JOINT INTERAGENCY TASK FORCE 401

ORGANIZING THE FORCE FOR UAS INCURSION RESPONSE

JIATF-401 | DRAFT COMMANDER'S PLANNING GUIDE

INSTALLATION • OCONUS / DEPLOYED • MARITIME / AFLOAT

PURPOSE AND APPLICABILITY

This guide provides commanders and their staffs with practical considerations for refining installation C-UAS protection plans, integrating available capabilities, strengthening interagency coordination, and rehearsing UAS incursion response procedures.

Although primarily focused on homeland installations, these principles also apply to OCONUS installations, expeditionary forces, and maritime operations, with adjustments for applicable command relationships, operational requirements, and authorities.

RETHINK INSTALLATION DEFENSE FOR THE UAS THREAT.

INTEGRATE THE WHOLE FORCE, MAXIMIZE EXISTING CAPABILITIES, AND ESTABLISH REHEARSED PROCEDURES THAT UNITE MILITARY AND CIVILIAN PARTNERS IN PROTECTING CRITICAL ASSETS.



1 RETHINK THE APPROACH TO INSTALLATION DEFENSE

Commanders should assess whether existing installation protection plans fully account for the UAS threat and the capabilities available across the installation. Effective defense requires more than dedicated C-UAS equipment or a security forces response. It requires clearly established command relationships, integration of available forces and systems, and coordinated action across installation and jurisdictional boundaries.

1.1 ORGANIZE AROUND THE ASSETS UNDER PROTECTION

Tailor detection, protective measures, response responsibilities, and supporting capabilities to the mission and assets at risk (airfields, strategic assets, munitions, ports, facilities, personnel, etc.).

1.2 ESTABLISH CLEAR RESPONSIBILITY FOR C-UAS DEFENSE

Ensure the designated organization has clear relationships with the BDOC or equivalent, tenant units, airfield operations, higher headquarters, and outside partners.

1.3 INCORPORATE PHYSICAL PROTECTION MEASURES

C-UAS response should complement broader physical protection and asset defense efforts, including "HOP" — Harden, Obscure, Perimeter. Link conceptually to the JIATF-401 Physical Protection Guide.

2 MAXIMIZE TENANT-UNIT CAPABILITIES

Operational formations may possess organic C-UAS equipment, trained operators, communications, and sensors that can contribute to installation protection when not committed to their primary missions.

COMMANDERS SHOULD CONSIDER ARRANGEMENTS TO:

- Integrate organic sensors into the installation common operating picture (COP) through approved interfaces.
- Assign protection responsibilities for monitoring sectors, observing sensitive facilities, or protecting mission-essential assets.
- Augment installation protection forces with qualified personnel and capabilities under approved command arrangements.
- Establish equipment availability, including readiness, maintenance, operational tasking, and return to unit training.
- Clarify tasking and authorities. Possession of a C-UAS system does not itself convey mitigation authority.

INTEGRATE TENANT CAPABILITIES INTO THE INSTALLATION COP

TENANT SENSORS / OPERATORS	→	BDOC / COP	→	COMMANDER / SECURITY FORCES / C-UAS ELEMENT
Organic C-UAS sensors, trained crews, and equipment		Integration and shared situational awareness		Coordinated response and asset protection

The objective is not to create competing defense organizations, but to coordinate available resources into a coherent, installation-wide protection effort.

3 OPERATIONAL INSIGHTS: APPLY ESTABLISHED DEFENSE CONCEPTS TO C-UAS

3.1 AIR RAID MODEL — EVERY ORGANIZATION HAS A ROLE

Use UAS-specific warning procedures to establish clear responsibilities for security forces, tenant units, asset owners, operational command posts, and emergency responders. Rehearse the response beyond security forces alone.

3.2 DEFENSE OF THE AMPHIBIOUS TASK FORCE — INTEGRATE THE WHOLE FORCE

Protection should not be limited to the organization traditionally responsible for it. Treat tenant units as contributors to installation defense, with responsibilities established in advance.

3.3 COMPOSITE WARFARE COMMANDER / COMMAND BY NEGATION

Clearly assign responsibilities and appropriately delegated decisions to subordinate organizations can act within established responsibilities while keeping higher command informed. This does not independently grant engagement authority.

3.4 UNIFIED AIR DEFENSE — ELIMINATE ORGANIZATIONAL SEAMS

Do not allow informal divides between smaller UAS and larger airborne threats to create gaps in airspace management, threat assessment, or engagement responsibility.

ON PAGE 2: RELATIONSHIPS, AUTHORITIES, AND "A WAY" — A COORDINATED UAS INCURSION RESPONSE.

4. ESTABLISH THE RELATIONSHIPS, RESPONSIBILITIES, AND AUTHORITIES BEFORE AN INCURSION

MANY OF THE MOST CONSEQUENTIAL DECISIONS DURING A UAS INCURSION INVOLVE ORGANIZATIONS OUTSIDE THE INSTALLATION CHAIN OF COMMAND.

Commanders should ensure established coordination procedures identify who responds, who has authority to act, who takes custody, and who reports at each stage of an incident.

KEY ORGANIZATIONS AND COORDINATION REQUIREMENTS

INSTALLATION SECURITY / BDOC	Provost Marshal, Security Forces Squadron, installation operations center: detection and incident coordination, installation alerts, deployment of authorized response capabilities, external notifications, scene security, and operational reporting.
TENANT UNITS / DEDICATED C-UAS ELEMENTS	Sensor integration, assigned observation and asset-protection responsibilities, personnel augmentation, tasking arrangements, and authorized C-UAS employment.
STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT	County sheriff, municipal police, state police, tribal police: real-time information exchange, response to suspected operators outside the installation, public safety, recovery-site coordination, and jurisdictional handoffs.
MILITARY CRIMINAL INVESTIGATIVE ORGANIZATIONS	Army CID, AFOSI, NCIS: investigative notification, case coordination, evidence requirements, investigative referrals, and coordination with federal authorities.
FEDERAL LAW ENFORCEMENT	FBI field office or resident agency: federal investigative coordination, evidence and forensic support, possible technical exploitation, and applicable criminal or national-security investigation.
SPECIALIZED AND SUPPORTING AGENCIES	EOD, fire/EMS, Staff Judge Advocate, U.S. Attorney's Office, FAA/ATC: render-safe procedures, emergency response, legal authorities, warrants, prosecution considerations, and airspace coordination.

AUTHORITIES MUST BE INCORPORATED INTO THE RESPONSE PLAN

Commanders should distinguish detection, passive protection, active mitigation, law-enforcement actions, recovery, evidence handling, and exploitation. Different personnel and agencies may possess authority for different actions. Homeland, OCONUS / deployed, and maritime environments require tailored authorities and command relationships.

Self-Defense and Target Engagement Authority. Commanders retain the inherent right and obligation of unit self-defense in response to a hostile act or demonstrated hostile intent. Where permitted by applicable authorities, target engagement authority should be delegated to the appropriate operator or tactical level, with clearly established procedural controls, engagement criteria, and ROE/RUF. Decisions should not be unnecessarily retained at the installation or O-6 / garrison command level when operators can act within preapproved authorities.

A WAY: COORDINATED INSTALLATION UAS INCURSION RESPONSE

1 INITIAL REPORT

SLT law enforcement reports a possible UAS near the installation boundary through an established channel with the BDOC. Treat the visual report as a cue for investigation — not confirmation of a drone.

- **Observe, don't assume.**
- **Get a second set of eyes.**
- **Use fixed references.**
- **Consider alternate explanations.**

2 CORROBORATE AND TRACK

The BDOC correlates law enforcement observations with installation sensors and organic C-UAS systems operated by tenant units. These systems feed the installation COP and support tracking, confidence assessment, and information sharing.

- **Correlate with available sensors.**
- **Report observations — not conclusions.**

3 ACTIVATE THE "AIR RAID" PROCEDURE

The BDOC initiates the established UAS warning procedure. Security forces and C-UAS elements assume response responsibilities; tenant units acknowledge the alert, monitor assigned areas, and protect designated assets. The BDOC maintains the common picture and coordinates the installation-wide response.

4 RESPOND TO THE THREAT

The UAS appears to be surveilling a sensitive asset from just outside the installation perimeter. Under assumed approved authorities and ROE/RUF, the designated C-UAS operator mitigates the threat using pre-delegated target engagement authority and established procedural controls, without requiring additional approval from the installation commander. Commanders and their forces retain the inherent right of self-defense against a hostile act or demonstrated hostile intent. Simultaneously, SLT law enforcement coordinates the response to the suspected operator and potential recovery site outside the installation.

5 RECOVER AND INVESTIGATE

The UAS is recovered outside the installation. Local law enforcement secures the scene and coordinates EOD / render-safe support as required. Installation security notifies the appropriate MCIO and FBI. Investigative partners establish evidence custody and coordinate forensic and technical exploitation.

6 REPORT AND IMPROVE

The installation completes required Service, combatant command, Department, and interagency reporting as applicable. Leaders review the response, incorporate lessons into the protection plan, and share relevant findings to improve future C-UAS readiness.

RELATED JIATF-401 RESOURCES

The JIATF-401 resources website includes the Physical Protection Guide, the Nighttime Airborne Contact Validation Guide, and other resources to help commanders and units better understand the C-UAS threat and access capabilities to counter it.