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

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

PROTECTING AGAINST THE THREAT OF UNMANNED AIRCRAFT SYSTEMS (UAS)

Features:
- Unmanned Aircraft System (UAS) threat assessment
- Identifying critical infrastructure
- Mitigating risks
- Best practices for UAS security

COMPLIMENTARY ISC PUBLICATIONS:
- Interagency Security Committee (ISC) Guidelines on[...]
- ISC Security Standards for[...]

THE INTERAGENCY SECURITY COMMITTEE (ISC) was formed by Executive Order 13377 following the bombing of the Federal Aviation Administration (FAA) headquarters in Washington, DC. The ISC is charged with the Department of Homeland Security and representatives of the interagency to develop and implement policies, procedures, and standards to protect Federal facilities and critical infrastructure. An ISC Standard Appendix A: Design-Build Threat (DBT) provides guidance to Federal facilities and critical infrastructure on the implementation of the DBT.
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
Step 2 Assess the threats:

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

Source: https://earthexplorer.usgs.gov/
Step 3 Identify likely launch points and patterns of traffic:

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

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

## Relevant ISC Protective Measures and Activities

<table>
<thead>
<tr>
<th>Security Administration and Structure Countermeasures</th>
<th>Environmental Countermeasures</th>
<th>Risk Protection Activities</th>
<th>Communications and Planning Protection Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security awareness training</td>
<td>Protection of air intakes</td>
<td>Identify threats</td>
<td>Interoperable communications</td>
</tr>
<tr>
<td>Security control center</td>
<td>HVAC control</td>
<td>Identify pre-incident indicators</td>
<td>Exercise continuity of operations plans</td>
</tr>
<tr>
<td>Blast resistance - windows</td>
<td>Isolated ventilation systems</td>
<td>Identify threat actors</td>
<td>Exercise occupant emergency plan</td>
</tr>
<tr>
<td>Blast resistance - facade &amp; structure</td>
<td>CBR detection technology</td>
<td>Identify threat TTPs</td>
<td>Suspicious activity detection</td>
</tr>
<tr>
<td>Blast resistance - progressive collapse</td>
<td>Biological filtration</td>
<td>Identify vulnerabilities</td>
<td>Mandatory law enforcement and security training</td>
</tr>
<tr>
<td></td>
<td>- general building</td>
<td>Threat information sharing</td>
<td>Advanced first-aid training</td>
</tr>
<tr>
<td></td>
<td>Chemical filtration</td>
<td>Integration of protection activities</td>
<td>Mobile tactical communications</td>
</tr>
</tbody>
</table>

## UAS-Specific Protective Measures and Activities

<table>
<thead>
<tr>
<th>UAS-Specific Protective Measures and Activities</th>
<th>Hostile Surveillance</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>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Post “No Drone” signs at the facility/site and at potential Launch, Land, and Operate (LLO) sites.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Publish deterrent communications on public websites and through social media.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement Temporary Flight Restriction or request a Special Security Instruction (See Section 7.2).</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increase UAS detection capability:</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Increase workforce and visitor awareness and ability to report.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Increase security organization’s ability to visually detect UAS.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td>Conceal or disguise the asset, including:</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Cover from view screens around the building, perimeter, or at the most vulnerable locations.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Non-transparent screens fitted to fencing.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Foliage and other natural landscaping.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conceal or disguise assets or information within buildings to include:</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Privacy film or blinds fitted to windows and maintained at a minimum 45-degree angle.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Reconfigure rooms to reduce vulnerability (e.g., computer screens).</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relocate important assets as far away from the perimeter as possible.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place a physical barrier around the asset, including:</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Locate it within a building</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Net/grillage</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop and exercise UAS response, recovery, and forensics plans.</td>
<td>● ● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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/
# Vulnerability Matrix with Countermeasures

<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/</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
For more information:
www.cisa.gov/isc

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