A Lawful Drone Security Framework for Private Texas Port Operators

WRITTEN BY
Art Wolfskill, Ph.D.
Michael A. Wolfskill

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

A Lawful Drone Security Framework for Private Texas Port Operators

Art Wolfskill, Ph.D.

Michael A. Wolfskill

September, 2026

EXECUTIVE SUMMARY

This section summarizes key points in this paper.

1. What Ports Can and Cannot Legally Do

There is a clear legal distinction between passive observation and active interference. As of 2026, Texas port operators can legally build layered surveillance and deterrence programs but are strictly prohibited from independently "taking down" rogue drones without federal oversight.

Legal Actions for Private & Non-Federal Operators

Routine surveillance, visual and thermal documentation, perimeter patrol, deterrence (signage, lighting, visible patrols), and passive detection (RF, radar, Remote ID, EO/IR).

Prohibited Actions (Active Drone Countermeasures):

Jamming, spoofing, seizing, capturing, damaging, or destroying a drone. These actions violate federal criminal law (18 U.S.C. § 32) and communications law (47 U.S.C. § 333) and carry severe penalties. Commercial availability of a "counter-drone" jammer or netgun does not grant legal authority to use it.

The SAFER SKIES Act (FY2026 NDAA):

This legislation provides a limited pathway for mitigation (disabling/destroying drones), but *only* for federally trained and certified State, Local, Tribal, and Territorial (SLTT) law-enforcement and correctional agencies using authorized technologies. Private critical infrastructure owners currently possess no such authority.

Pending UAFR Rules (May 2026)

FAA proposed Unmanned Aircraft Flight Restrictions (UAFR) rule which would allow high-risk facilities (including MTSA-regulated maritime ones) to request restricted airspace. But it explicitly does *not* grant facility operators self-help mitigation powers.

2. Recommended Operational Architecture: Layered Defenses

Because private and non-sworn port operators cannot lawfully shoot down drones, the operational focus must shift to a "detect-document-deter-deconflict-escalate" model. A legally defensible, highly effective drone security architecture relies on multi-sensor fusion. No single sensor works reliably across cluttered maritime environments.

A Lawful Six-Layer Defense

(a) **Organic Patrol Drones:** FAA Part 107-compliant patrol UAVs for fast-response perimeter patrol, berth inspections, and incident overwatch.

(b) **Passive Airspace Awareness:** Remote ID receivers and passive RF detection to identify and geolocate drone emissions without jamming.

(c) **Drone Radar:** Short-to-medium range 3D radar to track non-cooperative targets that are not broadcasting RF or Remote ID.

(d) **EO/IR Confirmation:** Electro-Optical/Infrared cameras to visually confirm radar/RF hits and gather prosecutorial evidence.

(e) **Resilient Communications:** Encrypted, secure networks to ensure video, telemetry, and control backbones remain stable.

(f) **Law-Enforcement Integration:** Pre-negotiated escalation pathways with local police, Coast Guard Captain of the Port (COTP), and SAFER SKIES-certified SLTT officers for immediate response to credible threats.

3. Strategic Implementation and Execution Plan

Ports that purchase hardware before establishing their legal boundaries and governance structures risk both mission failure and federal liability. Implementation must be phased.

Recommended Actionable Phases

First Month

Appoint a UAS Security Program Manager. Issue an order or SOP update prohibiting active mitigation. Inventory existing site assets, airspace, and vulnerabilities. Conduct management awareness training.

First Quarter

Procure two currently legal patrol UAVs and initial passive detection equipment. Train Part 107 pilots. Execute MOUs with local LE, port police, and COTP.

Six Months

Establish a fused detection cell. Conduct tabletop field exercises with LE and FSO. Implement NIST CSF 2.0 governance and 800-53 cyber controls. Finalize privacy/civil liberties reviews.

One Year

Evaluate docked/remote operations scaling. Prepare future UAFR application package. Sponsor SAFER SKIES certification if port utilizes sworn police. Establish annual audit and red-team processes.

4. Risk Management, Procurement, and Cybersecurity

The core legal risk for port leadership is a mismatch between what the port can lawfully use and the technology it enables. Procurement and IT security must be tightly governed.

Prohibited Technologies

Avoid the Chinese drone ecosystem entirely. Texas state networks are explicitly prohibited from using hardware/software from DJI, Autel, RoboSense, Hikvision, and others. Public ports must strictly adhere to the DIR prohibited-technology list; private ports are strongly advised to mimic this posture utilizing Blue or Green UAS-validated systems.

Cybersecurity Imperatives

Implement NIST CSF 2.0 and NIST SP 800-53 controls. Key requirements include strong identity/access management, encrypted telemetry, segmented networks between UAS and OT environments, immutable audit logging, and supply-chain risk management.

Liability and Insurance

Confirm specialized coverage including aviation liability for owned UAS, cyber coverage for cloud-hosted drone data, and clear contractual indemnity from systems integrators.

5. Recommended Policy Adoption

Ports must immediately adopt Standardized Operating Procedure (SOP) language that definitively outlines authorized uses and strictly prohibits unlawful mitigation. Additionally, privacy and data minimization clauses are essential to reduce exposure under Texas Government Code Chapter 423 regarding image capture.

As the regulatory landscape evolves, ports should actively monitor the rollout of SAFER SKIES authorized-tech lists and the finalization of the FAA's UAFR rules. At the state level, operators should advocate for a narrow maritime-security exception in Texas Chapter 423. This would provide a defense to prosecution for legitimate, non-intrusive security observation and passive detection by MTSA-regulated ports acting under written security programs.

Table of Contents

INTRODUCTION 1

DISCUSSION 2

- Scope, Assumptions, and Core Distinctions 2
- Governing Law and Authorities 4
- Operational Architecture and Equipment 8
- Currently Unlawful Equipment 10
- Executable Plan and Rules of Engagement 13
- Staffing Model for Execution 14
- Risk, Liability, Insurance, and Procurement 18

RECOMMENDATIONS 21

- Recommended Draft Port Policy Language 21
- Legislative Agenda for Texas Law Updates 23

CONCLUSION 24

APPENDIX A: Examples of Currently Legal Equipment by Function 26

END NOTES 34

INTRODUCTION

Texas port operators can lawfully build a robust drone-based security program today, but the program must be designed around a sharp legal distinction: private and non-federal port operators may generally conduct lawful Unmanned Aircraft System (UAS) surveillance, documentation, patrol, and passive detection, but they may not independently jam, spoof, seize, capture, disable, damage, or destroy a drone absent a specific federal statutory authorization[1]. That boundary is driven principally by FAA airspace rules[2], federal criminal and communications statutes[3], and the interagency DHS/DOJ/FAA/FCC legal advisory[4], which warns that non-federal entities may be restricted or penalized for acquiring or using many detection and mitigation capabilities depending on how the system functions[5]. 18 U.S.C. § 32 criminalizes damaging or disabling aircraft[6]; 47 U.S.C. § 333 prohibits willful radio interference[7]; and the FCC continues to treat jammer use as unlawful outside narrow federal authorizations[5].[8]

The major change since late 2025 is the SAFER SKIES Act[9], which was enacted in the FY2026 NDAA and codified through amendments to 6 U.S.C. § 124n. The act creates a limited path for State, Local, Tribal, and Territorial (SLTT) law-enforcement and correctional agencies to detect, track, seize, and (in some cases) disable, damage, or destroy a credible-threat drone, but only after federally prescribed training and certification, and only with technologies from a jointly maintained federal authorized technology list[10]. The statute also requires post-mitigation notification within 48 hours and sunsets SLTT authority on December 31, 2031. Critically, the statute does not grant those powers to private critical infrastructure owners, though Congress expressly required reporting on whether critical infrastructure owners may need expanded authorities in the future. Drone regulations are continually evolving. Therefore, maintaining current knowledge of applicable legal requirements is essential for port managers and authorities.

For Texas ports, the immediately executable path is therefore a layered, lawful, evidence-centered architecture: FAA-compliant patrol drones under Part 107[8] or public-aircraft authority where available; passive RF/Remote ID/radar/EO-IR detection; tethered or docked overwatch where operationally justified; strict privacy and cybersecurity controls; and pre-negotiated escalation to port police, local law enforcement, the Coast Guard Captain of the Port, and SAFER SKIES-certified SLTT officers for any mitigation action where those are available. This approach is strengthened by the FAA's pending fixed-site UAFR Notice of Proposed Rulemaking (NPRM)[11], which as of the draft proposal of May 22, 2026 would allow certain high-risk facilities (including MTSA-regulated maritime facilities with an active Facility Security Plan or Commandant-approved Alternate Security Plan)[12] to request unmanned-aircraft

flight restrictions, while explicitly not authorizing self-help detection or mitigation. The public comment period for that proposal is scheduled to close July 6, 2026. This NPMR would establish a framework for unmanned aircraft flight restrictions (UAFRs) around eligible fixed-site facilities, including certain critical infrastructure and sensitive federal sites.

The most defensible governance model is a two-track framework. If the port is a private operator without sworn police, it should adopt a “detect-document-deter-deconflict-escalate” model and stop short of actual aircraft interference. However, if the port is a public authority with its own police department or a dedicated law-enforcement partner, it should add a second track for federally certified mitigation under SAFER SKIES once training and authorized technologies are in place. In both cases, the recommended procurement baseline is a trusted-supply-chain stack that avoids Texas-prohibited technologies for public-sector networks and devices[13], favors Blue or Green UAS-validated systems[14] where practical, and implements NIST CSF 2.0[15] plus NIST SP 800-53[16] control families for identity, logging, encryption, software integrity, and supply-chain risk.

The practical bottom line is straightforward. Texas ports can use drones to enhance the security of their facilities. They cannot, by themselves, lawfully “take down” drones. A working framework therefore relies on lawful surveillance and deterrence, passive detection, strong incident handling, and tightly integrated law-enforcement escalation. That is the framework this article develops.

DISCUSSION

Scope, Assumptions, and Core Distinctions

This analysis is current as of mid-2026 and assumes no fixed budget, no specified terminal type, and no stated governance structure for the port. Texas ports vary, from public navigation districts with sworn peace officers to private marine terminals without police powers. As a result, the report analyzes both private operator and public-port / port-police scenarios, as both are categorized as Texas Critical Infrastructure. It also assumes the port is either subject to or materially coordinated with Maritime Transportation Security Act (MTSA) facility-security requirements[12], because that status now matters directly under the FAA’s pending UAFR proposal for maritime facilities. Legal uncertainties are flagged where the federal government has enacted authority but

has not yet finalized the implementing guidance, authorized-technology list, or training pipeline.

For operational design, four functional categories matter: surveillance, deterrence, interdiction, and active Counter-UAS (C-UAS). We use the following general definitions for each of these terms:

Surveillance: observing, recording, mapping, and documenting activity with FAA-compliant drones or passive sensors.

Deterrence: non-interference measures such as visible patrol presence, lighting, public-address warnings, signage, guard posture, and lawful communication with persons on site.

Interdiction: person-focused or access-control actions short of touching the aircraft, such as locating the operator, directing trespassers off property, or requesting law-enforcement intervention.

Active C-UAS: technical or physical interference with the aircraft or its links: jamming, spoofing, protocol exploitation, takeover, net capture, kinetic defeat, or destruction.

Under current law, the first three categories are the practical domain of private port operators; the fourth is generally reserved to federally authorized actors and, after SAFER SKIES implementation, qualified SLTT law enforcement and corrections organizations under controlled conditions[1].

Permissible Drone Security and Counter-UAS Measures by Port Actor

Operational authorities compared across private operators, public port authorities, and certified law-enforcement actors

FUNCTION	TYPICAL MEASURES	PRIVATE TEXAS PORT OPERATOR	PUBLIC PORT AUTHORITY WITHOUT POLICE POWER	PORT POLICE OR LOCAL LE CERTIFIED UNDER SAFER SKIES
Surveillance	Part 107 patrols; EO/R; inspections; passive RF detection; Remote ID receivers; radar; fixed cameras	✅ Lawful if FAA-compliant and privacy-governed	✅ Lawful if FAA-compliant and privacy-governed	✅ Lawful; may also support enforcement referrals
Deterrence	Visible drone patrols; lighting; announcements; signage; patrol vehicles; physical hardening over vulnerable assets	✅ Lawful	✅ Lawful	✅ Lawful
Interdiction	Locate pilot; trespass enforcement: secure gates/roofs; pause cargo transfer; notify LE/COTP/FAA	✅ Lawful if directed at people/property, not aircraft interference	✅ Lawful	✅ Lawful
Active C-UAS	Jamming; spoofing; remote takeover; net capture; kinetic defeat: drone-on-drone interception; destruction	❌ Not lawful today	❌ Not lawful today	⚠️ Potentially lawful only if federally trained/certified and using authorized technology in response to a credible threat

Note: The functional boundaries in this table synthesize the 2025 interagency legal advisory; 18 U.S.C. § 32; 47 U.S.C. § 333; the FAA public-safety guidance[17]; and 6 U.S.C. § 124n as amended by the FY2026 NDAA / SAFER SKIES Act.

Governing Law and Authorities

The federal aviation baseline remains 14 C.F.R. Part 107[8], which applies to the registration, airman certification, and operation of civil and public small UAS in the United States. For Texas port operators, that means the baseline patrol and inspection fleet should ordinarily be built around FAA Drone-Zone registered aircraft, certificated remote pilots, preflight and communications-link checks, airspace authorization where required, and documented operating procedures for night operations, people/vehicle exposure, and restricted areas. Part 107 accident reporting remains mandatory within 10 calendar days for qualifying injury or property-damage events. FAA guidance also continues to treat Part 107 as the principal rule for commercial, educational, and public-safety drone use below 55 pounds.

Remote ID is no longer discretionary. The FAA states that all drone pilots who are required to register or have registered their drones must operate in accordance with the Remote ID rule[18], and the FAA ended the discretionary enforcement grace period in March 2024[19]. For ports, this matters operationally because UAFR applicants under the May 2026 NPRM would need the ability to receive broadcast Remote ID messages near the requested restricted airspace and because passive Remote ID reception is now the cleanest lawful first layer in a port detection stack. The D.C. Circuit's Remote ID decision (often referred to in industry shorthand as the *Race Day Quads* case) also makes an important privacy point: the Remote ID broadcast itself does not expose the owner's nonpublic registration data[20], which remains protected by the Privacy Act and is not generally available for public lookup.

The FAA and TSA's pending BVLOS (Beyond Visual Line of Sight) NPRM proposes to create a Part 108[21] to normalize certain BVLOS and autonomous operations and establish a more scalable, performance-based framework, with TSA proposing complementary security measures. As of May of 2026, however, Part 108 is still only proposed[22]. Ports therefore cannot plan on routine BVLOS authority as a final rule yet; they must still rely on Part 107 operations, existing waivers and exemptions, or public-aircraft / COA pathways where those are available. Public port authority can include navigation districts, port authorities, or other governmental operators. Whether they can operate as "public aircraft" operators depends on the mission and legal posture, so this report recommends separate counsel review for any public aircraft or COA pathway. The NPRM is nevertheless strategically important because it points toward future port

use cases such as drone-as-first-responder, persistent dock inspection, remote site patrol, and inter-terminal response.

The most consequential pending rulemaking for maritime facilities would establish a formal process for fixed-site operators to request unmanned-aircraft flight restrictions (UAFR)[11]. For maritime transportation operations, the UAFR NPRM proposes to permit a covered facility to designate itself as a permanent no-fly area for drones[11]. It expressly covers a facility regulated by the MTSA that has an active Facility Security Plan or a Commandant-approved Alternate Security Plan. The proposal requires layered protective security, including restricted access, designated security personnel, and security monitoring capable of receiving broadcast Remote ID. It also expressly states that the resulting UAFR would not create a physical barrier and would not authorize the facility operator to detect, take control of, destroy, or otherwise interfere with unmanned aircraft. For Texas ports, this implies that the UAFR rule is a meaningful future deterrence and enforcement tool, but not a grant of self-help defeat authority.

The federal non-aviation constraints are equally important. The 2025 interagency legal advisory (issued through DHS and reflected in the FCC publication) states that legality of any system depends on the specific functions it has[5], not simple labels such as “passive,” “active,” “detection,” or “mitigation.” It warns non-federal public and private entities that federal laws may prevent, limit, or penalize the sale, possession, or use of many UAS detection and mitigation capabilities[5]. At a minimum, ports must evaluate the advisory against 18 U.S.C. § 32, the Federal Wiretap Act (and related criminal code chapters), the Communications Act, and FAA safety rules before purchasing detection or C-UAS equipment[5]. CISA’s *Be Air Aware* program now supplements that advisory with infrastructure-specific materials on detection technology[23], suspicious UAS activity, UAS cybersecurity, and critical-infrastructure/public-gathering protection.

Under 18 U.S.C. § 32, willfully damaging, destroying, disabling, or wrecking “covered aircraft”[6] (including UAS) is a federal crime. Essentially, under current law, taking down a drone is the same as taking down a Boeing 737. Under 47 U.S.C. § 333, no person may willfully or maliciously interfere with authorized radio communications[7], and the FCC’s jammer enforcement guidance continues to state plainly that jammers are unlawful except for narrowly scoped federal uses. For ports, those statutes are why “defending” facilities must not be translated into improvised RF defeat, protocol hacking, shotgun use, net-launches into navigable airspace, or protocol takeover by private security teams. A port can harden assets, document threats, coordinate with law enforcement, and lawfully fly its own aircraft. It cannot unilaterally become an anti-aircraft actor.

The major federal exception to active defense is Safer Skies; 6 U.S.C. § 124n as amended now authorizes *trained and certified* SLTT law-enforcement and correctional agencies[1] to take actions necessary to mitigate a credible threat to people, facilities, assets, large public gatherings, critical infrastructure, or correctional facilities. The statute's enumerated actions include detecting, identifying, monitoring, tracking, warning, disrupting control, seizing, and when necessary, using reasonable force to disable, damage, or destroy the UAS[1]. But the same statute also requires a) federal training and certification; b) a jointly maintained list of authorized technologies; c) federal oversight; d) privacy controls; and e) notice to DOJ and DHS within 48 hours after mitigation. FBI testimony in April 2026 indicates that, while final guidelines and regulations are still being completed, the Bureau is using a task-force model to put certified officers to work in the interim. Two conclusions follow. First, and most important, private ports are still outside the mitigation authority. Second, public ports or private ports with strong law-enforcement partnerships now have a realistic escalation path that did not exist before.

Texas adds another layer. Chapter 423 of the Texas Government Code[24] includes an offense for illegal use of an unmanned aircraft to capture images and separately addresses operation over critical infrastructure facilities; the Fifth Circuit's January 2024 decision in NPPA v. McCraw reversed the district court and held that facial constitutional challenges to these provisions failed, while leaving open the possibility of future as-applied defense[25]. Earlier district-court proceedings documented that journalists had been warned about Chapter 423 criminal penalties after using Part 107-compliant drones for reporting. The doctrinal lesson is that Texas's drone statute remains a live operational constraint, especially on image capture and sensitive-facility overflight, aside from federal airspace law.

Texas's broader public-sector security environment also matters. DIR's current prohibited-technology page states that state-owned devices and networks may not use listed prohibited hardware and software.[13] The February 2026 hardware list includes Autel Robotics, SZ DJI Technology, RoboSense, Wuhan Geosun, Hikvision, Dahua, Huawei, Hytera, Uniview, TP-Link, and others. Governor Abbott's January 2026 press release confirms that Autel, RoboSense LiDAR, and Wuhan Geosun LiDAR were among the newly added items[26]. For public port authorities, navigation districts, and any port police operating on governmental networks or state-procured systems, this list is not a theoretical concern but rather a procurement issue. The Chinese drone ecosystem must be excluded from public port operations in its entirety. For private terminals it is not automatically binding in the same way, but it remains a prudent minimum supply-chain baseline and not to be totally discounted.

Texas penal law underscores the risk of improvised counter-drone action:

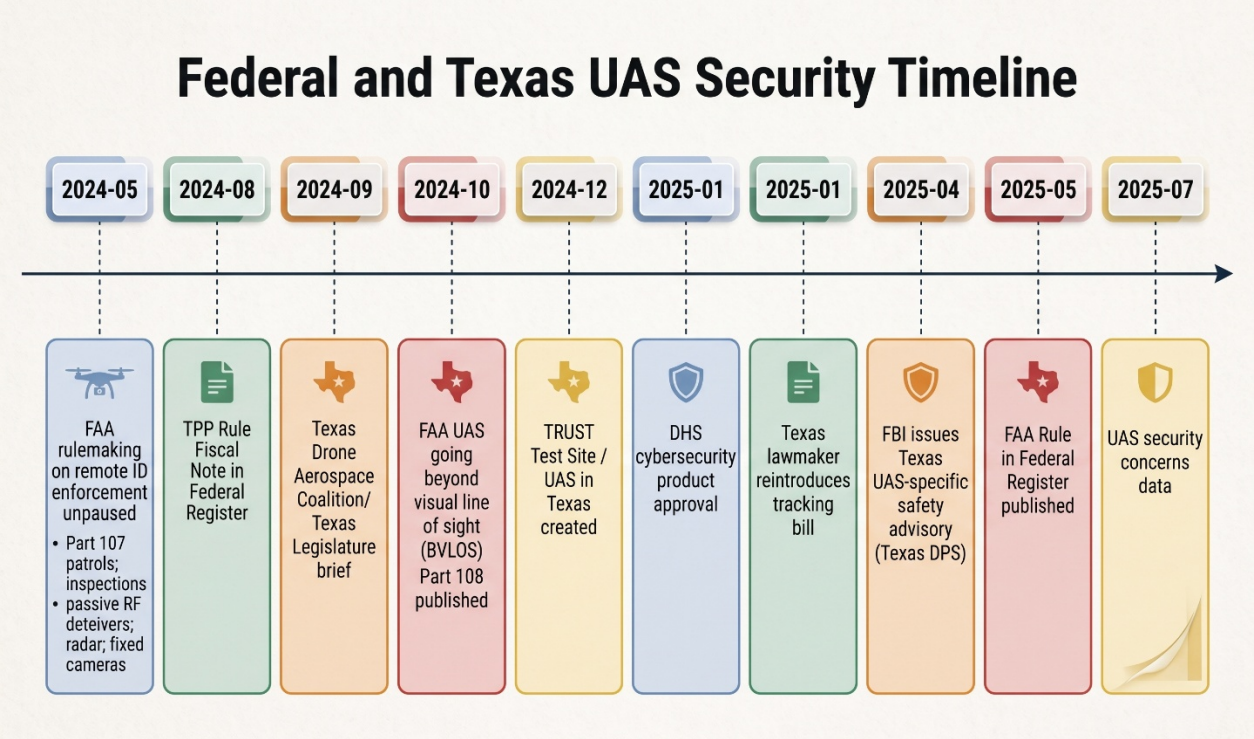
- Penal Code § 22.05[27] criminalizes reckless conduct that places others in imminent danger through deadly conduct, including discharging a firearm in certain circumstances;
- Penal Code § 28.09[28] elevates damage or interruption of critical infrastructure and expressly contemplates conduct using a firearm, drone, cyber-attack, or explosive;
- Penal Code § 31.01[29] provides the statutory definition of "critical infrastructure facility.

In practice, a private security guard who shoots at a drone over a port may simultaneously create federal aircraft-destruction exposure, FCC interference issues, state deadly-conduct risk, and civil liability.

Recent case law refines the privacy and preemption picture. The D.C. Circuit's Remote ID decision upheld the FAA's rule against constitutional attack[20] and emphasized the separation between public Remote ID broadcasts and nonpublic owner registry data. Singer v. City of Newton[30], while only a District Court decision and not a Texas case, remains a persuasive preemption precedent because it invalidated local drone registration and effectively prohibited local flight restrictions that conflicted with federal regulation. Later courts and commentators continue to cite it as an example of conflict preemption rather than total field preemption. Long Lake Township v. Maxon[31], from the Michigan Supreme Court, is important for public-sector inspections: it held that the exclusionary rule did not bar allegedly unconstitutional drone evidence in a civil zoning/nuisance proceeding seeking prospective relief, even though the lower court had treated the targeted drone surveillance as raising Fourth Amendment problems. For port operators, the safe takeaway is that privacy law and evidence admissibility are not the same question; a search may be legally problematic while evidence from it later survives to be used in some civil contexts.

FAA enforcement policy has also tightened. The FAA proposed more than $341,000[32] in civil penalties against drone operators in 2024 and stated that fines can reach up to $75,000 per violation under the FAA Reauthorization Act of 2024[33]. In 2026, the agency launched an expedited-enforcement pathway for certain drone violations[34] while separately stating that significant safety risks, such as restricted-airspace operations, remain in the standard enforcement lane. FAA public-safety pages and law-enforcement reporting tools now explicitly encourage immediate reporting[17] of dangerous or criminal drone operations to local law enforcement first, followed by FAA referral as appropriate. For ports, this supports a reporting-centered response model: the quickest lawful lever is often rapid referral, not technical defeat.

The following timeline captures the practical legal environment in which a Texas port must operate: Remote ID is enforceable now; BVLOS normalization is still pending; maritime UAFRs are proposed but not yet final; and SLTT mitigation authority exists in statute but depends on federal implementation, certification, and authorized technology lists.



Operational Architecture and Equipment

A port security design for C-UAS operations should not begin with “How do we shoot down drones?” It should begin with “What is the minimum lawful stack that provides continuous awareness, admissible evidence, and fast escalation?” The best-performing answer in the literature and in current federal guidance is a layered, multi-sensor fusion. Peer-reviewed reviews of drone detection systems consistently conclude that no single sensor works reliably across all backgrounds, weather conditions, and target types. Radar, RF sensing, Electro-Optical/Infrared (EO/IR), and other modalities perform differently in clutter, at low altitude, and in dense electromagnetic environments[35]. For maritime ports with cranes, metal structures, water reflections, AIS/VHF traffic, mixed industrial clutter, and who knows what else, understanding this concept is especially important. The correct system design is therefore not one miracle box but a layered array that cross-cues across sensor types[35], with one sensor feeding information to another to develop the full picture.

A lawful Texas port stack should have at least six layers:

- First, organic patrol drones for perimeter patrol, accident scene capture, berth inspection, and rapid overwatch;
- Second, passive airspace awareness through Remote ID receivers and passive RF detection;
- Third, short- to medium-range radar for non-cooperative targets and low-visibility approaches;
- Fourth, EO/IR confirmation and forensics;
- Fifth, resilient communications for any docked, tethered, or BVLOS-adjacent architecture; and
- Sixth, law-enforcement integration for the rare case in which the drone is not merely suspicious but a credible threat.

CISA's critical-infrastructure guidance[23] and NIST's UAS/public-safety communications work both align with this layered conception of port defense protocols.[36]

Appendix A contains graphics that highlight some examples of equipment that is lawfully deployable under current regulations. Many more exist, and this should not be considered an exhaustive, or even recommended list. They are broken out by their function in a well-designed defensive array.

Capability, compliance-status, and price information in the equipment in Appendix A are drawn from official manufacturer pages and, where the official page was quote-only, from cited authorized reseller listings for indicated pricing. Blue/Green status references come from DIU's Blue UAS list, AUVSI's Green UAS cleared list, or vendor statements where specifically cited.

While these are simply examples of lawful equipment currently available at the time of writing, other brands and systems exist, and we expect that more options will become available as the programs and guidance roll out. Appendix A's procurement logic is deliberate. Skydio X10 and Parrot ANAFI USA are excellent for daily patrol and rapid response. Freefly Astro Max, Inspired Flight IF800, Ascent Spirit, and Hoverfly Spectre are better suited to public-sector or critical-infrastructure procurement where cybersecurity, domestic sourcing, and trusted-supply-chain posture matter more than lowest acquisition cost. Dedrone RF-360, Robin IRIS, and EchoShield form a passive detection triad that is operationally stronger in cluttered maritime environments than any one layer by itself. Silvus and Elsight address the communications problem that port drone programs can be prone to underestimate. If the video, telemetry, and control backbone are fragile, the security mission is fragile.

While the previous information shows legal and effective hardware that could be considered in a port drone defense program, many active C-UAS systems are available that are currently not lawful for private deployment. The following highlights the types of equipment that port users should avoid, at least under the current regulatory landscape.

Currently Unlawful Equipment

Portable Jammers

1



Example system or class	DroneShield DroneGun Mk4
Technology	Portable RF jammer / defeat effector
Why operators find it attractive	Rapid handheld response to rogue drones
Private Texas port deployment today	No
Legal rationale	Jamming implicates 47 U.S.C. § 333; interference/disablement can implicate 18 U.S.C. § 32; non-federal private actors lack statutory mitigation authority

2



Example system or class	DedroneDefender 2
Technology	Smart jammer
Why operators find it attractive	Designed for urban mitigation with reduced collateral effects
Private Texas port deployment today	No
Legal rationale	Same federal radio-interference and aircraft-disablement constraints; interagency advisory warns non-federal entities to assess legality by system function

Interceptor Systems

3



Example system or class	Fortem DroneHunter F700
Technology	Drone-on-drone autonomous capture / defeat
Why operators find it attractive	Standoff interception and net-based or physical defeat of target drones
Private Texas port deployment today	No
Legal rationale	Physical interception, seizure, disablement, or destruction of an aircraft is not privately authorized; SAFER SKIES authority is limited to trained/certified SLTT law enforcement and corrections

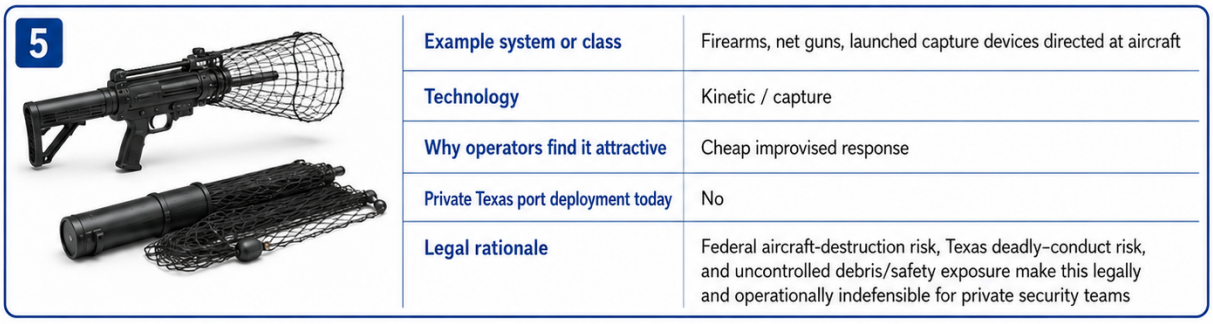
Spoofing Devices

4



Example system or class	GPS/GNSS spoofers, protocol takeover tools, "take-control" systems
Technology	Spoofing / cyber interference
Why operators find it attractive	Appears cleaner than kinetic defeat
Private Texas port deployment today	No
Legal rationale	Can implicate communications law, computer-crime statutes, and the interagency advisory's restrictions on non-federal detection/ mitigation tools

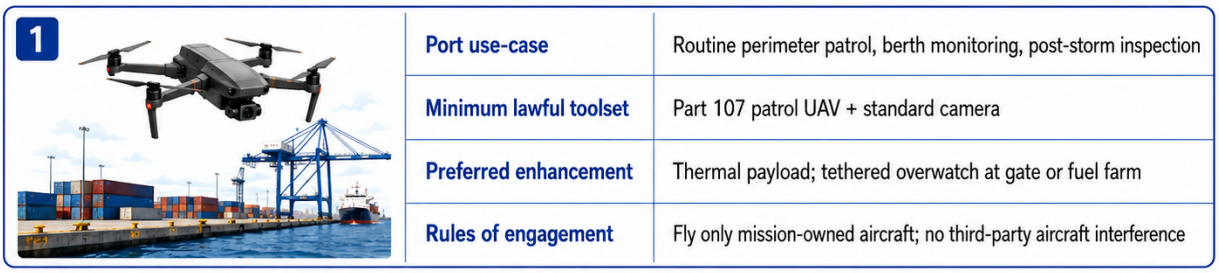
Capture Devices



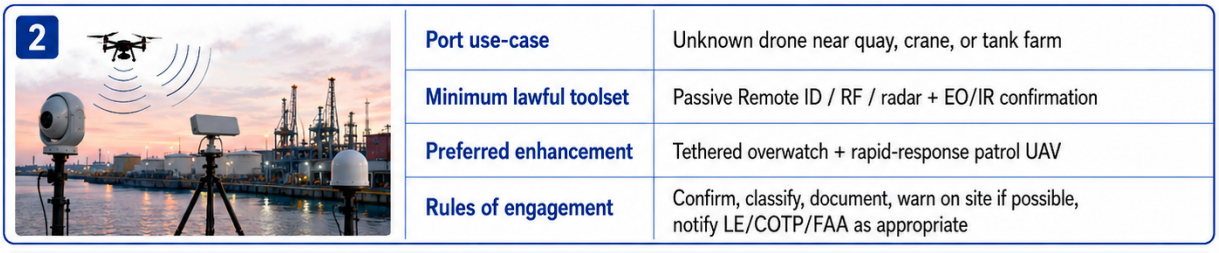
The systems listed are commercially marketed C-UAS products or common active-defeat classes of equipment, but market availability does not imply deployment authority. The controlling legal constraints are the interagency legal advisory, 18 U.S.C. § 32, 47 U.S.C. § 333, FAA safety constraints, and the fact that SAFER SKIES extends mitigation authority only to trained/certified SLTT law-enforcement and correctional agencies using authorized technologies. Several “counter-drone” products marketed to civilian critical infrastructure are not lawfully usable by private port operators in Texas today even though the vendor page is public. Market visibility is not the same thing as legal authority.[37]

The following graphics show the mapping of various use-cases onto a set of legal considerations that should be considered. These can be used to guide thinking and planning for the particular scenarios that each operator expects to face.

Routine Patrol



Unknown Drones Identified



Waterside Reconnaissance



Port use-case	Suspected smuggling or waterside reconnaissance
Minimum lawful toolset	Radar/RF detection + high-zoom EO/IR + evidence workflow
Preferred enhancement	Integrated comms backbone for mobile interdiction team
Rules of engagement	Focus on evidence, pilot-location efforts, waterside security response, law-enforcement handoff

Public Gatherings



Port use-case	Drone near large public gathering on port property
Minimum lawful toolset	Patrol UAV + passive detection + crowd security coordination
Preferred enhancement	Dedicated law-enforcement command post; SLTT certified mitigation if available
Rules of engagement	Escalate early; private operators stay in observe-document-deter lane

Persistent Coverage



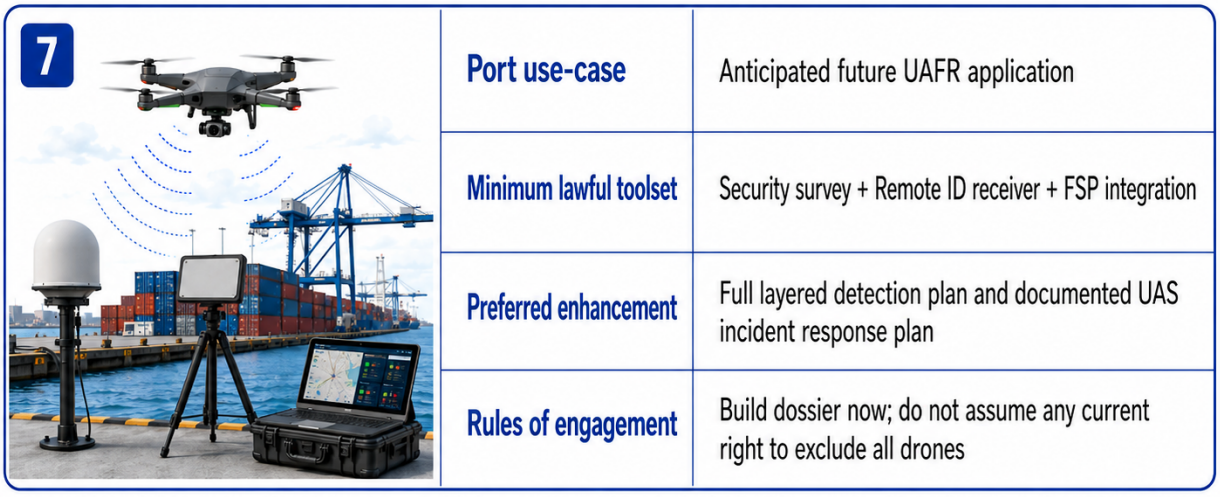
Port use-case	Persistent blind-spot coverage over gates or hazardous process equipment
Minimum lawful toolset	Tethered drone + fixed cameras + radar
Preferred enhancement	Docked drone when waivers/authorizations allow
Rules of engagement	Use as overwatch and deterrence, not as active interceptor

Reconstruction



Port use-case	Accident scene, spill, fire, or security breach reconstruction
Minimum lawful toolset	Patrol UAV + RGB/thermal payload
Preferred enhancement	LiDAR payload for 3D reconstruction
Rules of engagement	Preserve evidence chain; follow FAA and Coast Guard reporting requirements

Future UAFR Planning



Executable Plan and Rules of Engagement

The executable plan should be developed in stages, with each stage linked to an operational ability and a specific timeline. A port that tries to procure everything at once usually makes two mistakes: it buys technology before writing the legal concept of operations, and it underfunds staffing, training, and data governance. The better sequence would be governance procedures and documentation first, passive detection capabilities second, persistent overwatch third, and mitigation partnerships fourth. That order matches both the law and the operational maturity curve. It also prevents a likely failure mode in critical-infrastructure security programs: the purchase of counter-drone products whose active functions are not lawful for the buyer to use.

Time band	**Actionable directive**	**Why this should happen in this time band**
First month	Appoint a UAS Security Program Manager under the port security chain; issue a legal hold memo that active mitigation is prohibited unless federally authorized; identify whether the port is private, public, or has sworn police; inventory airspace, cranes, tank farms, passenger zones, waterside approaches, and existing camera/radio coverage; begin budget analysis. Work with a service provider to design training and awareness events (perhaps sim-table style) to begin indoctrination of current management	Governance and legal boundaries must exist before procurement or flight operations; enlightening managers to potential hazards and capabilities must begin early

Time band	Actionable directive	Why this should happen in this time band
First quarter	Register aircraft; procure two patrol UAV types plus passive detection equipment; train or hire Part 107 remote pilots; designate evidence-retention process; execute MOUs with local LE, port police if any, and Coast Guard COTP; screen all public-sector procurements against Texas prohibited technologies	This creates immediate lawful capability while preventing supply-chain or authority mistakes
By six months	Stand up a small, fused detection cell; conduct detailed tabletop and field exercises with local LE and FSO; add tethered overwatch at one high-risk location; finalize privacy and civil-liberties review; deploy NIST CSF 2.0[15] governance and 800-53-derived technical controls[16]	Six months is a reasonable point to move from ad hoc drone use to a durable security program
By one year	Decide whether to scale to docked or remotely managed operations; prepare a future UAFR application package in anticipation of rule finalization; if the port has sworn police, sponsor SAFER SKIES certification and authorized-tech planning; establish annual audit, sensor accuracy test, and red-team process	Mature programs require recurring oversight, external coordination, and a clear pathway to restricted-airspace relief

The implementation logic in this table tracks the current legal environment: immediate flight and passive detection are available, while active SLTT mitigation depends on the federal training, guidance, and an authorized-tech list as required by SAFER SKIES.

Staffing Model for Execution

A workable staffing model for a medium-to-large port is modest but specialized. Depending on the scale of the program, it could involve onboarding anywhere from six to upwards of twenty-three trained specialists. A complete program should consider the following positions:

a) One accountable program lead, ideally reporting to the Facility Security Officer or deputy FSO;

b) Two to six certificated pilots depending on the coverage model;

c) One or two airspace/detection analysts per shift if radar and RF sensing are used;

d) One cyber / systems administrator shared with port IT or OT security; and

e) A designated law-enforcement liaison.

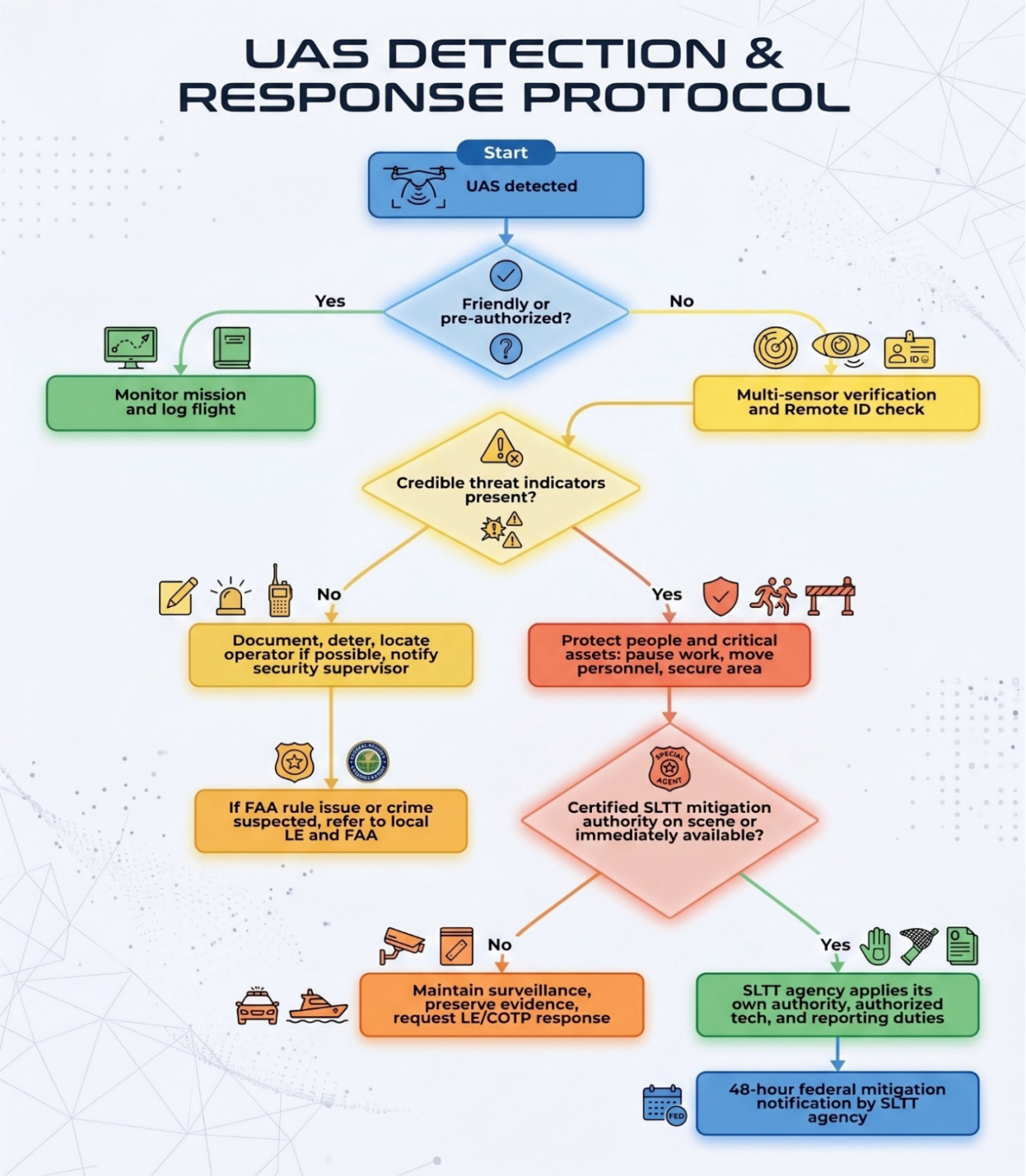
Depending on the extent of port operations, further positions may be warranted. If the port has docked or tethered operations or large event responsibilities, a two-person security-operations crew per active shift becomes the minimum safe model: one sensor/airspace operator and one field or flight operator. If the port intends to support future SLTT mitigation, at least a subset of sworn officers (not private guards) should be identified early for federal training and certification. This is a recommended operating model rather than a statutory requirement, but it follows directly from the chain-of-custody, airspace, and incident-management burdens revealed in current federal guidance.

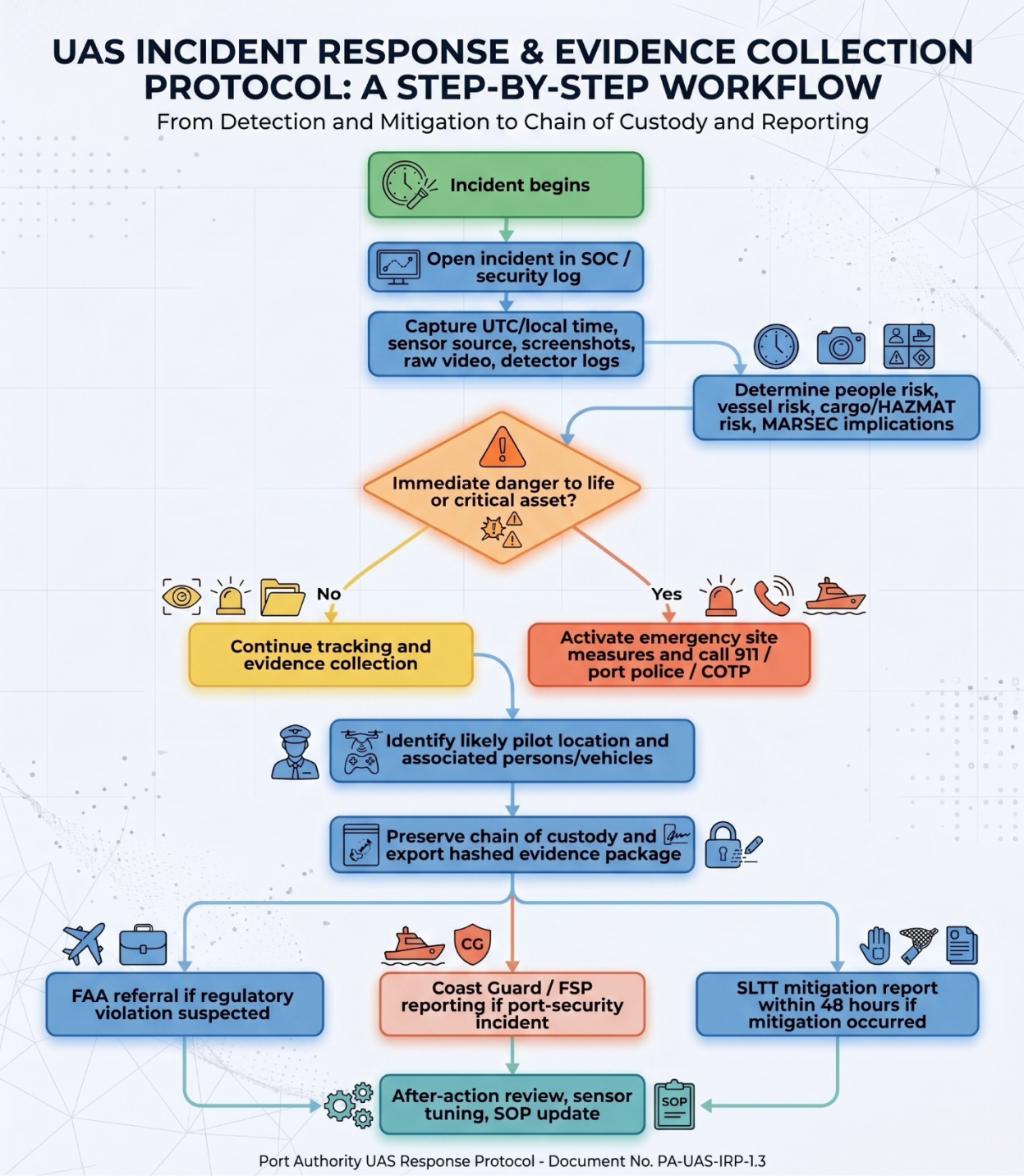
Training should also be layered. The baseline package is: FAA Remote Pilot certification; recurrent training (every 24 months per Part 107); site-specific airspace and LAANC procedures; night-operations competency; Remote ID and detection familiarization; MTSA facility security procedures[38]; evidence handling; privacy and civil-rights constraints; basic RF interference awareness; and cyber hygiene for aircraft, ground stations, and cloud systems. If the port is MTSA-regulated, the FSO training and drill obligations under 33 C.F.R. Part 105 should explicitly incorporate drone scenarios. If the port has police or a dedicated government partner, that agency should separately pursue SAFER SKIES training certification for mitigation-capable officers once these are available.

The Rules of Engagement (ROE) should be written in plain language and taught the same way. The port should operate under a four-step ROE: verify, classify, contain, and escalate. “**Verify**” means sensor confirmation and immediate determination on whether the aircraft is friendly, permitted, or unknown. “**Classify**” means applying threat indicators such as proximity to hazardous cargo, unusual loitering, payload characteristics, waterside coordination, or repeated probing runs. “**Contain**” means people- and asset-centered defensive action: pause lifting or fueling, move personnel, secure access points, activate public-address warnings, re-task patrol UAVs, and preserve evidence. “**Escalate**” means notifying the correct authority based on severity: local law enforcement first for dangerous or criminal operations, FAA for suspected regulatory violations[39], Coast Guard/COTP for port-security implications, and federally certified SLTT units if mitigation authority may be needed.

The following decision trees can aid in the logical and legal flow of actions and information based on the identified threats and the port operator's legal status and assets available. These decision flows align the port's operational steps with current law: private operators must stop at surveillance, deterrence, containment, and escalation; qualified SLTT agencies are the only non-federal actors who may cross into mitigation under SAFER SKIES[1].

These incident-response models are intentionally evidence-heavy. Ports are not merely trying to "see" drones; they are trying to build defensible cases, support federal and local enforcement actions, and improve protective measures over time, all within the current legal framework. FAA, Coast Guard, and SAFER SKIES reporting requirements all reward disciplined recordkeeping[40].


UAS DETECTION & RESPONSE PROTOCOL
Start
UAS detected
Friendly or pre-authorized?
Yes
No
Monitor mission and log flight
Multi-sensor verification and Remote ID check
Credible threat indicators present?
No
Yes
Document, deter, locate operator if possible, notify security supervisor
Protect people and critical assets: pause work, move personnel, secure area
If FAA rule issue or crime suspected, refer to local LE and FAA
Certified SLTT mitigation authority on scene or immediately available?
No
Yes
Maintain surveillance, preserve evidence, request LE/COTP response
SLTT agency applies its own authority, authorized tech, and reporting duties
48-hour federal mitigation notification by SLTT agency



Risk, Liability, Insurance, and Procurement

The core legal risk for procurement actions relates to an authority mismatch: buying or enabling functionality that the port cannot lawfully use. The 2025 interagency advisory

explicitly warns against relying on vendor descriptions alone and stresses that legality turns on what the system actually does, especially if it intercepts communications, disrupts links, or affects navigation or control. That warning should drive both procurement language and day-to-day system configuration. An RF disruptor is not legally equivalent to a passive RF receiver merely because both are sold under the banner of "counter-drone." Ports should therefore require a feature-by-feature legal review of every sensor, firmware option, API, and response module before purchase or activation.[5] In-depth knowledge of the equipment is critical to legal and appropriate procurement and use. The legal and cyber risk drives in the following matrix are grounded in the interagency legal advisory, FAA operational rules and enforcement materials, Texas Prohibited technology policy, and NIST's cybersecurity framework and control catalog. The insurance recommendations are analytical risk-transfer recommendations rather than a statement of any general legal requirement.

Risk, Liability, Insurance, and Procurement

Risk matrix

Risk type	Representative failure mode	Consequence	Practical mitigation
Legal authority	Private security uses jammer or takeover capability	Federal criminal exposure, FCC action, civil claims	Contractually disable active effects; use passive-only systems absent federal authority
Aviation safety	Patrol drone conflicts with manned traffic or vessel helos	FAA enforcement, injury, mission shutdown	Part 107 discipline, airspace authorization, pilot training, preplanned launch zones
Privacy / civil liberties	Overbroad image capture or unnecessary retention	Chapter 423 exposure, tort claims, public trust loss	Narrow mission purpose, retention limits, masking/redaction, review for sensitive imagery
Evidence integrity	Logs overwritten, video edited, no chain of custody	Lost prosecutions and weak incident response	Hash raw files, preserve original telemetry, timestamp and custody logs
Cybersecurity	Drone, ground station, or cloud account compromised	Data exfiltration, spoofed feeds, mission failure	NIST CSF 2.0 governance, segmented networks, MFA, signed updates, audit logs
Supply chain / procurement	Public port buys prohibited technology	Regulatory noncompliance, grant and network issues	DIR/TXCC screening, Blue/Green posture, origin and subcomponent representations
Liability / insurance	Drone crash or privacy claim outside policy grant	Uncovered loss	Tailored UAS aviation liability, cyber, professional/E&O, and contractual indemnity review

A baseline cybersecurity plan needs to meet standards on several levels: the high-level NIST CSF 2.0 framework so the executives know what the overall goals are,[15] as well as the specific rules from NIST SP 800-53 Rev. 5 so the IT team can accurately build the defenses[16]. At the minimum, Texas ports should implement the following practices:

- Strong identity and access management for controllers and cloud platforms;
- Encryption for stored evidence and telemetry;

- Audit logging;
- Network segmentation between UAS systems and business / OT networks;
- Signed firmware and patch discipline;
- Supply-chain risk management for aircraft, radios, and sensors; and
- Documented incident response and recovery playbooks.

The Coast Guard's 2025 maritime cybersecurity final rule makes these even more important for MTSA-regulated facilities by adding minimum cyber requirements to the marine transportation system security framework.

While a full discussion of the 800-53 control subsets is beyond the scope of this paper, some of the important ones for drone programs include AC for role-based access, IA for strong authentication, AU for immutable logging and review, SC for encryption and communications protection, SI for monitoring and integrity checks, CM for baseline configuration control, MP for evidence/media handling, and SR for supply-chain governance. The BVLOS NPRM (aka Part 108) itself reinforces the importance of cybersecurity risk assessment and mitigation for UAS equipment, systems, and networks, which strengthens the case for using NIST controls even before Part 108 is finalized.

Insurance and contractual risk transfer should be shaped to the actual mission envelope. A port running only occasional Part 107 patrols has a risk profile much different than a port operating tethered overwatch, dock-based launch systems, or contractor-run detection networks. Even so, a prudent insurance baseline would require at a minimum: aviation liability for owned or operated UAS; hull/equipment coverage for aircraft and payloads; cyber coverage that expressly includes operational technology and cloud-hosted drone data; professional and technology Errors and Omissions (E&O) where monitoring or analytics are outsourced; and contractual indemnity plus additional insured language from systems integrators and data-service vendors. These recommendations are general best practices, but they flow directly from the legal, safety, privacy, and cyber risk profile documented above. Clearly, appropriate insurance professionals should be included in the discussion and decision-making.

Procurement compliance should be stricter for public ports than for private terminals in several ways, but the recommendations are the same. Public ports should screen procurements against the Texas prohibited-technology list[13], adopt a "trusted supply chain" preference for Blue or Green UAS-validated systems where feasible, require country-of-origin and subcomponent disclosures for aircraft, sensors, radios, batteries, and cloud services, and require contract language on firmware support, vulnerability disclosure, log export, data-location transparency, and end-of-life notice. Private ports

are not necessarily bound by all state-public-entity restrictions, but if they want smooth law-enforcement integration and future grant compatibility, mimicking the public-sector restrictions is wise.

Incident reporting and evidence handling should be formalized from the start. FAA accident reporting is due within 10 days for qualifying Part 107 incidents. The FAA considers an accident reportable if the labor and parts required to repair the damage exceeds $500 not including the drone value, or if the incident caused serious injury. Since the term serious injury is not explicitly defined, port operators should err on the side of reporting all but the most minor of injuries. Section 107.9 provides more detail[40]. Additionally, the NTSB has reporting requirements for certain aircraft (including drone) accidents.

Dangerous or criminal third-party drone activity should be reported to local law enforcement first, consistent with FAA guidance, and then referred to the FAA where regulatory violations appear likely. Law-enforcement partners can use the FAA's *UAS Incident Report Questionnaire* to expedite enforcement proceedings. If the facility is MTSA-regulated, the incident must also be handled under the Facility Security Plan and related Coast Guard security and cyber procedures. If mitigation occurs under SAFER SKIES, the SLTT agency must notify DOJ and DHS within 48 hours.

RECOMMENDATIONS

This document has outlined a multi-step process for upgrading the operations of Texas ports to include broad-based defensive measures for protecting against drone incursions. The body of the text is replete with recommendations, and the authors advise each port governing body to study them carefully, identifying the path to a feasible structure for that particular installation. Along with these hardware and system recommendations, we advise that the following policy changes be implemented. Additionally, advocating for updates to the laws is an important strategy for improving the overall legal landscape.

Recommended Draft Port Policy Language

The following SOP language, or similar verbiage, is recommended for immediate adoption by Texas port operators:

> **Authorized uses.** Port-operated unmanned aircraft systems may be used only for lawful security patrol, safety observation, inspection, incident

documentation, emergency support, training, and other written mission sets approved by the port's UAS Security Program Manager and the Facility Security Officer or equivalent security authority. All operations shall comply with applicable FAA requirements, including registration, pilot certification, Remote ID, airspace authorization, and accident reporting.

Prohibited acts. No port employee, contractor, or security provider shall jam, spoof, hack, seize, capture, net, strike, disable, damage, destroy, or otherwise interfere with an unmanned aircraft or its communications, navigation, or control links unless the action is taken by a federal agency or by a State, Local, Tribal, or Territorial law-enforcement or correctional agency lawfully exercising authority under 6 U.S.C. § 124n and using federally authorized technology.

Detection systems. The port may deploy passive detection systems, including Remote ID receivers, radar, electro-optical / infrared cameras, and passive RF sensors, only after legal and technical review confirms that the configuration does not perform unlawful interception, disruption, or takeover functions. Vendor "counter-drone" labeling shall not substitute for legal review.

Escalation and reporting. When an unknown or suspicious unmanned aircraft is detected, port personnel shall verify the contact, classify the threat, document the event, protect people and critical assets, and notify appropriate law-enforcement, FAA, and Coast Guard authorities in accordance with the incident severity matrix and the Facility Security Plan.

The above policy language is legally conservative by design. It tracks the interagency advisory's function-based legality analysis[5], the federal radio-interference and aircraft-disablement statutes, FAA reporting rules, and the new SLTT carveout in 6 U.S.C. § 124n.

A companion privacy clause is equally important:

Privacy and data minimization. The port shall collect, use, retain, and disclose UAS imagery, telemetry, Remote ID data, and sensor detections only to the extent reasonably necessary for a documented security, safety, or evidentiary purpose. Data unrelated to a valid mission shall be promptly deleted or minimized. Access shall be role-based, logged, and periodically audited. Sensitive imagery of private persons or property shall be reviewed for minimization, masking, or redaction before external release, except where preservation is necessary for law-enforcement, litigation hold, or mandatory reporting.

The previous clause is not just good governance; it is the practical way to reduce exposure under Texas statutes' image-capture restrictions, constitutional privacy concerns, and modern cyber-risk expectations.

Legislative Agenda for Texas Law Updates

For legislation, the most useful Texas change would be a narrow maritime-security exception in Chapter 423. The current statute can chill legitimate security and documentation conduct even when the operator is FAA-compliant and not doing anything invasive. A carefully drafted amendment should not authorize private anti-drone force. It should instead create a defense to prosecution and civil liability for non-intrusive security observation, documentation, and passive detection by MTSA-regulated ports and terminals acting under a written security program. A model amendment could read as follows:

Proposed Texas Government Code Chapter 423 amendment.
"It is a defense to prosecution under this chapter, and to civil liability under this chapter, that the capture, receipt, or use of an image or unmanned-aircraft-system detection data was undertaken by or on behalf of the owner or operator of a facility regulated under the MTSA, or a person acting under the written authority of such owner or operator, for the purpose of security monitoring, incident response, safety inspection, cargo protection, or protection of critical infrastructure, provided that:

(a) The operation complied with applicable federal aviation law;

(b) No person engaged in radiofrequency interference, protocol exploitation, takeover, seizure, capture, disablement, damage, or destruction of an aircraft unless separately authorized by law;

(c) Collected data were handled under written minimization, retention, and access-control procedures; and

(d) disclosure outside the owner or operator's security, law-enforcement, legal, or regulatory functions was prohibited except as required by law."

Such a proposal would solve a real operational problem without invading federal airspace or communications authority. It would also align Texas law[41] with the federal reality that ports need to observe and document threats even when they cannot mitigate them.

At the federal level, four updates would materially improve the architecture for ports. First, DOJ, DHS, DOT, FCC, and NTIA should publish the authorized-tech list and training procedures required by SAFER SKIES as quickly as possible. Second, the FAA

should finalize the UAFR rule with special attention to MTSA-regulated maritime facilities and a clear, practical process for recurring vessel and contractor access. Third, the FAA should finalize Part 108 in a way that accommodates critical-infrastructure patrol, emergency response, and secure remote operations without forcing every port use-case to require individually tailored waivers. Fourth, Congress should consider a tightly audited, privacy-protective pilot program for critical-infrastructure owners to use a very narrow set of non-RF, non-debris-producing emergency measures in partnership with certified law enforcement agencies, where immediate response times are operationally difficult or impossible. Congress has already required a formal determination on whether SLTT agencies are able to fully protect critical infrastructure and, if unable, to provide recommendations for expanding authority to owners[1].

Open questions and present legal uncertainties: The main unsettled questions as of Mid-2026 are not whether private ports can actively counter drones, since they generally cannot. The real issues are how quickly the federal government will finish SAFER SKIES implementation for SLTT agencies, which specific technologies will make it onto the authorized list, and whether the FAA will finalize the UAFR and Part 108 proposals in a way that actually helps MTSA-regulated maritime facilities. Another practical gray area is exactly how certain Texas procurement restrictions apply across different port governance models.

However, these uncertainties do not change the core recommendation of this paper. If anything, they reinforce it. Ports need to build their security frameworks right now around lawful surveillance, passive detection, evidence preservation, asset hardening, and tight integration with law enforcement. Any actual mitigation authority should be treated as an outside capability that must be separately certified, documented, and audited.

CONCLUSION

The practical reality for Texas port operators is that a robust drone security program must be built entirely around current legal boundaries, not future capabilities or commercially available active countermeasures. Because private and non-federal entities do not possess the statutory authority to independently jam, capture, or destroy rogue aircraft, the operational focus must center strictly on a "detect-document-deter-deconflict-escalate" framework. By deploying an integrated, multi-sensor set of passive RF detection, radar, and FAA-compliant patrol drones, ports can establish highly effective domain awareness and evidence collection without violating federal airspace

or communications statutes.

The governance structure supporting the sensor array is just as critical as the physical architecture. Ports must align their procurement with trusted supply-chain requirements, avoiding prohibited technologies while implementing strict NIST-derived cybersecurity controls. Furthermore, adopting definitive standard operating procedures and privacy policies is essential to manage legal liability and state-level image capture restrictions. Ultimately, a legally defensible program relies on lawful observation, disciplined evidence preservation, and pre-negotiated escalation pathways with SAFER SKIES-certified law enforcement. As federal regulations continue to evolve, ports that establish these foundational compliance and detection layers today will be uniquely positioned to integrate active mitigation capabilities if and when the law permits.

APPENDIX A: Examples of Currently Legal Equipment by Function

Core UAV Patrol Platforms

Product: Parrot ANAFI USA



Manufacturer / model:	Parrot ANAFI USA
Why it fits port security:	Lightweight thermal / visual patrol, law-enforcement style rapid deployment
Key cited capabilities:	3 × 32-min batteries per pack; optional AES-256 encrypted Microhard radio pack
Blue / Green / NDAA posture:	U.S.-made; Blue status not asserted on cited page
Approximate cost:	About $7,000 via authorized reseller
Deployable by private Texas port today?	Yes
Typical procurement source:	Parrot direct or authorized reseller

Layer: Portable thermal UAV

Product: Ascent AeroSystems Spirit



Manufacturer / model:	Ascent AeroSystems Spirit
Why it fits port security:	High wind tolerance, compact coaxial form factor for industrial sites
Key cited capabilities:	Up to 58 min dual-battery no-payload, >60 mph, modular payload design
Blue / Green / NDAA posture:	Green UAS listed; Blue history noted by vendor
Approximate cost:	Quote-only
Deployable by private Texas port today?	Yes
Typical procurement source:	Manufacturer / integrator

Layer: Rugged compact UAV

Product: Freefly Astro Max



Manufacturer / model:	Freefly Astro Max
Why it fits port security:	Secure mapping/inspection/security base platform for public-sector procurement
Key cited capabilities:	From $28,995; DIU Approved / NDAA-Blue on cited store page
Blue / Green / NDAA posture:	NDAA / Blue stated
Approximate cost:	From $28,995
Deployable by private Texas port today?	Yes
Typical procurement source:	Freefly direct

Layer: Trusted industrial UAV

Product: Skydio X10



Manufacturer / model:	Skydio X10
Why it fits port security:	Fast-response security patrol, incident overwatch, dock or vehicle launch
Key cited capabilities:	45 mph, 40 min max flight time, under 40-sec deployment, IP55
Blue / Green / NDAA posture:	Vendor civil page does not state Blue status; verify in procurement
Approximate cost:	Quote-only
Deployable by private Texas port today?	Yes, under FAA rules
Typical procurement source:	Direct from manufacturer

Layer: Patrol UAV

Product: Inspired Flight IF800 Tomcat



Manufacturer / model:	Inspired Flight IF800 Tomcat
Why it fits port security:	Longer endurance and payload flexibility for ports needing heavier sensors
Key cited capabilities:	Max 54-min flight time; hot-swappable dual batteries
Blue / Green / NDAA posture:	NDAA / Green posture should be verified at purchase; Green list includes IF800 Tomcat
Approximate cost:	Quote-only
Deployable by private Texas port today?	Yes
Typical procurement source:	Inspired Flight direct or integrator

Layer: Medium-lift secure UAV

Product: Hoverfly Spectre



Manufacturer / model:	Hoverfly Spectre
Why it fits port security:	Tethered 24/7 fixed-site surveillance and network extension over gates or tank farms
Key cited capabilities:	Unlimited flight time; multi-payload; purpose-built for radios; Blue and Green listed
Blue / Green / NDAA posture:	Blue / Green stated
Approximate cost:	Quote-only
Deployable by private Texas port today?	Yes
Typical procurement source:	Direct from manufacturer

Layer: Persistent overwatch / comms

Detection Systems

Product: Echodyne EchoShield (Longer-range radar)



Manufacturer / model:	Echodyne EchoShield
Why it fits port security:	Medium-range, all-weather 4D tracking for channel and perimeter approaches
Key cited capabilities:	• 4D radar, low SWaP, high angular accuracy, 10 Hz data rate
Blue / Green / NDAA posture:	Conventional sensor procurement
Approximate cost:	Quote-only
Deployable by private Texas port today?:	Yes
Typical procurement source:	Direct / integrator

Layer: Longer-range radar

Product: Dedrone RF-360



Manufacturer / model:	Dedrone RF-360
Why it fits port security:	Detects and geolocates drone and remote-control RF emissions without jamming
Key cited capabilities:	Passive network-attached RF detection, classification, geolocation
Blue / Green / NDAA posture:	Security vendor system; supply-chain review required
Approximate cost:	Quote-only
Deployable by private Texas port today?	Usually yes if configured as passive detection; legal review required by function
Typical procurement source:	Direct / integrator

Layer: Passive RF detection

Product: Robin IRIS



Manufacturer / model:	Robin IRIS
Why it fits port security:	360°, 3D drone detection in clutter; strong early warning layer
Key cited capabilities:	360° coverage, micro-doppler classification, DNN-based discrimination
Blue / Green / NDAA posture:	Vendor not marketed as Blue/Green UAV; conventional sensor procurement
Approximate cost:	Quote-only
Deployable by private Texas port today?	Yes
Typical procurement source:	Direct / integrator

Layer: Drone radar

Connectivity Payloads

Product: Elsight Halo



Manufacturer / model	Elsight Halo
Why it fits port security	Multi-link beyond-line-of-sight connectivity for remote operations
Key cited capabilities	Multi-network secure connectivity for BVLOS; Blue UAS list milestone announced April 2026
Blue / Green / NDAA posture	Blue UAS stated in April 2026 announcement
Approximate cost	Quote-only
Deployable by private Texas port today?	Yes
Typical procurement source:	Direct / integrator

Layer: BVLOS connectivity

Product: Silvus StreamCaster 4200EP



Manufacturer / model:	Silvus StreamCaster 4200EP
Why it fits port security:	Resilient encrypted wireless backhaul for docks, mobile teams, and remote ops
Key cited capabilities:	2×2 MIMO; Blue UAS Framework Certified; NDAA and DoD cyber compliant
Blue / Green / NDAA posture:	Blue / NDAA stated
Approximate cost:	Quote-only
Deployable by private Texas port today?:	Yes
Typical procurement source:	Direct / public-safety integrator

Layer: Secure MANET comms

Mapping Payloads

Product: Sentera 65R (RGB mapping payload)



Manufacturer / model:	Sentera 65R
Why it fits port security:	High-detail visual evidence, orthomosaics, damage documentation
Key cited capabilities:	• 65 MP global shutter; ~3 fps; • sub-centimeter GSD depending altitude
Blue / Green / NDAA posture:	Sensor vendor; verify supply-chain reps
Approximate cost:	About $11,950 via reseller
Deployable by private Texas port today?:	Yes
Typical procurement source:	Sentera / authorized reseller

Layer: RGB mapping payload

Product: Freefly Flux L1 (LiDAR payload)



Manufacturer / model:	Freefly Flux L1
Why it fits port security:	Scene reconstruction, standoff modeling, powerline / hard-geometry capture
Key cited capabilities:	• $13,995; 450 m range; 6 channels; • triple returns; ±5 cm accuracy
Blue / Green / NDAA posture:	Mounted on trusted platform; subcomponent origin should be reviewed
Approximate cost:	$13,995
Deployable by private Texas port today?:	Yes
Typical procurement source:	Freefly direct

Layer: Freefly Flux L1 (LiDAR payload)

Product: GeoCue TrueView 535



Manufacturer / model	GeoCue TrueView 535
Why it fits port security	More advanced 3D imaging for port asset baselines and post-incident mapping
Key cited capabilities	LiDAR with 3 cameras; dual drone / optional mobile mapping
Blue / Green / NDAA posture	Sensor procurement; verify origin of all subcomponents
Approximate cost	Quote-only / subscription-based pricing model
Deployable by private Texas port today?	Yes
Typical procurement source	GeoCue / integrator

Layer: Survey-grade LiDAR

END NOTES

[1] 6 U.S.C. § 124n. Protection of certain facilities and assets from unmanned aircraft; as amended by Pub. L. 119-60. Retrieved from https://uscode.house.gov/view.xhtml?req=%28title%3A6+section%3A124n+edition%3Aprelim%29" \h

[2] Federal Aviation Administration. (2024). Pilot's handbook of aeronautical knowledge (FAA-H-8083-25C). U.S. Department of Transportation. (Specifically see Chapter 15: Airspace).

[3] See, e.g., Wiretap Act, 18 U.S.C. § 2511 (prohibiting the intentional interception of wire, oral, or electronic communications); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (governing unauthorized access to protected computers and digital control links).

[4] Communications Act of 1934, as amended, 47 U.S.C. § 151 et seq.; see also Federal Communications Commission. (2012). Enforcement advisory: Anti-jammer enforcement. Enforcement Bureau. https://www.fcc.gov/document/enforcement-advisory-anti-jammer-enforcement

[5] U.S. Department of Homeland Security, DOJ, FAA, and FCC. (2025). Interagency legal advisory on UAS detection and mitigation technologies. Retrieved from https://docs.fcc.gov/public/attachments/doc-366222a1.pdf

[6] U.S. Congress. 18 U.S.C. § 32. Destruction of aircraft or aircraft facilities. Retrieved from https://uscode.house.gov/view.xhtml?req=%28title%3A18+section%3A32+edition%3Aprelim%29

[7] U.S. Congress. 47 U.S.C. § 333. Willful or malicious interference. Retrieved from https://uscode.house.gov/view.xhtml?req=%28title%3A47+section%3A333+edition%3Aprelim%29

[8] Federal Aviation Administration. (n.d.). 14 CFR Part 107—Small unmanned aircraft systems. Electronic Code of Federal Regulations. Retrieved May 26, 2026, from https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107

[9] The SAFER SKIES Act was enacted in the FY2026 NDAA and codified through amendments to 6 U.S.C. § 124n.

[10] U.S. Congress, House. (2025). Safer Skies Act of 2025, S.B. 3481, 119th Cong. U.S. Government Publishing Office. https://www.congress.gov/bill/119th-congress/senate-bill/3481/text/is

[11] Federal Aviation Administration, Designation—Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility, 91 Fed. Reg. 19148 (May 6, 2026). https://www.federalregister.gov/documents/2026/05/06/2026-08943/designation-restrict-the-operation-of-unmanned-aircraft-in-close-proximity-to-a-fixed-site-facility

[12] 33 C.F.R. Part 105 - Maritime Security: Facilities. Retrieved from https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105

[13] Texas Department of Information Resources. (2026). Covered applications and prohibited technologies. Retrieved from https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies

[14] "Blue" and "Green" status in the equipment table reflects only what is stated in the cited source for that model or product class; procurement counsel should still document origin, subcomponents, cloud dependencies, and firmware provenance. (https://www.diu.mil/blue-uas-cleared-list)

[15] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. Retrieved from https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

[16] National Institute of Standards and Technology. (2020; upd. 2025). SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[17] Federal Aviation Administration. (2026). Public safety toolkit and Handling sightings and reports. Retrieved from https://www.faa.gov/uas/public_safety_gov

[18] Federal Aviation Administration. (2025, March 19). Remote identification of drones. Retrieved from https://www.faa.gov/uas/getting_started/remote_id

[19] Federal Aviation Administration. (2024, March 15). FAA ends discretionary enforcement policy on drone remote identification. Retrieved from https://www.faa.gov/newsroom/faa-ends-discretionary-enforcement-policy-drone-remote-identification

[20] Brennan / RaceDayQuads Remote ID litigation, D.C. Circuit opinion discussing FAA Remote ID privacy protections. Retrieved from https://media.cadc.uscourts.gov/opinions/docs/2022/07/21-1087-1956978.pdf

[21] Federal Aviation Administration & Transportation Security Administration. (2025, August 7). Normalizing unmanned aircraft systems beyond visual line of sight operations (proposed rule). Federal Register. Retrieved from https://www.federalregister.gov/documents/2025/08/07/2025-14992/normalizing-unmanned-aircraft-systems-beyond-visual-line-of-sight-operations

[22] Federal Aviation Administration & Transportation Security Administration. (2026, January 28). Normalizing unmanned aircraft systems beyond visual line of sight operations; reopening of comment period. Federal Register. Retrieved from

[23] Cybersecurity and Infrastructure Security Agency. (2025–2026). Be Air Aware resources, including guidance for protecting critical infrastructure and public gatherings, UAS detection technology guidance, suspicious UAS activity guidance, and UAS cybersecurity. Retrieved from https://www.cisa.gov/topics/physical-security/be-air-aware/protect-critical-infrastructure-and-public-gatherings

[24] Tex. Gov't Code § 423.0045 (2026). Offense: Operation of unmanned aircraft over correctional facility, detention facility, or critical infrastructure facility. Texas Constitution and Statutes. https://statutes.capitol.texas.gov/?tab=1&code=GV&chapter=GV.423&artSec=423.0045

[25] 14 C.F.R. § 107.9. Retrieved from https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107/subpart-A/section-107.9

[26] Office of the Texas Governor. (2026, January 26). Governor Abbott updates Texas' prohibited technologies list. https://gov.texas.gov/news/post/governor-abbott-updates-texas-prohibited-technologies-list

[27] Tex. Penal Code § 22.05 (2026). Deadly conduct. Texas Constitution and Statutes. https://statutes.capitol.texas.gov/?tab=1&code=PE&chapter=PE.22&artSec=22.05

[28] Tex. Penal Code § 28.09 (2026). Damaging critical infrastructure facility. Texas Constitution and Statutes. https://statutes.capitol.texas.gov/Docs/PE/htm/PE.28.htm#28.09

[29] Tex. Penal Code § 31.01 (2026). Definitions. Texas Constitution and Statutes. https://statutes.capitol.texas.gov/GetStatute.aspx?Code=PE&Value=31.01

[30] Singer v. City of Newton, 284 F. Supp. 3d 125 (D. Mass. 2017). https://www.govinfo.gov/app/details/USCOURTS-mad-1_17-cv-10071

[31] Long Lake Township v. Maxon, 546 Mich. 65, 11 N.W.3d 123 (Mich. 2024). https://law.justia.com/cases/michigan/supreme-court/2024/164948-0.html

[32] Federal Aviation Administration. (2024, August 23). FAA proposed $341,413 in civil penalties against drone operators. U.S. Department of Transportation. https://www.faa.gov/newsroom/faa-proposed-341413-civil-penalties-against-drone-operators

[33] FAA Reauthorization Act of 2024, Pub. L. No. 118-63, 138 Stat. 1025 (2024). https://www.govinfo.gov/app/details/PLAW-118publ63

[34] Federal Aviation Administration. (2026, April 16). FAA launches new program to accelerate enforcement of drone violations. Retrieved from https://www.faa.gov/newsroom/faa-launches-new-program-accelerate-enforcement-drone-violations

[35] Seidaliyeva, U., Ilipbayeva, L., Taissariyeva, K., Smailov, N., & Matson, E. T. (2024). Advances and challenges in drone detection and classification techniques: A state-of-the-art review. Sensors, 24(1), Article 125. https://doi.org/10.3390/s24010125

[36] National Institute of Standards and Technology. (2024). Autonomous aerial drones connecting public safety: Opportunities and challenges for future public safety communications. Retrieved from https://www.nist.gov/publications/autonomous-aerial-drones-connecting-public-safety-opportunities-and-challenges-future

[37] Droneshield DroneGun Mk4 https://www.droneshield.com/products-dismounted

[38] 33 C.F.R. § 105.205. Retrieved from https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105/subpart-B/section-105.205

[39] Federal Aviation Administration. Report UAS Sighting. Retrieved from https://www.faa.gov/uas/contact_us/report_uas_sighting

[40] 14 C.F.R. § 107.9. Retrieved from https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107/subpart-A/section-107.9

[41] National Press Photographers Association v. McCraw, No. 22-50337 (5th Cir. Jan. 10, 2024). Justia. https://cases.justia.com/federal/appellate-courts/ca5/22-50337/22-50337-2024-01-10.pdf?ts=1704911441

AUTHOR BIOGRAPHIES

Dr. Art Wolfskill, Ph.D., is a Professor of Agribusiness at Sam Houston State University, where he specializes in finance, entrepreneurship, and the integration of unmanned aerial systems (UAS) within critical infrastructure and primary industries. A leading expert in aerial applications, he teaches Drone Applications in Agriculture and Industry, focusing on the dual-use nature of UAS technology for both economic efficiency and site security.

Dr. Wolfskill brings over eight years of experience flying drones, with FAA TRUST and Part 107 certifications, as well as a portfolio built upon a distinguished career as a U.S. Army helicopter pilot. During his military service, he was assigned to Air Cavalry units, where he developed a foundational understanding of aerial reconnaissance, threat detection, and airspace management in high-stakes environments.

His current research for the Institute for Homeland Security leverages this unique blend of tactical military aviation and academic rigor to address emerging vulnerabilities in maritime and industrial sectors. By combining operational experience with strategic policy analysis, Dr. Wolfskill provides actionable insights into defending Texas' ports and critical infrastructure against the evolving threat of drone incursions.

Michael A. Wolfskill is an independent researcher and operations specialist with over a decade of experience leading international, high-pressure teams in Latin America. A graduate of Sam Houston State University with a degree in Mass Communications, Michael has built a career at the intersection of technical infrastructure and strategic management. He possesses extensive experience in operations, sales, and marketing management, specializing in scaling complex operations, designing customer acquisition initiatives, and navigating the needs of cross-functional stakeholders.

As a technologist and drone enthusiast, Michael focuses his research on the evolving role of Unmanned Aerial Systems (UAS), matching their technological potential with modern-day use cases and practice. By leveraging his professional background in

technology and global operations, he provides a unique perspective on the critical balance between national security, economic resilience, and civil liberties in the age of autonomous systems.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

© 2026 The Sam Houston State University Institute for Homeland Security.

Wolfskill, A & Wolfskill, M. (2026). A Lawful Drone Security Framework for Private Texas Port Operators. (Report No. 2026 - 1038). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/AUTNS

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY