JIATF Checklist for Non-DoW Sites

Phase-driven assessment for non-military and commercial sites housing critical assets

BLUF	Assessing non-military sites (e.g., leased commercial spaces, civilian infrastructure) requires a layered approach that prioritizes existing structural resilience, local law enforcement integration, and interagency coordination before committing to costly physical C-UAS hardware.
Key Takeaway	For non-military facilities, always exhaust procedural and interagency defense options (like local police response SOPs and DHS/FPS coordination) before pursuing tactical, hardware-based C-UAS procurement.

Phase 1: Structural & Threat Baseline Assessment

Focus: *Determine the inherent resilience of the facility and map the specific threats to critical assets.*

Category	Evaluation Item	Tasks / Action Output
Asset Mapping	**Task Critical Assets (TCAs)**	☐ Identify Task Critical Assets (TCAs) housed on-site. ☐ Use floorplans and schematics to map the exact location of TCAs within the facility. ☐ Include servers, personnel nodes, power supplies, communications equipment, and other mission-essential assets.
Structural Resilience	**Building Composition**	☐ Assess the building's physical shell (e.g., reinforced concrete, glass, steel, masonry, or mixed materials). ☐ Determine if the structure inherently mitigates Group 1-2 (small) kinetic UAS threats. ☐ Document areas where structural protection is limited or insufficient. ☐ Determine whether passive base defense measures may improve physical protection for TCAs.
Threat Profiling	**Local UAS Activity**	☐ Review local intelligence and incident reports involving UAS activity. ☐ Determine the likelihood of Group 1-3 UAS activity in the surrounding airspace. ☐ Identify nearby facilities, events, or infrastructure that may increase UAS threat exposure.
Vulnerability Gap	**Penetration Risks**	☐ Identify weak points where UAS activity could compromise TCAs. ☐ Assess rooftop HVAC, large windows, loading docks, roof access points, parking areas, courtyards, and utility access points. ☐ Determine whether a Group 3 (larger payload) UAS could compromise a TCA.
Passive Base Defense Measures	**Reinforced walls, barriers, mesh or cable netting, scrims, etc.**	☐ Identify passive base defense measures that can physically protect TCAs. ☐ Assess reinforced walls, barriers, mesh or cable netting, scrims, and similar measures. ☐ Determine whether passive measures can defeat a Group 1-2 UAS by increasing the physical difficulty in reaching the protected asset. ☐ Document passive measures that can reduce or eliminate the need for tactical C-UAS hardware.

Phase 2: Procedural & Interagency Evaluation

Focus: *Maximize low-cost and no-cost protective measures utilizing existing local and federal authorities.*

Category	Evaluation Item	Tasks / Action Output
Jurisdictional Mapping	**Site Ownership & Security**	☐ Identify site ownership and the primary security authority. ☐ Determine whether security responsibility belongs to private property management, DHS Federal Protective Service, local municipality, another federal agency, or a blended authority structure. ☐ Document who has decision authority during a UAS incident.
Law Enforcement (LE) Integration	**Response Capabilities**	☐ Evaluate local LE response times. ☐ Identify local LE points of contact and notification procedures. ☐ Determine whether local LE has existing C-UAS, hazardous materials, or explosive ordnance response capabilities. ☐ Confirm escalation procedures for suspected UAS activity.
Standard Operating Procedures	**Incident SOPs**	☐ Determine if explicit SOPs exist for a UAS event. ☐ Confirm procedures for detection reporting, perimeter lockdown, shelter-in-place or evacuation, and LE intercept handoff. ☐ Draft UAS incident SOPs if none exist. ☐ Coordinate SOPs with site security, local LE, DHS/FPS, and other responsible agencies.
Federal Coordination	**Facility Security Assessments**	☐ Ensure the next formal Facility Security Assessment (FSA) explicitly accounts for the UAS threat. ☐ Ensure the FSA evaluates UAS threats against the specific critical assets housed on-site. ☐ Document gaps that require federal, local, or interagency coordination.

Phase 3: C-UAS Capability Matrix

Focus: *Determine the appropriate level of technical and tactical investment required based on Phase 1 and Phase 2 findings.*

Option Level	Capability Profile	Tasks / Implementation Trigger
Baseline	**No active C-UAS hardware**	☐ Confirm the facility's structure is highly resilient. ☐ Confirm threats are negligible or fully mitigated by existing physical barriers. ☐ Document the decision to remain at baseline protection level.
Procedural	**LE/Security Integration**	☐ Confirm moderate threat level and reliance on local LE for interception. ☐ Establish visual detection, reporting, facility guards, and lockdown protocols. ☐ Confirm local LE and site security understand their roles during a UAS event.
Tactical (Mobile)	**Mobile RF detection/mitigation**	☐ Determine whether mobile RF detection/mitigation is required for elevated threat to TCAs. ☐ Consider patrol hand-held mitigation, vehicle-mounted, or deployable mobile detection/mitigation systems when fixed sensors are too costly or administratively complex. ☐ Identify who will operate, authorize, maintain, and sustain mobile C-UAS equipment.
Tactical (Fixed)	**Permanent RF/Radar sensors and mitigation systems**	☐ Determine whether permanent RF sensors, radar sensors, or mitigation systems are required. ☐ Confirm the site is a high-risk target and the structure is vulnerable. ☐ Confirm whether LE response times are inadequate to protect TCAs. ☐ Identify approval, legal, spectrum, operational, sustainment, and lifecycle requirements before procurement.

Phase 4: Sustainment & Continuous Review

Focus: *Ensure the defensive posture evolves with the threat landscape.*

Category	Evaluation Item	Tasks / Action Output
Threat Reassessment	**Annual Intelligence Review**	☐ Establish a recurring schedule, such as annually, to review evolving local threat reports and commercial UAS capabilities. ☐ Update the facility threat profile based on new intelligence, incidents, or mission changes. ☐ Reassess whether the selected protection level remains appropriate.
Drills & Exercises	**LE Response Testing**	☐ Conduct tabletop or physical exercises with local LE and site security to test UAS event SOPs. ☐ Test detection reporting, perimeter lockdown, shelter-in-place or evacuation, and LE handoff procedures. ☐ Capture lessons learned, and update SOPs based on exercise results.
Hardware Audits	**System Effectiveness**	☐ If tactical C-UAS systems are deployed, conduct periodic system effectiveness audits. ☐ Ensure software and firmware are updated to detect the latest commercial UAS signatures. ☐ Validate operator training, access controls, maintenance, sustainment, and lifecycle replacement requirements.

Final Review

Focus: *Confirm that procedural and interagency options have been exhausted before tactical hardware procurement is pursued.*

Decision Gate	Checklist Tasks
Go / No-Go Review	☐ Have all TCAs been identified and mapped? ☐ Has the facility's structural resilience been assessed? ☐ Have passive base defense measures been considered to physically protect TCAs before tactical C-UAS hardware procurement? ☐ Has local UAS threat activity been reviewed? ☐ Have major vulnerability gaps and penetration risks been identified? ☐ Has site ownership and security jurisdiction been confirmed? ☐ Has local LE integration been evaluated? ☐ Do UAS incident SOPs exist and include reporting, lockdown, and LE handoff procedures? ☐ Has DHS/FPS or other federal coordination occurred, if applicable? ☐ Has the Facility Security Assessment incorporated the UAS threat against TCAs? ☐ Have procedural and interagency defense options been exhausted before hardware procurement? ☐ Has the appropriate C-UAS option level been selected and documented? ☐ Has sustainment, training, review, and exercise planning been established?