

DRONE SECURITY

Integrating Drones into Physical Security Programs and Mitigating Unauthorized Drone Threats

A White Paper

Prepared by:

Michelle L. Chace, MSSM
Mitigation Assessor, LLC

November 2026

www.mitigationassessor.com
mchace@mitigationassessor.com
402-312-7955

© 2026 Mitigation Assessor, LLC
All rights reserved.

For security directors and operating executives responsible for privately operated distribution centers. U.S. regulatory scope. See the disclaimer and status notes in this paper.

Executive summary

A distribution center needs a workable response for the interval between a suspicious drone sighting and the arrival of authorized responders. Staff must know when to protect people, whom to notify, and what evidence to preserve. Since July 1, 2026, a federal framework has enabled qualifying state, local, Tribal, and territorial agencies to exercise counter-drone powers subject to accreditation, personnel certification, and operational requirements. It does not authorize ordinary private property owners or security contractors to conduct active mitigation. [1]

An authorized drone can provide a useful perspective during alarm verification, perimeter assessment, emergency support, and post-incident documentation. Its value depends on whether that perspective improves a specific decision. Weather, obstructions, staffing, battery endurance, airspace limitations, and privacy obligations can restrict availability. Ground personnel and fixed systems must remain capable when the aircraft cannot fly.

The first investment should be a fixed-scope drone security readiness assessment. It should identify exposed operations, evaluate whether an authorized security drone would improve decisions, establish response and evidence procedures, and compare passive protection with detection equipment. Design follows assessment; a limited pilot proceeds only when the business case, lawful operating concept, and response arrangements are approved.

Detection alone does not establish hostile intent or authority to interfere with an aircraft. For private distribution centers, the practical priority is to protect people and operations while supplying reliable information to the appropriate agency. Table 5 assigns approval roles, proposed budget sources, and target dates for that work.

Who this paper is for

The primary reader is the security director responsible for a privately operated U.S. distribution center with an outdoor truck yard, perimeter alarms, and continuous operations. The chief operating officer owns the business outcome; the chief financial officer or delegated budget holder approves spending. The site general manager owns local execution, supported by facilities management, legal counsel, procurement, and IT. These are recommended roles and may be mapped to equivalent positions.

Recommended first step: the security director should submit a fixed-scope assessment request to the COO and budget holder. The request should identify one site, deliverables, a fee ceiling, and a completion date. Later readers can use a ten-business-day approval target from the date they adopt this plan.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Contents

Executive summary 2
1 Define the mission before selecting equipment 4
2 Use drones as part of the security program 6
3 Establish the legal and governance foundation 6
4 Understand drone threats without assuming intent 7
5 Select detection capabilities against site conditions 9
6 Mitigate risk and evaluate interceptor drones separately 10
7 Adopt a practical incident response framework 11
8 Implement in phases and measure results 13
Readiness checklist 16
Appendix A Drone security governance 17
Table of Figures 21
References 21
About the author 25
Professional Review 25
Disclaimer 25

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

1 Define the mission before selecting equipment

For the distribution center security director, the initial workflow is a perimeter or truckyard alarm followed by verification, dispatch, and a decision about protecting people or interrupting operations. Determine where aerial observation would change that decision and where a fixed camera, lighting improvement, or patrol adjustment would work better. The COO should define acceptable operational disruption before equipment is selected.

Other settings can use the same assessment method with different priorities. A campus may focus on hazardous-area observation and privacy. An event venue may prioritize exposed queues and public-safety coordination. Neither should adopt a distribution center operating concept without adjusting authority, staffing, and response triggers.

Assess assets, exposure, existing controls, previous incidents, surrounding land uses, nearby aviation activity, and the consequences of both a missed threat and an unnecessary response. Include rooftops, courtyards, outdoor queues, loading areas, and other spaces that ground-level cameras may not fully observe. Assess what the organization can actually do with additional information, including available staffing and authority.

Use scenario-based judgments when reliable local incident data is unavailable. Distinguish demonstrated incidents from plausible scenarios, and record uncertainty. This paper does not claim a national drone attack frequency or a universal financial return.

A documented case illustrates the potential consequence. In November 2024, DOJ announced charges against Skyler Philippi over a disrupted plan to attack a Nashville-area electrical substation using a drone. DOJ subsequently reported his guilty plea on September 9, 2025. This is evidence of a specific attempted attack and law-enforcement disruption, not a completed destructive drone strike or a measure of national attack frequency. It does not establish the likelihood of an attack at a particular distribution center. [2, 3]

Function	Purpose	Key distinction
Security drone operations	Use an authorized aircraft to support a defined security mission.	Flight authorization and site permission must both be addressed.
Drone detection and assessment	Observe, locate, track, and evaluate aircraft activity.	A sensor alert does not establish intent.
Protective mitigation	Reduce exposure and manage consequences.	May include sheltering, operational changes, and site design.
Active counter-UAS intervention	Disrupt, capture, disable, or otherwise interfere with an aircraft.	Requires specific legal authority and operational safeguards.

Figure 1 - Drone security program functions

Structured threat vulnerability and consequence assessment

Use a scenario register to connect each drone-related concern to an exposed asset, existing controls, and a defined adverse outcome. DHS risk terminology distinguishes threat, vulnerability,

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

and consequences. [30] The following method is a proposed application for this paper, rather than a prescribed DHS scoring system. For each scenario, record the location, operating period, people or processes exposed, supporting evidence, assessor, and review date.

Assess threat using relevant incident history, credible reporting, adversary capability and intent where supported, and the opportunity for the event to occur. Assess vulnerability by testing how existing physical protection, detection, staffing, and response arrangements could fail in that scenario. Assess consequences separately for injury, operational downtime, financial loss, and other material impacts. Define the baseline explicitly as current controls; estimate residual risk after the proposed measures. Record assumptions and confidence for each input.

Where defensible estimates exist, calculate expected annual loss as event frequency per year × probability of the defined harmful outcome given an event × average monetary consequence of that outcome. Frequency describes the scenario, not every drone sighting. The conditional probability represents vulnerability under the stated controls. Use consistent units and avoid counting the same event or loss in multiple scenarios. Retain life-safety and other nonmonetized consequences alongside the calculation.

For illustration only, assume 0.2 relevant events per year, a 0.40 probability of a disruptive outcome given an event, and a $250,000 loss per disruptive outcome. Baseline's expected annual loss is $20,000. If tested controls support reducing the conditional probability to 0.15 while other assumptions remain unchanged, residual expected annual loss is $7,500 and modeled annual risk reduction is $12,500. These hypothetical inputs are not drone incident rates, vendor performance claims, or a forecast for any facility.

When evidence cannot support probabilities, use a documented qualitative or semi-quantitative rubric with anchored categories for threat, vulnerability, and consequence. Record the three ratings separately and apply a management-approved priority matrix; multiplying ordinal scores does not produce a probability or dollar loss. Test low, central, and high assumptions and show whether the preferred countermeasure changes. The COO should accept remaining exposure explicitly, with a responsible owner and review date. Reassess after incidents, exercises, operating changes, or new credible threat information.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

2 Use drones as part of the security program

Figure 2 compares potential security missions with the limitations that the site must resolve before approving flight operations.

Use case	Potential value	Operational limitation
Alarm verification	Provide a timely view of a remote alarm location.	Launch delays, weather, and visual obstructions may prevent useful imagery.
Perimeter and property assessment	Inspect fences, roofs, and outdoor areas from additional viewpoints.	Aerial observation does not physically secure a breach.
Emergency support	Help incident command assess access routes and hazardous areas.	Deconflict with emergency aviation and responder activity.
Event support	Observe selected exterior conditions and access routes.	Crowds, privacy, and flight-over-people requirements constrain use.
Post-incident documentation	Record conditions for later review and investigation.	Preserve original files, timing, and evidence handling records.

Figure 2 - Security drone use cases

Integrate the drone feed with the security operations center and the existing incident record. Identify who requests a flight, who authorizes the mission, who pilots the aircraft, and who directs the ground response. The remote pilot must retain authority to delay, change, or stop a flight when safety or flight requirements demand it. Assign image interpretation and dispatch to another person when workload warrants.

Document launch and recovery locations, communications, flight boundaries, weather limits, minimum battery reserves, lost-link actions, emergency landing areas, and maintenance checks. Test these arrangements under realistic site conditions. A docking station or automated flight plan should be evaluated as a complete operating system, including supervision, communications, maintenance, and fallback procedures.

Do not claim that thermal imaging reliably identifies a person or sees through walls. Treat imagery as contextual information that may require confirmation. Similarly, a drone can help verify activity without guaranteeing identification, prevention, or uninterrupted coverage.

3 Establish the legal and governance foundation

For many private-sector small-drone missions, FAA Part 107 is the relevant operating framework. FAA guidance addresses remote pilot certification, aircraft registration, and operational limitations. Night flights and flights over people or moving vehicles may be permitted when their applicable requirements are satisfied; these are not blanket permissions. Controlled airspace authorization remains a separate consideration. [4]

Visual-line-of-sight requirements must be incorporated into the operating concept. A camera feed or automated dock does not authorize beyond-visual-line-of-sight (BVLOS) flight. The proposed

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Part 108 rule was published August 7, 2025, at 90 FR 38212. The OIRA record reviewed for this revision lists the final rule as pending review, received July 10, 2026; it is not a basis for current operating permission. Use an applicable Part 107 waiver, a section 44807 exemption with any other required approvals, or another valid FAA authorization. [5, 6]

Remote ID is an identification and location broadcast requirement for covered operations, subject to applicable exceptions and authorizations. Standard Remote ID and broadcast modules provide different location information: standard systems include control-station information, while modules include takeoff-location information. A received broadcast is useful context, not proof of a pilot's identity, site permission, or benign intent. Failure to receive a broadcast is not, alone, proof of criminal activity. [7]

The 2020 interagency advisory identifies laws that drone detection and mitigation systems may implicate. Review the actual collection and intervention functions rather than relying on vendor assurances. Read older federal-only authority summaries alongside the SAFER SKIES Act, enacted in Pub. L. 119-60, division H, title LXXXVI, on December 18, 2025, and its implementing rule. [8, 9]

The rule at 6 CFR and 28 CFR Part 124 establishes Detection and Warning certification (Tier 1) for authorized detection, identification, tracking, and warning. Mitigation certification (Tier 2) covers authorized disruption, seizure or control, and other permitted intervention, and requires approved hands-on training through the FBI National Counter-UAS Training Center. Verify the responding agency's accreditation, operators' certification, equipment, and operating approvals. Under this SLTT framework, contractors cannot operate mitigation systems or make credible-threat determinations, including through managed services. Contractors may support installation, maintenance, training, and detection that does not require special statutory authority. The SLTT authority terminates December 31, 2031, absent extension. [1, 9]

This paper addresses ordinary private facilities. Specialized federal-authority arrangements and the statute's definition of correctional agency require separate review; they do not provide an ordinary distribution center with counter-drone powers. Property ownership, signs, and an agreement with police do not confer those powers. [9]

Before procurement, obtain a written review of intended collection, flight activity, communications effects, intervention functions, and applicable state and local requirements. Property ownership or a no-drone sign should not be treated as sufficient authority to disable an aircraft. Keep the ordinary private-security response centered on protective measures and authorized agency coordination. [8, 9]

Adopt policies governing approved purposes, prohibited uses, access to recordings, retention, disclosure, and complaints. Limit unnecessary recording of neighboring residences and unrelated activity. Define incident preservation and legal-hold exceptions to routine deletion. Review vendor data handling, remote access, security updates, account protection, and the ability to export or delete organizational records. CISA provides drone privacy and data-protection guidance supporting this governance work. [10]

4 Understand drone threats without assuming intent

An unfamiliar drone may be a permitted contractor flight, a lawful nearby operation, a careless flight, deliberate surveillance, contraband delivery, or a more serious threat. The appropriate

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

response depends on observed conduct, proximity, persistence, credible threat information, and potential consequences. Staff should record what they saw separately from what they infer.

Maintain an authorized flight register for the organization and its contractors, including mission time, contact, aircraft description, and operating area. This is an internal coordination control; it does not establish authority over all surrounding airspace. Share relevant flight details with the monitoring team so the organization's own aircraft do not create avoidable alarms.

Maintain a second register for unauthorized or unexplained sightings. Record date and time with time zone, location, direction or track, estimated altitude and its basis, duration, observed conduct, source, confidence, and actions taken. Record unavailable fields as unknown. A site's lack of permission does not necessarily mean that a nearby flight is unlawful. Retain links to original imagery and sensor records under the approved retention policy.

The security supervisor should review this register monthly for repeated times, routes, or attention to particular assets and escalate supported concerns. Patterns can help distinguish isolated activity from conduct warranting investigation; they do not prove surveillance or intent. Log completeness should be a standing performance measure.

The records may also support an eligible site's future application under the proposed FAA Part 74 fixed-site flight-restriction process. The May 6, 2026, proposal asks applicants to demonstrate a need for protection and document relevant security measures and vulnerabilities. It remains a proposal in the sources reviewed, not an available approval or a grant of counter-drone authority. [11]

Assess scenarios such as repeated observation of sensitive outdoor activity, interference with emergency operations, unexpected landing or object release, and flight near exposed gatherings. Evaluate each against existing protective measures. Avoid assuming that the most dramatic scenario is the most likely or that every sighting requires evacuation.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

5 Select detection capabilities against site conditions

Detection, tracking, classification, and identification are different functions. Specify the decision each must support. Sensor placement, installation, and response actions must be coordinated to avoid unintended aviation impacts. The FAA cautions that detection does not determine intent or threat level; airport-specific obligations should not automatically be applied to an ordinary distribution center. [12]

Table 3 separates how sensors collect information from the legal review they require. Radar uses RF energy but ordinarily does not intercept drone communications. “Non-RF” is therefore an inaccurate label for a group that includes radar. A design that avoids communications interception can simplify one part of legal review while retaining spectrum, privacy, installation, and data-handling obligations. [8]

Capability	Contribution and limitation	Legal review category
Remote ID receiver	Broadcast context; incomplete coverage and no proof of site permission.	Public broadcast reception. Review configuration and data use; not equivalent to intercepting control traffic.
RF communicati ons detection	Detects supported signals and protocols; may miss unsupported or absent transmissions.	Potential communications interception or signaling collection; assess 18 U.S.C. 2511 and 3121 in writing.
Radar	Tracks reflect energy; clutter, birds, and structures affect results.	Non-communications sensing, but an RF transmitter. Review spectrum, equipment, and sitting requirements.
Optical and infrared	Supports visual assessment; resolution, weather, and obstructions limit results.	Non-communications imaging. Review privacy, surveillance, retention, and placement.
Acoustic	Sound-based cue; performance varies with background noise.	Ordinary signature sensing is not drone-link interception; assess incidental speech recording and audio privacy.
Combined sensors	Corroborates alerts; integration and operator workload still matter.	Review every sensor and enabled function. A lawful component does not establish system-wide legality.

Figure 3 - Detection capabilities and legal review

The table is a planning comparison, not a performance rating or legal approval. Require a lawful, site-specific acceptance demonstration using representative aircraft, locations, weather, and operating periods. Record both misses and false alerts. Test the ability to distinguish authorized site flights and to export a useful incident record. Reject proposals that substitute maximum advertised range for demonstrated usable coverage.

Integrated detection and AI supported decision making

An integrated architecture should connect legally reviewed sensors to a common operating picture and the site response workflow. A proposed arrangement combines radar tracks, permitted RF or Remote ID observations, fixed optical and thermal cameras, and an authorized security-drone feed

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

when available. Video management, access control, perimeter alarms, the authorized-flight register, and dispatch records add ground context. Evaluate each interface and collection function under Section 3 before deployment.

Correlate observations by time, location, and track history; retain the source, confidence, and data age. A radar cue may direct a camera toward an object, while a perimeter alarm helps an operator assess related ground activity. Show conflicting reports, blind areas, stale tracks, and sensor health. Multiple alerts derived from one source should not be treated as independent confirmation. Common power, network, or software failures may disable several sensors at once; test these dependencies and the manual fallback.

AI tools may assist object classification, track association, anomaly detection, and alert prioritization. Assess their value against the existing operator workflow using representative site conditions. NIST's voluntary AI Risk Management Framework supports defined human oversight, testing, and ongoing monitoring. [31] Display the underlying observations and uncertainty so an operator can challenge a recommendation. An AI confidence score should not be represented as the probability of hostile intent unless that interpretation has been independently validated for the intended use.

The monitoring operator should verify alerts, the supervisor should assess protective actions, and the incident commander should coordinate response under existing procedures. AI output does not supply legal authority or replace an authorized agency's required threat determination. Preserve the model version, alert evidence, operator decision, and resulting action in the incident record. Require human approval for consequential response decisions and a means to override or disable automation.

Before acceptance and after material model or configuration changes, evaluate missed detections, false alerts, classification errors, processing delay, and operator workload across day, night, weather, clutter, and representative aircraft conditions. Use evaluation data separate from training data and record sample sizes. Monitor performance deterioration and maintain access to raw observations when automated analysis is unavailable. Integration is successful when it improves timely, supported decisions and coordinated action under these conditions.

6 Mitigate risk and evaluate interceptor drones separately

Protective mitigation reduces the opportunity for harm or its consequences. Potential measures include moving sensitive activities indoors, improving overhead protection where engineering review supports it, managing outdoor queues, securing access to roofs and sensitive equipment, and preparing shelter or relocation options. Evaluate structural loading, fire access, emergency egress, and maintenance before changing the physical environment.

Passive physical protection can provide continuous benefit without a dedicated flight operator or dependence on a detection alert. Suitable structures and site modifications can often be installed by qualified local contractors. They avoid the intentional radio interference and airborne interception hazards of active countermeasures. They are not liability-free: engineering, permits, obstruction limits, emergency access, inspection, and maintenance still apply. Compare lifecycle costs and the exposure actually reduced before selecting either construction or electronics.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Security personnel should have predefined triggers for notifying supervisors, restricting a localized area, pausing exposed work, or requesting emergency assistance. A blanket instruction to evacuate can move people into a more exposed location. The incident commander should select sheltering, relocation, or evacuation based on the observed hazard and the site's emergency plan.

"Mitigation drones" may describe aircraft used to observe a threat or interceptor aircraft intended to capture or disable another drone. These functions must be separated in policy and procurement. Observation remains subject to flight safety and operating requirements. Interception adds collision, falling-debris, loss-of-control, and legal risks. An organization's ability to fly a security drone does not establish authority to use it as an interceptor. [8]

Private security teams should not improvise pursuit, capture, jamming, spoofing, takeover, or destruction. Any proposed active intervention should proceed only after authority is specifically established and the responsible, authorized organization approves its use. The site response plan should identify how staff will support that organization, protect people, and preserve information without independently escalating the airspace hazard.

Before an incident, the security director should seek a written response agreement or documented coordination protocol with the nearest suitably accredited agency that has Mitigation-certified personnel and jurisdiction to assist. The closest police department may need a regional mutual-aid partner. Confirm capability directly; this paper does not assert how many agencies currently qualify. Record contact numbers, hours, request routing, access arrangements, evidence delivery, expected limitations, and who controls the site response. An agreement cannot guarantee dispatch or authorize a specific interception. [1]

Exercise the notification and evidence-transfer path at least annually and after material personnel or system changes. If no capable partner is available or willing to sign, document the gap, maintain ordinary emergency reporting, and strengthen protective measures rather than implying that intervention coverage exists.

7 Adopt a practical incident response framework

Table 4 assigns the immediate response tasks. The incident commander should use observed conditions and the site emergency plan to determine protective actions.

Stage	Required action	Accountability
Observe and report	Record time, location, direction, duration, description, and observed behavior.	Reporting employee or monitoring operator
Validate	Check authorized flights and corroborating observations; mark uncertainty.	Security operations center
Assess	Consider proximity to people, operational interference, and credible threat indicators.	Security supervisor / incident commander
Protect and coordinate	Apply proportionate site measures; contact emergency services for immediate danger.	Incident commander
Preserve	Retain original imagery, sensor records, dispatch logs, and witness accounts.	Designated evidence custodian

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Recover and review	Document the basis for resuming operations and corrective actions.	Security management

Figure 4 - Incident response responsibilities

For a downed drone or unexplained dropped object, keep people away and notify appropriate responders. Do not direct untrained personnel to approach, move, power on, connect to, or inspect the device. Preserve the scene and observations from a safe location. Treat possible hazardous payloads and damaged batteries through established emergency procedures.

Prepare a standard evidence package containing time-synchronized sensor tracks, available Remote ID records, original imagery, witness accounts, an incident chronology, and an estimated launch area when supported. Identify the source, confidence, and clock offset for each item. Distinguish a module's reported takeoff location from a standard Remote ID control-station location; neither independently proves where a person is now. [7]

Preserve originals and metadata, document exports and transfers, and give responders an index of files and a site contact. An illustrative readiness objective is to provide an initial track history and supported location estimate within minutes, rather than relying solely on a guard's recollection. Measure the actual time during exercises; do not promise a response time the site has not demonstrated.

Synchronize system clocks where practicable and record any known time offsets. Preserve original records, document exports and transfers, and separate observations from conclusions. Review whether a sensor failure, incomplete imagery, or uncertainty about the aircraft affected the response. Keep external communications factual and protect personal information.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

8 Implement in phases and measure results

Figure 5 proposes a schedule for a single-site assessment authorized by October 30, 2026. Dates are planning targets, not provider commitments or regulatory deadlines. Legal authorization and agency availability control whether later phases can proceed. Finance should confirm expense versus capital treatment; equipment bought solely for an unproven pilot should not automatically be capitalized.

Phase and target	Required decision and approver	Proposed budget source
Assessment approval October 30, 2026	COO sponsors the site scope; CFO or delegated holder approves the fee ceiling. Security director leads.	Security operating budget.
Assessment acceptance November 30, 2026	COO accepts prioritized findings and residual risks; legal counsel identifies approval gaps.	Security operating budget.
Design approval December 18, 2026	COO approves procedures and requirements after legal, facilities, IT, and procurement review. CFO approves next-phase spending.	Security operating budget; approved design or capital planning allocation.
Pilot decision January 29, 2027	COO and CFO approve a limited trial only after required authorizations and response arrangements. Security director defines acceptance tests.	Approved pilot budget; operating costs and eligible capital items separated.
Expansion decision March 31, 2027	COO accepts test results and risk; CFO or capital committee approves expansion or directs redesign/stop.	Capital plan for eligible assets; recurring security operating budget.

Figure 5 - Phases approvals budgets and target dates

Measure time to useful visual assessment, mission completion, weather-related unavailability, false alerts per monitoring hour, detection performance in controlled trials, response time, completeness, and safety or privacy events. Define denominators and test conditions. Measure log completeness as the percentage of sighting records with all mandatory fields completed, including an explicit unknown and reason where data were unavailable.

Countermeasure effectiveness and lifecycle investment analysis

Tie each proposed control to the scenario and failure mechanism it is intended to change. Detection supports protection only when assessment and response occur before the relevant exposure; passive protection may reduce consequences without an alert. Compare the existing arrangement with the proposed arrangement using the same lawful test scenarios and operating conditions. Record unsuccessful trials as well as successes and distinguish measured performance from assumptions used in the risk estimate.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Define acceptance measures before the pilot: detection rate is detected eligible test events divided by all eligible test events; false-alert burden is false alerts per monitoring hour; timely protective-action rate is scenarios meeting a defined protective-action deadline divided by scenarios requiring that action. Also report operational availability against required coverage hours, median and 95th-percentile time from first observable event to useful assessment, and evidence-package completeness. Give sample sizes, conditions, and uncertainty intervals where practicable; a small successful demonstration does not establish near-perfect reliability.

The security director should propose scenario-specific thresholds with operations and the response team, then obtain approval before testing. Exercise sensor outages, delayed assessment, unavailable agency support, and alternative protective actions. Feed demonstrated changes in vulnerability or consequence back into the Section 1 register. Do not equate a detection percentage with the percentage of risk removed. Report residual exposure, failed acceptance criteria, corrective actions, and the date for retesting to the COO.

Compare investment options over one common service period, using a finance-approved discount rate and consistent inflation assumptions. Include acquisition, integration, staffing, training, licensing, connectivity, maintenance, replacement cycles, insurance, evidence storage, outage coverage, and disposal, less any supported residual value. NIST Handbook 135 explains present-value lifecycle methods for federal facility investments; those general methods can inform this comparison, while its program-specific assumptions are not automatically applicable to private security. [32]

For each option, present discounted lifecycle cost and the remaining scenario risks. Where monetary loss estimates are defensible, calculate incremental net present value as the present value of avoided losses and other nonduplicated benefits minus incremental lifecycle costs relative to the baseline. Using the Section 1 hypothetical $12,500 annual avoided loss, five years of constant end-of-year benefits discounted at an illustrative 5 percent total approximately $54,118. This is the break-even present value of incremental costs for that benefit alone, not an equipment budget or promised return.

Include a sensitivity analysis for event frequency, control effectiveness, useful life, staffing costs, and discount rate. Where losses cannot be credibly monetized, compare the lifecycle costs of options meeting the same approved protection objectives and disclose remaining qualitative risks. Present life-safety requirements and legal obligations independently of financial return. The COO should accept residual operational risk; the CFO or capital committee should approve the associated funding and recurring commitments. At each phase gate, use performance evidence and updated costs to expand, redesign, defer, or stop the program.

Evaluate total cost, including trained staffing, recurrent training, aircraft and sensors, docking infrastructure, connectivity, software, maintenance, replacement batteries, insurance, legal review, integration, and evidence storage. Compare the proposed program with alternatives such as fixed cameras, better lighting, alarm changes, or revised patrol coverage. Do not count reduced staffing as a benefit unless a documented workload and coverage assessment supports it.

Public funding may improve regional response capability. FEMA's Counter-UAS Grant Program provides $500 million across FY2026 and FY2027, with $250 million in each phase. State Administrative Agencies are the direct applicants; local public agencies work through state

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

processes. Ordinary private owners cannot apply directly. A private facility may benefit indirectly from a funded agency's lawful coverage, subject to grant terms, jurisdiction, priorities, and a documented coordination arrangement. Funding does not guarantee protection or permit the private site to operate restricted systems. [13]

Contracts should specify acceptance criteria, outages, support, data ownership, exports, retention, remote access, and termination assistance. Separate provider-dependent services from owned capabilities and name who maintains coverage during an outage.

Before award, verify the FCC authorization or other lawful compliance basis required for each radio device and intended use, rather than assuming every component needs a separate certification. The December 22, 2025, Covered List action restricts new authorizations for covered foreign-produced UAS and critical components. It does not itself prohibit previously authorized models; January 2026 exceptions cover specified categories, with stated expiration dates. Check current model-level status and applicable exceptions instead of using nationality as the sole procurement test. [14, 15]

For federal funding or contracts, screen suppliers and equipment under the American Security Drone Act and applicable award terms. The restrictions apply to procurement and operation of FASC-prohibited systems, subject to exceptions and waivers; ordinary FCC authorization alone does not establish federal-funding eligibility. [16]

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Readiness checklist

The security director should record Yes or No for each question. A No identifies an assessment action; these questions are not a compliance certification.

Yes	No	
		Has the COO accepted ownership of drone-related operational risk and named the spending approver?
		Can staff distinguish authorized site flights from unexplained sightings and maintain complete records?
		Do written procedures identify when to shelter, relocate, pause work, and request emergency assistance?
		Have we confirmed a capable agency contact and documented the response arrangement or coverage gap?
		Can we deliver time-aligned imagery, tracks, Remote ID records, and witness accounts through an agreed evidence channel?
		Have legal counsel and procurement reviewed every proposed sensor, flight mission, vendor role, and funding restriction?
		Have we compared passive protection and existing system improvements with drone and detection purchases?
		Does each proposed phase have an approver, budget source, date, and measurable acceptance criteria?
		Have we documented scenario-specific threat, vulnerability, consequence, assumptions, and residual-risk acceptance?
		Have we tested sensor integration, AI decision support, human oversight, and degraded-mode response under site conditions?
		Have executives compared measured effectiveness, lifecycle costs, and residual risks before approving investment?

Figure 6 - Readiness checklist

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Appendix A Drone security governance

Figure 7 summarizes the governance framework and separates effective requirements, proposals, and unresolved status. The business implications are planning inferences, not grants of authority or assurances of funding. The table is selective and does not replace a jurisdiction-specific review. The FCC petition disposition noted below could not be confirmed from the primary material located for this revision.

Instrument and source	Status at revision	Business implication
DHS and DOJ 6 U.S.C. 124n; Preventing Emerging Threats Act of 2018, as amended [9]	Statutory authority, with conditions and designated scope.	Protection of covered facilities/assets. Coordinate through competent agencies; site ownership alone is insufficient.
Department of Defense 10 U.S.C. 130i [17]	Separate federal statutory authority.	Limited to the statutory defense mission and covered facilities/assets; not authority for general private use.
Department of Energy 50 U.S.C. 2661 [18]	Separate federal statutory authority.	Applies to specified nuclear-security missions and assets. Confirm the federal program and personnel authority.
SAFER SKIES Act Pub. L. 119-60, div. H, title LXXXVI; 6 U.S.C. 124n [9]	Enacted December 18, 2025. SLTT authority ends December 31, 2031, unless extended.	Creates a conditional agency pathway, not an ordinary private-owner power. The correctional-agency definition includes certain contracted private operators; obtain specialist advice.
Aircraft and computer offenses 18 U.S.C. 32, 1030, 1367; 49 U.S.C. 46502 [8]	Federal prohibitions; application depends on conduct and any statutory relief.	Review interception, damage, takeover, and computer-access functions before buying active countermeasures.
Interception and signaling collection 18 U.S.C. 2511 and 3121 [8]	Federal prohibitions with defined exceptions.	Communications-based RF detection requires a design-specific legal review; do not equate receiving all RF with public Remote ID reception.
Radio interference 47 U.S.C. 333 [8, 19]	Prohibits willful or malicious interference with covered radio communications.	FCC July actions address qualifying agency use; pending challenges are not private permission to jam.
FAA Reauthorization Act of 2018 49 U.S.C. 44801–44813 [4, 6]	Framework for UAS operations, including §44807 and recreational §44809.	Security work needs the appropriate operating basis; an exemption is specific and may require further approvals.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Instrument and source	Status at revision	Business implication
14 CFR Part 107 [4]	Effective small-UAS operating rule.	Pilot qualifications, operational limits, applicable night/over-people provisions, and waivers govern security flights.
14 CFR Part 89 [7]	Remote ID requirements apply to covered operations.	Broadcast reception can provide context; neither reception nor non-reception establishes permission or intent.
Proposed Part 108 90 FR 38212; FAA-2025-1908; RIN 2120-AL82 [5]	Proposed August 7, 2025. OIRA final-rule review pending in the record reviewed.	Plan docked/BVLOS missions against current authorizations. Do not budget on an assumed effective date.
Section 2209 and proposed Part 74 Pub. L. 114-190, §2209; 91 FR 24650; FAA-2026-4558 [11]	Proposal published May 6, 2026. Extended comment period ended August 5; no final rule located.	Eligible fixed sites could seek a flight restriction under the proposed process. Eligibility, evidence, and FAA approval would still be required.
Airspace restrictions 49 U.S.C. 40103(b)(3); 14 CFR 99.7 and 91.137–91.145 [20]	Existing authorities; individual restrictions have specific scope and duration.	Check current notices and applicable event restrictions. Restricted airspace does not transfer enforcement powers to a facility.
FCC Covered List FY2025 NDAA §1709; FCC December 2025 and January 2026 actions [14, 15]	New equipment authorizations restricted for covered foreign UAS/components, with stated exceptions.	Verify the actual device authorization and current exceptions. Previously authorized products are not automatically prohibited by the listing action.
American Security Drone Act Pub. L. 118-31, §§1821–1833; FAR 40.202 [16]	Procurement/operation restrictions include federal-funds restrictions from December 22, 2025, subject to exceptions/waivers.	Check FASC coverage, SAM information, award terms, and permitted exceptions before using federal funds.
FCC counter UAS actions DA 26-656 and related July 2, **2026,** actions; GN 26-74 [19]	180-day STA and related conditional relief. CTIA filed petitions August 3; DA 26-853 set September 14/29 deadlines. No later disposition confirmed.	Agency procurement must verify current spectrum authority and authorized system status. Do not assume relief is permanent or that a petition automatically stays an order.
DOJ and DHS interim final rule	Effective July 1, 2026; published July 6.	Accreditation, certifications, authorized technology, coordination, privacy, and

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Instrument and source	Status at revision	Business implication
91 FR 41466; 6 CFR and 28 CFR Part 124 [1]		reporting condition agency deployment. Vendor support is distinct from exercising mitigation authority.
FEMA Counter UAS Grant Program Pub. L. 119-21, §90005(a) [13]	$500 million across FY2026–FY2027. First $250 million was awarded December 30, 2025, to 11 host states and NCR.	Direct applications go through SAAs. Private sites may coordinate with public recipients but cannot assume eligibility, access to funds, or dedicated coverage.
EO 14305 Restoring American Airspace Sovereignty, June 6, 2025 [21]	Executive policy direction.	Drives federal counter-UAS and fixed-site restriction work; not self-executing private intervention authority.
EO 14307 Unleashing American Drone Dominance, June 6, 2025 [22]	Executive policy direction.	Supports BVLOS rulemaking and domestic industry. Procurement and flights remain subject to effective requirements.
Interagency advisory and CISA guidance [8, 10]	Guidance, not independent operating authority; older material predates SAFER SKIES.	Use for design review, privacy, and site preparedness; resolve conflicts against current statutes and rules.
NERC CIP 014 [23]	NERC lists CIP-014-3 as mandatory and CIP-014-4 as subject to future enforcement.	Applicable transmission facilities need risk-based physical protection. Evaluate relevant aerial threats within scope; no universal drone-purchase mandate follows.
NRC suspicious activity reporting 10 CFR 73.1215(c), (d)(1)(v); related §73.1200 [24]	Specified licensees assess and report qualifying suspicious activity as soon as possible, within four hours of discovery.	Aircraft activity potentially indicating surveillance is covered; not every innocent sighting is reportable. Applying the faster physical-security event rules were triggered.
Water system resilience AWIA §2013; 42 U.S.C. 300i-2 [25]	Covered community water systems serving more than 3,300 people must assess risk and maintain emergency plans.	Consider relevant malevolent acts and certify completion. Aerial threats may be included based on risk; the law does not require a particular drone system.
Pipeline and chemical facilities TSA Pipeline Security	TSA guidelines provide recommendations; check separate directives.	Maintain risk-based controls. The CFATS lapse does not mean all other federal, state, contractual, or

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Instrument and source	Status at revision	Business implication
Guidelines; CFATS, 6 CFR Part 27 [26, 27]	CFATS statutory authority lapsed July 28, 2023.	sector security obligations disappeared.
Critical Infrastructure Airspace Defense Act S. 4380 and H.R. 9232, 119th Congress [28]	Introduced versions located; not treated as enacted authority.	Would change the private critical-infrastructure pathway if enacted. Do not purchase intervention capability on the assumption it will become law.
State flight privacy and procurement rules Examples: Fla. Stat. 330.41 and 934.50; Tex. Gov't Code ch. 423 [29]	Jurisdiction-specific requirements, definitions, exceptions, and possible litigation.	Review the site's state law, consent, privacy, and public-agency purchasing rules. State restrictions do not supply federal interception authority.

Figure 7 - Governance reference – A Federal counter UAS authority

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

Table of Figures

Figure 1 - Drone security program functions....4
Figure 2 - Security drone use cases....6
Figure 3 - Detection capabilities and legal review....9
Figure 4 - Incident response responsibilities....12
Figure 5 - Phases approvals budgets and target dates....13
Figure 6 - Readiness checklist....16
Figure 7 - Governance reference – A Federal counter UAS authority....20

References

[1] DOJ and DHS. Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies. 91 FR 41466, July 6, 2026; particularly §§124.4–124.5 and 124.21.

https://www.federalregister.gov/documents/2026/07/06/2026-13609/counter-uas-authority-for-state-local-tribal-and-territorial-law-enforcement-and-correctional

[2] DOJ. Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility. November 4, 2024.

https://www.justice.gov/archives/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility

[3] DOJ. Man Pleads Guilty to Attempting to Use a Weapon of Mass Destruction and Attempting to Destroy an Energy Facility. September 9, 2025.

https://www.justice.gov/opa/pr/man-pleads-guilty-attempting-use-weapon-mass-destruction-and-attempting-destroy-energy

[4] FAA. Certificated Remote Pilots including Commercial Operators.

https://www.faa.gov/uas/commercial_operators

[5] FAA. BVLOS proposal, August 2025; OIRA pending review record, RIN 2120-AL82, received July 10, 2026.

https://www.faa.gov/newsroom/beyond-visual-line-sight-bvlos

https://www.reginfo.gov/public/do/eoDetails?rrid=1457213

[6] FAA. Section 44807 exemption process.

https://www.faa.gov/uas/advanced_operations/certification/section_44807

[7] FAA. Remote Identification of Drones.

https://www.faa.gov/uas/getting_started/remote_id

[8] DOJ, FAA, DHS, and FCC. Advisory on Federal Laws Applicable to UAS Detection and Mitigation Technology. August 2020.

https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

[9] SAFER SKIES Act. Pub. L. 119-60, division H, title LXXXVI; current 6 U.S.C. 124n.

https://www.govinfo.gov/link/uscode/6/124n

[10] CISA. Secure Your Drone and Be Air Aware guidance.

https://www.cisa.gov/resources-tools/resources/secure-your-drone-privacy-and-data-protection-guidance

https://www.cisa.gov/topics/physical-security/be-air-aware

[11] FAA. Proposed fixed-site unmanned aircraft flight restriction process, 91 FR 24650, May 6, 2026; extension, June 30, 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

https://www.federalregister.gov/documents/2026/06/30/2026-13126/designation-restrict-the-operation-of-unmanned-aircraft-in-close-proximity-to-a-fixed-site-facility

[12] FAA. UAS Detection, Mitigation, and Response on Airports. June 23, 2025. Read older authority statements with references 1 and 9.

https://www.faa.gov/airports/new_entrants/uas_detection_mitigation_response

[13] FEMA. Counter-UAS Grant Program NOFO fact sheet; DHS award announcement, December 30, 2025.

https://www.fema.gov/fact-sheet/notice-funding-opportunity-nofo-counter-unmanned-aircraft-systems-c-uas-grant-program

DHS announcement: FEMA awards $250 million for counter-UAS security

[14] FCC. Covered List FAQs for UAS and UAS Critical Components.

https://www.fcc.gov/covered-list-faqs-uas-and-uas-critical-components

[15] FCC. Covered List exceptions, DA 26-22, January 7, 2026, and explanatory fact sheet.

https://docs.fcc.gov/public/attachments/DA-26-22A1.pdf

https://docs.fcc.gov/public/attachments/DOC-417528A1.pdf

[16] Acquisition.gov. FAR 40.202 and 40.202-3; American Security Drone Act implementation.

https://www.acquisition.gov/far/40.202

https://www.acquisition.gov/far/40.202-3

[17] U.S. Code. 10 U.S.C. 130i, protection of certain facilities and assets from unmanned aircraft.

https://www.govinfo.gov/link/uscode/10/130i

[18] U.S. Code. 50 U.S.C. 2661, protection of certain nuclear facilities and assets.

https://www.govinfo.gov/link/uscode/50/2661

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

[19] FCC. DA 26-656, July 2, 2026, and DA 26-853, August 14, 2026. The latter confirms CTIA petitions and September deadlines; a later disposition was not verified.

https://docs.fcc.gov/public/attachments/DA-26-656A1.pdf

https://docs.fcc.gov/public/attachments/DA-26-853A1.pdf

[20] FAA. Airspace restrictions and temporary flight restrictions.

https://www.faa.gov/uas/getting_started/where_can_i_fly/airspace_restrictions

[21] White House. Executive Order 14305, Restoring American Airspace Sovereignty. June 6, 2025.

https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/

[22] White House. Executive Order 14307, Unleashing American Drone Dominance. June 6, 2025.

https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/

[23] NERC. Critical Infrastructure Protection reliability standards catalog and CIP-014-3.

https://www.nerc.com/standards/reliability-standards/cip

https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-014-3.pdf

[24] CFR. 10 CFR 73.1215, especially (c)(2)–(3) and (d)(1)(v); related 73.1200.

https://www.ecfr.gov/current/title-10/chapter-I/part-73/section-73.1215

[25] EPA. AWIA risk and resilience assessment and emergency response plan requirements.

https://www.epa.gov/waterresilience/fact-sheet-risk-and-resilience-assessment-and-emergency-response-plan-requirements

[26] TSA. Pipeline Security Guidelines.

https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

[27] CISA. Chemical Facility Anti-Terrorism Standards program status.

https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats

[28] U.S. Congress. Critical Infrastructure Airspace Defense Act, S. 4380, introduced April 22, 2026; H.R. 9232, introduced June 9, 2026. Introduced texts.

https://www.govinfo.gov/app/details/BILLS-119s4380is

https://www.govinfo.gov/content/pkg/BILLS-119hr9232ih/pdf/BILLS-119hr9232ih.pdf

[29] Florida Legislature. Fla. Stat. 330.41 and 934.50. Texas Legislature. Government Code chapter 423.

https://www.flsenate.gov/Laws/Statutes/2026/0330.41

https://www.flsenate.gov/Laws/Statutes/2026/0934.50

https://statutes.capitol.texas.gov/Docs/GV/htm/GV.423.htm

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

[30] U.S. Department of Homeland Security. DHS Risk Lexicon, September 2008. Terminology reference for threat, vulnerability, consequence, and residual risk.

https://www.govinfo.gov/content/pkg/GOVPUB-HS-PURL-LPS113852/pdf/GOVPUB-HS-PURL-LPS113852.pdf

[31] NIST. Artificial Intelligence Risk Management Framework 1.0, 2023. AI RMF Core, particularly human oversight, measurement, and monitoring.

https://airc.nist.gov/airmf-resources/airmf/5-sec-core/

[32] Kneifel, J. and Webb, D. Life Cycle Costing Manual for the Federal Energy Management Program. NIST Handbook 135e2025, August 2025.

https://doi.org/10.6028/NIST.HB.135e2025

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com

About the author

Michelle L. Chace, MSSM, prepared this white paper for Mitigation Assessor, LLC. The paper addresses physical security planning, operational readiness, and the integration of drone-related risks into a facility security program.

Mitigation Assessor, LLC
www.mitigationassessor.com
mchace@mitigationassessor.com
402-312-7955

Professional Review

The author acknowledges Louis Barani, Principal - Strategic Security & Risk Consult, Inc. and Mark Hatcher, Principal - ESI Convergent, for providing an independent subject-matter review of this white paper. The review included comments concerning security staffing, operational responsibilities, training, insurance, contract administration, and risk management. The author evaluated and incorporated appropriate recommendations and retains sole responsibility for the final content, interpretations, and conclusions.

Disclaimer

This white paper provides general educational information for U.S. physical security planning. It is not legal advice or authorization to fly, intercept communications, or interfere with an aircraft. Aviation, communications, privacy, surveillance, criminal, and state laws depend on the activity and jurisdiction. Consult qualified counsel and relevant authorities before procurement or deployment. Regulatory status reflects sources reviewed through October 16, 2026, subject to the specific uncertainties stated in Appendix A. Recommendations and illustrative schedules are planning guidance, not guarantees of safety, performance, funding, or agency response.

© 2026 - Mitigation Assessor, LLC | www.mitigationassessor.com