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.
PROTECTING AGAINST THE THREAT OF UNMANNED AIRCRAFT SYSTEMS (UAS)

An Interagency Security Committee Best Practice

November 2020 Edition

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

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
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

Source: https://earthexplorer.usgs.gov/
### Step 2 Assess the threats:

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

#### Frequent UAV Flight Location

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

### Legend

- Protection Concern
- Perimeter

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

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

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

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

### 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
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

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