INTERAGENCY SECURITY COMMITTEE WEBINAR:

PROTECTING AGAINST THE THREAT OF UNMANNED AIRCRAFT SYSTEMS (UAS)

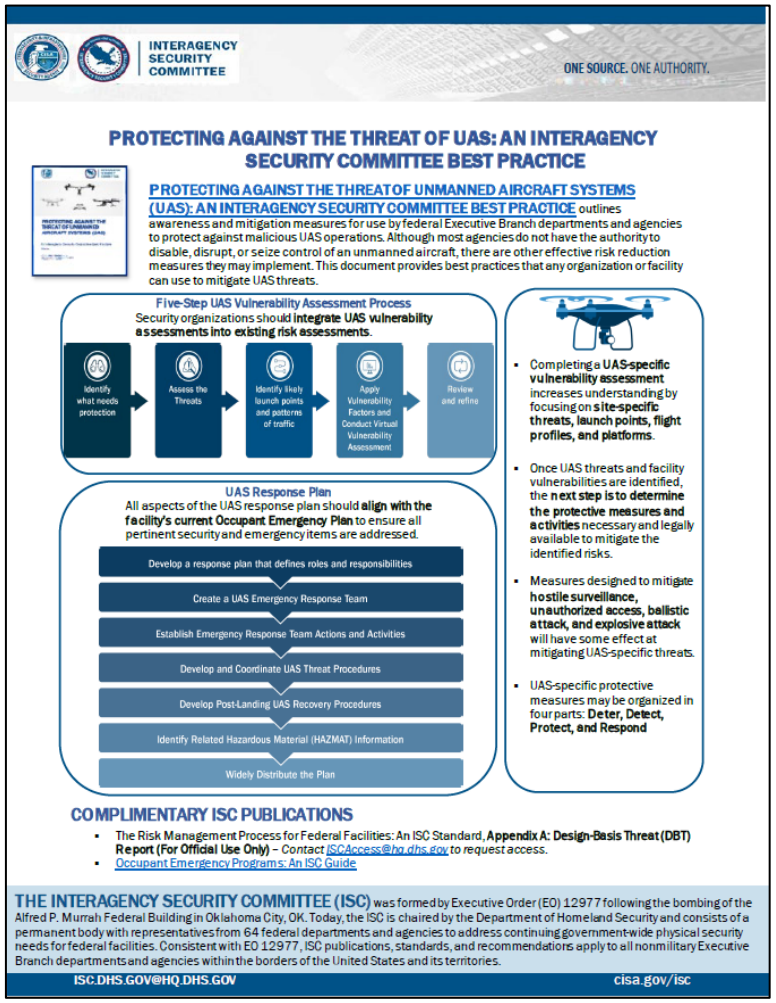
Agenda

- ISC UAS resources
- Malicious Use of UAS
- UAS Vulnerability Assessments
- Notional UAS Vulnerability Scenario
- UAS Protective Measures & Activities
- UAS Response Plan Development
- Q&A

* This presentation and this webinar uses the term UAS to be consistent with the source guidance. Since publication, the term sUAS has been introduced to reflect a vehicle 55lbs and smaller at take off.

ISC UAS Resources

Protecting Against the Threat of Unmanned Aircraft Systems



Protecting Against the Threat of Unmanned Aircraft Systems (One-pager)

Malicious Use of UAS

Malicious uses include:

- **Hostile Surveillance** – collects information about government operations or security operations.
- **Smuggling or contraband delivery** – bypasses security measures to deliver illegal or prohibited items
- **Disruption of Government Business** – through presence, on-board cyber-capabilities or distribution of propaganda
- **Weaponization** – mounted firearm, explosive, chemical, or biological agent on a UAS

UAS Vulnerability Assessments

- Boundaries
- Environment
- Federal interests
- Likely targets
- Tenant mission
- Critical assets

- Threat info
- Potential actors
- UAS activity
- Likely platforms

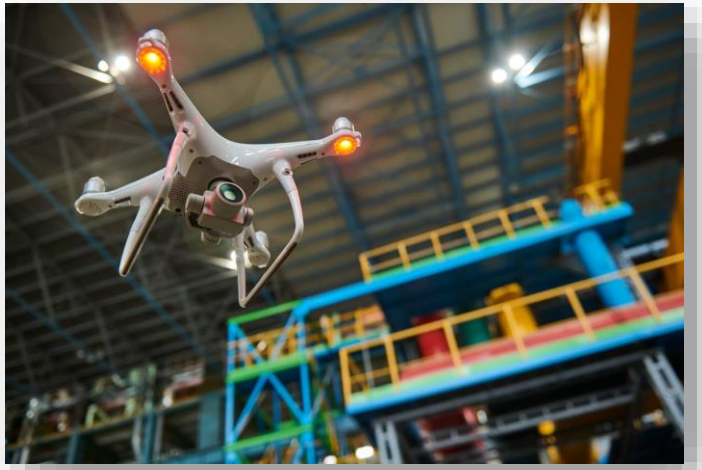
- Reference Points
- Launch locations
- UAV flight paths
- FAA restrictions
- Other aircraft

- Facility vulnerability
- Cyber/Comms vulnerability
- Operations vulnerability
- Personnel vulnerability
- History of UAS activity

- Walk the facility to validate analysis
- Workshops or Tabletop Exercises
- Gather protection info and assess overall risks

Notional UAS Vulnerability Scenario

- Notional federal facility
- Facility mission is contentious and increases target attractiveness
- Facility contains a senior agency official (VIP)
- Facility contains a communications center that supports national essential government functions



Step 1 Identify what needs protection:

- Boundaries
- Environment
- Federal Interests
- Likely targets
- Tenant mission
- Critical assets

Legend

Areas of Protection Concern

Perimeter

Action	Threat actor	Undesirable Event / Threat scenario	Likely UAS type	Flight Method
Disruption/ Propaganda	Protestor	A UAS is purposely positioned to restrict site operations and drop leaflets	Multicopter	LoS with FPV assistance
Weaponization	DVE or Terrorism	UAS carrying explosives impacts into infrastructure	Multicopter + payload	LoS with FPV assistance
Weaponization	DVE or Terrorism	UAS delivers lethal payload on to sensitive location	Multicopter/ fixed wing + payload	LoS or GPS with FPV assistance
Disruption	Reckless user	Accidental incursion into operating area creates safety risk	Multicopter	LoS with FPV assistance

Source: https://earthexplorer.usgs.gov/

Step 2 Assess the threats:

- Threat information
- Potential actors
- UAV activity
- Likely platforms are familiar to hobbyist platforms

Legend

Areas of Protection Concern

Perimeter

Step 3 Identify likely launch points and patterns of traffic:

- Point of references
- Launch locations
- UAV flight paths
- FAA restrictions
- Other aircraft

Legend

	L#	Likely UAV launch point
		UAV
	V#	Likely UAV flight path
		Dense Vegetation

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

UAS Vulnerability Categories:

- **Facility vulnerability:** adjacent to public space busy 4 lane road, park
- **Cyber/Communications vulnerability:** communications system supporting essential government functions
- **Operations vulnerability:** contentious high-visibility mission
- **Personnel Vulnerability:** 800+ government personnel including senior leadership
- **History of UAS activity:** history of UAS activity in adjacent fields

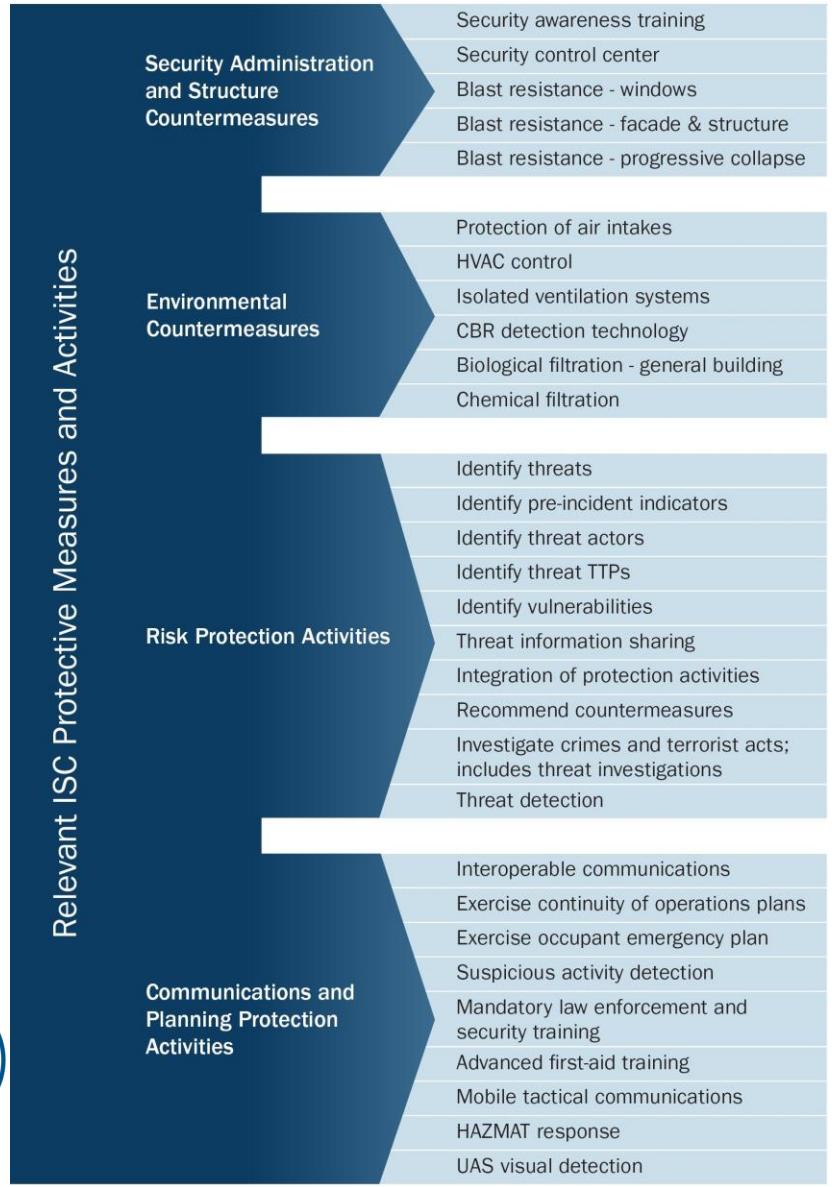
Vulnerability Assessment Matrix

Likely Launch point	Likely Vectors / flight paths	Likely UAS activity areas	Action	Threat actor	Undesirable Event / Threat scenario	Possible Target Locations	Likely UAS type	Flight Method	Countermeasures
L14, L16	V14, V16	11, 13, 14	Disruption/ Propaganda	Protestor	A UAS is purposely positioned to restrict site operations and drop leaflets	Access point and front entrance along highly trafficked road	Multicopter	LoS with FPV assistance	
L6, L8	V8, V6, V5, V7	7, 8 11, 26	Weaponization	DVE or Terrorism	UAS carrying explosives impacts into infrastructure	C-Suite targeting Senior Officials	Multicopter + payload	LoS with FPV assistance	
L6, L8	V6, V5, V7	5, 6, 7, 25	Weaponization	DVE or Terrorism	UAS delivers lethal payload on to sensitive location	Communications Capability / IT / Satellite dishes	Multicopter/ fixed wing + payload	LoS or GPS with FPV assistance	
L6, L8	V8, V7, V6, V5	6, 5, 7, 8	Disruption	Reckless user	Accidental incursion into operating area creates safety risk	Entire Facility	Multicopter	LoS with FPV assistance	

Step 5: Review and Refine

- Walk the facility and surrounding areas
  - Validate geospatial maps and analysis
  - Update the analysis
- Gather relevant protection information
  - Security Assessments
  - ID security plans and procedures
  - ID all relevant LE agencies and POCs
  - Identify FAA resources (e.g. LEAP Special Agents)
  - Identify any existing UAS detection systems
- Workshops or Tabletop Exercises: hsin.dhs.gov/ci/sites/exerciseinfo/Pages/CITEP.aspx

UAS Protective Measures and Activities



	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.	●	●	●	●
DETER	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.	●	●	●	●
DETECT	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.	●		●	●
PROTECT	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).	●		●	●
PROTECT	Relocate important assets as far away from the perimeter as possible.	●		●	●
PROTECT	Place a physical barrier around the asset, including: • Locate it within a building • Net/grillage	●			●
PROTECT	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.	●	●	●	●

Protection Measures and Activities:

- Post No Drone signage
- Ballistic glass (existing)
- Increase Security ability to detect
- Suspicious Activity & Reporting (UAS Club)
- Conceal/Disguise Asset (fence/screen)
- Deterrent messaging public website
- Est. UAS response team & plan

Legend

Likely UAS activities

No UAS Signage

Vulnerability Matrix with Countermeasures

Likely Launch point	Likely Vectors / flight paths	Likely UAS activity areas	Action	Threat actor	Undesirable Event / Threat scenario	Possible Target Locations	Likely UAS type	Flight Method	Countermeasures
L14, L16	V14, V16	11, 13, 14	Disruption/ Propaganda	Protestor	A UAS is purposely positioned to restrict site operations and drop leaflets	Access point and front entrance along highly trafficked road	Multicopter	LoS with FPV assistance	No Drone Signs Coordinate with Local LE for increased patrols Temp flight restriction request (critical high-profile events)
L6, L8	V8, V6, V5, V7	7, 8 11, 26	Weaponization	DVE or Terrorism	UAS carrying explosives impacts into infrastructure	C-Suite targeting Senior Officials	Multicopter + payload	LoS with FPV assistance	Suspicious activity detection and reporting (UAS Club) Ballistic glass (existing)
L6, L8	V6, V5, V7	5, 6, 7, 25	Weaponization	DVE or Terrorism	UAS delivers lethal payload on to sensitive location	Communications Capability / IT / Satellite dishes	Multicopter/ fixed wing + payload	LoS or GPS with FPV assistance	Increase Security Patrols ability to detect Conceal/Disguise Asset
L6, L8	V8, V7, V6, V5	6, 5, 7, 8	Disruption	Reckless user	Accidental incursion into operating area creates safety risk	Entire Facility	Multicopter	LoS with FPV assistance	Employee awareness and reporting No Drone Signs Outreach (UAS Club) Deterrent Messages on public website

UAS Response Plan Development

- Develop, distribute and exercise UAS response, recovery and forensics plans
- Align with current Occupant Emergency Plan (OEP)
- Increase workforce awareness
- Engage with Community Partners

For more information:
www.cisa.gov/isc

Questions?
Email: ISC.DHS.GOV@HQ.DHS.GOV