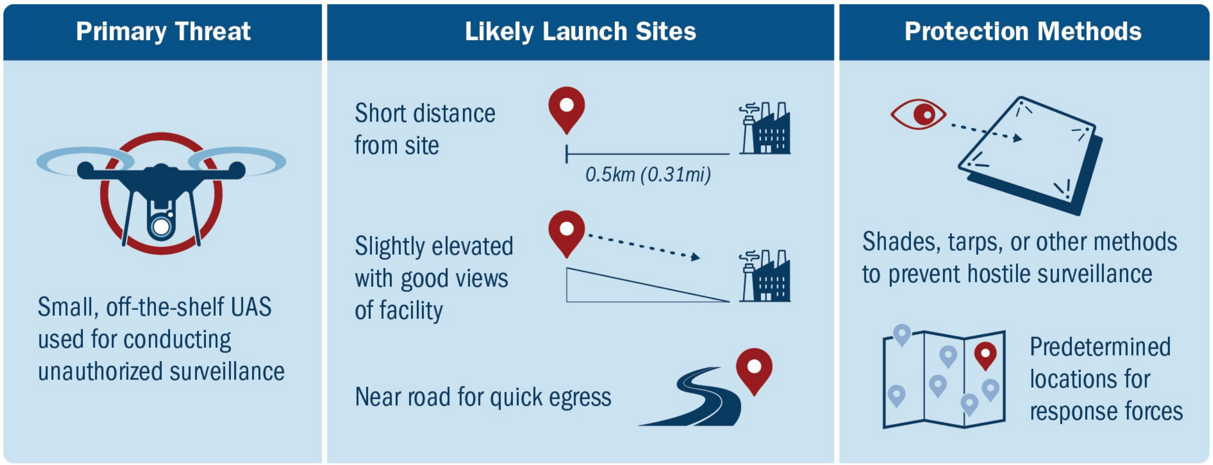
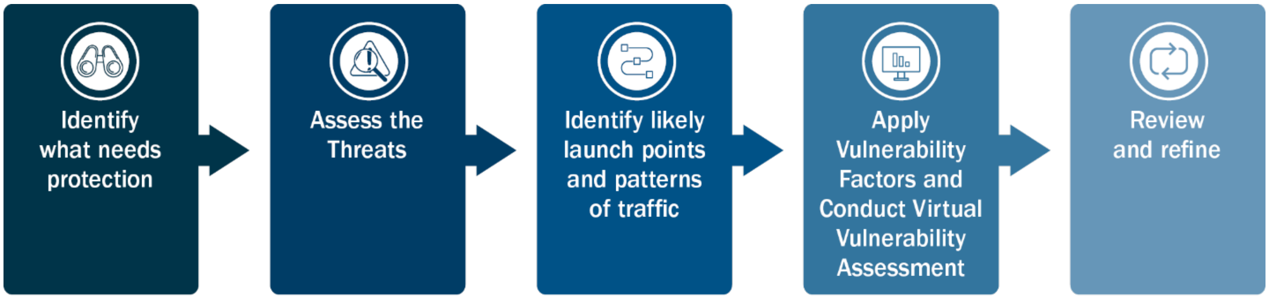

Primary Threat
Small, off-the-shelf UAS used for conducting unauthorized surveillance
Likely Launch Sites
Short distance from site
0.5km (0.31mi)
Slightly elevated with good views of facility
Near road for quick egress
Protection Methods
Shades, tarps, or other methods to prevent hostile surveillance
Predetermined locations for response forces

Figure 3: Example of Mitigating UAS Threat

Security organizations should integrate UAS vulnerability assessments into existing risk assessments. The following steps will assist in developing and integrating a UAS-risk mitigation component into the overall set of countermeasures.



Identify what needs protection

Assess the Threats

Identify likely launch points and patterns of traffic

Apply Vulnerability Factors and Conduct Virtual Vulnerability Assessment

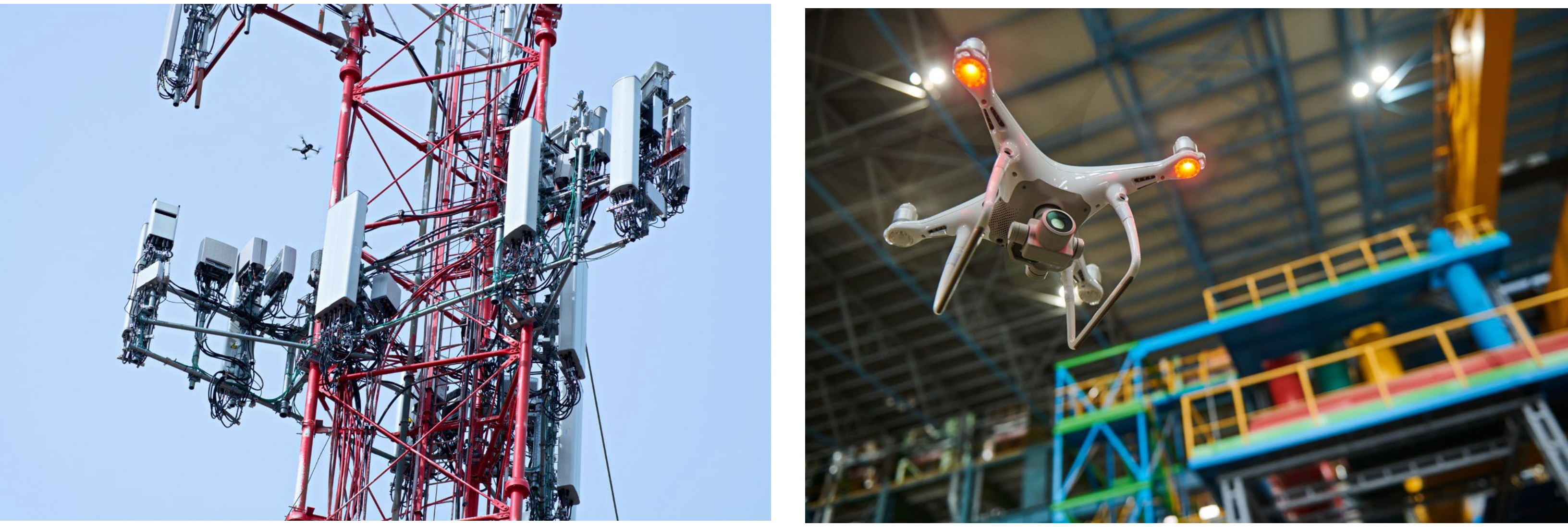
Review and refine

Figure 4: UAS Vulnerability Assessment Process

Step 1: Identify What Needs Protection

Consider factors including, but not limited to:

- Geographic boundaries of the facility in three dimensions;
- Environment (e.g., terrain, urbanization, surrounding ground and air traffic);
- Associated federal interests (e.g., mobile assets and personnel);
- Likely target points (e.g., locations where the threat actor may choose to achieve their purpose);
- Mission ofthe tenant(s) within the facility; and
- Critical assets (i.e., assets which, if comprised or neutralized, may affect the ability of the facility to function). Possible assets include:
    - Communication capabilities;
    - Key personnel (e.g., leaders, IT, guard force);
    - Supply chain storage; and
    - Workforce (including mass casualty).



Left: UAS critical infrastructure inspection, 5G communication tower. Right: UAS inspecting equipment of industrial power plant.

Step 2: Assess the Threats

Consider factors including, but not limited to:

- Location(s) and relevant threat information identified in Step 1, determine the likely type(s) of adversarial use of UAS.
- Potential threat actors and their intent, capabilities, targeting, and history of UAS use.
- Historical reports of UAV flights over and near these locations.
- Likely UAS platforms and their technical specifications, including:
    - Operating range;
    - Maximum flight time;
    - Maximum speed;
    - Payload capacity (type and amount);
    - Control system;
    - Type(s) of navigation (e.g., visual line of sight, GPS, first-person view);
    - Operating environment;
    - Operating temperature range; and
    - Remote controller operating frequency.

Photo courtesy of Customs and Border Protection Air and Marine Operations.

Photo courtesy of Cybersecurity and Infrastructure Security Agency.

Step 3: Identify Likely Launch Points and Patterns of Traffic

Consider identifying factors including, but not limited to:

- Terrain features an operator could use for flight point of reference (e.g., a communications tower that can be seen from a distance).
- Likely locations from which an operator could launch, operate, and land a UAV. Look for locations that provide:
  - Access for a person carrying a UAS or transporting a UAS with a motor vehicle;
  - Unrestricted motor vehicle parking;
  - Space for preparing a UAV for flight;
  - Line of sight to a terrain feature that an operator could use for flight reference;
  - Line of sight to the covered facility/asset(s);
  - Concealment of the operator during flight preparation and during flight; and
  - Elevated control positions from which a UAV may be more readily directed to the facility.
- Likely UAV flight paths and aerial avenues of approach to the facility.
- Federal Aviation Administration (FAA) flight-restricted areas and their corresponding altitude restrictions. Note that a nefarious operator is unlikely to comply with FAA regulations, but could use unrestricted airspace to disguise their operation.
- Nearby airports, heliports, and other air operations and the associated flight paths.

- Nearby UAS clubs and authorized recreational flight areas and become familiar with patterns of normal, legitimate UAS operations in the vicinity.[9]
- Forecast weather conditions and ambient temperature to determine when weather and temperature will be suitable for UAS flights.
- Buildings, topography, and horticulture that affect line of sight, both in terms of UAS operation and in terms of your ability to see UAVs.

Step 4: Apply UAS Vulnerability Factors and Conduct Virtual Vulnerability Assessments

Based on Steps 1-3, estimate the site's vulnerability to UAS threats. This estimate is intended to help determine whether a location might be vulnerable to UAS threats and whether further vulnerability analysis should be conducted.

UAS vulnerabilities are categorized according to five decision factors:

1. **Facility Vulnerability:** A vulnerability associated with a building's structure, systems, historical significance, notoriety, proximity to public access points (e.g., transportation networks, stadiums, shopping, tourist venues), or attachments.

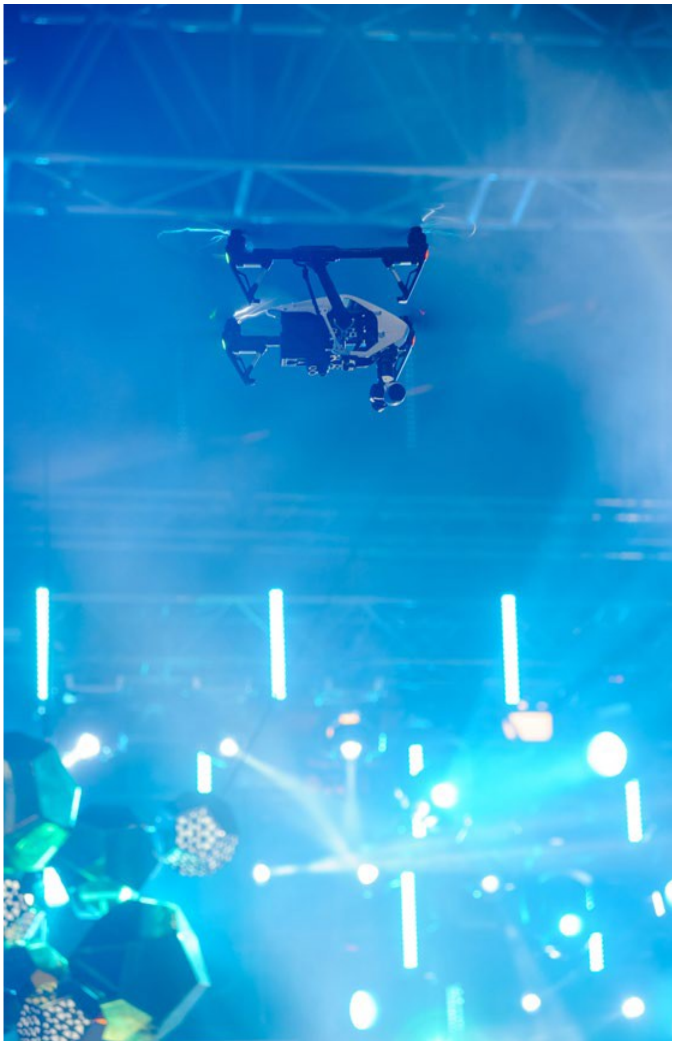
2. **Cyber/Communications Vulnerability:** A vulnerability associated with cyber infrastructure or externally exposed communications.

3. **Operations Vulnerability:** A vulnerability associated with covert and overt law enforcement operations or sensitive federal operations (e.g., federal trials).

4. **Personnel Vulnerability:** A vulnerability associated with the presence of very important people (VIP) or crowds.

5. **History of UAS Activity:** Whether UAVs have flown near or over this location.

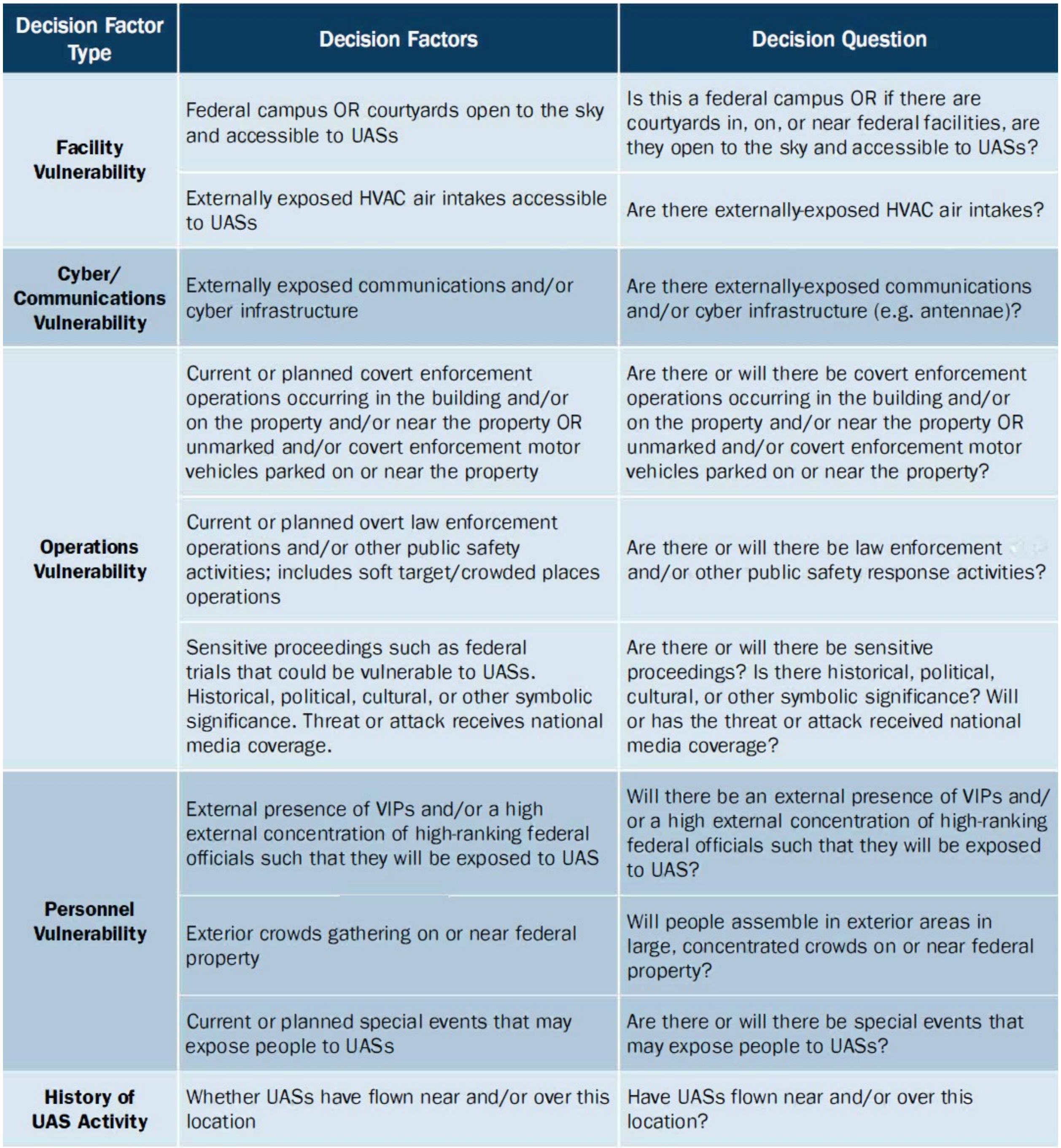
See the following table for the decision factors and their respective decision questions.



Professional camera drone flying over stage.

[9] 49 U.S.C. 44809

Table 2: Decision Factors



Decision Factor Type	Decision Factors	Decision Question
Facility Vulnerability	Federal campus OR courtyards open to the sky and accessible to UASs	Is this a federal campus OR if there are courtyards in, on, or near federal facilities, are they open to the sky and accessible to UASs?
	Externally exposed HVAC air intakes accessible to UASs	Are there externally-exposed HVAC air intakes?
Cyber/ Communications Vulnerability	Externally exposed communications and/or cyber infrastructure	Are there externally-exposed communications and/or cyber infrastructure (e.g. antennae)?
Operations Vulnerability	Current or planned covert enforcement operations occurring in the building and/or on the property and/or near the property OR unmarked and/or covert enforcement motor vehicles parked on or near the property	Are there or will there be covert enforcement operations occurring in the building and/or on the property and/or near the property OR unmarked and/or covert enforcement motor vehicles parked on or near the property?
	Current or planned overt law enforcement operations and/or other public safety activities; includes soft target/crowded places operations	Are there or will there be law enforcement and/or other public safety response activities?
	Sensitive proceedings such as federal trials that could be vulnerable to UASs. Historical, political, cultural, or other symbolic significance. Threat or attack receives national media coverage.	Are there or will there be sensitive proceedings? Is there historical, political, cultural, or other symbolic significance? Will or has the threat or attack received national media coverage?
Personnel Vulnerability	External presence of VIPs and/or a high external concentration of high-ranking federal officials such that they will be exposed to UAS	Will there be an external presence of VIPs and/or a high external concentration of high-ranking federal officials such that they will be exposed to UAS?
	Exterior crowds gathering on or near federal property	Will people assemble in exterior areas in large, concentrated crowds on or near federal property?
	Current or planned special events that may expose people to UASs	Are there or will there be special events that may expose people to UASs?
History of UAS Activity	Whether UASs have flown near and/or over this location	Have UASs flown near and/or over this location?

For each decision factor type, answer the decision question as a simple yes-or-no. The person conducting the assessment may choose to weigh all factors equally or to weigh some factors higher or lower than others. Depending on the answers, determine whether the facility's current security protocols adequately protect the facility from UAS threats and evaluate whether further vulnerability analysis should be conducted.

Step 5: Review and Refine

Steps 1-4 provide a basis for determining future required action. The organization, Facility Security Committee (FSC) or Designated Official (DO) may determine that the UAS vulnerability assessment requires further development. A series of workshops or tabletop exercises can further help to refine the analysis as needed.[10]

An on-site assessment should be conducted to refine and to validate the vulnerability assessment and to identify the overall risks posed to the facility by UAS. Consider the following recommendations when conducting an on-site assessment at the facility:

- Walk the facility and surrounding areas to validate the geospatial maps and analysis. Update the analysis based on ground-level observations.
- Gather relevant protection information and assess the overall risk(s) posed to the facility:
    - Review UAS and non-UAS security assessments;
    - Identify all security plans and procedures;
    - Identify all relevant law enforcement agencies, including your FAA Law Enforcement Assistance Program (LEAP) special agent;
    - Identify points of contact, plans, procedures, and relevant local laws pertaining to UAS operators;
    - Identify FAA resources that can address issues related to airspace overlying your facility as well as Air Traffic Control (ATC)-related operational responses; and
    - Identify existing UAS-detection systems. Note that the use of UAS-detection systems may also implicate provisions of federal law that should be assessed prior to acquisition or deployment.

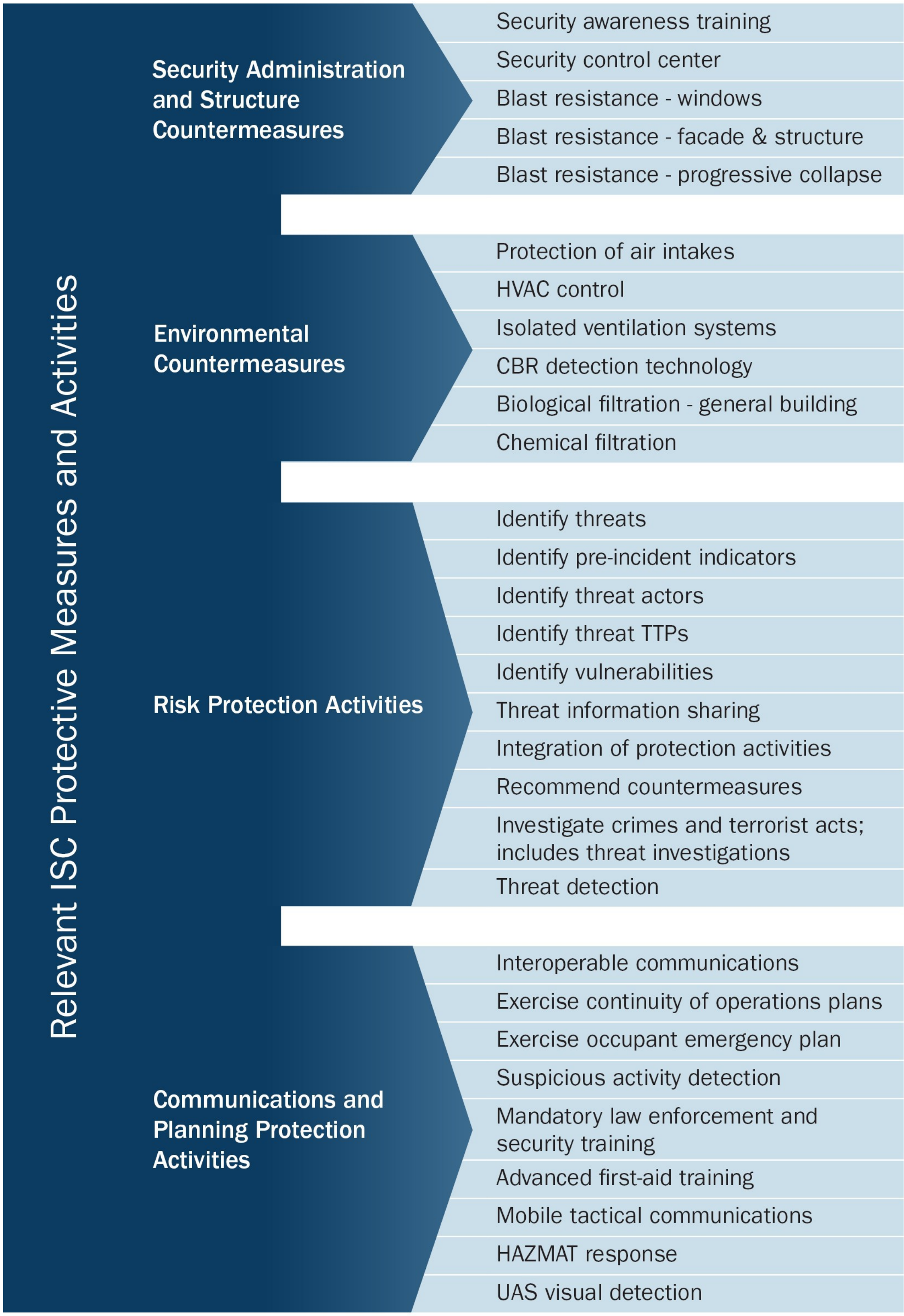
7.0 Protective Measures and Activities

Once UAS threats and facility vulnerabilities are identified, the next step is to determine the necessary and legally available protective measures. The selection of appropriate mitigation strategies will depend on the nature of the threat.

Many protective measures designed to mitigate the risks from other threat vectors can also help mitigate the UAS risk. For instance, measures designed to mitigate hostile surveillance, unauthorized access, ballistic attack, and explosive attack will also help to mitigate UAS-specific threats. The following chart lists relevant protective measures and activities that mitigate UAS risks.

[10] CISA developed the CISA Tabletop Exercise Program (CTEP), a downloadable exercise package that provides a robust situation manual (SITMAN) and exercise support documentation that can be customized by the end user to conduct their own internal exercises. These documents can be found on the Homeland Security Information Network (HSIN) Critical Infrastructure portal at: https://hsin.dhs.gov/ci/sites/exerciseinfo/Pages/CITEP.aspx

Figure 5: Protective Measures and Activities[11]



Relevant ISC Protective Measures and Activities

Security Administration and Structure Countermeasures

- Security awareness training
- Security control center
- Blast resistance - windows
- Blast resistance - facade & structure
- Blast resistance - progressive collapse

Environmental Countermeasures

- Protection of air intakes
- HVAC control
- Isolated ventilation systems
- CBR detection technology
- Biological filtration - general building
- Chemical filtration

Risk Protection Activities

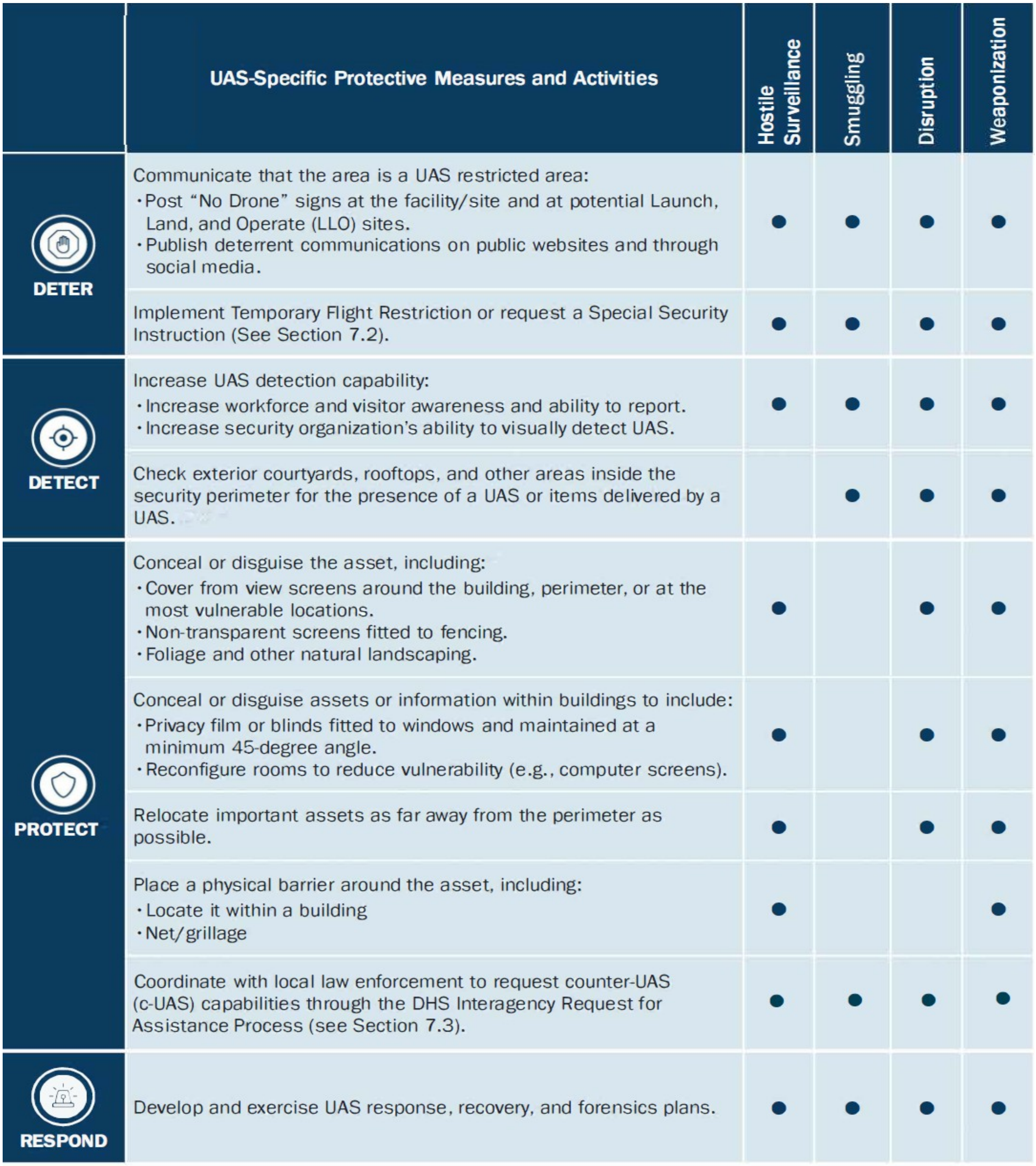
- Identify threats
- Identify pre-incident indicators
- Identify threat actors
- Identify threat TTPs
- Identify vulnerabilities
- Threat information sharing
- Integration of protection activities
- Recommend countermeasures
- Investigate crimes and terrorist acts; includes threat investigations
- Threat detection

Communications and Planning Protection Activities

- Interoperable communications
- Exercise continuity of operations plans
- Exercise occupant emergency plan
- Suspicious activity detection
- Mandatory law enforcement and security training
- Advanced first-aid training
- Mobile tactical communications
- HAZMAT response
- UAS visual detection

The organization or facility may develop additional UAS-specific protective measures based on the vulnerability assessment. The following chart provides examples based on the principles of **Deter**, **Detect**, **Protect**, and **Respond**.

Table 3: UAS-Specific Protective Measures and Activities[12]



	UAS-Specific Protective Measures and Activities	Hostile Surveillance	Smuggling	Disruption	Weaponization
DETER	Communicate that the area is a UAS restricted area: • Post "No Drone" signs at the facility/site and at potential Launch, Land, and Operate (LLO) sites. • Publish deterrent communications on public websites and through social media.	●	●	●	●
	Implement Temporary Flight Restriction or request a Special Security Instruction (See Section 7.2).	●	●	●	●
DETECT	Increase UAS detection capability: • Increase workforce and visitor awareness and ability to report. • Increase security organization's ability to visually detect UAS.	●	●	●	●
	Check exterior courtyards, rooftops, and other areas inside the security perimeter for the presence of a UAS or items delivered by a UAS.		●	●	●
PROTECT	Conceal or disguise the asset, including: • Cover from view screens around the building, perimeter, or at the most vulnerable locations. • Non-transparent screens fitted to fencing. • Foliage and other natural landscaping.	●		●	●
	Conceal or disguise assets or information within buildings to include: • Privacy film or blinds fitted to windows and maintained at a minimum 45-degree angle. • Reconfigure rooms to reduce vulnerability (e.g., computer screens).	●		●	●
	Relocate important assets as far away from the perimeter as possible.	●		●	●
	Place a physical barrier around the asset, including: • Locate it within a building • Net/grillage	●			●
	Coordinate with local law enforcement to request counter-UAS (c-UAS) capabilities through the DHS Interagency Request for Assistance Process (see Section 7.3).	●	●	●	●
RESPOND	Develop and exercise UAS response, recovery, and forensics plans.	●	●	●	●

[11] Consideration should be given to any implications on safety, other security measures (e.g., video surveillance systems), or operational responses

7.1 Signage

If the appropriate authorities[12] determine that UAV-takeoff or -landing is prohibited on federal property, they should post "No Drone Zone" signs. Depending on terrain- and ground-level visibility, these signs should be placed such that any person can see at least one sign from any position near and outside the federal property line.

Each sign should be labeled with a unique location number that can be provided to authorities if a UAS is sighted. On each sign, consider including the phone number for the nearest local law enforcement or Federal Protective Service (FPS) mega-center (on or near federal property) to report UAV sightings or UAS operators.

National Aeronautics and Space Administration
NASA
John F. Kennedy Space Center
↑ Official Visitor Complex
6 Miles
NOW ENTERING NASA / KSC PROPERTY
NASA
NO DRONE ZONE

"No Drone Zone" sign at John F. Kennedy Space Center. Photo courtesy of NASA.

7.2 Temporary Flight Restrictions

Temporary flight restrictions (TFRs) and special security instructions (SSIs) are significant actions that restrict flight operations. These actions must be justified based on a significant, compelling risk balanced against the presumptive right of access to the airspace.

- A U.S. federal organization at the departmental level may request that the FAA issue a TFR for a high-risk or emergency event for a limited duration if all applicable regulatory requirements are met.[13]
- A U.S. federal security or intelligence agency or component of the Department of Defense (DoD) at the departmental level that can demonstrate a UAS-specific national security interest at a federal facility may request that the FAA issue a UAS-specific SSI based on an agreement between the agency and the FAA.[14]

[12] An appropriate authority is defined by the FAA as a person in a position of authority over the facility or property who can determine whether UAS-takeoff or -landing is prohibited on that property. For example, the National Park Service has prohibited takeoff and landing within national parks with limited exceptions. This authority is often the Facility Security Manager or equivalent.

[13] Refer to FAA Advisory Circular 91-63D: https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1028851

[14] Refer to 14 Code of Federal Regulations (C.F.R) 99.7.

7.3 Counter-UAS Interagency Request for Assistance

In some circumstances, federal agencies may request counter-Unmanned Aircraft Systems (c-UAS) support from those agencies who are authorized to employ these capabilities. Such circumstances may include events that occur in national parks or in other federally-owned, non-FPS protected facilities.

In these circumstances, an agency may request assistance through the DHS c-UAS Requests for Assistance Process. The first step is to coordinate with local law enforcement to submit a request to either the DHS Special Event Federal Coordinator, appointed by the Secretary of Homeland Security; other field- based DHS representative; or to the DHS Special Events Program (ops-sewg@hq.dhs.gov, carbon copied (cc'd) to specialeventsprogram@hq.dhs.gov).

8.0 Develop a UAS Response Plan

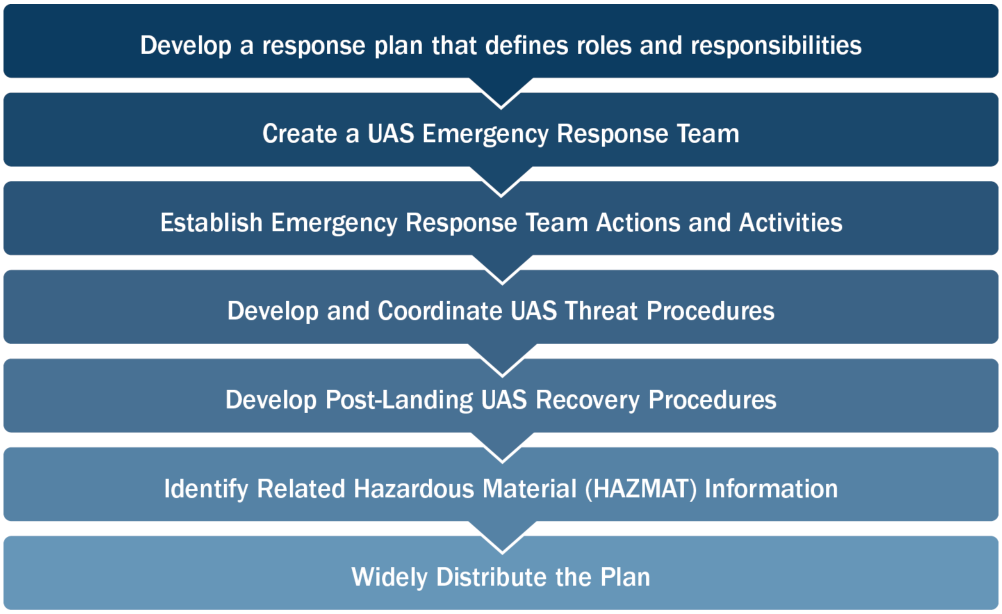
All aspects of the UAS response plan should align with the facility's current Occupant Emergency Plan (OEP) to ensure all pertinent security and emergency items are addressed. A review of the OEP should confirm that FSC members, the Designated Official (DO), the security organization, and other key personnel with assigned duties under the OEP are not over-tasked or given responsibilities that require them to be in two places at once. Close coordination between the developers of the OEP and the developers of the UAS-response plan is essential to ensure that both plans complement each other.

Consult with your department or agency's legal counsel to develop plans and procedures. Legal advice can be especially helpful in determining whether an organization or facility can take action against a UAS or against the operator of a UAS. Some specific federal statutes to consider include:

- 18 U.S.C. § 32: Destruction of aircraft or aircraft facilities;
- 18 U.S.C. § 39A: Aiming a laser pointer at an aircraft;
- 18 U.S.C. § 2510: Wire and electronic communications interception and interception of oral communications;
- 18 U.S.C. §§ 3121: General prohibition on pen register and trap and trace device use;
- 18 U.S.C. §§ 3125: Emergency pen register and trap and trace device installation;
- 49 U.S.C. § 40103: Sovereignty and use of airspace; and
- 49 U.S.C. § 46502: Aircraft piracy.

The following diagram shows an overview of the steps to follow when developing an incident response plan. Additional considerations are listed below.

Figure 6: Developing a UAS Incident Response Plan


Develop a response plan that defines roles and responsibilities
Create a UAS Emergency Response Team
Establish Emergency Response Team Actions and Activities
Develop and Coordinate UAS Threat Procedures
Develop Post-Landing UAS Recovery Procedures
Identify Related Hazardous Material (HAZMAT) Information
Widely Distribute the Plan

Step 1: Develop a Response Plan that Defines Roles and Responsibilities

Key considerations:

- Include key stakeholders in the development of these plans, including the security organizations, owning or leasing organization, FSC or tenant agency, and local law enforcement.
- Identify the goals and objectives of the response.

Step 2: Create a UAS Emergency Response Team

Key considerations:

- Determine how many people will be available to implement the response procedures and where they may be located.
- Identify the members of emergency response teams not identified elsewhere.
- Include facility management staff and the facility security organization.
- Identify local/federal law enforcement officials that would respond to an active UAS threat.
- Connect with your local FAA LEAP special agent (see Appendix A for more information).
- Develop procedures to coordinate with the FAA regarding overlying airspace and any needed operational responses (e.g., implementation of flight restrictions).
- Review the LEAP Toolkit.[15] Use and share materials as appropriate.

[15] Available online: https://www.faa.gov/uas/public_safety_gov/

Step 3: Establish Emergency Response Team Actions and Activities

Key considerations:

- Evacuate employees and visitors when it is safe to do so.
- Determine who will provide first aid.
- Determine response procedures influenced, controlled, or executed by external resources(e.g., emergency services).

Step 4: Develop and Coordinate UAS Threat Procedures

Key considerations:

- How to locate the operator;
- How to assess the immediate threat posed by an airborne UAV;
- How the response procedures will differ based on the perceived threat. It is possible the threat will be identified in real time and therefore a suite of response procedures will be required to cover the range of threats;
- Who can, and how should those people, engage with an operator while a UAV is airborne;
- What information to seek; and
- Who will be notified of the procedures once they have been developed?

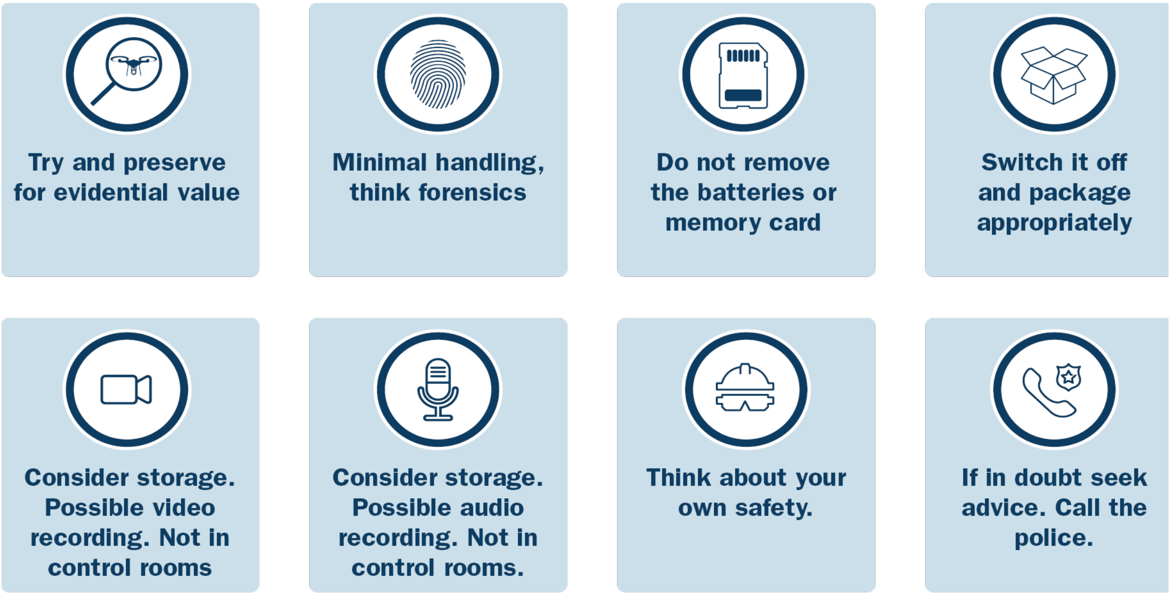
Step 5: Develop Post-Landing UAS Recovery Procedures

Key considerations:

- Identify who has authority to secure the UAV or detain/interrogate the operator.
- Do **not** touch or move the UAV or any parts that may have fallen from the device.
- When feasible, do **not** allow personnel other than law enforcement to touch or move the device.
- When feasible, have all persons leave the immediate area and treat the UAV as a possible suspicious package.
- Identify possible render safe landing zones for first responders, HAZMAT, and EOD personnel

The following figure provides recommendations to consider when responding to an area in which a UAS sighting or incident has been reported.

Figure 7: Considerations During a UAS Incident Response[16]



Try and preserve for evidential value

Minimal handling, think forensics

Do not remove the batteries or memory card

Switch it off and package appropriately

Consider storage. Possible video recording. Not in control rooms

Consider storage. Possible audio recording. Not in control rooms.

Think about your own safety.

If in doubt seek advice. Call the police.

Step 6: Identify Related Hazardous Material Information

Key considerations:

- HAZMAT and the risks associated with a UAS incident.
- Potential outcomes when HAZMAT is present at an incident.
- Basic hazard and risk assessment techniques.
- How to select and use proper personal protective equipment (PPE).

Step 7: Widely Distribute the Plan

Key considerations:

- Distribute to members of the emergency response team, security organization, all security guard posts, and departmental heads. A master copy of the document should be maintained by the emergency response team leader. The plan should be available for review by all employees.
- Provide print copies of the plan within the room designated as the emergency operations center (EOC). Store multiple copies within the facility EOC to ensure that team members can quickly review roles, responsibilities, tasks, and reference information when the team is activated.
- Use agency policies for the storage, retrieval, and use of sensitive electronic documents that allows for employee access in emergency and degraded-communications environments.

[16] Consideration factors provided by the United Kingdom's Centre for the Protection of National Infrastructure (CPNI). Figure redrawn for this report.

9.0 Increasing Workforce Awareness

It is important for employees to be trained and to understand the risks associated with malicious use of UAS. During security-operations planning and security-awareness training, federal departments and agencies should provide guidance on the appropriate response for employees and contractors who encounter UAS on federal property.

Topics to address during planning include, but are not limited to:

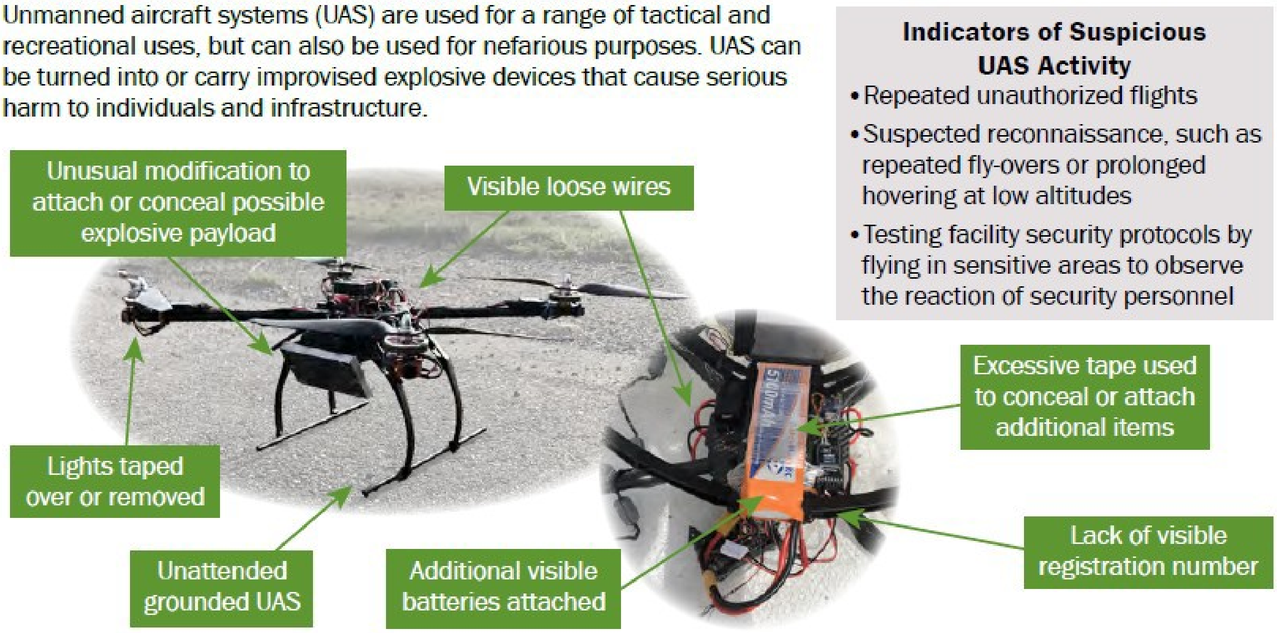
- Integrating UAS reporting into existing communications and reporting procedures or developing new procedures as appropriate.
- Reporting authorized UAS operations in the vicinity of the facility to the security organization. Reporting will assist in distinguishing authorized activity from suspicious activity.
- Integrating all existing and legal means of identifying UAS into the facility's security plans.

Some topics to address during training are:

- Do **not** approach or otherwise attempt to interfere with a UAV in flight.
- Do **not** approach a landed or crashed UAV. Instead, notify the security organization or building security personnel.
- Note the following details when reporting a UAS:
  - Location and description of the UAS operator and their vehicle or mode of transportation (if known);
  - Basic description of the UAV, including wing-type, color, lights displayed, approximate size and shape, and any visible payload or camera;
  - Activity and behavior of the UAV;
  - Relative altitude of the UAV, including reference to terrain features that offer an approximate altitude; and
  - Direction of travel.
- Record the UAS via photograph or video, if it is safe to do so.

The figure below provides an example of suspicious UAS-indicators.

Figure 8: Recognize Suspicious UAS[17]



Unmanned aircraft systems (UAS) are used for a range of tactical and recreational uses, but can also be used for nefarious purposes. UAS can be turned into or carry improvised explosive devices that cause serious harm to individuals and infrastructure.

Indicators of Suspicious UAS Activity

- Repeated unauthorized flights
- Suspected reconnaissance, such as repeated fly-overs or prolonged hovering at low altitudes
- Testing facility security protocols by flying in sensitive areas to observe the reaction of security personnel

Unusual modification to attach or conceal possible explosive payload
Visible loose wires
Lights taped over or removed
Unattended grounded UAS
Additional visible batteries attached
Excessive tape used to conceal or attach additional items
Lack of visible registration number

If you observe suspicious indicators, it is recommended that you treat the grounded UAS as a potential explosive threat. Call local law enforcement and do not touch the UAS until a bomb squad or appropriate authority clears the scene.

10.0 Engaging with Community Partners

In 2017, the FAA created a UAS Integration Pilot Program (IPP) to help state, local, and tribal governments accelerate safe drone integration alongside private-sector entities, such as drone operators and manufacturers. The IPP's overarching goal is to help the Department of Transportation and the FAA gather data to develop new rules, policies, and guidance that support more complex low-altitude operations.

Specifically, the IPP:

- Identifies ways to balance local and national interests related to droneintegration;
- Improves communications with state, local, and tribal jurisdictions;
- Addresses security and privacy risks;
- Accelerates the approval of operations that currently require special authorizations;and
- Engages people where they live and work to understand communitysentiment.

State, local, and tribal governments have all worked closely with their industry partners to tackle challenges to safe and secure integration, including night operations, flights over people, operations beyond the pilot's line of sight, package delivery, detect-and-avoid technologies, remote identification, and the reliability and security of data links between pilot and aircraft.

[17] Image provided courtesy of CISA.

The data collected by the FAA during the program will help inform future policy, guidance, and rule-making. The IPP has influenced current and future activities in the areas of package delivery, emergency management, disaster damage assessment, agricultural support, and infrastructure inspections.[18] Detection technology itself could violate existing statutes. Any critical infrastructure owner should engage in a careful review of this issue prior to purchasing and deploying such technology.

[18] For more information, refer to the FAA's "Fact Sheet – The UAS Integration Pilot Program." Accessed August 3, 2020. https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=23574

Appendix A: Incident Reporting Pocket Cards

A.1 Law Enforcement Assistance Program

The Law Enforcement Assistance Program (LEAP) consists of field investigative and operational activities that support federal, state, and local agencies. LEAP serves as the liaison between law enforcement and the FAA, providing aviation-related support to law enforcement agencies seeking criminal prosecution or conducting airborne drug interdiction. LEAP special agents also provide training to law enforcement officers in aviation smuggling techniques and educate participants in available FAA resources. LEAP is a subsidiary of the FAA Office of National Security Programs and Incident Response.

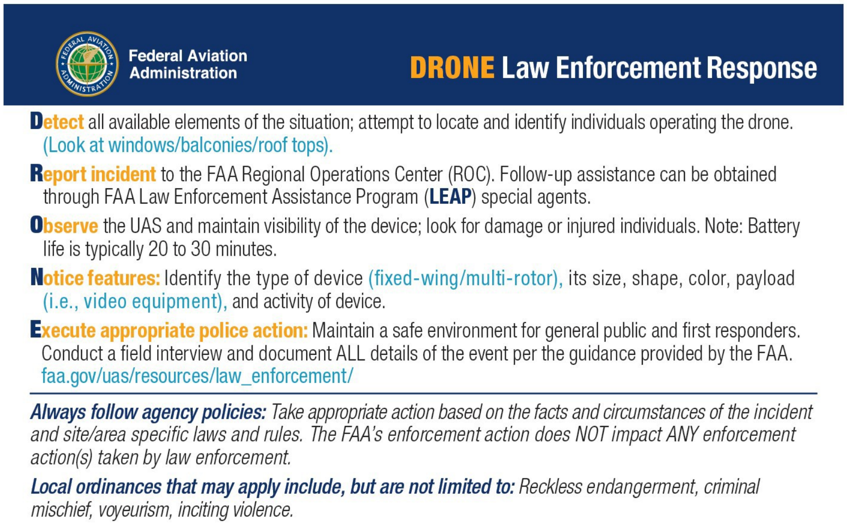
The LEAP special agent will decide whether a violation has occurred and whether further action needs to be taken. The LEAP special agent may request that the affected law enforcement entities contact LEAP during the investigation process to provide additional information.

Law enforcement requests for UAS registration information can be made by contacting LEAP special agents. If the LEAP special agent is not available, law enforcement may contact an alternate LEAP special agent designated within the same region. If no contact can be made, contact the main Law Enforcement Assistance Unit by email at 9-amc-700-leau@faa.gov or call (405) 954-3784.

The following pocket cards are available on the FAA website at:
https://www. faa.gov/uas/public_safety_gov/media/Basic_Law_Enforcement_Response_Drone_Card.pdf

The **D-R-O-N-E** acronym defines the basic federal law enforcement response for UAS incidents.

Figure 9: DRONE Law Enforcement Response Pocket Card



Federal Aviation Administration

DRONE Law Enforcement Response

Detect all available elements of the situation; attempt to locate and identify individuals operating the drone. (Look at windows/balconies/roof tops).

Report incident to the FAA Regional Operations Center (ROC). Follow-up assistance can be obtained through FAA Law Enforcement Assistance Program (**LEAP**) special agents.

Observe the UAS and maintain visibility of the device; look for damage or injured individuals. Note: Battery life is typically 20 to 30 minutes.

Notice features: Identify the type of device (fixed-wing/multi-rotor), its size, shape, color, payload (i.e., video equipment), and activity of device.

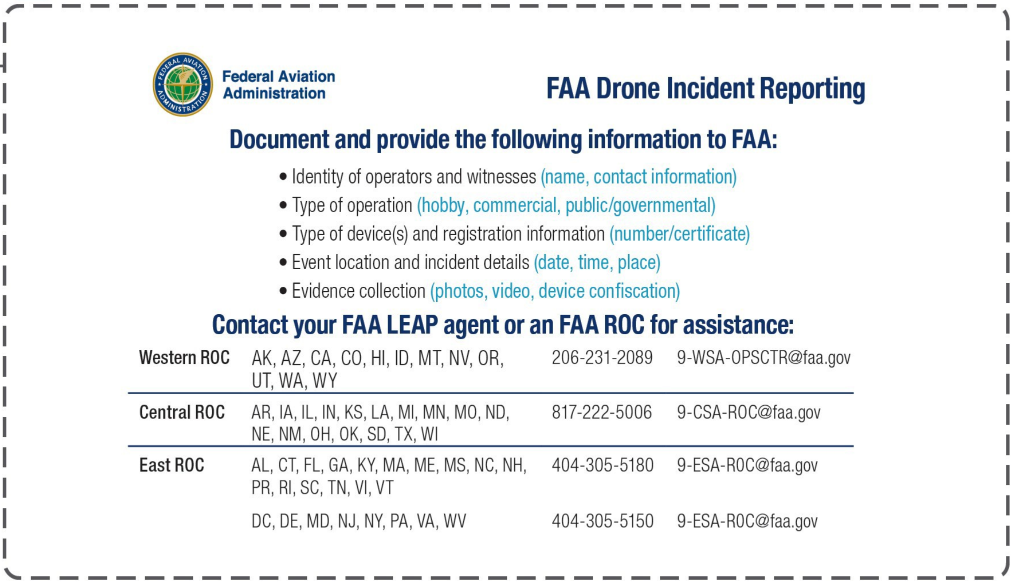
Execute appropriate police action: Maintain a safe environment for general public and first responders. Conduct a field interview and document ALL details of the event per the guidance provided by the FAA. faa.gov/uas/resources/law_enforcement/

Always follow agency policies: *Take appropriate action based on the facts and circumstances of the incident and site/area specific laws and rules. The FAA's enforcement action does NOT impact ANY enforcement action(s) taken by law enforcement.*

Local ordinances that may apply include, but are not limited to: *Reckless endangerment, criminal mischief, voyeurism, inciting violence.*

For more information on contacting a LEAP agent, email UAShelp@faa.gov or call (844) 359-6982 (844-FLY-MY-UA).

Figure 10: FAA Drone Incident Reporting Pocket Card



Federal Aviation Administration

FAA Drone Incident Reporting

Document and provide the following information to FAA:

- Identity of operators and witnesses (name, contact information)
- Type of operation (hobby, commercial, public/governmental)
- Type of device(s) and registration information (number/certificate)
- Event location and incident details (date, time, place)
- Evidence collection (photos, video, device confiscation)

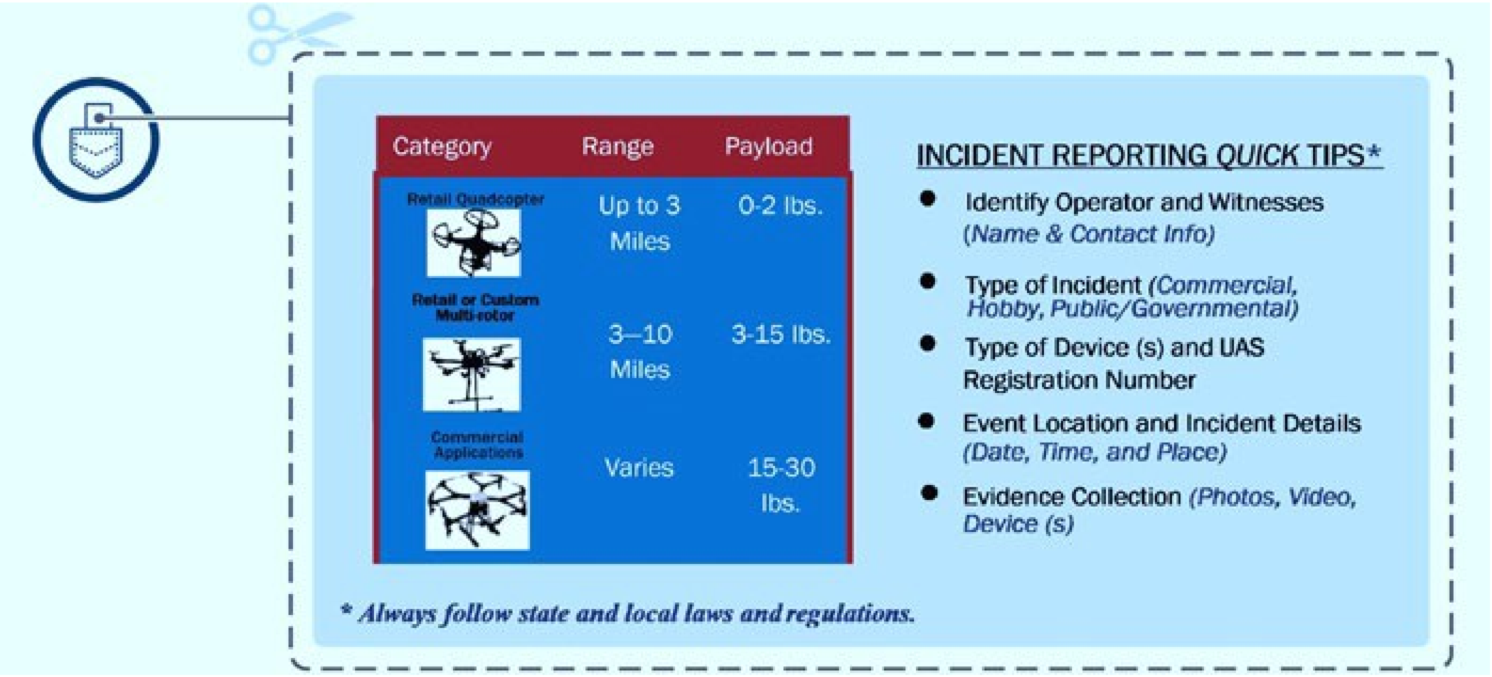
Contact your FAA LEAP agent or an FAA ROC for assistance:

Western ROC	AK, AZ, CA, CO, HI, ID, MT, NV, OR, UT, WA, WY	206-231-2089	9-WSA-OPSCTR@faa.gov
Central ROC	AR, IA, IL, IN, KS, LA, MI, MN, MO, ND, NE, NM, OH, OK, SD, TX, WI	817-222-5006	9-CSA-ROC@faa.gov
East ROC	AL, CT, FL, GA, KY, MA, ME, MS, NC, NH, PR, RI, SC, TN, VI, VT	404-305-5180	9-ESA-ROC@faa.gov
	DC, DE, MD, NJ, NY, PA, VA, WV	404-305-5150	9-ESA-ROC@faa.gov

A.2 CISA Incident Reporting Quick Tips

The following pocket card is available on the CISA website: https://www.cisa.gov/publication/uas-ci-drone-pocket-card

Figure 11: Incident Reporting Quick Tips Pocket Card



Category	Range	Payload
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.

INCIDENT REPORTING *QUICK* TIPS*

- Identify Operator and Witnesses (*Name & Contact Info)*
- Type of Incident *(Commercial, Hobby, Public/Governmental)*
- Type of Device (s) and UAS Registration Number
- Event Location and Incident Details *(Date, Time, and Place)*
- Evidence Collection *(Photos, Video, Device (s)*

*** Always follow state and local laws and regulations.***

Appendix B: Resources

B.1 Frequently AskedQuestions

Q1: Who is authorized to use Counter-UAS?

A1: Unless a federal department, agency, or component has affirmative Cabinet-level Executive Branch and express Congressional authorization, it may be unlawful to disrupt, disable, or seize control of a UAV or UAS.

The Preventing Emerging Threats Act of 2018 (Title 6 U.S.C. § 124n) authorizes the Departments of Justice and Homeland Security to mitigate credible UAS threats by:

- Detecting, identifying, monitoring, and tracking UAS without prior consent of the operator by means of intercepting or otherwise accessing wire, oral, or electronic communications used to control the UAS.
- Disrupting control of a UAS without prior consent from the operator by disabling the UAS by intercepting, interfering with, or causing interference with wire, oral, electronic, or radio communications used to control the UAS.
- Seizing, exercising control of, or otherwise confiscating a UAS.
- Using reasonable force to disable, damage, or destroy a UAS.

In addition, the Departments of Defense and Energy have similar authorities to protect covered facilities and assets as determined by the Secretary or Attorney General, in consultation with the Secretary of Transportation under 10 U.S.C. § 130i and 50 U.S.C. § 2661, respectively.

Q2: Are unmanned aircraft really a threat?

A2: In general, and when legally operated, unmanned aircraft are not a threat. Under the FAA Reauthorization Act of 2018 and applicable regulations, the FAA authorizes public and civil use of unmanned aircraft. However, security professionals should be concerned with the potential nefarious or illegal use of unmanned aircraft. Like any other vehicular device, an unmanned aircraft may be used to transport illegal substances and devices, bypass security measures, and conduct hostile surveillance.

Q3: My agency does not have counter-UAS authorities. What can we do to reduce risks associated with nefarious or illegal unmanned aircraft use?

A3: Even without counter-UAS authorities, a federal agency may implement security countermeasures to protect facilities and people from nefarious or illegal UAS activities. This document explains those countermeasures available to facilities without counter-UAS authorities.

B.2 Glossary

Covered Facility: As defined in 50 U.S.C. § 2661(e)(1), "covered facility" means any facility that is: (A) identified by the Secretary of Energy for purposes of this section; (B) located in the United States (including the territories and possessions of the United States); and (C) owned by the United States or contracted to the United States, to store or use special nuclear material.

Small Unmanned Aircraft: As defined in 49 U.S.C. § 44801, an "unmanned aircraft weighing less than 55 pounds, including the weight of anything attached to or carried by the aircraft."

Suspicious Package: As defined by CISA, any item (e.g., bag, package, vehicle) that is reasonably believed to contain explosives, an improvised explosive device (IED), or other hazardous material (HAZMAT) that requires a bomb technician or specialized equipment for further evaluation.[19]

Unmanned Aircraft: As defined in 49 U.S.C. § 44801, an "aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."

Unmanned Aircraft System (UAS): As defined in 49 U.S.C. § 44801, 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."

UAS Detection: Technological detection of an unmanned aircraft launching, landing, or flying.

UAS Incident: As defined by DHS, a UAS incident is an interaction with a UAS during which there is: (1) an inadvertent or intentional incursion of restricted airspace; (2) operation by a hobbyist operator which is not in compliance with FAA guidelines; (3) operation by a civil or commercial operator which is outside the limitations of an FAA-issued certificate of waiver or authorization; or (4) use of UAS in furtherance of a criminal or terrorist activity.

Unmanned Aircraft Risk Mitigation: Technical countermeasures and general protection activities that may be implemented without counter-UAS statutory authority codified in 6 U.S.C. § 124n.

UAS Sighting: As defined by DHS, a UAS sighting is a reported visual observation of UAS by security officials that does not meet the criteria for either an encounter or an incident. Sightings are typically the result of an encounter by either concerned citizens or security personnel: the operations of the UAS are not known to be in violation of state, local, or federal requirements.

[19] Refer to CISA: https://www.cisa.gov/what-to-do-bomb-threat

B.3 Abbreviations, Acronyms, and Initialisms

Term	Definition
ATC	Air Traffic Control
CBR	Chemical, Biological, and Radiological
CISA	Cybersecurity and Infrastructure Security Agency
C-UAS	Counter-UAS
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DO	Designated Official
DoD	Department of Defense
EO	Executive Order
EOC	Emergency Operation Center
FAA	Federal Aviation Administration
FPS	Federal Protective Service
FPV	First-Person View
FSC	Facility Security Committee
HVAC	Heating, ventilation, and air conditioning
HAZMAT	Hazardous Material
IED	Improvised Explosive Device
IPP	Integration Pilot Program
ISC	Interagency Security Committee
LEAP	Law Enforcement Assistance Program
OEP	Occupant Emergency Plan
PPE	Personal Protective Equipment
SSI	Special Security Instruction
TTPs	Tactics, Techniques, and Procedures (TTPs)
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
USC	United States Code

Appendix C: References

This section contains a non-exhaustive list of guidance documents for unmanned aircraft systems.

Federal Policies, Standards, and Regulations

Executive Office of the President. E.O. 12977 (1995). "Interagency Security Committee." Accessed June 17, 2020. https://www.federalregister.gov/documents/1995/10/24/95-26497/interagency-security-committee

Crimes and Criminal Procedure, 18 U.S.C. § 32 (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:18%20section:32%20edition:prelim)

Crimes and Criminal Procedure, 18 U.S.C. § 39A (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:18%20section:39A%20edition:prelim)

Crimes and Criminal Procedure, 18 U.S.C. § 2510 (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:18%20section:2510%20edition:prelim)

Crimes and Criminal Procedure, 18 U.S.C. §§ 3121-3127 (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:18%20section:3121%20edition:prelim)

Interagency Security Committee. *The Risk Management Process for Federal Facilities: An ISC Standard*. Available online: https://www.cisa.gov/publication/isc-risk-management-process. See also:

- *Appendix A: The Design-Basis Threat Report (FOUO)*
- *Appendix B: Countermeasures (FOUO)*

Transportation, 49 U.S.C. § 40103 (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:49%20section:40103%20edition:prelim)

Transportation, 49 U.S.C. § 46502 (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:49%20section:46502%20edition:prelim)

Transportation, 49 U.S.C. § 44801 (2020). Accessed August 3, 2020. https://uscode.house.gov/view.xhtml?req=(title:49%20section:44801%20edition:prelim)

Federal Publications

Federal Aviation Administration. *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*. Accessed August 14, 2020. https://www.faa.gov/uas/public_safety_gov/media/faa_uas-po_lea_guidance.pdf

Federal Bureau of Investigation. "Private Industry Notification: PIN 20191120-001." Published 2019.

Federal Protective Service. *Strategy for Countering Threats Posed by Unmanned Aircraft Systems*, Version 3.0. Published 2019.

Interagency Security Committee. *Occupant Emergency Programs: An ISC Guide*. Available online: https://www.cisa.gov/publication/isc-occupant-emergency-programs-guide

State and Local Resources

National Conference of State Legislatures. "Current Unmanned Aircraft State Law Landscape." Accessed August 14, 2020. https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

International and Partner Publications

Centre for the Protection of National Infrastructure. *Developing a Plan to Counter Unmanned Aerial Systems at a Site*. Accessed August 14, 2020. https://www.cpni.gov.uk/countering-threats-unmanned-aerial-systems-0

Centre for the Protection of National Infrastructure. *Guidance on Security Guardforce Response to Security Risks Posed by Unmanned Aerial Systems*. Published 2018.

Centre for the Protection of National Infrastructure. *Managing the Security Risks of Small Unmanned Aerial Systems*. Published 2018.

Interpol. *Framework for Responding to a Drone Incident*. Accessed August 14, 2020. https://www.interpol.int/en/Resources/Documents#Publications

Fact Sheets and Digital Resources

Cybersecurity and Infrastructure Security Agency. *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems* (Fact Sheet). Accessed August 14, 2020. https://www.cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems

Cybersecurity and Infrastructure Security Agency. *Unmanned Aircraft Systems (UAS): Addressing Critical Infrastructure Security Challenges* (Fact Sheet). Accessed August 14, 2020. https://www.cisa.gov/publication/uas-fact-sheets

Cybersecurity and Infrastructure Security Agency. "Unmanned Aircraft Systems (UAS): Considerations for Law Enforcement Action" (website). Accessed August 14, 2020. https://www.cisa.gov/uas-law-enforcement

Cybersecurity and Infrastructure Security Agency. *Unmanned Aircraft Systems (UAS): Considerations for Law Enforcement Action* (Fact Sheet). Accessed August 14, 2020. https://www.cisa.gov/publication/uas-fact-sheets

Cybersecurity and Infrastructure Security Agency. "Unmanned Aircraft Systems (UAS) – Critical Infrastructure" (website). Accessed August 14, 2020. https://www.cisa.gov/uas-critical-infrastructure

Federal Aviation Administration. “No Drone Zone” (website). Accessed August 14, 2020. https://www.faa.gov/uas/resources/community_engagement/no_drone_zone/

Federal Aviation Administration. “Public Safety and Government” (website). Accessed August 3, 2020. https://www.faa.gov/uas/public_safety_gov/

Federal Aviation Administration. “Public Safety and Law Enforcement Toolkit” (website). Accessed August 14, 2020. https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit/

Federal Aviation Administration. “Security Sensitive Airspace Restrictions” (website). Accessed August 14, 2020. https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_restrictions/security_sensitive/

Federal Aviation Administration. *State and Local Regulation of Unmanned Aircraft Systems (UAS)* (Fact Sheet). Accessed August 14, 2020.
https://www.faa.gov/uas/resources/policy_library/media/UAS_Fact_Sheet_Final.pdf

Federal Aviation Administration. “Understanding Your Authority: Handling Sightings and Reports” (website). Accessed August 3, 2020. https://www.faa.gov/uas/public_safety_gov/sightings_reports/

Contact Information

Cybersecurity and Infrastructure Security Agency: central@cisa.gov. Contact CISA Central for more information about cyber, communications, or physical security and resilience. For additional UAS-specific resources, contact IP-UAS@hq.dhs.gov. Visit CISA’s Critical Infrastructure UAS website at https://www.cisa.gov/uas-critical-infrastructure. For information about suspicious packages, visit the CISA Office for Bombing Prevention at https://www.cisa.gov/obp.

Federal Protective Service: FPS-Public.Affairs@hq.dhs.gov. Contact FPS for more information about the *Unmanned Aircraft Systems Occupant Threat Mitigation Fact Sheet*.

Interagency Security Committee: ISC@hq.dhs.gov. Contact the ISC with questions about security for federal facilities. To request the ISC’s FOUO materials, email ISCAccess@hq.dhs.gov.

Acknowledgements

The ISC would like to thank the participants of the UAS Working Group.

Todd Consolini, Chair
Federal Protective Service

Jared Pennington, Co-Chair
Federal Protective Service

Patrick Allen
Department of Homeland Security

Bryan Cisar
U.S. Army Corps of Engineers

Lynn Enos
Interagency Security Committee

Sarah Golden
Interagency Security Committee

Jim Longanecker
Interagency Security Committee

James McPhillips
U.S. Secret Service

Jason Randor
General Services Administration

Mike Turner
Central Intelligence Agency

Gean Alston
Department of Homeland Security

William (Bill) Earl
General Services Administration

Josh Freedman
Department of Defense

Thad Groghan
Federal Protective Service

William Lovelace
National Security Agency

Shannon Miers
Federal Emergency Management Agency

Antonio (Tony) Reynolds
Interagency Security Committee

Peter White
Federal Aviation Administration

Jonathan Blaine
Interagency Security Committee

Gary Eisenbraun
Cybersecurity and Infrastructure Security Agency

Derek Gaines
Department of Homeland Security

Troy Hasting
National Security Agency

Marcia McCrimmon
U.S. Secret Service

Dennis Ouellette
Internal Revenue Service

Jerry Stanphill
Federal Aviation Administration