SOL ENGINEERING SERVICES

Strategic Advisory

C-UAS INTEGRATION IN MILITARY RANGE MANAGEMENT SERVICES

Readiness Governance in the Contested Airspace Era

April 2026

solengrs.com

EXECUTIVE SUMMARY

Military training ranges are the Army's primary mechanism for converting policy into combat readiness. Every hour of live-fire training executed on a range complex represents an irreplaceable readiness input. The incursion of an unauthorized unmanned aircraft system over a range complex does not merely create a security concern; it triggers a mandatory firing stand-down under DA Pamphlet 385-63, converting every UAS incursion event directly into a readiness degradation event. This is the operational reality that current C-UAS governance has failed to confront.

The governing framework for range management, centered on DA Pam 385-63 and AR 385-63, was written before small UAS became an accessible, affordable, and operationally significant threat platform. It contains no C-UAS integration requirements. The Army's C-UAS doctrine, ATP 3-01.81, provides a layered defense model but does not address range management as a C-UAS planning domain. The result is that range safety and C-UAS operate as parallel and largely disconnected functions within the same installation structure, with range control officers lacking both the authority framework and the sensor architecture to respond to the threat most directly impairing their mission.

This paper advances three primary findings. First, the legal authority gap under 10 U.S.C. Section 130i creates a coverage ceiling that excludes most Army range complexes from domestic C-UAS operational authority, leaving range control officers without lawful defeat options even when UAS incursions are actively degrading training operations. Second, the absence of C-UAS as a formally required element of range operations planning, range safety plans, and range management service contracts means that even installations with C-UAS assets cannot integrate them systematically into range control operations. Third, the procurement and fielding failures documented by the House Armed Services Committee and DoD Inspector General have produced a C-UAS inventory insufficient in scale to address the 350-plus incursion events per year documented across 100 U.S. military installations.

The governing implication is direct: C-UAS must be treated as a core range management service, not a force protection addendum. This requires amendment of the range safety regulatory framework, revision of range management service contract requirements, and a targeted legislative fix to extend Section 130i coverage to range complexes meeting a defined readiness-impact threshold.

CENTRAL FINDING

The readiness cost of UAS incursion over military range complexes is structurally guaranteed by current range safety doctrine. Until C-UAS is embedded as a required element of range operations planning and range management service delivery, every unauthorized drone over a range complex will produce a mandatory training stand-down. The question is not whether this degrades readiness. It is whether the Army will govern that degradation or continue absorbing it.

SECTION I: REGULATORY, POLICY, AND DOCTRINE ARCHITECTURE

Five governing authorities define the legal, doctrinal, and policy architecture within which C-UAS integration into range management must be planned and executed. Each carries specific provisions, thresholds, and gaps that directly shape what is operationally possible and what is legally prohibited at the installation level.

10 U.S.C. Section 130i: The Authority Ceiling

Section 130i, as amended through the National Defense Authorization Act for Fiscal Year 2025 (P.L. 118-159), is the governing statutory authority for DoD C-UAS operations at domestic installations. It defines covered facilities and assets, enumerates permitted defeat actions, and establishes the legal boundary within which any domestic C-UAS operation must occur.

The critical operational problem is the coverage definition. Section 130i designates covered facilities and assets primarily as those associated with nuclear weapons, missile defense, special operations, and a limited set of other nationally significant assets. Most Army range complexes do not meet this threshold. The legal consequence is that a range control officer observing an active UAS incursion over a live-fire range has no lawful authority to direct defeat action under the statute. Detection is permitted. Tracking is permitted. Defeat is not, absent designation as a covered asset.

NDAA FY2025 Sections 925, 1073, and 1090 direct the C-UAS Task Force to consolidate all DoD C-UAS directives within 90 days, mandate a large-scale exercise in DoD special use airspace, and require a strategy specifically addressing facilities, personnel, and assets within the United States. These provisions create the legislative architecture within which a coverage expansion for range complexes could be pursued, but they do not themselves resolve the gap.

DA Pamphlet 385-63 and AR 385-63: The Safety Mandate

DA Pamphlet 385-63 and its companion regulation AR 385-63 constitute the Army's governing framework for range operations and range safety. Together they establish the procedures, responsibilities, and mandatory actions that govern all live-fire training at Army range complexes worldwide.

The provision most directly relevant to C-UAS is the mandatory stand-down requirement. Upon notification of an airspace incursion, range control officers are required to cease all firing activity immediately. This requirement is not discretionary. It is a safety compliance mandate. Its operational effect is that any UAS, regardless of intent, operator identity, or actual threat level, that enters range airspace during live-fire operations produces an immediate and mandatory training halt.

Neither DA Pam 385-63 nor AR 385-63 contains any provision addressing C-UAS detection, C-UAS response authority, sensor integration, or C-UAS coordination requirements in range safety plans. The regulatory framework governing the event that most directly connects UAS incursion to readiness degradation contains no mechanism for managing that connection.

ATP 3-01.81: The Doctrinal Baseline

Army Techniques Publication 3-01.81, Counter-Unmanned Aircraft System, published August 2023, is the Army's current C-UAS doctrinal publication. It establishes the layered defense model, airspace control planning requirements, and the shared-responsibility framework for C-UAS across Army warfighting functions.

ATP 3-01.81 provides the doctrinal foundation for integrating C-UAS into operational planning. It addresses sensor employment, defeat system integration, airspace coordination, and command authority relationships. What it does not address is the range management context specifically. Range control operations, range safety plans, and range management service contracts are not addressed as C-UAS planning domains. The publication treats C-UAS as a tactical warfighting function rather than an installation readiness management function, leaving the range management application without doctrinal grounding.

DoD Strategy for Countering Unmanned Systems (December 2024)

The Department of Defense Strategy for Countering Unmanned Systems, signed by Secretary Austin in December 2024, establishes five strategic implementation pathways and designates the Army as executive agent for C-UAS requirements, doctrine, and training. It is the Department's current capstone C-UAS strategy and creates the departmental mandate under which range management service providers operate.

The strategy's relevance to range management is twofold. First, it establishes that C-UAS is a departmental priority requiring systematic integration across all DoD operational domains. Second, by designating the Army as executive agent, it places the responsibility for closing the range management C-UAS gap squarely within Army institutional authority. The strategy does not resolve the gap, but it eliminates any ambiguity about who is responsible for resolving it.

The Governance Gap

Taken together, these five authorities produce a coherent picture of a governance gap rather than a capability gap. The legal authority to defeat UAS over range complexes does not exist for most installations under Section 130i. The regulatory framework governing range safety contains no C-UAS integration requirements. The doctrinal publication governing C-UAS does not address the range management domain. The capstone strategy assigns responsibility without providing the regulatory and legal tools needed to execute it.

The result is a framework in which the operational connection between UAS incursion and readiness degradation is legally certain, doctrinally unaddressed, and contractually invisible. Range management service providers operating under current contract structures have no requirement to deliver C-UAS detection capability, no authority framework within which to coordinate defeat action, and no regulatory hook that would make C-UAS integration a contract performance standard.

SECTION II: SITUATIONAL ANALYSIS

The scale of the UAS incursion threat at U.S. military installations has moved from an emerging concern to a documented operational problem. The quantitative record now available through congressional testimony, DoD Inspector General reporting, and federal aviation data establishes both the frequency of incursion events and their direct connection to readiness outcomes.

Incursion Frequency and Installation Exposure

General Glen Guillot, Commander of NORAD and USNORTHCOM, testified before Congress in February 2025 that 350 drone incursions had been detected across 100 U.S. military installations in a single year. This figure represents detected incursions only. It does not account for incursions that occurred outside sensor coverage, were misidentified, or were not reported through formal channels.

The geographic distribution across 100 installations indicates that UAS incursion is not concentrated at a small number of high-profile sites. It is a broad-based operational condition affecting the majority of the Army's installation infrastructure. For range-intensive installations, where live-fire training operations are conducted across large airspace footprints on a daily basis, the probability of incursion during active range operations is not a planning assumption. It is a planning certainty.

Federal Aviation Administration data provides additional context. The FAA recorded 326 drone-related incidents in the first four months of 2024 alone. The Transportation Security Administration documented more than 2,000 drone sightings near U.S. airports between 2021 and 2023. These figures establish that the broader airspace environment within which military ranges operate is characterized by high UAS activity, much of it uncoordinated and conducted by operators with no awareness of military airspace restrictions.

The Readiness Cost Equation

The readiness cost of each range incursion event is a function of the mandatory stand-down requirement under DA Pam 385-63 and the operational tempo of the affected range complex. A stand-down on a range complex executing a battalion-level live-fire exercise does not merely pause one unit's training. It disrupts the range schedule for all subsequent units, creates ammunition accountability issues, requires reset of range safety conditions before resumption, and in some cases results in training days that cannot be recovered within the available training window.

At installations where range time is allocated months in advance and competing unit training requirements create chronic range availability constraints, a single incursion-driven stand-down can cascade across multiple units and multiple training cycles. The readiness cost is multiplicative, not linear.

The Coverage and Authority Gap at Scale

The DoD Inspector General has reported that a large percentage of installations lack operational approval to employ C-UAS capabilities. The IG's specific finding regarding Luke Air Force Base, where 75 percent of the world's F-35 pilots receive training, is particularly instructive: Luke was not designated a covered asset under Section 130i at the time of inspection, meaning the installation training the majority of allied F-35 pilots had no lawful authority to defeat a UAS threat over its airspace.

GAO-22-105705, published in March 2022, established that as of that date only four federal agencies held domestic C-UAS operational authority. No state or local agencies held any such authority. While the legislative framework has evolved since that report, the fundamental scarcity of lawful C-UAS operational authority at the installation level remains the defining characteristic of the domestic C-UAS posture.

Data Point	Figure	Source
UAS incursions at U.S. military installations (single year)	350 detected across 100 installations	Gen. Guillot, NORAD/NORTHCOM, Feb. 2025
FAA drone incidents (first 4 months of 2024)	326 reported incidents	Federal Aviation Administration, 2024
TSA drone sightings near U.S. airports (2021-2023)	More than 2,000 sightings	Transportation Security Administration
Federal agencies with domestic C-UAS authority (2022)	4 agencies; no state or local authority	GAO-22-105705, March 2022
DHS C-UAS development contract, Amentum (April 2022)	$260 million over 5 years	DHS Science and Technology Directorate
Additional DHS C-UAS award (May 2023)	$48 million	DHS Science and Technology Directorate

SECTION III: RISK ENVIRONMENT AND DOCUMENTED FAILURE MODES

The authority fragmentation, coverage gaps, and procurement failures documented across DoD IG reports, congressional oversight findings, and GAO audits produce concrete operational failures at range installations that directly impair the Army's ability to execute its training mission.

Authority Fragmentation as an Operational Failure Mode

The division of C-UAS authority across multiple statutory, regulatory, and command channels creates a coordination burden that exceeds the response time available during an active incursion event. A range control officer detecting a UAS incursion must simultaneously manage the mandatory stand-down, notify installation leadership, coordinate with installation airspace management, and potentially engage multiple command echelons before any defeat action can be authorized. By the time that coordination chain is complete, the incursion event has typically resolved itself, either through the UAS departing range airspace or through the training window being lost.

The DoD IG finding that a large percentage of installations lack operational approval to employ C-UAS capabilities reflects not merely a paperwork deficiency but a structural authority gap. Installations cannot self-designate as covered assets under Section 130i. The designation process runs through the Office of the Secretary of Defense and requires a formal determination that is neither rapid nor administratively simple. The result is that installation commanders who understand their C-UAS exposure cannot unilaterally resolve it.

Procurement and Fielding Failures

The House Armed Services Committee, in its report accompanying the FY2024 NDAA, documented that the Army had not transitioned Joint Counter-small UAS Office validated C-UAS systems to production at scale. This finding has direct operational consequences for range management. If validated C-UAS systems are not available in sufficient quantities, installations cannot field them even when they have the authority and the requirement to do so.

The Luke Air Force Base finding illustrates the compounding effect of procurement and authority failures. An installation training the majority of allied F-35 pilots was neither designated as a covered asset nor in a position to employ C-UAS defeat capabilities. Both failures would need to be resolved simultaneously before effective C-UAS protection could be provided. Neither failure is within the installation commander's authority to resolve independently.

Contractual Invisibility

Range management service contracts across the Army enterprise do not currently include C-UAS detection, reporting, or coordination as performance requirements. This is a structural failure with

direct operational consequences. Range management service providers, who are physically present at range complexes during operations and who bear responsibility for range safety plan execution, have no contractual obligation to maintain UAS detection capability, no reporting requirement for incursion events, and no coordination protocol connecting their range safety operations to installation C-UAS assets.

The consequence is that the contractor workforce most directly positioned to detect, document, and respond to UAS incursions is operating without the tools, requirements, or authority framework to do so effectively. C-UAS capability exists at some installations but is not connected to range management operations through any contractual or procedural mechanism.

SECTION IV: OPERATIONAL AND EXECUTION FRAMEWORK

Effective C-UAS integration into range management services requires action across four domains: planning, contracting, sensor architecture, and command authority. Each domain has specific, executable requirements that can be implemented within the existing regulatory and legal framework while the longer-term legislative fixes are pursued.

Planning Integration

Range operations plans and range safety plans must be amended to include C-UAS as a required planning element. At a minimum, every range safety plan should address three C-UAS-specific requirements: the identification of available detection assets and their coverage boundaries relative to range airspace; the coordination protocol connecting range control to installation C-UAS operators; and the notification and documentation procedures for incursion events that currently trigger mandatory stand-downs.

The planning integration requirement does not depend on legislative action. It requires a revision to DA Pam 385-63 to add C-UAS coordination as a required element of range safety planning, and a corresponding update to range management service contract performance work statements to require that contractors support and participate in that coordination. Both changes are within existing Army institutional authority.

Contracting Requirements

Range management service contracts must be updated to include three categories of C-UAS-related performance requirements. First, detection and reporting: contractors must be required to maintain a capability to detect and report UAS activity within range airspace, using either government-furnished detection equipment or contractor-provided systems meeting Army C-UAS sensor standards. Second, coordination protocol compliance: contractors must be required to execute the C-UAS coordination procedures established in the range safety plan, including real-time notification to installation C-UAS operators and post-event documentation. Third, data retention: contractors must be required to retain records of all UAS incursion events, stand-down durations, and training impacts, providing the Army with the operational data needed to quantify readiness costs and support the Section 130i coverage expansion case.

These contracting requirements can be implemented through contract modifications to existing range management service contracts and incorporated as standard requirements in future range management solicitations. They do not require new legislation and do not require defeat authority to be extended to the contractor workforce.

Sensor Architecture

The sensor architecture required for effective range management C-UAS integration is detection-oriented, not defeat-oriented. Range control officers need persistent, reliable detection capability that covers range airspace with sufficient fidelity to distinguish authorized from unauthorized UAS activity and to provide early warning before a UAS enters the live-fire danger area. Defeat authority remains with designated installation C-UAS operators under existing command authority structures.

The sensor architecture should be treated as government-furnished equipment under range management service contracts, with contractors responsible for operating and maintaining the detection systems as part of their range safety mission. This approach places defeat authority where it legally resides while ensuring that detection capability is persistently operational during range hours rather than dependent on force protection schedules that may not align with training windows.

Command Authority Integration

The command authority chain for C-UAS response during range operations must be pre-established, exercised, and documented before incursion events occur. The range control officer's authority to direct a stand-down is clear. The pathway from stand-down notification to C-UAS operator engagement to defeat authorization must be equally clear and must be short enough to be operationally relevant.

This requires a standing coordination agreement between range management operations and the installation C-UAS authority, with defined response timelines, communication channels, and authority thresholds that do not require real-time escalation to senior leadership for each incursion event. The agreement should be exercised quarterly as part of range safety rehearsals and updated whenever range management service contractor personnel or installation C-UAS operators change.

SECTION V: RISK MANAGEMENT MATRIX

Risk Domain	Primary Driver	Primary Consequence	Management Action
Legal Authority Gap	Section 130i coverage excludes most range complexes; installation commanders cannot self-designate	No lawful defeat authority during active incursions; stand-downs absorb full readiness cost with no mitigation option	Pursue Section 130i coverage expansion for range complexes meeting a defined readiness-impact threshold; document incursion frequency and training loss data to support the legislative case
Doctrine Misalignment	ATP 3-01.81 addresses C-UAS as a tactical warfighting function; DA Pam 385-63 contains no C-UAS planning requirements	Range safety plans lack C-UAS integration requirements; range control officers have no doctrinal framework for C-UAS coordination	Revise DA Pam 385-63 to add C-UAS coordination as a required range safety planning element; update ATP 3-01.81 to address the range management domain specifically
Contractual Invisibility	Range management service contracts contain no C-UAS detection, reporting, or coordination requirements	Contractor workforce lacks tools, requirements, and authority framework; detection capability is not persistently operational during training hours	Modify existing range management contracts to add detection, reporting, and data retention requirements; incorporate as standard PWS language in future solicitations
Procurement and Fielding Shortfall	JCO-validated C-UAS systems not transitioned to production at scale; inventory insufficient for installation-wide fielding	Installations with authority cannot field adequate capability; detection coverage gaps persist even where command authority exists	Prioritize range complex sensor fielding within Army C-UAS procurement planning; treat detection infrastructure as range safety equipment rather than force protection equipment
Readiness Data Opacity	No systematic collection of incursion event data, stand-down durations, or training loss metrics across range complexes	Army cannot quantify readiness cost of UAS incursions; cannot build evidence base for legislative or regulatory action	Mandate incursion event reporting through range management contracts; establish centralized data collection at Army Materiel Command or TRADOC level

SECTION VI: PRIORITY MANAGEMENT ACTIONS

0 to 90 Days

Army G-3/5/7 (Training): Issue a policy memorandum directing all range-intensive installations to inventory existing C-UAS detection assets, map coverage against range airspace, and document gaps. Deliverable: installation-level C-UAS coverage assessments submitted to HQDA within 60 days.

Installation Commanders (Range-Intensive Posts): Establish a standing C-UAS coordination agreement between range control and the installation C-UAS authority. Define the notification chain, response timelines, and communication protocols for incursion events. Exercise the agreement within 90 days.

Range Management Contracting Officers: Issue contract modifications to all active range management service contracts adding incursion event reporting requirements. Require contractors to document all UAS incursions, stand-down durations, and training impacts beginning immediately. Establish data submission cadence and format.

90 Days to 12 Months

Army G-3/5/7 and Office of the Judge Advocate General: Submit a legislative proposal to HASC and SASC recommending amendment of 10 U.S.C. Section 130i to extend covered asset designation to range complexes meeting a defined readiness-impact threshold, defined as installations where UAS incursions have produced a documented stand-down frequency of greater than four events per calendar year. Ground the proposal in the incursion and training loss data collected under the 0-90 day actions.

Army Training and Doctrine Command: Initiate revision of DA Pam 385-63 to add C-UAS coordination as a required element of range safety planning. Publish interim guidance pending formal regulation update. Assign revision to the Range Safety proponent at Fort Novosel.

Army Acquisition Executive: Direct that all future range management service solicitations include C-UAS detection, reporting, and coordination as standard performance work statement requirements. Assign development of standard PWS language to the Range Management program office.

12 Months and Beyond

Army Materiel Command: Incorporate range complex sensor coverage into the Army C-UAS fielding prioritization framework. Treat range airspace detection infrastructure as range safety equipment with a dedicated program line rather than as a subset of installation force protection

equipment. Establish a fielding timeline with measurable coverage milestones by installation category.

TRADOC: Update ATP 3-01.81 to include a dedicated chapter addressing C-UAS integration in range management operations. The chapter should address sensor employment, command authority coordination, range safety plan integration, and contractor coordination requirements specific to the range management context.

Army G-3/5/7 (Training): Establish an annual readiness impact report quantifying the training loss attributable to UAS incursions across the Army range complex inventory. Use the report as the primary accountability mechanism for measuring progress against C-UAS integration objectives and as the evidence base for sustaining legislative and budgetary support.

CONCLUSION

The Army faces a readiness governance problem that is both structurally simple and institutionally complex. The mechanism by which UAS incursions degrade training readiness is not ambiguous. DA Pamphlet 385-63 mandates a firing stand-down upon airspace incursion. Every unauthorized drone over a range complex produces that outcome. The readiness cost is certain, recurring, and growing as UAS proliferation continues.

What is absent is not awareness of the problem. It is the institutional treatment of C-UAS as a core range management function. The regulatory framework, the contract structure, the sensor architecture, and the command authority chain are all organized around a model in which C-UAS is a force protection addendum rather than a range operations requirement. Changing that model requires action at the legislative, regulatory, contractual, and doctrinal levels simultaneously, but none of those actions require new technology or new funding at program scale. They require institutional decision-making.

The Army is the DoD executive agent for C-UAS requirements, doctrine, and training. That designation is an instruction as well as an authority. The range management application of C-UAS is the most direct and most measurable point at which the Army's C-UAS posture connects to its readiness output. Treating it as a peripheral force protection concern rather than a central training readiness function is a choice that produces a quantifiable and preventable readiness cost at every range complex in the Army inventory.

REFERENCES AND SOURCES

- 10 U.S.C. Section 130i, Authority to Operate Unmanned Aircraft System Threat Detection Equipment at Certain Facilities and Assets, as amended through P.L. 118-159, National Defense Authorization Act for Fiscal Year 2025.
- National Defense Authorization Act for Fiscal Year 2025, P.L. 118-159, Sections 925, 1073, and 1090.
- Department of the Army, DA Pamphlet 385-63, Range Safety, with all current changes.
- Department of the Army, Army Regulation 385-63, Range Safety, with all current changes.
- Department of the Army, Army Techniques Publication 3-01.81, Counter-Unmanned Aircraft System (C-UAS), August 2023.
- Department of Defense, Strategy for Countering Unmanned Systems, December 2024.
- General Glen Guillot, Commander, NORAD and USNORTHCOM, Congressional testimony on UAS incursions at U.S. military installations, February 2025.
- U.S. Government Accountability Office, GAO-22-105705, Counter-Unmanned Aircraft Systems: DoD Should Take Actions to Address Identified Challenges, March 2022.
- DoD Office of Inspector General, findings on C-UAS operational approval at U.S. military installations, including Luke Air Force Base designation status.
- House Armed Services Committee, Report accompanying the National Defense Authorization Act for Fiscal Year 2024, findings on JCO C-UAS system transition to production.
- Federal Aviation Administration, Drone Incident Data, first four months of 2024.
- Transportation Security Administration, UAS Sighting Data near U.S. Airports, 2021-2023.
- Department of Homeland Security, Science and Technology Directorate, C-UAS development contract with Amentum, April 2022; supplemental award May 2023.

This document is produced for strategic advisory purposes. All doctrine and statutory references are drawn from publicly released government sources.

SOL | solengrs.com | Distribution intended for senior leadership and advisory use.